Impact Assessment and Mitigation of the effect of Cyber-physical Attacks on the Electric Vehicles High-Power Fast Charging Stations Considering Open Charge Point Protocol

by

Kandarp Kalpesh Gandhi

A thesis submitted to the
School of Graduate and Postdoctoral Studies in partial
fulfillment of the requirements for the degree of

Master of Applied Science in Electrical and Computer Engineering

Faculty of Engineering & Applied Sciences (FEAS)

University of Ontario Institute of Technology (Ontario Tech University)

Oshawa, Ontario, Canada

December 2022

THESIS EXAMINATION INFORMATION

Submitted by: **Kandarp Kalpesh Gandhi**

Master of Applied Science in **Electrical and Computer Engineering**

Thesis title: Impact Assessment and Mitigation of the effect of Cyber-physical Attacks on the Electric Vehicles High-Power Fast Charging Stations Considering Open Charge Point Protocol

An oral defense of this thesis took place on **November 23, 2022**, in front of the following examining committee:

Examining Committee:

Chair of Examining Committee	Dr. Vijay Sood
Research Supervisor	Dr. Walid Morsi Ibrahim
Examining Committee Member	Dr. Khalid Elgazzar
Thesis Examiner	Dr. Lixuan Lu, Ontario Tech University

The above committee determined that the thesis is acceptable in form and content and that a satisfactory knowledge of the field covered by the thesis was demonstrated by the candidate during an oral examination. A signed copy of the Certificate of Approval is available from the School of Graduate and Postdoctoral Studies.

ABSTRACT

Electric Vehicles are on the rise worldwide, and the increasing demand also increases the need for High Power Fast Charging Stations. The deployment of such charging stations dictates the establishment of information and communication infrastructure that uses communication protocols. Such an infrastructure makes these charging stations prone to cyber-physical attacks. This thesis focuses on the impact assessment and mitigation of these cyber-physical attacks on the operation of the existing assets and the voltage quality. Additionally, the thesis displays the weakness in the communication protocol between the electric vehicles and the charging stations that intruders can exploit to gain unauthorized access to pose threats to the microgrid. A microgrid embedded with the vehicle-to-grid operation and renewable energy sources is simulated in MATLAB SIMSCAPE and used to demonstrate such cyber-physical attacks' impacts on the transformer. Finally, the results showed a significant transformer overload impacting the overall system and costing millions in damages.

Keywords: Electric Vehicles; Fast Charging Stations; Cyber-attacks; Cybersecurity; Open Charge Point Protocol

AUTHOR'S DECLARATION

I hereby declare that this thesis consists of original work of which I have authored. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize the University of Ontario Institute of Technology (Ontario Tech University) to lend this thesis to other institutions or individuals for the purpose of scholarly research. I further authorize University of Ontario Institute of Technology (Ontario Tech University) to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my thesis will be made electronically available to the public.

Kandarp Kalpesh Gandhi

STATEMENT OF CONTRIBUTIONS

The majority of the work in this thesis was conducted in a simulation test bed environment utilizing publicly available datasets and modifying a sample microgrid test model for simulation. I was responsible for testing numerous simulation versions by testing a set of defined parameters and collecting all the data for analysis afterward. This research was conducted under the supervision of Dr. Walid Morsi Ibrahim.

Part of the work described in this thesis has been accepted for publication in:

K. Gandhi, and W.G. Morsi, "Impact of the Open Charge Point Protocol Between the Electric Vehicle and the Fast Charging Station on the Cybersecurity of the Smart Grid", in *2022 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2022.

ACKNOWLEDGEMENTS

I want to take this opportunity to thank my parents, who stood by me and supported me throughout my journey to get me where I am today. Without their support, I would not have been able to succeed in life and especially in completing my thesis and graduating from Ontario Tech University.

I would also like to say a very warm and hearted thanks to my supervisor Dr. Walid Morsi Ibrahim, for his continuous support, guidance, and motivation in helping me complete this milestone. Without his support and numerous hours of discussions, this would not have been possible. Thank you, professor, for not giving up on me.

I would also like to thank NSERC for supporting the work presented in this thesis and allowing me to pursue this research.

Table of Contents

THESIS EXAMINATION INFORMATION ..... *ii*

ABSTRACT ..... *iii*

AUTHOR'S DECLARATION ..... *iv*

STATEMENT OF CONTRIBUTIONS ..... *v*

ACKNOWLEDGEMENTS ..... *vi*

LIST OF TABLES ..... *xi*

LIST OF FIGURES ..... *xii*

LIST OF ABBREVIATIONS AND SYMBOLS ..... *xix*

Chapter 1 Introduction *1*

1.1 Electric Vehicles and Fast Charging Stations **1**

1.2 Addressing the Growth of HP-FCS on the Cybersecurity of the Smart Grid **7**

1.3 Rise of Cyber-Physical Attacks **8**

1.4 Popularity of Isolated Microgrids within the Smart Grid **10**

1.5 Problem Statement **12**

1.6 Research Objectives **13**

1.7 Thesis Organization **13**

Chapter 2 Literature Review *16*

2.1 Introduction **16**

2.2 Recent Research Activities Concerning Cyber Security **16**

2.3 Recent Research Activities Pertaining to the Cyber Security within the Smart Grid 22

2.4 Cybersecurity using the Open Charge Point Protocol & EV charging system within the smart grid 26

2.5 Cyber Security in Smart Grids with Electric Vehicle Charging Stations 31

2.6 Research Gaps 35

Chapter 3 Open Charge Point Protocol 37

3.1 Introduction 37

3.2 Charge Point 38

3.3 The Central System 42

3.4 Communication Between the Charge Point and the Central System 48

3.5 SteVe 52

Chapter 4 Methodology 55

4.1 Introduction 55

4.2 Microgrid System 55

4.3 Description of the Cyber-Physical Attacks 58

4.4 Cyber-Physical Attacks through the OCPP 58

4.5 Impact Assessment of Cyber-Physical Attacks 60

4.5.1 Transformer Overload and the Thermal Loading 62

4.5.1.1 Thermal Characteristics & Overload of the Transformer 62

4.5.1.2 Transformer Theta H Curve 64

4.5.2 Undervoltage 65

4.6 Microgrid System Modelling in SIMSCAPE 67

4.7 Mitigation of Cyber-Physical Attacks..... 70

Chapter 5 Results & Discussion 71

5.1 Introduction 71

5.2 Test System Description..... 71

5.3 Test System Scenarios and its parameters 76

5.4 Impacts of cyber-physical attacks on the components of the microgrid system ... 79

5.4.1 Transformer Overload.....80

5.4.2 Theta H Curve 86

5.4.3 Undervoltage.....93

5.5 Vulnerabilities of the OCPP and Cyber-Physical Attacks on the test system..... 99

5.6 Mitigation Techniques..... 101

5.6.1 Mitigation Technique #1 – Changing the Charging Times..... 102

5.6.1.1 Mitigation Technique #1 – Transformer Overload.....104

5.6.1.2 Mitigation Technique #1 – Theta H Curve.....107

5.6.1.3 Mitigation Technique #1 – Undervoltage.....109

5.6.2 Mitigation Technique #2 – Changing the Charging Times & the Rated Power . 112

5.6.2.1 Mitigation Technique #2 – Transformer Overload.....113

5.6.2.2 Mitigation Technique #2 – Transformer Overload at 11.5kW Charging Rate 113

5.6.2.3 Mitigation Technique #2 – Transformer Overload at 9.6kW Charging Rate 115

5.6.2.4 Mitigation Technique #2 – Transformer Overload at 7.7kW Charging Rate 118

5.6.2.5 Mitigation Technique #2 – Theta H Curve.....120

5.6.2.6 Mitigation Technique #2 – Theta H Curve at 11.5kW Charging Rate.....120

5.6.2.7 Mitigation Technique #2 – Theta H Curve at 9.6kW Charging Rate.....123

5.6.2.8 Mitigation Technique #2 – Theta H Curve at 7.7kW Charging Rate.....125

5.6.2.9 Mitigation Technique #2 – Undervoltage.....127

5.6.2.10 Mitigation Technique #2 – Undervoltage at 11.5kW Charging Rate 128

5.6.2.11 Mitigation Technique #2 – Undervoltage at 9.6kW Charging Rate 131

5.6.2.12 Mitigation Technique #2 – Undervoltage at 7.7kW Charging Rate 133

Chapter 6 Conclusion..... 135

References 140

LIST OF TABLES

Table 3-1 - Implementation of different OCPP operations by categories..... 49

LIST OF FIGURES

Figure 1-1 - Large Scale EV Development [1] 1

Figure 1-2 - Speed in bring EVs and charging sites to market [1] 2

Figure 1-3 - Driving factors for EVs [1] 2

Figure 1-4 - Global Electric Vehicle Sales Doubled in 2021 [4] 3

Figure 1-5 - Charging points per electric LDV in specific countries, 2021 [12] 6

Figure 1-6 - Typical Cyber-Physical Structure in the Smart Grid [16] 9

Figure 2-1 - High-level Diagram for Integration of SecCharge with Syntronic Charging Station as secure EV charging system using Open Charge Point Protocol [54] 29

Figure 2-2 - Flow chart of the user experience electric vehicle charging station using OCPP as seen in [55] 30

Figure 3-1 - Sequence Diagram for the Operation Authroize [51] 40

Figure 3-2 - Sequence Diagram for the Operation Boot Notification [51] 40

Figure 3-3 - Sequence Diagram for the Operation Heartbeat [51] 41

Figure 3-4 - Sequence Diagram for the Operation Remote Start Transaction [51] 43

Figure 3-5 - Sequence Diagram for the Operation Remote Stop Transaction [51] 43

Figure 3-6 - Sequence Diagram for the Operation Unlock Connector [51] 44

Figure 3-7 - Sequence Diagram for the Operation Charging Profile [51] 45

Figure 3-8 - Sequence Diagram for the Operation Trigger Message [51] 45

Figure 3-9 - Sequence Diagram for the Operation Trigger Message with Status Notification [51] 46

Figure 3-10 - Sequence Diagram for the Operation Update Firmware [51] 47

Figure 3-11 - General Operation of the OCPP [51] 50

Figure 3-12 - Charging Session and Energy Transfer in the OCPP [51] 51
Figure 3-13 - SteVe interface showing possible operations by the Central System on a sample created Charge Point named UOIT 53
Figure 3-14 - SteVe interface showing possible fields on a Charge Point 54
Figure 4-1 - Example of different types of Microgrids [71] 57
Figure 4-2 - Components of a typical Microgrid [82] 61
Figure 4-3 - Voltage Ranges as per ANSI C84.1 [87] 66
Figure 4-4 - Sample Microgrid System Identified Points of Measurements 68
Figure 5-1 - Test System [88] 72
Figure 5-2 - Example Wind Profile 73
Figure 5-3 - Example Irradiance Profile 74
Figure 5-4 - Transformer Demand at different EV Penetration in case of no attack 81
Figure 5-5 - Transformer Demand at different EV Penetration in case of attack case #1 82
Figure 5-6 - Transformer Demand at different EV Penetration in case of attack case #2 83
Figure 5-7 - Transformer Demand at different EV Penetration in case of attack case #3 84
Figure 5-8 - 24-hour Transformer Demand Profile for all three attack cases at 200% penetration 85
Figure 5-9 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of no attack 87
Figure 5-10 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of attack case #1 88
Figure 5-11 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of attack case #2 89

Figure 5-12 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of attack case #3 91
Figure 5-13- 24-hour Transformer Temperature Curve (Theta H) for all three attack cases at 200% penetration 92
Figure 5-14 - Highlighted portion identifies Bus 3 in the microgrid system 94
Figure 5-15 - 24-hour Voltage Profile of Bus 3 in case of no attack case 95
Figure 5-16 - 24-hour Voltage Profile of Bus 3 in case of attack case #1 96
Figure 5-17 - 24-hour Voltage Profile of Bus 3 in case of attack case #2 97
Figure 5-18 - 24-hour Voltage Profile of Bus 3 in case of attack case #3 98
Figure 5-19 - 24-hour Voltage Profile of Bus 3 for all the attacks at 200% penetration .. 99
Figure 5-20 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times according to Mitigation Technique #1 105
Figure 5-21 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times according to Mitigation Technique #1 106
Figure 5-22 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times according to Mitigation Technique #1 106
Figure 5-23 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times according to Mitigation Technique #1 107
Figure 5-24 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times according to Mitigation Technique #1 108
Figure 5-25 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times according to Mitigation Technique #1 108

Figure 5-26 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times according to Mitigation Technique #1 110
Figure 5-27 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times according to Mitigation Technique #1 111
Figure 5-28 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times according to Mitigation Technique #1 111
Figure 5-29 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2..... 114
Figure 5-30 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2..... 114
Figure 5-31 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2..... 115
Figure 5-32 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2..... 116
Figure 5-33 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2..... 117
Figure 5-34 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2..... 117
Figure 5-35 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2..... 118
Figure 5-36 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2..... 119

Figure 5-37 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 119
Figure 5-38 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2 121
Figure 5-39 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2 122
Figure 5-40 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2 122
Figure 5-41 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 124
Figure 5-42 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 124
Figure 5-43 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2 125
Figure 5-44 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 126

Figure 5-45 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 126
Figure 5-46 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 127
Figure 5-47 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2 129
Figure 5-48 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2 130
Figure 5-49 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2 130
Figure 5-50 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2 131
Figure 5-51 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2 132
Figure 5-52 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2 132
Figure 5-53 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 133
Figure 5-54 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2 134

Figure 5-55 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2..... 134

LIST OF ABBREVIATIONS AND SYMBOLS

EVs	Electric Vehicles
FCS	Fast Charging Stations
HP-FCS	High-Power Fast Charging Stations
IEA	International Energy Agency
LDV	Light Duty Vehicles
EPS	Electrical Power Systems
OCPP	Open Charge Point Protocol
DoS	Denial of Service
IDS	Intrusion Detection System
ERI	EnrtRegistry, Inc
ADWT	Analytical Discrete Wavelet Transform
UFSM	Federal University of Santa Maria
PCA	Principle Component Analysis
MSPCA	Multi-Scale Principal Component Analysis
DDoS	Distributed Denial of Service
AMI	Advanced Metering Infrastructure
PMU	Phasor Measurement Unit

DDOA	Dirichlet-Based Detection Scheme
HANs	Home Area Networks
VPNs	Virtual Private Networks
V2G	Vehicle to Grid
SCMS	Smart Charging Management System
PEVs	Plug-in Electric Vehicles
EVSE	Electric Vehicle Supply Equipment
EI	Energy Internet
DC-MGs	DC-Microgrids
SV	Sampled Values
GOOSE	Generic Object-Oriented Substation Event
MMS	Manufacturing Message Specification
OSCP	Open Smart Charging Protocol
OCA	Open Charging Alliance
OCPI	Open Charging Point Interface
TCP	Transmission Control Protocol
IP	Internet Protocol
F_{AA}	Aging Acceleration factor of the transformer

Θ_H	Hottest-spot temperature in Celsius
F_{EQA}	Equivalent Aging Factor
Θ_A	Average Ambient Temperature in Celsius
$\Delta\Theta_{To}$	Top-Oil Rise Over Ambient Temperature in Celsius
$\Delta\Theta_H$	Winding Hottest-Spot Temperature in Celsius
Θ_{To}	Top-Oil Temperature in Celsius
SOC	State of Charge
ANSI	American National Standards Institute

Chapter 1 Introduction

1.1 Electric Vehicles and Fast Charging Stations

The revolution in the automotive industry has been growing through the widespread deployment of Electric Vehicles (EVs). According to the Climate Group [1], the electrification of the transportation system has been growing and many automakers have started to switch from gasoline to electric vehicles. The environmental benefits of using electric vehicles to reduce greenhouse gas emissions are now a priority for many governments worldwide. From the Climate Group in Figure 1-1, the large scale of EVs, charging sites, and the tremendous reduction in carbon dioxide emission are shown.

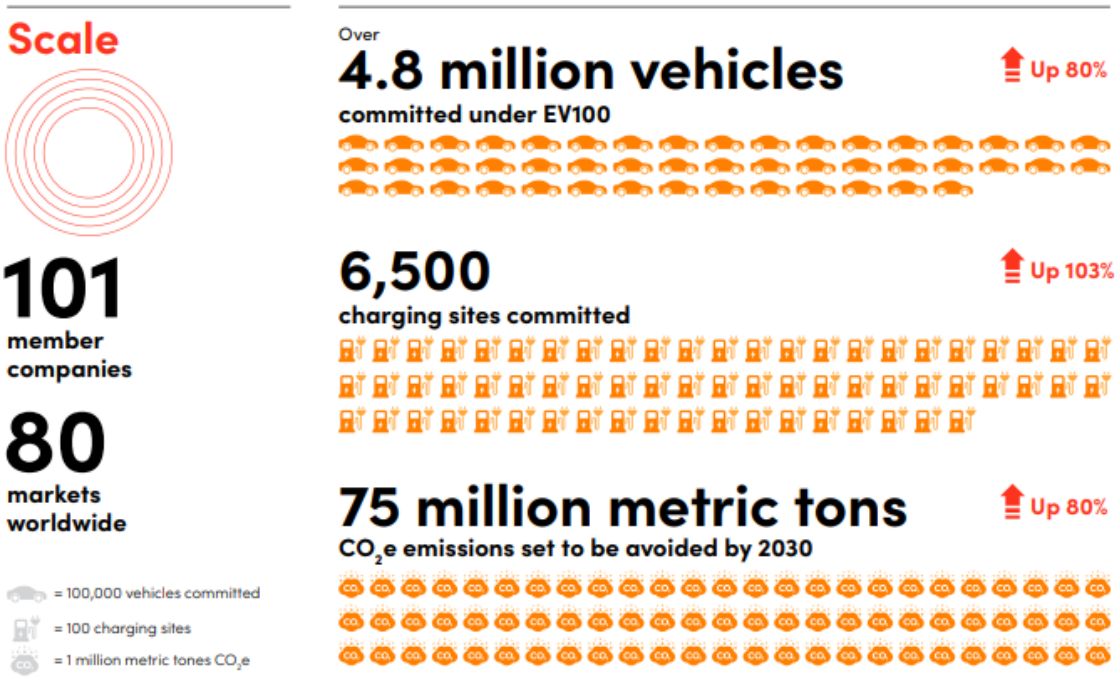

Figure 1-1 - Large Scale EV Development [1]

Additionally, with the large-scale commitment of EVs also comes the speed on how fast and the collaboration in driving this commitment is as important, as shown in Figure

1-2 and Figure 1-3. The factors that help drive EVs are reducing greenhouse gases and targeting air pollution caused by gasoline vehicles.

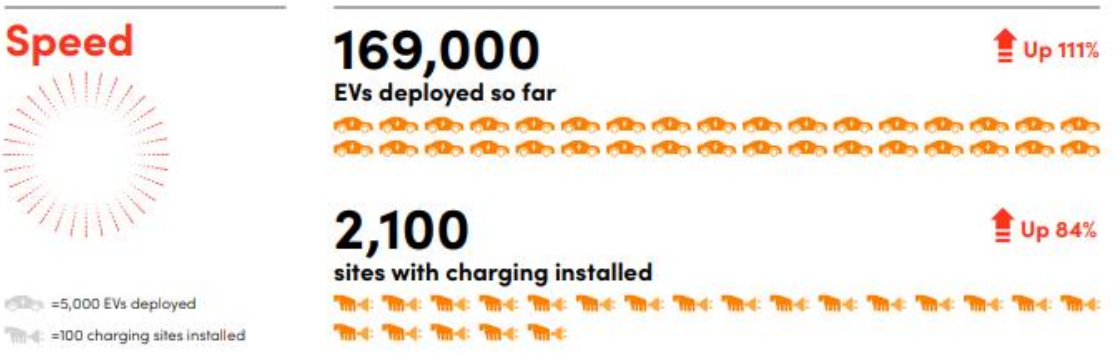

Figure 1-2 - Speed in bring EVs and charging sites to market [1]

Figure 1-3 - Driving factors for EVs [1]

With the increase of EVs, the growth of Fast Charging Stations (FCS) or High-Power Fast Charging Stations (HP-FCS) also needs to grow as fast as well. According to the International Energy Agency (IEA), EVs have increased much fasters than the growth of FCS. [2] This raises concerns for consumers in the market deciding whether they want to buy an EV or not. Think of a scenario in that you are driving in a gasoline-powered vehicle and realize you are low on gas. Within a couple km, you will quickly be able to find a gas station and rectify the situation. As a consumer, you don't need prior information on where

the gas station is located and do not have to plan your trip in a way where you will find a gas station. Consider the same scenario, but if you are driving an EV, then you have to make sure you plan well in advance to know where you are going, how many stops you will have to take and where you will be charging your EV. The reasoning behind this is that you cannot always find a charging station or FCS within a few km of where you are. Either way, consumers are still buying EVs worldwide, as shown in Figure 1-4, where the sales of EVs doubled worldwide in 2021. In Canada, according to Statistics Canada, a new milestone was achieved for EVs as they were 5.2% of all the newly registered vehicles in 2021. [3]

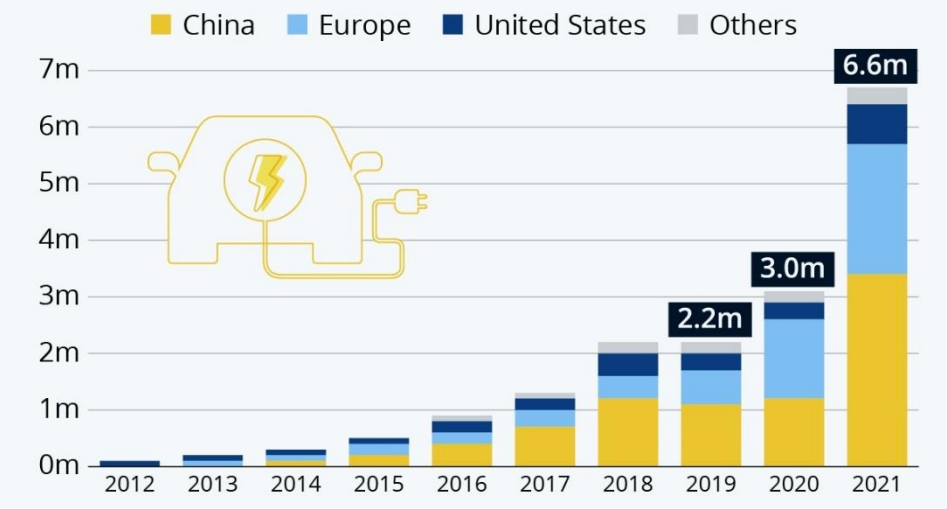

Figure 1-4 - Global Electric Vehicle Sales Doubled in 2021 [4]

The growth of charging stations and FCS is growing as well but slower to keep up with the growth of EVs. Refer to Figure 1-5 to see a worldwide trend for specified countries, which shows the number of electric light duty vehicles (electric LDV) or EVs per charging point in that country. In Canada, there are 20 EVs for every charging point, which means if every charging point was utilized at a given time, then 1 in 20 vehicles

could charge simultaneously. Compared to the United States, there are about 18 vehicles for every charging point, which is better than Canada but not by a lot. Compared to New Zealand, it is about 57 EVs for every charging point, which may seem like a high ratio, but it is still much better compared to gasoline.

According to [5], the United States has 225 gasoline vehicles to 1 gas station ratio versus 16 EVs to 1 charging station. The comparison is completed correctly as each EV owner may be able to charge their vehicle at home then, that can also be assumed as a charging point as well, which is not considered in the ratio. The idea for charging stations is that it requires much more time to charge the vehicles than you will spend filling up a gas tank at the gas station. This is where FCS or HP-FCS become much more important and the need to grow more compared to the regular charging stations. Using FCS decreases the waiting time to charge the vehicle, and will get a similar experience to filling your vehicle at the gas station. Therefore, the call to update this electrical infrastructure has been a priority in Canada as calls to take the initiative to meet the reduction in 12 megatons of greenhouse gas emission by 2030 and new vehicles sold by 2040 to be 100% in EVs. [6]

Furthermore, in Canada, the growth and investment into HP-FCS are growing and at the federal level, the government has allowed all provinces to invest and start the development of more HP-FCS. Specifically, in the province of Ontario, there are more than 2500 HP-FCS, the highest number of HP-FCS in construction, and some are already in service for use by consumers [7]. In other provinces like British Columbia, there are 1500 HP-FCS and 300 HP-FCS in the province of Quebec, which are also under construction [7]. The increasing growth of HP-FCS in strategic locations in Ontario will allow consumers to travel with the security that they can find a charger when they need it the

most [8]. Additionally, through the Ivy Charging Network in partnership with Hydro One Inc. and Ontario Power Generation, there is a proposal to make a vast charging network throughout Canada [9]. These immense commitments will help Canada meet their goal to have EV sales to 50% by 2030 and 100% by 2040 to meet the government mandates to make Canada emission-free. [6, 10]

Finally, with all the information from the climate studies and concerns regarding reducing greenhouse gases has led more people towards EVs, which in turn has increased the growth of HP-FCS [11]. An increase in HP-FCS allows customers to charge their vehicles faster than charging the vehicles at home. It gives a similar experience when someone uses the gas station to fill up their vehicle but slightly longer and much faster than charging at home. This fast charging ends up challenging the critical infrastructure responsible for supplying an immense amount of power in a very short period for cyber-physical attacks.

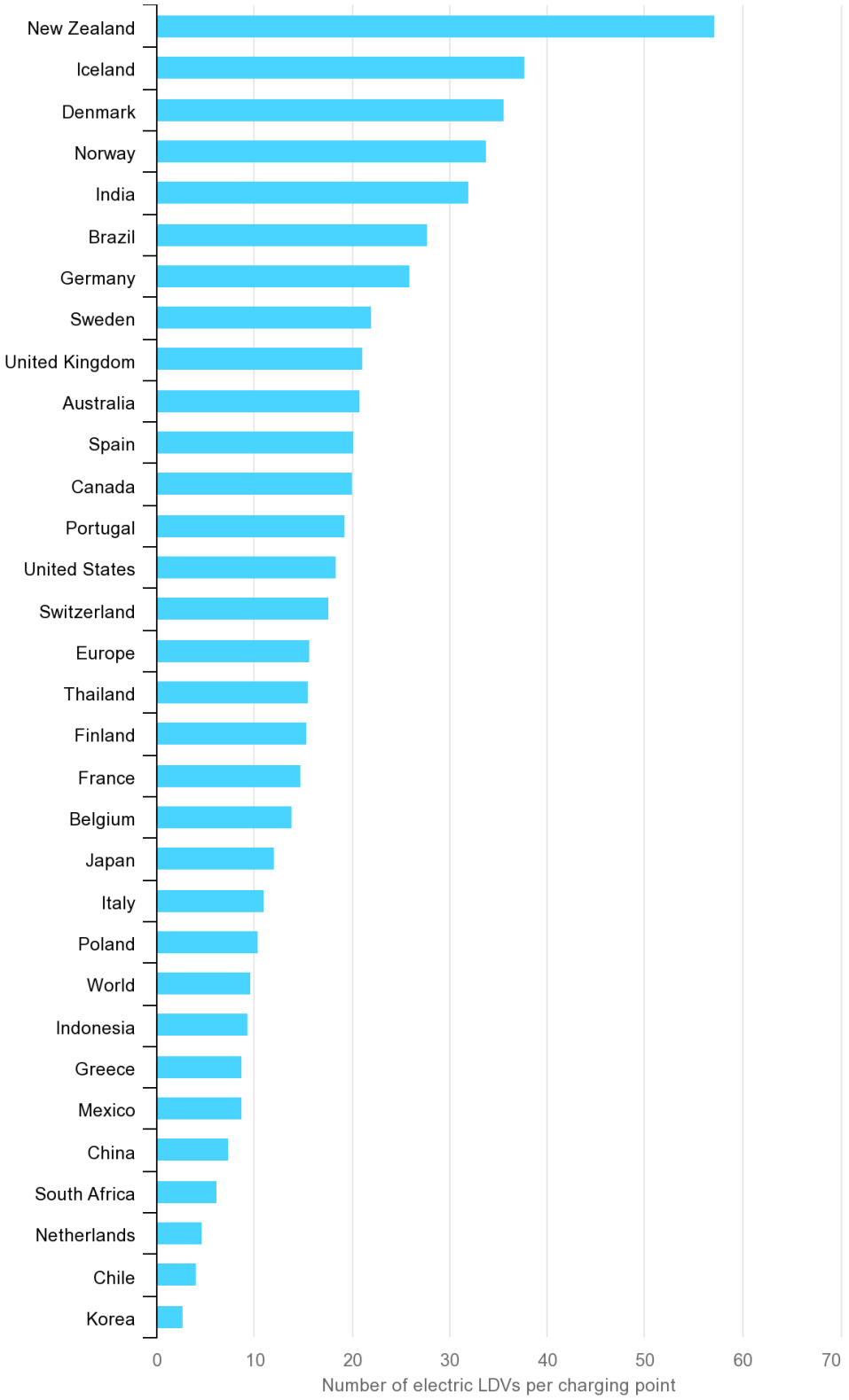

Figure 1-5 - Charging points per electric LDV in specific countries, 2021 [12]

1.2 Addressing the Growth of HP-FCS on the Cybersecurity of the Smart Grid

As mentioned, the increase in HP-FCS will lead to challenges specifically related to cybersecurity in the smart grid. According to [13], it addresses cybersecurity challenges that occur within electrical power systems (EPS) in the near future. Since our society is very dependent on EPS, which handles our most prominent and critical infrastructure, the impacts of the HP-FCS become vulnerable. If for any reason, the EPS were to fail due to the supply and demand issues regarding the HP-FCS, then critical infrastructures like hospitals, government buildings, and everyday consumers. A famous cyberattack occurred on December 2015 [14] in Ukraine, where up to 225,000 customers were without power for several hours. Compared to a natural disaster, these impacts may be very low in terms of outage timing, but this can occur without any intimation and can cause severe long-lasting impacts on the smart grid. These impacts may not be seen right away. Still, over time they become more visible, and by then, it becomes too late to make any changes and may result in financial loss, equipment failure, and more outages for the consumers and the producers.

Another cybersecurity perspective can be analyzed in [15], where the roll-out of more EVs results in more FCS or HP-FC being built. These results in growing demand from the FCS for both at the residential and commercial applications. The integration of EVs, FCS, and the smart grid creates a complex cyber-physical interdependence between components, communication, and other means, which are left open to maliciously be used and exploited to cause damage. These cyber vulnerabilities will affect the components connected to the system but will also spread and impact the smart grid causing more damage and power outages downstream toward other consumers. Therefore, it is important to research and

investigate these outcomes that may occur due to the growth in EVs and HP-FCS specifically. Upon studying and assessing the impacts of cyber threats, the work in this thesis will analyze the results of these impacts and bring awareness to them. Finally, the thesis will develop mitigation techniques that will address these cyber threats' impacts and help the evolution of EVs and the growing demand market for them.

1.3 Rise of Cyber-Physical Attacks

Cyber-Physical Attacks are defined as intrusions into the cyberinfrastructure that impacts the physical environment. According to [16], cyber-physical attacks exploit the vulnerabilities of the cyber-physical structure of the smart grid. Referring to Figure 1-6 shows the distinction between the cyber portion and the physical portion of the cyber-physical structure in the smart grid. The information loop within the cyber-physical structure illustrates the operations that can be compromised via the two-way communication channels and the physical assets in the physical part of the power systems. The interconnection between the cyber and the physical part represents vulnerabilities to attacks from both domains of the structure.

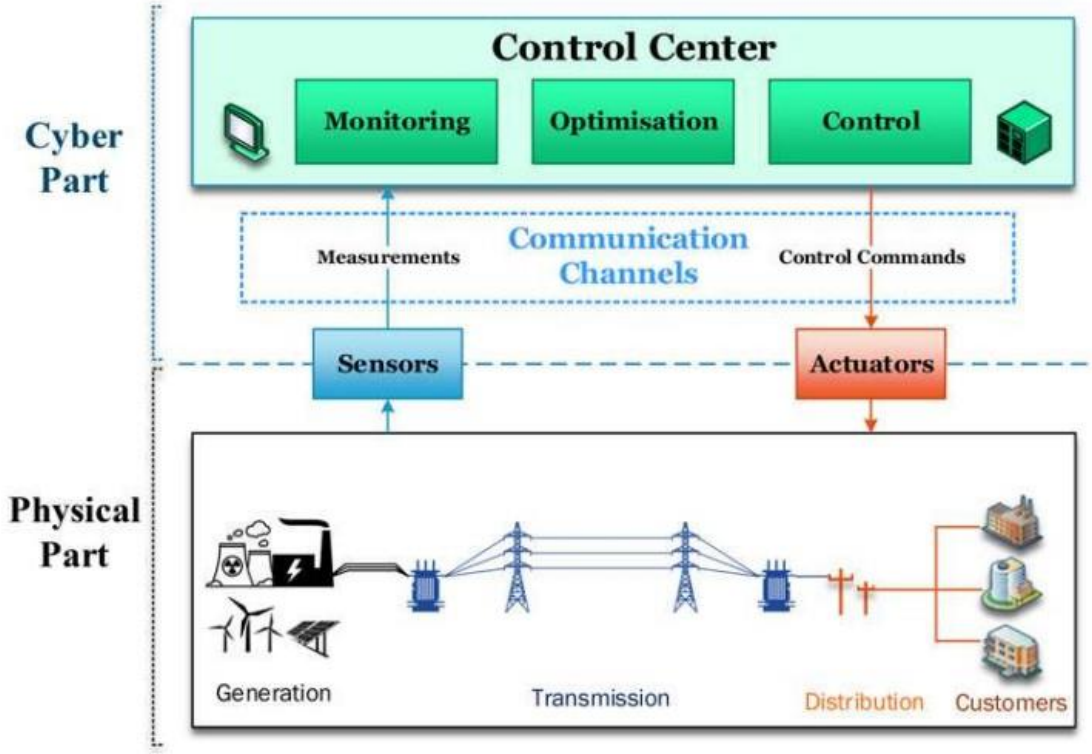

Figure 1-6 - Typical Cyber-Physical Structure in the Smart Grid [16]

The vulnerability of the cyber and physical structure can be seen in the recent Ukraine Power Grid attack in 2016 [17], where malware was injected from the communication channels allowing the intruder to gain access to the control center. Upon this, the intruders sent malicious commands to trip the power lines and create a widespread blackout. This is a perfect example of a cyber-physical attack, where intrusions in the cyber part of the structure allowed the intruders to cause physical impacts on the smart grid via the resulting blackout. Furthermore, the Aurora attack was a test scheme that exploited the vulnerability of the automatic generation controller. [18] The original attack test scheme was conducted by the Idaho National Lab, where the cyber intruder had access to the opening and closing

of the circuit breakers of the generator. The short-term impacts of the Aurora attack resulted in a power outage, while the long term impact resulted in the generator efficiency. [19] The cyber-physical attacks on the automatic generator control resulted in a long-term economic burden on the utility. The cyber-physical attack also identified secondary controller which demonstrated the ability to impact the power system frequency. This resulted in the load frequency control to incorrectly calculate the frequency deviation resulting in performing a fake frequency deviation causing an unintentional load shedding and affecting power system stability. [20]

The nature of cyber-physical attacks and their ability to affect the physical environment through a cyber intrusion needs to be examined. With the rise in cyber-physical attacks, the impact assessment of these cyber-physical attacks on the smart grid cannot be overlooked. In addition, the impact assessment needs to look at long-term impacts, since the severity of the damage may not be visible immediately. Furthermore, any mitigation techniques that can be implemented should be presented to help mitigate the impacts of the cyber-physical attacks on the cyber-physical structure of the smart grid.

1.4 Popularity of Isolated Microgrids within the Smart Grid

Microgrids are a group of interconnected loads and distributed energy resources that act as a single controllable entity with respect to the grid. In addition, microgrids can be permanently connected to the grid, isolated from the grid, or switch between the two modes. [21] According to Natural Resources Canada [22], isolated microgrids were popular among the 292 remote communities in Canada, such as Hartley Bay in British Columbia. New approaches in isolated microgrids and the introduction of smart meters and

smart controllers for integrating renewables and energy storage have increased the popularity of microgrids. According to [23], the popularity of isolated microgrids has significantly increased in Canada as there is 535 million dollars of publicly funded money in about 72 projects across 45 companies and 15 utilities across Canada.

According to Electricity Canada [24], the future of energy solutions lies in microgrids. Additionally, the project by Electricity Canada suggests that microgrids will increase customer comfort and maintain power in certain buildings during outages by functioning as a standalone isolated microgrid. The utility perspective by Hydro Quebec suggests that microgrids allows the company to purchase less power during peak periods and avoid making extra investments in the power system. According to the Ministry of Energy [25], several projects are funded by the Smart Grid fund across Ontario in and around the Greater Toronto Area. Specifically, one project funded by the Ministry of Energy is the Microgrid Research and Innovation Park – University of Ontario Institute of Technology for about 4 million dollars. [25] The project at the University of Ontario Institute of Technology demonstrates the benefits of the microgrid to operate as backup power during a utility power outage and provide seamless connection and disconnection from the grid. When the microgrid is not operating, it helps the university save energy and electricity costs during peak periods.

The increased popularity of isolated microgrids and growing demand brings an important question, “why are microgrids becoming an important part of the energy infrastructure.” [26] Microgrids are customer-driven since they seek predictability, sustainability, and reliability in receiving their energy services. This makes it the perfect motivation and selection of the isolated microgrid as the system utilized in this research to

investigate the impact assessment and mitigation of cyber-physical attacks on the microgrid system utilizing the vehicle-to-grid operation. In addition, the future growth of microgrids will consist of many electric vehicles which will utilize the vehicle-to-grid operation to support the microgrids that serve the community in both isolated or gird connected modes.

1.5 Problem Statement

The problem statement of this research is to focus on the impacts of cyber-physical attacks on Electric Vehicles High-Power Fast Charging Stations. The focus of the research will understand the impact assessment of the cyber-physical attacks has on the transformers and voltage quality within the simulated microgrid system. The challenges will involve understanding and implementing the cyber-physical attacks on the charging stations to see the effects on the smart grid's overall power demand. Additionally, the challenges will include identifying the cyber threats through means of communication protocols utilizing fast charging and highlighting the areas of weakness for the intruders. In end, the research will focus on providing mitigation techniques that can be utilized to mitigate these cyber-physical attacks and provide solutions to the impacts on the microgrid system and its associated components. In conclusion, the research will summarize the problem statement by showing the impacts and potential mitigation techniques to highlight the assessment of the cyber-physical attacks on the electric vehicle fast charging stations considering the communication protocol between them.

1.6 Research Objectives

The research objectives of this thesis are as follows:

- To study the communication protocol used in the EV fast charging stations and the weaknesses of such protocol that can be exploited by intruders to impose cyber-physical attacks.
- To identify the types of cyber-physical attacks that may target the EV fast charging stations.
- To assess the impacts of the cyber-physical attacks on EV charging, the system assets, and the voltage quality.
- To study the effect of different charging times, different vehicle penetrations, and the rated power of the electric vehicle fast charging stations.
- To develop suitable and effective mitigation techniques to address the effect of the cyber-physical attacks on the EV charging process, the system assets, and the voltage quality.

1.7 Thesis Organization

The thesis is organized into six chapters that outlines the different parts of the research. The following will explain what each chapter consists off and how they make up the complete thesis.

- Chapter 1 – Introduction
    - This chapter introduces the reader to the basis of this research and the increased demand for EVs and how those results have increased demand in HP-FCS or FCS. In addition, the reader will be introduced to the rise of cyber-physical attacks and how they can be targeted on the electric vehicle

fast charging stations. Furthermore, the popularity of the isolated microgrid system will be introduced. Finally, the problem statement will be clearly written along with research objectives of this work. At the end, the organization of the thesis will be discussed.

- Chapter 2 – Literature Review
  - This chapter consists of six sections where different research from previous authors will be investigated, analyzed, and understood to get a clear path on how to proceed with the research tasks at hand. The multiple sections of the literature review will try and break the relevant research into its respective categories as by area of research and the path of targeting the problem statement in this thesis. At the end, the research gaps will be identified to support the motivation of this work.
- Chapter 3 – Open Charge Point Protocol
  - The chapter focus on the communication protocol between the electric vehicle and the charging station and explains how it can be an input for cyber security.
- Chapter 4 – Methodology
  - This chapter focus on the microgrid system that will be utilized for the research and will clearly defined cyber-physical attacks. Afterwards, the impact assessment of cyber-physical attacks will be explained identifying the points of interest. Then, the chapter will highlight how the cyber-physical attacks can take place via the communication protocol. Finally, the chapter will show the microgrid system modelling in SIMSCAPE and will

end with the mitigation techniques towards the cyber-physical attacks on the HP-FCS. In addition, the chapter will include relevant standards, and state any formulas, equations, and information required to test the system.

- Chapter 5 – Results and Discussion
    - This chapter focus on the results of the system and will investigate each impact of the cyber-attack to see how it has impacted the smart grid. In addition, other features or combinations of impacts will also be investigated to get an overall understanding of the impacts on the smart grid as a whole. The chapter will also focus on the mitigation techniques or countermeasures for the impacts on the smart grid. The results will lead to specific targeted solutions for cybersecurity in the smart grid.
- Chapter 6 – Conclusion
    - The chapter concludes the thesis by summarizing the main outcome of the research and provide recommendations on how to address this problem and mitigating its impacts.

Chapter 2 Literature Review

2.1 Introduction

The literature review section presents a summary of the previous work in the literature that addressed the problem of cyber-physical security targeting the smart grids with focus on those targeting EV fast charging stations. The chapter starts first with an insight onto the recent research work providing an insight into the cybersecurity and how it can be implemented on the electricity systems. Furthermore, since the thesis focuses on the cyber-physical attacks, this chapter sheds the light on the research work done on cyber security within the smart grid as this will consist of intrusion and detection of these cyber or physical threats. Additionally, this thesis looks into the Open Charge Point Protocol (OCPP), which is used in EV fast charging stations and in smart grid applications. Finally, the chapter lists the research gaps, which will be addressed through the research work presented in this thesis.

2.2 Recent Research Activities Concerning Cyber Security

The study in [27] focus on the real-time detection of anomalies that may occur over the computer networks via wavelet-based signal processing techniques. The study refers to using the framework Waveman, which uses a used open-source tool called LastWave, to analyze real-time wavelet-based network anomalies. The anomalies that are targeted in the study are three Denial of Service (DoS). The attacks include Neptune, Smurf, and Mailbomb and two portscan traffic, which are ipsweep and stealth scan. Lastly, the research used two very well-known datasets, which are the MIT Lincoln Laboratory Intrusion Detection System (IDS) and EnrtRegistry, Inc (ERI). The study was found helpful in understanding cyber-attacks and how they behave in real-time networks.

The work in [28] performed anomaly detection for a network-based intrusion detection system using wavelet transform. The goal of this paper is to have a proactive technique instead of comparing it to the traditional intrusion detection system where the attacks are only detected after they have entered the network. The proactive technique uses the changes in the Hurst parameter to see the change in the intrusion detection system. The wavelet transform of the Haar wavelet was utilized to the see the scenarios with and without multi resolution techniques. Additionally, the MATLAB codes that were utilized were the Pareto distribution for the network traffic and in the future the best wavelet using the multi resolution technique and real time traffic and real intrusion is suggested. Finally, the shortcomings of the anomaly detection were discussed which says that if anything unusual is to be detected then it means that it will have a high false positive and false negative rate. Also, having security data and normal network data on the same network causes for a potential security risk as well which may result in reduced bandwidth for normal operation on the network. This paper helps in understanding network traffic while trying to detect anomalies and will be helpful during cyber-attack detection.

The paper [29] asks the question where wavelet basis functions have an important impact on the intrusion detection performance or not. It begins with questioning the signal processing techniques which are great for analyzing and detecting network anomalies for finding unknown intrusions. Therefore, this paper presents a novel intrusion detection approach using wavelet analysis, approximate autoregressive, and outlier detection techniques. The idea is to have fifteen features and applied them to the input signals from the network. The use of 1999 DARPA intrusion detection dataset from MIT [30] was utilized against four of the wavelet basis functions (Daubechies, Coiflets, Symlets, and

Discrete Meyer) to achieve the goal of detecting network attacks. In the end the three components to the framework are feature analysis, normal traffic modeling based on wavelet decomposition, and approximate autoregressive and intrusion detection. This leads to the ARX model which was utilized by the least squared method to result in Daubechies slightly higher performance than other wavelet families.

The paper [31] utilized the analytical strengths of neural networks to detect stepping-stone intrusions on the network. Network intruders are often launching attacks by creating some long connection chains by using multiple hosts. This allows them to keep the connection via the temporary hosts and this is essentially is called stepping stone as they do this to avoid detection from the intrusion detection system. Neural networks can be used to replace these conventional algorithms using statistical methods and powerful techniques of simulation intrusion detection techniques as well. Therefore, this paper proposed a new approach to overcome the scheme of the neural networks by essentially training the neural networks. By training the neural networks you can use the new packets of data as testing data and this allows you to monitor the connection chain at all the give time which reduces the stepping stone intrusion conducted by the intruders. Additionally, the paper also investigated performance of neural networks by looking at effects of the transfer function and processing the elements into the stepping stone intrusion detection.

The paper [32] proposes another signal processing and decomposing method for anomaly and intrusion detection based on matching pursuit technique. Matching Pursuit technique is a type of greedy algorithm which decomposes any signal into a linear expansion of waveforms which are taken from an overcomplete dictionary. This dictionary is called a set of base functions called atoms and it uses approximate signal to achieve good

sparse signal decomposition. Also, the paper focus on development in the feature extraction for the IDS are presented and showed that matching pursuit is a very promising methodology in the networks for the security framework. Finally, the novel algorithm will be used to detecting anomalies on signal decomposition. From [29, 31, 32], we gain a good understanding on intrusion detection and how the cyber-attacks occur in the network.

The paper [33] is a survey paper which explains the main techniques in the field of statistical based wavelet-based anomaly detection approaches and the role of the data traffic visualization tools. The anomaly detection techniques that are surveyed in the paper specifically for the wavelet-based approach and using signal processing tools include wavelet-based techniques, maximum entropy estimation, principal component analysis, and spectral analysis. Additionally, it discusses the network traffic visualizations tools that can be used are wavelet-based inference detection, Netviewer, Waveman, Vanguard, Parallel Anomaly Detection, and a few more. Overall, the paper introduces the wavelet techniques for anomaly detection and provides visualization tools using wavelets for modeling the network traffic and anomaly detection as well.

The paper [34] proposes a new detection mechanism for network traffic anomaly technique based on the Analytical Discrete Wavelet Transform (ADWT) using high-order statistical analysis. The detection mechanism consists of five components as follows: first being feature analysis, then wavelet transform with statistical analysis and thresholding, then wavelet synthesis and finally being anomaly detection. The use of 1999 DARPA intrusion detection dataset was utilized [30]. Overall, during anomaly detection there is a high chance of identifying actual attacks as normal traffic so the authors concluded that use of additional features will be required to characterize the network traffic behavior. If this

is possible then it can be possible to identify network traffic during an actual attack vs. when there is not an attack on the network.

In [35], is a future study of [34] where the author introduces the new component in addition to the 5 components mentioned in [34] and uses the technique to evaluate real traffic using a real traffic dataset over several days on a university public server. Additionally, a smaller threshold was set to detect more anomalies but this also lead to have more false alarms as well compared to before. The technique allows you to detect more but the drawbacks has higher false positive rates which leads to future work stated by the paper to reduce the false alarms by examining the server logs, source IP, port numbers, and more. Furthermore, other feature signals could be used with different characteristics for anomaly detection as well. According to [34, 35], some combinations of the features could be utilized on the electrical side of the system and use in detection cyber-attacks within the electrical network or smart grid as required.

In [36], the author proposes an intrusion detection tool which can quickly and effectively identify based on 2D Wavelet transform to detect anomalies in the computer networks. The examination of the network traffic is the key during a DoS attack in the computer networks. Additionally, the paper utilizes two datasets which consists of the DARPA and Federal University of Santa Maria (UFSM) to obtain a detection rate of 100% for the DARPA and 95% for the UFSM dataset respectively. This allows to examine DoS attack and how it behaves in the network traffic within a computer network and be implemented on the electrical smart grid.

According to [37], in a DoS attack the attacker targets the computer or the memory allocation to make it believe that it is full to handle any more requests and therefore affect

the legitimate users who are trying to access the network. Therefore, in [37] a fresh approach was identified where signal and image processing can occur for detecting network probe and DoS attacks assuming no information is provided. The advantage of this new method was it can detect with any prior information but it will detect any abnormal regions and identify than an attack is occurring which may not always be the case. The three-step method of converting packet of stream to a traffic signal then taking that signal and convert it by S-Transform into a time-frequency data. Upon which the last step will be analyzing using image processing to confirm identify of attack times.

Furthermore, in [38] Principle Component Analysis (PCA) is used to develop and improve Multi-Scale Principal Component Analysis (MSPCA) algorithm in the use of intrusion detection for Distributed Denial of Service (DDoS) attack. The MSPCA will utilize the anomaly-based detection algorithm by taking the advantages of the PCA and wavelet transform to improve the problem of high false alarm rate in intrusion detection. The authors were able to confirm using the 1999 DARPA dataset [30] that MSPCA has a better performance in detecting DDoS attacks than PCA in terms of detection accuracy and specifically reducing the high false positive alarm rates. Additionally, in [39] a frequency based DDoS attack detection was implemented by using the Naïve Bayes Classification. In addition of the previous work done on frequency analysis of DDoS on attack detection this paper contributes a much faster and easier way to implement traffic data using the Naïve Bayer classification technique. In this new technique the use of frequency-based methods such as Discrete Wavelet Transform and Discrete Fourier Transform as utilized and was concluded that Discrete Fourier Transform attributes to a better performance than the Discrete Wavelet Transform.

Finally, in [40, 41] anomaly behavior and detection are provided in an overview and table form identifying attack categories, assets, impact, and potential mitigation techniques for building automation systems and IP network-based systems respectively. Common threat categories were listed as network sniffing & port scanning, packet injection, replay attack, man-in-the-middle attacks, network flooding, and many others. Among these common threats attackers can gain knowledge of devices and infiltrate them and masquerade attacks as they are authorized users of the network. Additionally, this will allow the attackers to deny service to actual authorized workers and disrupt the network by revoking privileges of those who may be a threat to the network being takeover. At the end, a summary of selected methods is identified and summarized for anomaly detection based on the research experience conducted in the area.

The aforementioned discussion provided an insight on the types of attacks and the way they target the networks. This is critical to understand the potential impacts of such cyberattacks on the electricity systems and how to mitigate the effects of such attacks.

2.3 Recent Research Activities Pertaining to the Cyber Security within the Smart Grid

This subsection focuses on the research work addressing the cybersecurity when applied to the smart electric grid. According to [42], smart grid uses the information technology, which can intelligently supply energy to customers using two-way communication conducted through smart meters. This technology helps addressing some of the issues that are faced in the traditional grid but there are still some security challenges that need to be addressed within the smart grid. In [42], the study surveyed the cyber security in the smart grid and exposes the challenges that related to that. The study first

reviewed the security requirements then it investigated a number of important cyber-attacks and identify any potential vulnerabilities that are impacted. Additionally, a cyber security strategy solution was addressed to potentially identify those breaches, cyber-attacks, and provide future directions regarding where to identify the countermeasures within the smart grid.

In [42] the likelihood of cyber-attacks are identified along with the severity of that attack as well. The highest severity of the attack and the highest likelihood of the attack to be performed was identified as virus, worms, trojan horse, DoS, and backdoor list of cyber-attacks. Focusing on the DoS attack, the study breaks down the attack category of DoS into multiple areas where this attack can be targeted for compromised application or protocol in the smart grid. These areas include the Advanced Metering Infrastructure (AMI), instability of the smart grid systems, phasor measurement unit (PMU), and any other smart grid equipment. The potential countermeasures from the compromised security parameter for DoS is the availability of the service are intrusion detection system, sensing the time measurement and signal strength, and other reconfiguration methods to identify the cyber-attack within the smart grid. The study highlighted the need for more experimentation to understand these attacks and provide additionally ways for mitigations as future work.

The work in [43] provided another comprehensive analysis of smart grid systems against cyber-physical. The study presented a comprehensive study on the distinct functional components of the cyber-physical attacks on the smart grid. The study discussed a function-based methodology to show how the smart grid can be resilient to the cyber-physical attacks, identifies a Bayesian Attack Graph to compute the likelihood of compromising cyber components in the smart gird while providing risk analysis based on

the results. Furthermore, the study paid attention to the efficiency resource allocation in the smart grid domain using reinforcement learning to check vulnerability assessment of the smart grid against the cyber-physical attacks. With the use of cyber-physical security testbed as stated in [44] can be used to test the development of a smarter electric grid architecture, application and evaluation for the smart grid. The study in [44] also stated that an accurate cyber-physical system with components are required in a controlled environment to test the availability and integrity of the cyber-attacks on a real system.

The results of the attack from [43] along with the cyber-physical security testbed environment in [44] can demonstrate that an attack can create an imbalance in power supply and demand in a particular area that was targeted. The results also identified that once the attacker gains access to the cyber system to control a process then it is very difficult for the power engineers to prevent future attacks. Also, the study found that during contingency planning the power engineers do not plan for these sorts of attacks and therefore the study suggested multiple resources that can be used as potential countermeasures. The suggested resources are as follows: power storage at different levels, higher capacity of power lines, backup power lines, demand response as spinning reserve, gas storage to recover from an attack, and many more. The idea behind these countermeasures were to help the power engineers take these attacks into mind and plan them in their contingency planning for the smart grid.

The work in [45] proposed a Dirichlet-Based Detection Scheme (DDOA) for opportunistic based attacks to build and assess the reputation levels of the decentralized local agents in the cyber-physical system. The study proposed the adaptive detection algorithm with reputation incentives to detect a sort of opportunistic attack. This was

demonstrated by the use of a proposed scheme using data collected from PowerWorld simulator on an IEEE 39-bus power system. The proposed scheme was presented in a three-tier hierarchical framework with the goal of using in the future smart grids and emphasized the resilience against financially motived opportunistic cyber attackers. The study suggested the implementation of the DDOA in the real-world situation and refine the scheme based on efficiency and accuracy in detecting these opportunistic cyber-attacks.

Expanding on Intrusion Detection Systems, the work in [46] a model-based intrusion detection for home area networks specifically in the smart grid was presented. The study focused on the model-based intrusion detection system for home area networks (HANs) that exist within the smart grid. A new upcoming ZigBee is the dominant technology that is being used in the future of HANs. The study focused on targeting the IDS towards the ZigBee standard on the network as defined in IEEE 802.15.4. The IDS focuses on the abnormal behavior from the network and compare it with the specifications of the IEEE 802.15.4 to compare it with the normal behavior for malicious activities. The study assessed the performance of the proposed IDS through analysis and simulation for validation purposes. In [43], a Bayesian network intrusion detection system was tested in this HAN for the smart grid. The simulation results showed promising detection capability for the proposed approach but the study recommended the use of a larger data set to evaluate the performance and extends the IDS to cover more layers in the ZigBee technology.

In [47], a model-based IDS is proposed in the HAN part of the smart grid but specifically focusing on the smart meters. The study explained that smart meters have gained a very wide adoption in the smart grid but this still comes with drawbacks as there

are many attacks that discovered against the smart meters. Additionally, since smart meters are small devices, which have very limited power and memory and they are deployed in a very large scale adds a limitation on them where they cannot have no false positives for any IDS that is used on them. Therefore, the study proposed a model-based technique for the intrusion detection system for smart meters with keeping these limitations in mind and using an open-source smart meter platform to detect both known and unknown attacks on the smart meters. The open-source smart meter platform known as SEGMeter from the Smart Energy Group [48] was used in [47] to implement the IDS. The results showed that the IDS incurs low performance overhead with detection known and unknown attacks on the smart meters providing a reasonable detection coverage.

2.4 Cybersecurity using the Open Charge Point Protocol & EV charging system within the smart grid

According to [49], with the introduction of electric vehicles connects two infrastructures sections, one being transportation and the other being the electrical power network. The paper studied the Open Charge Point Protocol, which is specifically designed to communicate between the charging points and the energy management system associated with the electric chargers for the EVs. The OCPP is an open protocol, with the goal to provide an open communication between different standards charge points and different vendors who are providing the energy management systems. The paper studied the security properties of the OCPP and highlighted the subversion of the protocol or the malicious endpoints in the protocol can lead to the destabilization in the power grid. The theoretical and practical standpoints regarding the OCPP protocol on the cyber-attacks can interfere with the resource reservation when it comes to charging the EV. These attacks

can create over-shooting or under-shooting of power in the smart grid affecting the provisioning of power supply and demand within the power networks. Finally, the main concern the study highlighted with respect to the OCPP protocol on the reservations and managing of the charging process between the charge point and the central system with restricted security considerations.

To build upon the previous cybersecurity challenges with OCPP, the work in [50] performed a survey of security challenges and issues for the OCPP protocol for electric vehicle charging. The study pointed to the increased use of EVs will open a new era of research and development. This new era of research and development also comes with its challenges when we consider the number of EV charging sites are increasing the residential area and also increasing the charging sites at public locations as well. These charging sites need to communicate with each other and an efficient and secure mode of communication being utilized is the OCPP protocol. The OCPP based smart charging scenario presented in [51] helps identifying the security issues and threats along with potential solutions that have been investigated by many researchers. The study also addressed some security issues for the OCPP and recommended future work and research to enhance and improve the OCPP protocol.

In an attempt to highlight the security challenges for the OCPP protocol, the study in [52] addressed the man-in-the-middle cyber-attack within the OCPP protocol. The man-in-the-middle attack targets any communication occurring between two parties and attempts to intercept it and potentially altering any information that is exchanged between them. In the case of the OCPP protocol, the communication between the charge point and the central system is the two parties where the information can be exchanged and misinformation can

be provided to either end of the party. Therefore, the study suggested a countermeasure to the man-in-the-middle attack by simulating the behavior of the cyber-attack into the simulator. From the simulator setup, the study presented a privacy solution utilized in smart meters and apply it as potential countermeasure to the man-in-the-middle attacks. The results show that even in accordance with IEC 62351 standards [53], the security communication channels between the charge point and the central system still require additional security measures than the privacy feature. The implementation of the Virtual Private Networks (VPNs) between all peers in the EV infrastructure along with configured firewalls, and intrusion detection systems may be required to provide a complete trusted environment for both the users and operators in the EV charging infrastructure.

In [54] the deployment of secure EV charging system is used for the OCPP protocol by a large scale development of EVs. The study suggested that the large scale EVs will provide mobility paradigm shift along with the new upcoming demand requirements in the information and control components of the electric power network. Additionally, with this model, some obstacles will be removed when it comes to EV adoption and smart cities with smart grids will be able to facilitate the charging of new and upcoming EVs. With the OCPP protocol the study suggested to provide the interoperability and to reduce the maintenance cost associated with OCPP, which are crucial towards the communication within the EV charging systems. The study proposed a smart charging management system for community charging and large-scale public EV charging infrastructure using OCPP as seen in the Figure 2-1. The “SeeCharge” system proposed by the study implemented the OCPP version 1.6 but it is still susceptible to certain malicious activities and vulnerabilities.

With the updated OCPP version 2.0 and onwards, the further security initiatives will be implemented and upgrade the secure EV charging systems.

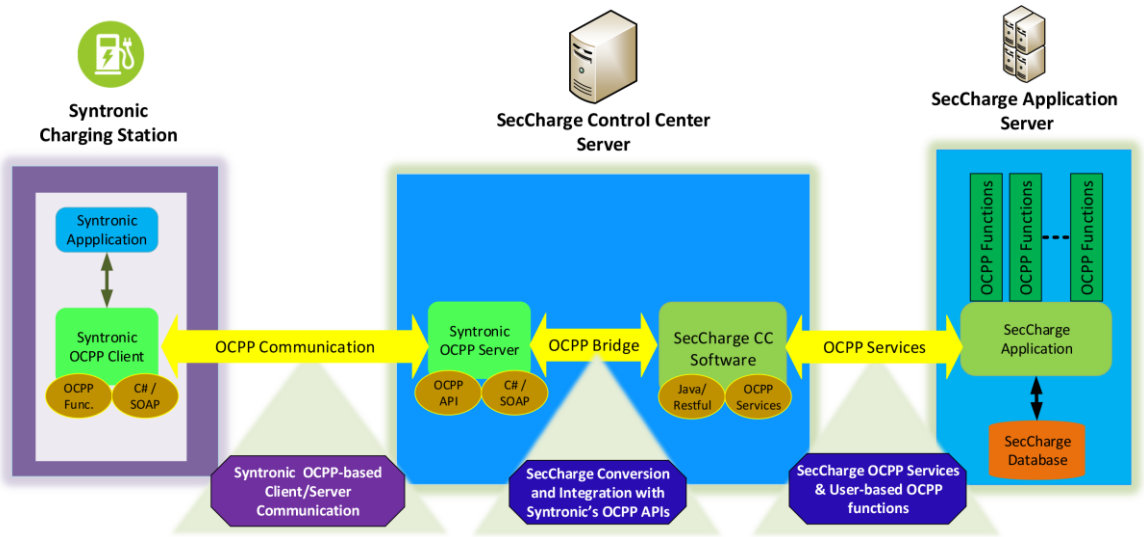

Figure 2-1 - High-level Diagram for Integration of SecCharge with Syntronic Charging Station as secure EV charging system using Open Charge Point Protocol [54]

In addition to development of EVs, a new concept presented in [55] uses the Open Charge Point Protocol for E-Scooters. With the demand for passenger vehicles growing and need to offset carbon emission, the study suggested a unique concept of E-Scooters. The basis of the idea is based out of India where 94.5% of an estimated 261 tons of carbon dioxide emitted is contributed from road transportation. The study assumes that the use of EVs may incentivize to switch from gasoline-based transportation methods and the case of e-scooters is more viable as out of 20 million 2 wheelers, 6 million were scooters. With the demand in the market, the study proposed the future of design and fabrication of the e-scooter with a growth in the electric vehicle charging station alongside as well. The proposed charging station for the e-scooter in the study required the utilization of the OCPP protocol to provide the safety requirements for the administrators, installers, consumers,

and the providers. The study outlined the architecture of the electric vehicle charging station, which involves quality, safety, and interoperability. As high-level idea of what the framework will look can be referred in Figure 2-2. The study suggested that the future work will be making it compatible with any smartphone and use a QR code localization to work with the electric vehicle charging system with utilization of the OCPP protocol.

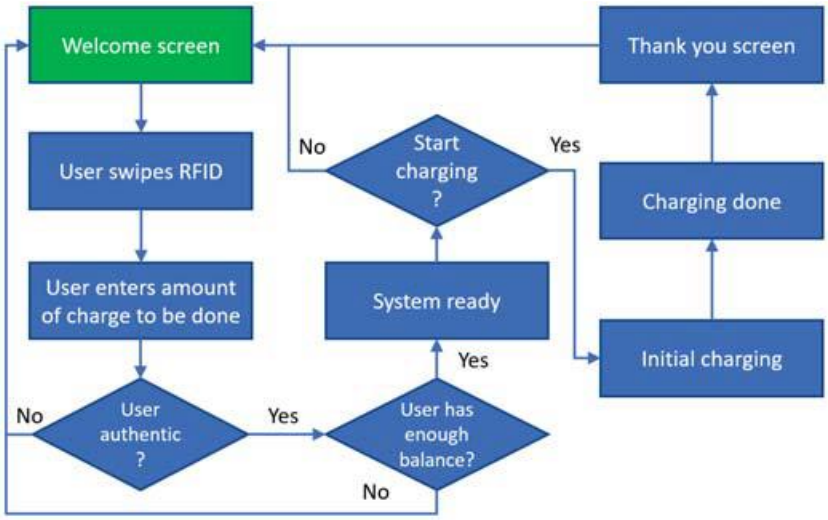

Figure 2-2 - Flow chart of the user experience electric vehicle charging station using OCPP as seen in [55]

Staying with trend on emerging EVs, in [56] a smart battery management scheme for vehicle to grid (V2G) is proposed. As mentioned in previous studies, the cybersecurity associated with an increase EVs into the smart grid will result in more imbalance of power between supply and demand. This study proposed to use the EVs in a V2G scheme where the EV will result as the spinning reserve for the smart grid. The spinning reserve acts as a reserve power ready to plugged into the grid in case of power shortages or frequency deviations within the smart grid [57]. Using this scheme, the electric vehicle can both absorb (charge) and store (supply) power from the grid which can help during times of

power shortages. If considering the effect of cybersecurity on the smart grid, as the communication protocol utilized will be OCPP, then impacts of the V2G model to the grid needs to be considered in the energy management of an electric vehicle. The proposed model in the study is expected to improve the performance of the energy management and acts as a potential countermeasure to power shortages assuming cybersecurity is secured in the smart grid.

2.5 Cyber Security in Smart Grids with Electric Vehicle Charging Stations

Referring to latest research in electric vehicles and fast charging stations, in [58] the cybersecurity of the electric vehicle charging is described by focusing on the smart charging management systems (SCMS) for the EVs. The concept of SCMS optimizes charging for plug-in electric vehicles (PEVs) and provides controlling techniques such as voltage control, frequency regulation, spinning reserve and demand response. The idea of SCMS can be applied to both physical and cyber threats on the smart grid. Specifically, focusing on the cyber threats such as man-in-the-middle attack or denial of charging are crucial when considering the components that are affected due to these attacks. The study provided a comprehensive review of the different aspects of electric vehicle supply equipment (EVSE) and EVs by the concept of SCMS to review the cybersecurity and the impacts on the power grid and the community. From the review, the research gaps were highlighted in the current available EV and EVSE charging infrastructure as most does not utilize any security software or developmental strategies towards cybersecurity. Also, the communication model from end-to-end is very early in the state of development and lacks the standards required for communications between EVs and EVSE securely. Furthermore, the charging stations are still managing the proper physical security guidelines required to

occur at charging site from the consumer end and it is not up to date on the technologies and equipment as well. Therefore, the need for cybersecurity is in high demand in regards to EVs and EVSE charging sites that accommodates the EVs every day.

In [59], the cybersecurity of EVs is considered when it comes to cyber-attack detection while charging is taking place. With the large-scale revolution of EVs and EVs that give many advantages towards the environmental concerns of by providing positive environmental benefits also comes with challenges. The growing market for EVs poses a cybersecurity related challenge when it comes towards cyber-attack specifically when they are charging. One type of disastrous cyber-attack or situation is Denial of Service, which leads to out of service EVS or overcharging, which leads to damaging the battery packs of the EVs. Either way cybersecurity needs to be discussed during charging the EVs as both types of attacks can affect the vehicles and the smart grid. The focus of the study was on designing algorithms for detecting cyber-attacks that can potentially affects the EVs battery packs during charging and to evaluate these algorithms for its effectiveness in DoS and overcharging attacks. The results were able to identify a no attack case, undetectable attack case, DoS attack case, and the overcharging attack case. According the Dynamic Detector algorithm, the cases were identified with various detection times and future work needs to work on the undetectable attacks and improving the detection times.

Furthermore into EVs, according to [60] the study pointed out that with EVs and the publicly available power grid data sets up for a new cyberattack vector. The goal was focusing on the information on the charging patterns at the FCS and EVs are becoming more accessible via smartphone applications. With more access to data will result in a new cyberattack vector towards the smart grid. Additionally, the study used public power grid

data available to find the charging patterns of the EVs in hopes of predicting a targeting vector for a cyberattack. Since the intruder can gain remote access via various physical assets from the consumer end to the electric charging station end, and the publicly available data makes is very probably to figure out when a cyberattack can occur. The study also identifies when the level of EVs increase than it will become much more practical to conduct a cyberattack as it will disrupt a lot grid and have other impacts that may be not seen upfront.

In [61], a secure and efficient scheme for Energy Internet (EI) based on the V2G framework was discussed. The EI scheme based V2G framework relies on the idea that EVs are not only able to distribute electricity into the grid but also receive as charging from the grid. The study focused on the drawbacks of several smart grid authentication protocols that disrupt proper functioning of the power grid. The EI scheme also focused on a most vulnerable types of attacks such as DoS or man-in-the-middle attack. Additionally, it proposes a new protocol between the framework of the V2G, which will help vehicles communicate more securely when they are charging or discharging at specified electrical charging stations. The study concluded that for this secure data and communication to take place an authentication protocol must be free from any cyberattacks. The approach proposed in that study had its limitation as it was not able to differentiate the scheme between session for a key security to the subscriber versus the intruder during login attempts. Considering the limitations, the study stressed on the subsequent proposed research should be conducted to evaluate the security properties and employ another model to attempt to identify the intruder attempts.

According to [62, 63] a systematic risk assessment of EVs is conducted under Cyber-Physical Threats towards the EV Charging System. The rapid growth of EVs and its integration into the transportation and power grid has risen necessitates that needs to deal with smart charging infrastructures. The inherent cyber-physical characteristics of the charging stations make them more likely to target them with cyber-physical attacks. Since there is a lack of cyber-physical security assessment in these stations, creating potential vulnerabilities for the consumers and the smart grid. Therefore, a generalized methodology is utilized to record the impacts analysis of cyber-attacks and address the vulnerabilities of the EVs and EV charging networks to develop effective countermeasures and attack detection based on the framework.

Finally, in [64, 65], the evolving trend of making traditional power grids much smarter has resulted in the creation of smart grids. These smart grids allow complex network to take place within the grid, allowing multiple points of the grid to have back-and-forth communication. Specifically, a type of smart grid which is in much demand is the DC-microgrids (DC-MGs), which uses the intelligent control, two-way monitoring, and other features and these make them very suspectable to various cyber threats. These DC-MGs typically contain EVs, solar or wind generation, smart homes, smart sensors, and network communication cables, allowing them to monitor and stay in constant contact from end-to-end of the grid. Given these assets in the smart DC-MGs, it is suspectable to cyber-attacks regarding false data injection via the communication layer utilized in the DC-MGs. Both studies focused on using Blockchain Technology and Hilbert Huang Transform for cyberattack detection and enhancing the cybersecurity of the DC-MGs.

2.6 Research Gaps

The literature review identifies many research gaps within the topic of cybersecurity in the smart grid focusing on EVs and FCS. From the recent research works, we saw that there were many topics pertaining to the cybersecurity in the smart grid. These topics focus on the smart grid and how power imbalance can occur due to cyber-physical attacks on the grid. Since most of the literature review on smart grid cybersecurity focused on microgrids in grid-connected mode highlights a research gap for isolated microgrids. The increased popularity of isolated microgrids and promised future growth demands research to investigate the impacts of cybersecurity on isolated microgrids. Many different parts of the smart grid like the metering infrastructure, backup power resources, and mismatch of power are mentioned, but one important component needs to be mentioned which are the electric vehicles fast charging stations. These are growing in demand due to the increase in demand for electric vehicles globally. Therefore, these fast-charging stations are the biggest target in the smart grid for cyber-physical attacks.

Additionally, another important research gap can be identified in the types of cyber-physical attacks that are present in the smart grid. Still, the literature review needs to have research that specifies in identifying this weakness from the intruder on how they are gaining access to this smart grid infrastructure. Importance of understanding where the cyber-physical attacks originate will help target the next research gap which is to provide mitigation techniques for these cyber-physical attacks.

Finally, the last important research gap that was not seen at all in the literature review focusing on the cyber threats was how to mitigate them and provide solutions. Many research showed the use of backup power supplies but there is a limitation on how much

you can store. Instead of targeting the problem the literature review showed temporary solutions to deal with the cyber threats to the smart grid. Considering these research gaps will be used to address the research and provide relevant research on them to address each of them in as much detail as possible.

Chapter 3 Open Charge Point Protocol

3.1 Introduction

Smart grids are electrical networks that rely heavily on communication technologies to service the power grid. These smart grids have many different types of communication protocols that get utilized, such as the Sampled Values (SV), Generic Object-Oriented Substation Event (GOOSE), and Manufacturing Message Specification (MMS) according to the IEC 61850 communication standard [66]. These communication protocols focus on the communication between different parts of the smart grid back and forth in both directions to keep all parts in constant communication of all events in the grid. In this research, the focus is on EVs and FCS, which utilizes another form of communication protocol to communicate between the chargers and station operators. Some of the communication protocols available for FCS include Open Charge Point Protocol (OCPP) [51], which is a global communication protocol between the charging station and the back-end system that operates the charging station. The next one is the Open Smart Charging Protocol (OSCP) [67], which is an open protocol between a charging management system and an energy management system which uses a 24-hour forecasted capacity on the grid. Both OCPP and OSCP are protocols are maintained by the Open Charge Alliance (OCA) for worldwide charging infrastructure. There are also other smaller protocols Open Charge Point Interface (OCPI) [68], which connects the charge station operators to the service providers and many other ones. From all these communication protocols, the greatest amount of availability to implement on EV charging infrastructure and overall functionality can be utilized on the OCPP. Also, there are many updates made by the OCA on the OCPP

protocol to make it accessible for any EV company and its infrastructure. Therefore, for the purposes of the research the OCPP communication protocol will be used.

This chapter focuses on studying the Open Charge Point Protocol (OCPP). The understanding of the protocol and analysis of OCPP will be referenced from [51] as it explains the OCPP in a manual type description and will be referenced multiple times to highlight key terms, procedure, and utilization of the OCPP in a web simulated interface.

The OCPP is a standard open protocol for communication between Charge Points and a Central System and it is designed to accommodate any type of charging technique [51]. The protocol does not define any specific communication technology as long as it has Transmission Control Protocol (TCP) / Internet Protocol (IP) connectivity then will suffice and will be able to accommodate that specific communication technology. The use of OCPP version 1.6 is utilized in this research as it was the one most widely available and provided all the features needed to accommodate any techniques that will be implemented for cybersecurity. In addition to the OCPP version 1.6, OCPP version 2.0 is also become available but since the 1.6 version is has been available for a longer time therefore more resources are available in cases of bugs or technical errors. Finally, the chapter will explain the uses of the protocol and understanding from both the Charge Point and Central System and also who they can be implemented together to have a proper functioning simulated model to see the protocol in action.

3.2 Charge Point

To begin, according to [51] the definition of a charge point is defined as the physical system where an electric vehicle can be charged and a charge point can have one or more connectors. This explains that the charge point is the consumer end where they will be

connecting their EV for charging and one charge point can have multiple outputs for charging similar to an extension cord utilized in a home. Also, the term connector that will be used in the chapter will refer to an independently operated and managed electrical outlet of specific power levels on the Charge Point. Additionally, the term connector can refer to a single outlet or multiple physical sockets where more than one vehicle can connect at a given time. Since the charge point is where the consumer connects the EV, there are fewer operations that are initiated by the Charge Point but still crucial in terms of the communication issue.

There are ten operations that are initiated by the charge point as per OCPP 1.6. They are as follows: 1) Authorize, 2) Boot Notification, 3) Data Transfer, 4) Diagnostics Status Notification, 5) Firmware Status Notification, 6) Heartbeat, 7) Meter Values, 8) Start Transaction, 9) Status Notification, 10) Stop Transaction. From these ten operations, not all of them are key or required for a simulated charge point or utilizing one in real-time. Some of the operations are like extra features that can be implemented by the company who is choosing to implement this protocol in their electric vehicle charging station. Focusing on a few important operations will help understanding how exactly a charge point work and functions. The first operation “Authorize” as seen in Figure 3-1 is utilized every time a new electric vehicle comes to the charge point. The most basic operation authorize will be implemented every time a user wants to start or stop charging the EV. This basic operation makes sure that no one will be able to disconnect or connect the physical wire form the vehicle until authorized to start or stop has been given. This ensures safety on the consumers end if they try to pull out the connector when the vehicle is the middle of

charging as they will first need to request to stop the transaction and only then they can safely remove the connector from the vehicle.

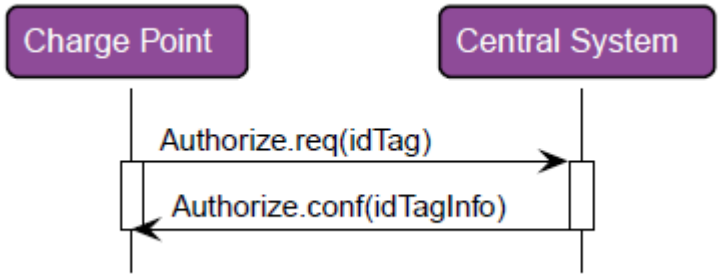

Figure 3-1 - Sequence Diagram for the Operation Authroize [51]

The next operation named “Boot Notification and Heartbeat” are next most critical operations required by the Charge Point. Prior to the authorize operation giving permission for the EV to start or stop charging, the Boot Notification operation is conducted. This operation requests all the information regarding the configuration like the version, vendor, and more as seen in Figure 3-2. This information is crucial in determining how much power and for how long will the vehicle need charging as no two electric vehicles are same and may not come with same battery percentage. Therefore, each time there is a boot or reboot (in case of power outage) then this information will be initiated by the Charge Point and the information will be received by the Central System upon which it will decide authorizing or no authorizing this transaction.

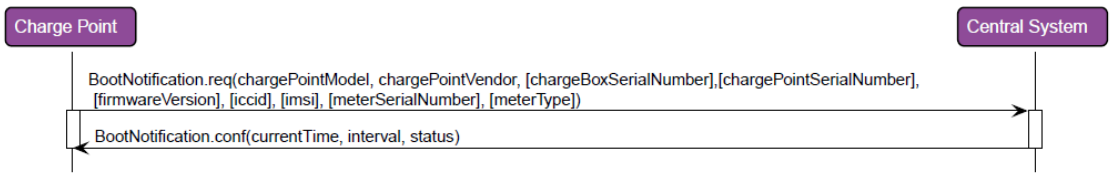

Figure 3-2 - Sequence Diagram for the Operation Boot Notification [51]

Now along with the Boot Notification, the next operation named “Heartbeat” is as crucial as well. This operation helps informing the EV user the time period and the amount of charging. Any information after charging has begun and until it has finished charging to the desired level can be updated by the Heartbeat operation. This simple job of this operation is to make sure to inform the Central System that the charge point is alive (in use or no in use) as seen in Figure 3-3. When this operation is initiated by the charge point at designated intervals updates the central system, it allows another operation to take place named “Data Transfer”. When the EV user knows the charge point is alive then communication between them also needs to keep going and that is why Heartbeat is more important as it tells the user that he needs to transfer data or stay updated and so on.

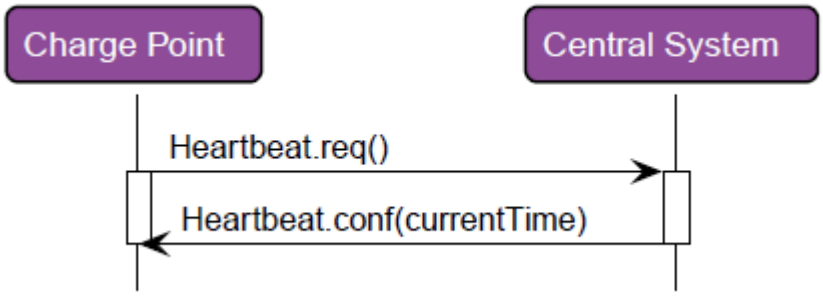

Figure 3-3 - Sequence Diagram for the Operation Heartbeat [51]

Finally, the other operations are important and required for operation of the charge point such as “Start Transaction” and “Stop Transaction”. Once these operations are initiated by the Charge Point then the Central System is notified when the transaction started and stopped. Along with the Meter Values operations, the time and power supplied from the charge point will later be used to calculate the cost of the charging for the consumer. Therefore, all these other operations are required for sure but without the basic ones, the user cannot try and simulate the charge point either. If anything goes wrong then

the status notification operation will keep the central system informed and generate an appropriate error code which can tell the user what has occurred.

3.3 The Central System

According to [51], the central system is defined as the Charge Point Management System, which manages the Charge Points and has all the information regarding the authorizing the consumers who are using those Charge Points. Also, the Central System will be the sole authority that will be managing those charge points therefore labelled as the Charge Point Management System. In addition to terminology introduced in the Charge Point section, the Central System has few other terms that will help in understanding its operation. The term charging profile is used when looking at different charging profiles as it holds the information of that profile and the charging schedule when a certain profile will be implemented. The term charging schedule is part of the charging profile and is defined as the block of charging power or current limits that are applied with a given start and stop time during the day. The term charging session is defined with the first interaction of the EV and when the transaction begins either physically or remotely by the central system. Finally, the last related term for the central system is the transaction, which is defined as the part of the charging process when all relevant preconditions (authorization, plug has been connected, and so on) are met and charging has begun. The term transaction ends when the charge point has been disconnected and all preconditions have been changed and leaves the state of charge and charging has stopped irrevocably. The usage of this terminology along with the operations will help in understanding operation from the central system standpoint.

There are nearly twenty operations that can be initiated by the central system. To begin, the most basic operations initiated by the central system are “Remote Start Transaction” or “Remote Stop Transaction” as referred in Figure 3-4 and Figure 3-5. These are the same basic operations initiated by the charge point but in the case where the charge points need to begin and stop charging this can be done remotely as well. Along with these the “Unlock Connector” is as important as well because even when the transaction has completed and charging has stopped this does not necessarily end the user experience. Until all information is not confirmed by the central system the “Unlock Connector” operation is not initialized and the user may not remove the plug from the electric vehicle as shown in Figure 3-6.

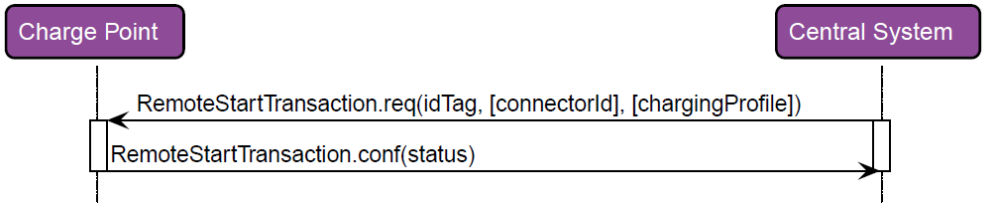

Figure 3-4 - Sequence Diagram for the Operation Remote Start Transaction [51]

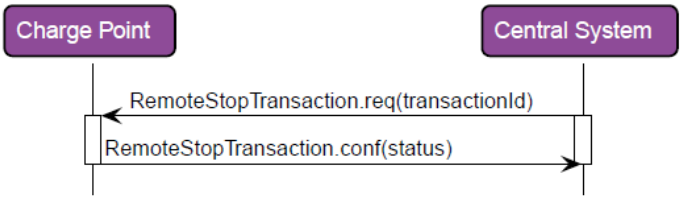

Figure 3-5 - Sequence Diagram for the Operation Remote Stop Transaction [51]

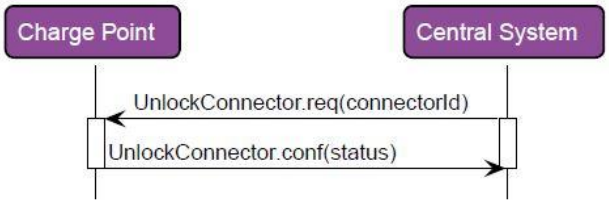

Figure 3-6 - Sequence Diagram for the Operation Unlock Connector [51]

Another important operation by the central system is the “Charging Profile” as mentioned in the terminology. Since OCPP protocol utilizes Smart Charging, which is defined when the central system gains the ability to influence the charging power of current towards a specific EV and/or the total energy consumption on an entire Charge Point or group of Charge Points. Overall, it allows the central system to determine which points gets how much power at what time and for how long. This will be later implemented in a test model that will be used to demonstrate the use of the OCPP protocol. As seen in Figure 3-7, it shows the breakdown beginning at the central system (direction of the arrows shows the initiation of operation) and starting the transaction and selecting the correct charging profile or selecting another based on the Charge Point in question at the beginning of the transaction. As we referred back in the Charge Point section, the “Heartbeat” operation provided at regular intervals a message to update the Central System. But this means that the Central System is always reliant and have to wait for the message from the Charge Point to get an update. In that case, the operation “Trigger Message” as seen in Figure 3-8 can be utilized and be initiated from the Central System to the Charge Point to get an update from a specific Charge Point. In the case that the Central System requires information other connection status, then it does a modified “Trigger Message” operation also very useful to

get specific information from the Charge Point as seen in Figure 3-9. As seen in the figure, the trigger message with status notification is useful when you be receiving the all okay from the Charge Point as a specific error code may not show up. With this dedicated operation the central system gains the exact error code that could be affecting the Charge Point.

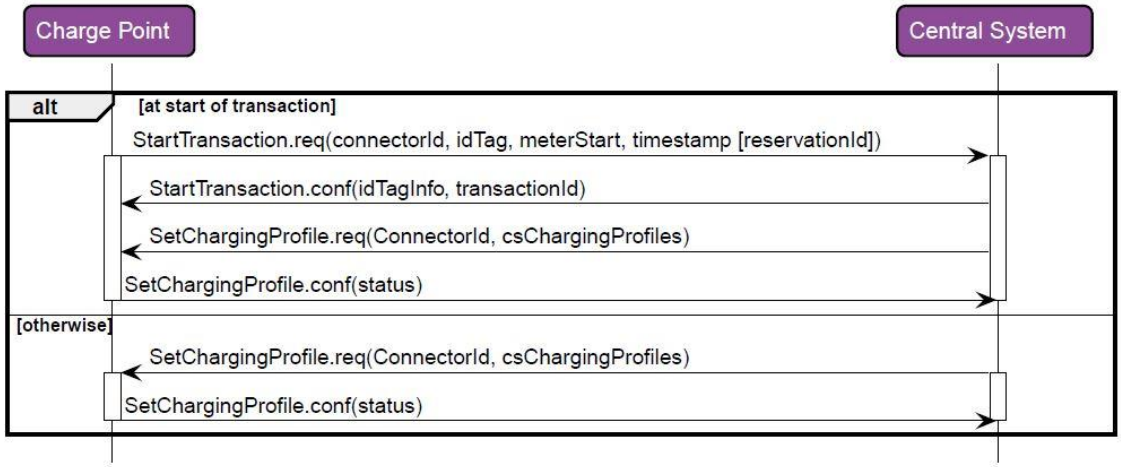

Figure 3-7 - Sequence Diagram for the Operation Charging Profile [51]

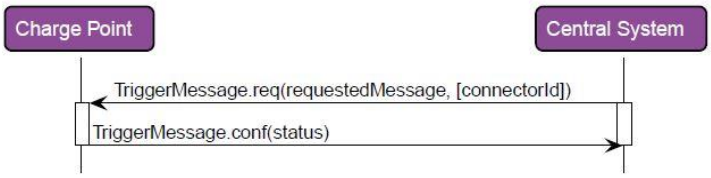

Figure 3-8 - Sequence Diagram for the Operation Trigger Message [51]

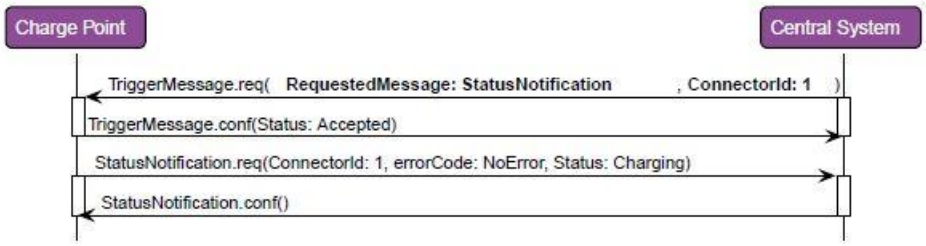

Figure 3-9 - Sequence Diagram for the Operation Trigger Message with Status Notification [51]

Furthermore, the "Trigger Message" with "Status Notification" is very useful after a firmware update. Another operation crucial towards keeping the Charge Points and the Central System up to date is make sure the firmware is always updated to the latest and more secure version. As seen in Figure 3-10, the update firmware operation has many steps and if any of them gets missed or skipped or simply results in an error then how will the central system get a notification from the charge point. With the dedicated Trigger Message operation, the Central System can request the Charge Point to give specified information that can help to figure out where the firmware update may have stalled or not being completed. Since the only way the Central System communicates with Charge Point with some remote TCP/IP connectivity, then these specific operations are crucial to keeping the communication between the two ends of the protocol.

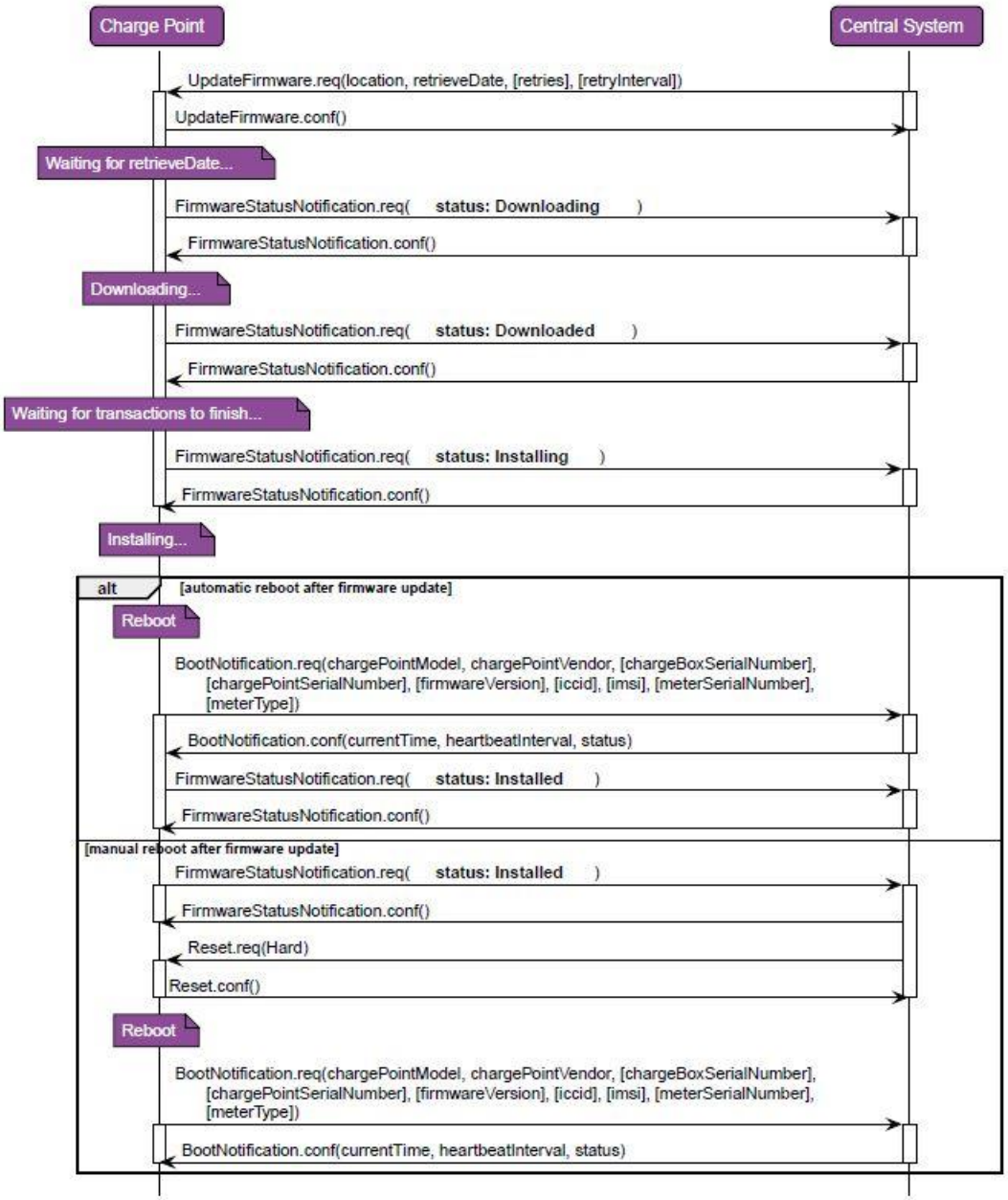

Figure 3-10 - Sequence Diagram for the Operation Update Firmware [51]

3.4 Communication Between the Charge Point and the Central System

This section sheds the light on the operations supported by the protocol and identify them in terms of different categories. The operations initiated by Charge Point or Central System will fall under one of six categories. The profile being the Core, which consists of all the basic charge point functionality comparable with OCPP 1.5 & OCPP 1.6 without any support from the firmware updates, local authorization or any management & reservations services. The second profile is the Firmware Management, which is the support from all the firmware update management and diagnostic logs for recording keeping for all changes. The third profile is the Local Auth List Management, which consists of all the local authorization list in the Charge Points. The local authorization applies when no central system exists and the charge points are controlling and maintain themselves. All the commands are given and executed by the charge points from the charge points. This profile applies to companies that may not have a very large electric vehicle charging infrastructure and may not be interested in remote monitoring of their assets. The fourth profile is Remote Trigger, which is the opposite of the local auth profile as it allows for support from remote triggering of the charge points. This allows the central system to be able to monitor and initiate messages remotely to the charge points. The fifth profile is Reservation, which supports the reservation for a Charge Point. The operations mentioned in the previous sections regarding charging profiles are related to the reservation profile as it allows for setting restrictions based several criteria. The last and sixth profile is Smart Charging, which supports basic smart charging and use of basic operations to get gain more information and stay up to date on what is occurring on the Charge Points and the Central System.

Table 3-1 - Implementation of different OCPP operations by categories

Operations	Core	Firmware Management	Local Auth List Management	Remote Trigger	Reservation	Smart Charging
Authorize	x					
BootNotification	x					
ChangeAvailability	x					
ChangeConfiguration	x					
ClearCache	x					
DataTransfer	x					
GetConfiguration	x					
Heartbeat	x					
MeterValues	x					
RemoteStartTransaction	x					
RemoteStopTransaction	x					
Reset	x					
StartTransaction	x					
StatusNotification	x					
StopTransaction	x					
UnlockConnector	x					
GetDiagnostics		x				
DiagnosticsStatusNotification		x				
FirmwareStatusNotification		x				
UpdateFirmware		x				
GetLocalListVersion			x			
SendLocalList			x			
CancelReservation				x		
ReserveNow				x		
ClearChargingProfile					x	
GetCompositeSchedule					x	
SetChargingProfile					x	
TriggerMessage						x

Now that all the profiles are identified with their respective operations, let's take a look a basic operation under the OCPP protocol. In Figure 3-11, the basic communication

starts from the Charge Point via communication to the Central System. The protocol goes through the respective operations until charging finished and transaction has stopped. The last communication points out from the Central System to the Charge Point indicating to unlock connector operation to disconnect the EV from the Charge Point.

Figure 3-11 - General Operation of the OCPP [51]

In addition to the general operation of the OCPP, the complete energy transfer from the beginning of the transaction to the end of transaction is shown in Figure 3-12.

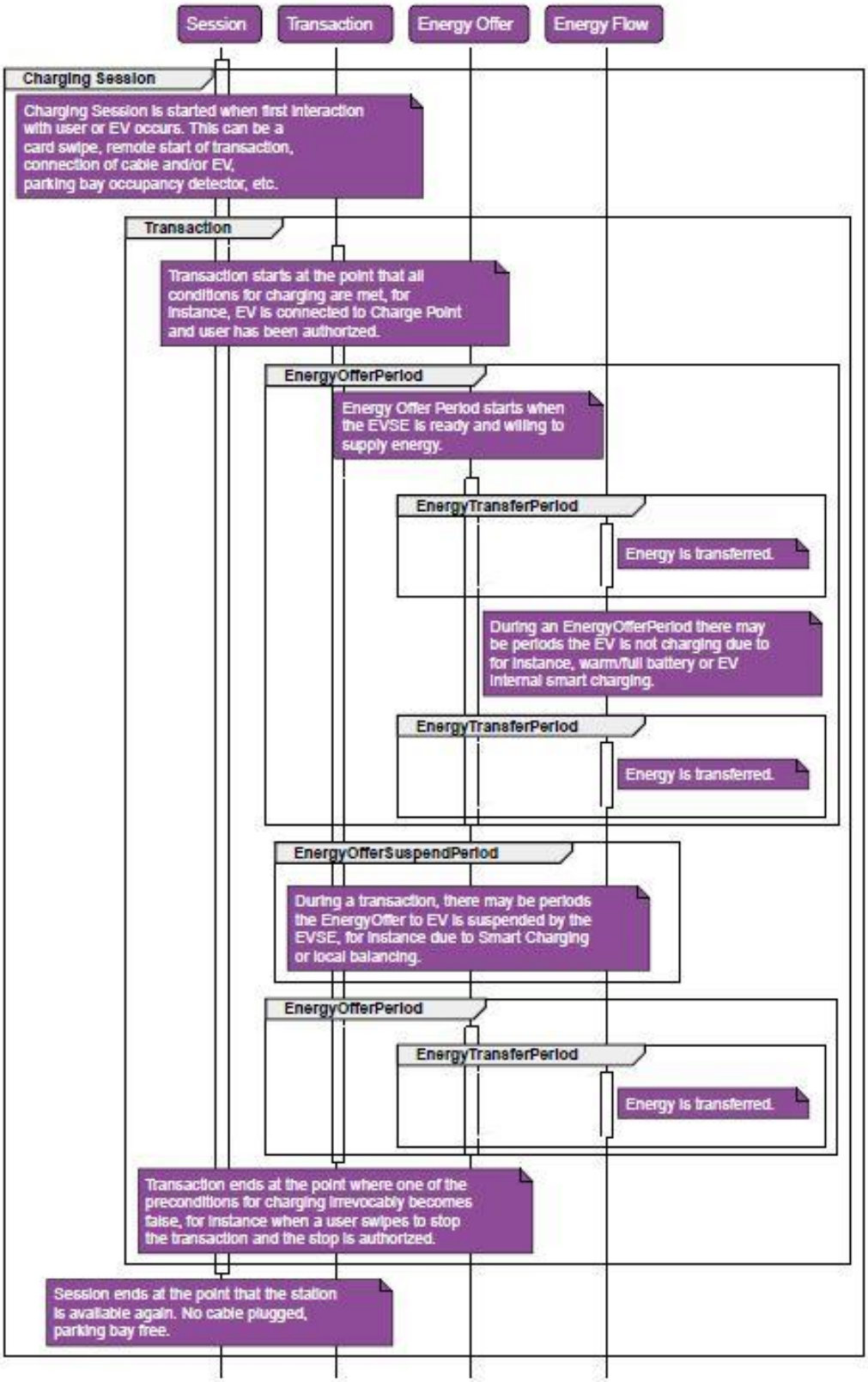

Figure 3-12 - Charging Session and Energy Transfer in the OCPP [51]

3.5 SteVe

With an understanding of the OCPP, the next obstacle deals with how this protocol can be simulated for research purposes and tested to see its behavior. This introduces the next part of research that was conducted on SteVe. SteVe which means Steckdosenverwaltung, namely socket administration in German was developed by RWTH Aachen University specifically for the OCPP Protocol. [69] The main idea behind SteVe is that it is a socket administration platform, which is usable through a web interface-based interactive server. The basic functions or the Core profile of the OCPP can be tested via virtual Charge Points and simulating the entire charging session from start to end. SteVe gives the ability to administration of charge points, user data, and RFID for user authentication and testing in operation.

The reason for choosing SteVe as the platform is that SteVe is an open platform where the user can implement, test, and evaluate any ideas for electric mobility including authentication protocols, reservations for charge points, and basic operations of the protocol. The ‘user’ is defined as anyone who wants to implement the OCPP protocol on their company who will focus on allowing the operation of charging stations for consumers. Another reason to pair SteVe and OCPP version 1.6 is that the OCPP version 1.6 is very compatible and most bug free to be available for testing on the SteVe platform. In the near future OCPP version 2.0 and above will be available for testing on SteVe and this is reason for choosing the specific version of the protocol and the web-based platform. Refer to Figure 3-13 to see the web-based SteVe platform with shows the operations that can be initiated by the Charge Point. Also, the figures show a sample Charge Point created named UOIT and can be added to the Connector ID. This web interface shows how a potential

central system can look like from the company's end who are monitoring all their charge points from one central location.

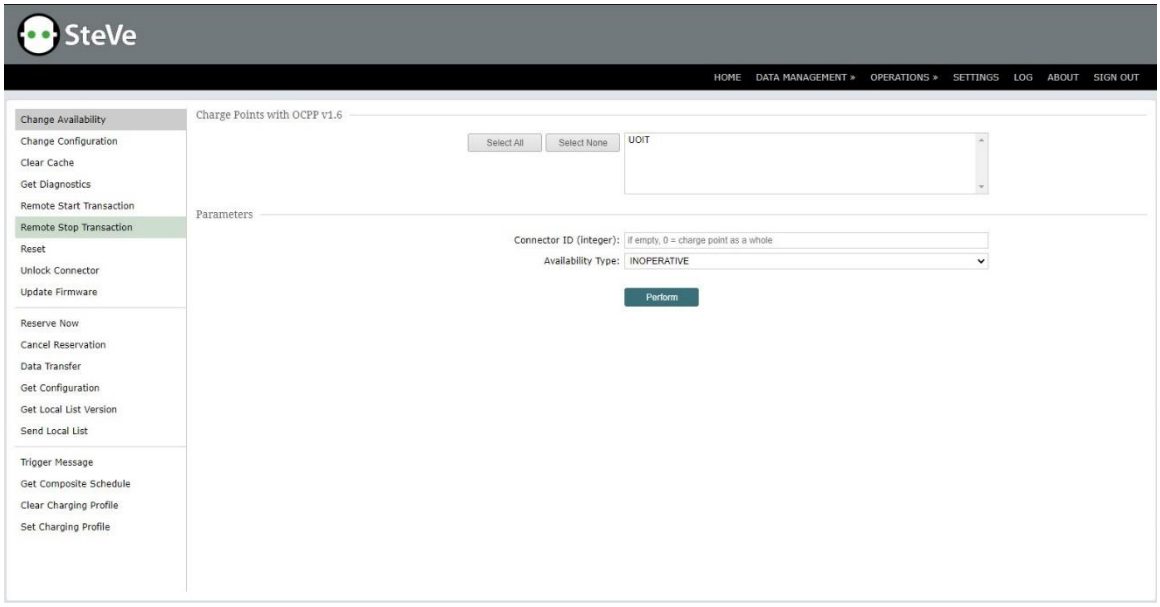

Figure 3-13 - SteVe interface showing possible operations by the Central System on a sample created Charge Point named UOIT

Figure 3-14, depicts all the possible information that can be acquired at the Charge Point. The figure refers to a sample Charge Point labelled "CP_1", which identifies the correct OCPP version as 1.6 utilized for communication. Then, the information of the Charge Point Vendor is identified as "Tesla" and Charge Point Model as "Charging Station", which to a consumer can read as follows "Tesla Charging Station". When creating the designated Charge Point each company can label and designate the points as they desire with the information required for identification and use by the consumers. In addition, any other diagnostic and status information place holders are also shown which get updated based on the operations initiated by either end of the protocol.

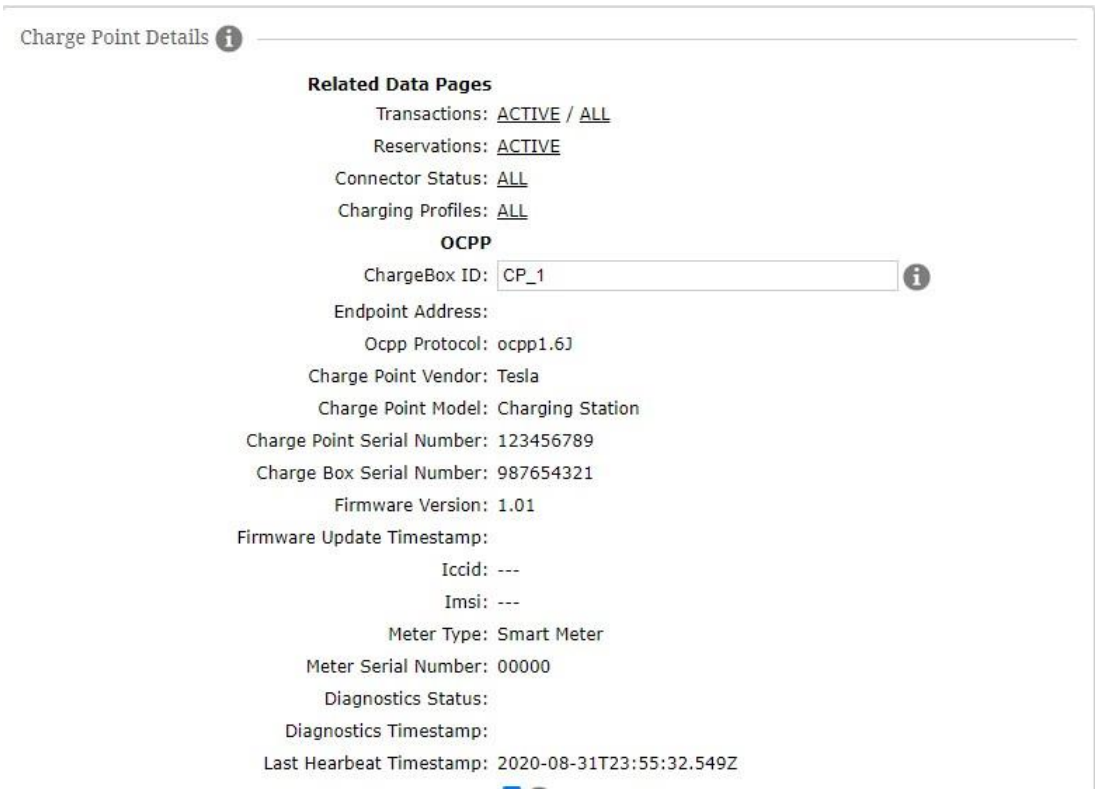

Figure 3-14 - SteVe interface showing possible fields on a Charge Point

Chapter 4 Methodology

4.1 Introduction

This chapter begins with the discussion of the microgrid system utilized to assess the impacts of the cyber-physical attacks on a typical community, which has electric vehicles and fast-charging stations. Afterwards, the chapter will introduce and describe the cyber-physical attacks and how they can be conducted via the OCPP communication protocol. Then, the next section will identify the components that exists in a typical community within a microgrid system along with which components that are impacted when a cyber-physical attack is implemented. In addition, the section will identify the components that are severely impacted from the attack and quantify the impacts of those components using the proper standards and measurements. The next section displays the microgrid system and how it can be modelled using SIMSCAPE. At the end, the chapter will also discuss potential mitigation techniques that can be implemented on the microgrid system to mitigate the impacts of the cyber-physical attacks.

4.2 Microgrid System

The concept of a microgrid refers to an energy grid that has its own control facility that allows it to disconnect from the traditional grid and operate autonomously [70]. The microgrid operates on grid connected mode, isolated mode, or both. The grid connected mode of the microgrid allows for continuous supply from the traditional grid referred as the infinite bus. While the isolated mode refers to when the microgrid is disconnected from the grid and is operating self-sustaining power.

To justify the choice of this system, it is important to understand that in case of a traditional grid then all homes, commercial properties, and other power sources are

connected together, which provides power all the loads. If the grid cannot provide power due to maintenance or faults of some kind, then all customers will be affected and will not be able to receive power. The microgrid operates normally when connected to the grid but during a loss of power a microgrid can maintain supplying power to the community. The microgrid consists of renewable energy sources of such as solar or wind or non-renewable sources such as diesel power. It can be a combination of distributed generation that allows the microgrid to operate autonomously during an outage from the grid. Additionally, when designing a microgrid, the power capacities of the energy resources must match the demand to avoid power outages and power quality problems.

For example, a microgrid for a small area can be one building or an apartment complex or can consist of an entire community of multiple homes. The grid area can be broken up into a small or large sub-area and can contain one or many components but the only goal is to make sure that the grid is satisfied to meet the power demand of the community. An example of what types of microgrids exists can be seen in Figure 4-1 where the figure shows a partial feeder microgrid, full feeder microgrid, or a full substation microgrid.

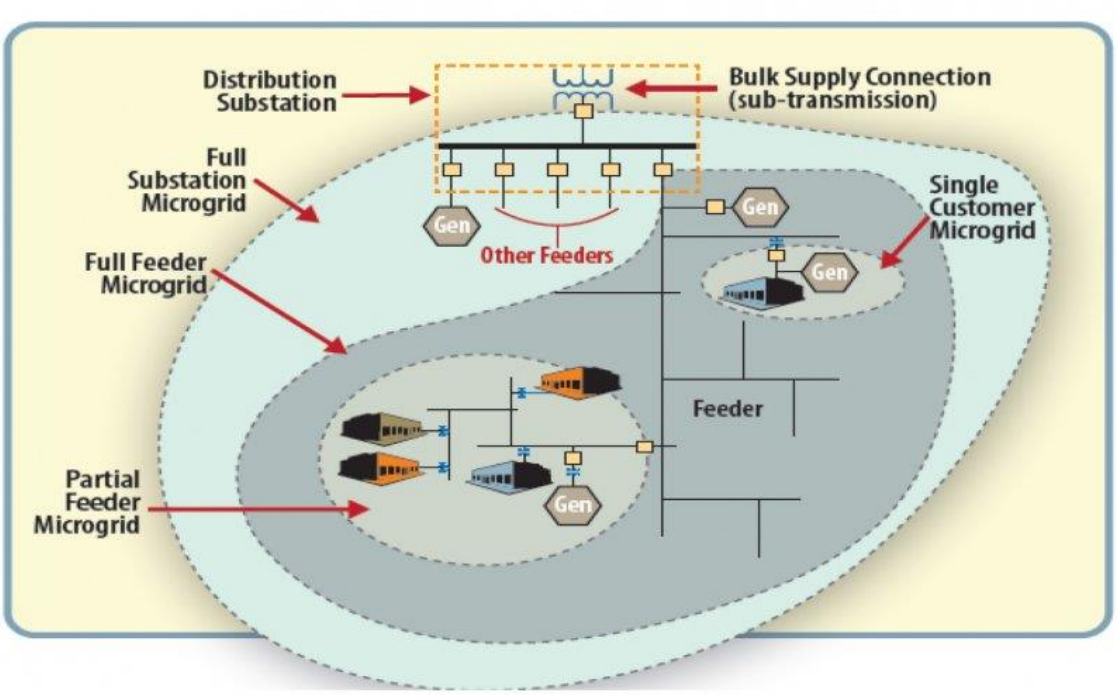

Figure 4-1 - Example of different types of Microgrids [71]

Therefore, the reason for choosing an isolated microgrid system allows for a greater reliability in terms of supplying power to the consumer. Since it has its own resources, it should be a much better option when we consider electric vehicles as well in the integrated system as well. The integration of electric vehicles using the vehicle to grid operation supports the microgrid when in isolated mode as the batteries of the EVs can help maintain power demand. This vehicle to grid can be crucial at times when renewable resources are not able to meet the demand of the microgrid in isolated mode. Therefore, considering the isolated microgrid system for test system is justified to study the impacts it has due the cyber-physical attacks on the charging stations. Additionally, with the concept of distributed generation gaining more traction within the new smart grids, it makes it a better option for the simulated test environment and whether or not it will stand up to the impacts of the cyber-physical attacks.

4.3 Description of the Cyber-Physical Attacks

In general, a DoS attack means that an intruder prevents the user to accessing a service and device. According to [72], the "Denial of Service" or "DoS" describes the class of cyber-physical attacks designed to render a service inaccessible. In addition, DoS events can cause physical damage by overloading the system and the intruder may deny you service in various ways. One of the various ways is when the intruder can cause destruction of physical equipment which is described when a cyber-physical attack causes physical damage through the digital means. Furthermore, in [73], the authors describe the DoS attack as the intruder blocking an entity to accessing a given service such as the charging of EVs. The explanation includes that the intruder can flood the network resulting in obstructing the communication channels and blocking the control signal from ever reaching the charging to stations to charge the EVs. Overall, as stated in [74], the threats and mitigation of cyber-physical attacks in the power grid is very crucial for EV charging.

Therefore, from the literature review [59-65] and description of the cyber-physical attack [72-74], in this thesis the definition of "Denial of Service" or "DoS" will refer to the inability to charge the EV due to the Cyber-Physical Attack on the HP-FCS.

4.4 Cyber-Physical Attacks through the OCPP

From [51, 69], the OCPP protocol and how it can be implemented by all different operations and features available to maintain and monitor the charging stations have been explained in the previous sections. Along with all the positives of the communication protocol it has some vulnerabilities as well when considering cybersecurity within the smart grid. The vulnerabilities lie within the minimum status duration setting between the Charge Point and the Central System. As explained previously, the "Boot Notification" is

the most basic operation that occurs each time a vehicle is connected to charge point. Each time the vehicle is connected, the central system will either send an accepted or pending or rejected response to charge point. Once the transaction starts then the Heartbeat operation keeping updating the central system in a set duration interval as stated in the protocol. Since this operation occurs multiple times during the status of the charging it becomes quite important to help monitor the state of the charge point. Along with Status Notification operation it will keep the central system apprised of any notifications or error that occur during the operation time.

Keeping this in mind, the vulnerability of the minimum status duration setting time between the Charge Point and Central System is crucial. Since the manufacturer always prefer to keep the setting lower as it reduces the interactions between the Charge Point and the Central System but this opens up for a time where the key notifications maybe left out. Therefore, limiting the number of transitions between them leaves it open for the intruder to place a cyberattack where the information between charge point and central system can be altered. Using this gap in communication the intruder can do some real harm to the system as well the EVs connected to them too. This type of cyber-attack is called the Denial-of-Service (DoS), which manipulates the flow of information that occurs through the communication protocol of OCPP between the EVs and the system.

Finally, the impact assessment of DoS cyber-physical attack will be shown in the results chapter of this work. Since SteVe is the open based platform, it opens up it to wide based on intrusions since it may be not secure enough to companies unless they add their own security policies in place. According to major companies who are in the electric charging infrastructure as mentioned in [75-81], the use of the Charge Points is done

through smartphones via web browser or an app. This implies that if the consumer using the smartphone can easily access the network of the Charge Point via their secure connection. If the smartphone is infected or the app then with the connection between the device and the Charge Points is the main input to where the intruder can gain access without directly targeting the Charge Point or the electric vehicle charging station or the company. On the other hand, the intruder can gain physical access to the Charge Point and physically tamper with the HP-FCS by inputting malicious code on the Charge Point directly. With the help of the malicious code inputted into the Charge Point can allow the intruder to gain access to communication signals between the Charge Point and the Central System.

Therefore, this is a crucial choke point that allows an intruder to execute a DoS attack and affecting the charging of the EV, the infrastructure or much more simply by altering information between the Charge Points and the Central System. In the next section this crucial point will be associated to the how exactly the EVs, electric charging infrastructure, and the smart grid will be affected and how this cyberattack can result is more impacts than one can predict. Additionally, the future sections will highlight the importance of mitigation techniques against the impacts of cyber-physical attacks.

4.5 Impact Assessment of Cyber-Physical Attacks

Typically, the microgrid consists of many different components. To begin, there is a connection to the infinite bus, which is represents a traditional centralized power from the utilities but, this is point where it can disconnect from the traditional grid and be self-sufficient in powering the area within. Referring to Figure 4-2, the figure shows the ON/OFF button, which essentially simulates being connected to the traditional grid.

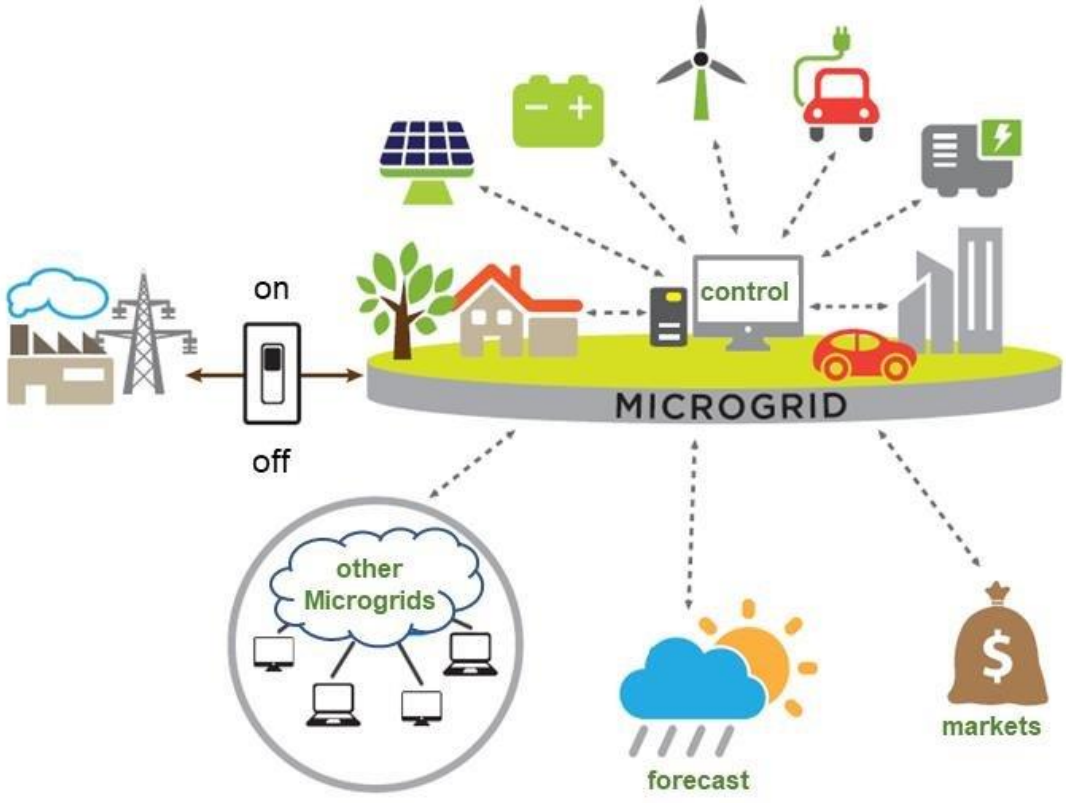

Figure 4-2 - Components of a typical Microgrid [82]

Additionally, some of the more crucial components other than the renewable and non-renewable resources are the actual components of required in the transmission and distribution of power. Upon generation of power, the component that allows the power transmission at higher voltages would be the transformer. This is a crucial component, which should be analyzed upon an impact of cyber-physical attack. Additionally, the actual voltage busses, which carry the power physically from the generation to the load should also be analyzed during a cyber-physical attack. If either of these components fail or not operate at their optimal capacity then it would result in serious damage in cost and an inability to provide power to the consumer.

Finally, the impacts of the cyber-physical attacks on the components can lead to short-term and long-term damage for the system. These cyber-physical attacks will cause massive extremes to occur on the components of the system leading to heavy damages in cost when it comes to replacing or repairing these components.

4.5.1 Transformer Overload and the Thermal Loading

The IEEE guide on loading mineral-oil-immersed transformers [83], helps identify the risks and limitations as per the guidelines for the acceptable use for transformers at various ratings. The purpose of utilizing this guide is to understand and analyze the risks that are associated by overloading the transformer overs it rated parameters. In certain applications, loads may be in excess of the nameplate ratings and this may involve a certain degree of risk when utilizing the component like the transformer. This does not limit the side effects that may occur due to the use higher than the rated limits of the equipment. For the transformer, aging and mechanical deterioration of the winding insulation may occur overtime but it definitely changes based on additional factors that may influence these factors to cause an earlier deterioration or end of life scenario. In reference to the IEEE guide mentioned earlier, section 4 outlines the many different risk factors that are associated to change the normal operation of the transformer and change the normal life expectancy of the equipment when under duress of additional stress factors.

4.5.1.1 Thermal Characteristics & Overload of the Transformer

According to the IEEE guide for transformer insulation life in [83], the life of the transformer can be calculated using aging equations and the hottest-spot temperature of the transformer. As a note, the “life” of the transformer is in reference to the insulation life of the transformer and not the actual life of the transformer. The aging acceleration factor of

the transformer (F_{AA}) is first calculated to obtain the per unit transformation insulation life as seen in equation 4-1. In addition, Θ_H in equation 4-1 refers to the winding hottest-spot temperature in degrees Celsius.

$$F_{AA} = e^{\left[\frac{15000}{383} - \frac{15000}{\Theta_H + 273}\right]} \quad (4\text{-}1)$$

Subsequently, the equivalent aging factor (F_{EQA}) of the transformer for a total time period or a 24-hour cycle is calculated as in equation 4-2. Also, in equation 4-2, Δt_n refers to the time interval in hours for the given time frame to calculate the equivalent aging factor.

$$F_{EQA} = \frac{\sum_{n=1}^{N} F_{AA,n} \Delta t_n}{\Delta t_n} \quad (4\text{-}2)$$

Finally, with the equivalent again factor and the normal insulation life the loss of life of the transformer can be calculated as per equation 4-3.

$$\%Loss\ of\ Life = \frac{F_{EQA} \times t \times 100}{Normal\ Insulation\ Life} \quad (4\text{-}3)$$

Furthermore, the normal insulation life of the transformer according to [83] is 180,000 hours at the operation of 110 ℃ at a loss of life of 0.0133%. These equations calculate a quantitative value on the loss of life for a transformer, but it does not reflect when the transformers may be overloaded to an extreme for a very short period of time. Additionally, the average ambient temperature in Canada according to [84] during the summer can assumed to be 25 ℃. Depending on the location in North America, the maximum temperature encountered during the summer time is much higher than 25 ℃. These additional factors help analyzing both qualitatively and quantitatively the effects of overload that occurs on the transformer. Also, the effects of the transformer overload also

depend on the Theta *H* temperature, as the aging factor depends solely on it. Therefore, investigating the Theta *H* curve may prove useful when analyzing the transformer overload.

4.5.1.2 Transformer Theta H Curve

Since the transformer overload depends on the Theta *H* temperature, it is thus another factor that should be calculated to get the most accurate impact on the transformer. Referring back to equation 4-1, where Θ_H was the winding hottest spot temperature in ℃, then the Theta H can be calculated by the following equations below.

$$\Theta_H = \Theta_A + \Delta\Theta_{To} + \Delta\Theta_H \tag{4-4}$$

$$\Theta_{To} = \Theta_A + \Delta\Theta_{To} \tag{4-5}$$

For the equations 4-4 & 4-5, Θ_H is the hottest spot temperature in ℃, Θ_A is the average ambient temperature in ℃, $\Delta\Theta_{To}$ is the top-oil rise over ambient temperature in ℃, $\Delta\Theta_H$ is the winding hottest-spot temperature in ℃, and Θ_{To} is the top-oil temperature in ℃. These equations along with the thermal parameters of the transformer can calculate the Theta H. The value of Theta H is calculated for each hour within the time interval of a given load profile. Therefore, the temperature Theta H should result in a Theta H curve, which shows the progress of temperature over time for that given time interval. For example, for a 24-hour time period cycle, there would be 24 calculated values of Theta H to show the change in temperature over time for the transformer. Additionally, a higher resolution time interval may be chosen if the overload is occurring for a period, which may be less than an hour as it may not be seen accurately on the one-hour interval. Finally, since the both the Theta H curve and transformer overload are intertwined then, they must be analyzed together to see the overall impact on the transformer.

4.5.2 Undervoltage

The definition of undervoltage according to Gonen [85], it is simply defined as a voltage value, which is 10% below the nominal voltage value for a period of time greater than 1 minute. To simply put it if the customers are experiencing a voltage value. which is lower than the nominal value then it can be classified as an undervoltage depending on the duration it occurs. For the purpose of the research, the work in this thesis use the American National Standard for Electric Power Systems and Equipment – Voltage Ratings (60 Hz) or ANSI C84.1-2020 [86], to classify what is undervoltage along with its quantitative values for the voltage values. From the standard, there are two types of voltages, first is the service voltage, which is the voltage at the electric utility service and the second is the utilization voltage, which is the voltage at the end user load. The focus of this work will be on the service voltage, which is occurring at the distribution level and how that can experience an undervoltage. Additionally, since the service voltage is responsible for the maintaining the voltage levels at the distribution side, it is having much stricter limits than the utilization voltage level at the consumer end.

As per the standard, the service voltage is broken up in to two ranges of voltages, where Range A focuses on normally expected voltage tolerance while Range B focuses on the limited but infrequency voltage tolerances. The service voltage for Range A shows the normal expected voltage tolerance that a utility has for a given voltage bus and the variations outside this tolerance should be very infrequent. The expected service voltage variation allows for the service voltage to be +5% or -5% of the system operating voltage level of 600V or below and for systems operating at above 600V has +5% to -2.5% tolerance limit. While for Range B, the voltage tolerances are occurring above and below

the limits of Range A and therefore, in practical and operating conditions these conditions should be limited and infrequent when occurring in duration on a voltage class. The expected service voltage tolerances for variation allowed under Range B is +5.8% to -8.3% of the systems operating at 600V and below and +5.8% to -5% for systems operating at above 600V. An example of the service voltage and utilization voltage shown with the two types of Range A and B can be seen in Figure 4-3 for a base system voltage of 120V. The figure shows the shaded portions of the ranges do not apply to the circuits supplying the lighting loads and not for 120-600V systems as well. The focus will be for the service voltage at 120-600V Systems, which is seen by the middle bar for both Range A and Range B categories as per the standard.

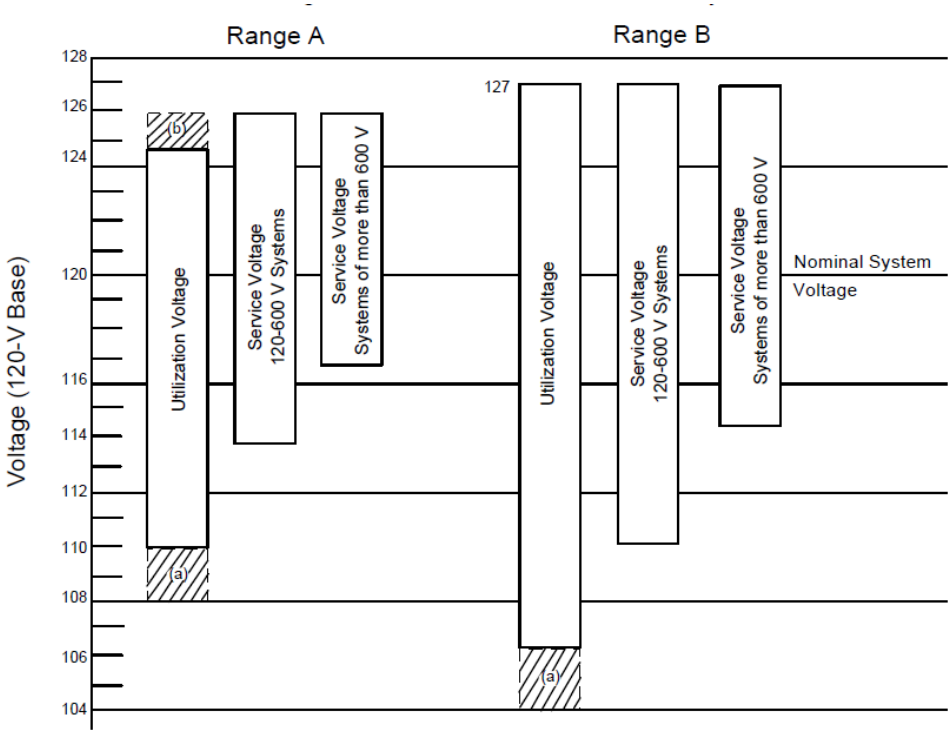

Figure 4-3 - Voltage Ranges as per ANSI C84.1 [87]

For a 600V system, the Range A service voltage tolerance would 570V as the lower limit to 630V as the higher limit and the Range B service voltage tolerance would be 550.2V as the lower limit and 634.8V as the higher limit. For the purposes of the undervoltage phenomenon, the lower limits of the voltage for both Range A and Range B will be considered and nearly a 50V difference than the rated 600V for Range B may be observed. This is the reason why Range B should only be occurring very infrequent and limited in duration and operation as it deviates a lot from the rated voltage value.

4.6 Microgrid System Modelling in SIMSCAPE

For a generic microgrid system, multiple quantities need to be measured from the simulation to get an accurate observation and analyze what is occurring in the system. To begin, the most basic measurements that needs to be measured using scopes in the Simulink simulation environment are the voltages and current on each of the buses in the system. Additionally, the voltage and current values needs to be measured before and after transformers, i.e., the primary and secondary sides of the transformer respectively. Depending on the simulation characteristics and scope's features power may be calculated within the same block or an additional calculation will be performed prior to the inspection of the results.

For the microgrid system as seen in Figure 4-4, it can see that the transformer that needs to observed requires quantities measured on the primary side (bus 2) and secondary side (bus 3). The primary side of the transformer is at 25kV and the secondary side is at 600V. Additionally, the V2G is also connected on the secondary side of the transformer at 600V, which consists of a maximum power demand or supply (based on direction of power flow) is 4 MW. The 4 MW consists of 100 vehicles each located at 40 kW electric chargers

giving a total power consumption of 4MW if all vehicles are charging at the same time. For the generic system the number of vehicles is set at 100 therefore the maximum power supplied or provided by the V2G will be limited to 4MW. All of the quantities that are observed above are solely done through Simulink and the use of scopes, voltage, current, & power measurement blocks. Therefore, in terms of system equations the utilization of basic electrical power equations is used to verify the results of the measurements blocks utilized within Simulink.

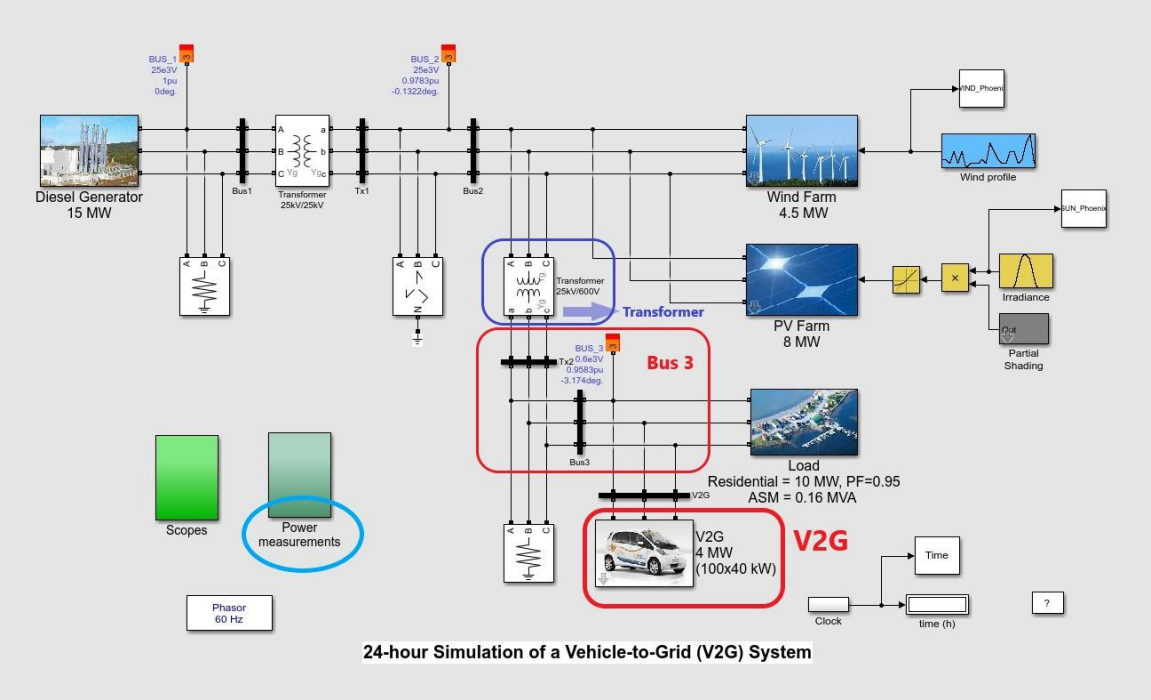

Figure 4-4 - Sample Microgrid System Identified Points of Measurements

Starting with the voltage calculations, the scopes are used to verify the primary voltage of the transformer to be at 25kV at bus 2 and the secondary voltage to be at 600V at bus 3. Then, with the power calculations, the voltage and current values at the transformer in three phase and with the utilization of the 3-phasor power block in Simulink are used to compute the real and reactive power of the transformer.

$$S = V \times I^{*} \quad (4\text{-}6)$$

$$S = P + jQ \quad (4\text{-}7)$$

This was verified using equation 4-6 where the voltage and the conjugate of the current measurement are used to compute the complex power (S) in units of Volt-Ampere (VA). Upon computing the complex power in VA, equation 4-7 is used to compute the real (P) and imaginary/reactive power (Q) by simply taking the rectangular form of the complex power and assigning the real component vector as the real power (P) in Watts and the imaginary (j) component as the reactive power (Q) in VAR. The same equations can be used to compute power of the V2G on the secondary side of the transformer as well by utilizing the voltage and current measurements at the V2G in the microgrid in Figure 4-4.

Finally, the remaining calculations for the rest of microgrid will include the wind and PV solar farm. To compute these power calculations, the same type of voltage and current measurement blocks can be used along with the scope used for recoding the values. Once the voltage and current values at both the PV and the wind farm are obtained, then equations 4-6 & 4-7 can be used to compute the apparent power in VA. Additionally, the in-built measurement block at the diesel generator is used to compute the power supplied to the entire microgrid as well. The essence of these calculations is used to verify and make sure the power generated/supplied from all sources from the microgrid equals to the power consumed by the loads (residential & industrial) & the charging of the V2G specifically. Furthermore, the calculation of power at each part of the microgrid, helps in understanding the impacts of cyber-physical attacks have on microgrid and to see what limits are exceeded for the components in them microgrid.

4.7 Mitigation of Cyber-Physical Attacks

Mitigation Techniques focus on temporarily or permanently resolving any impacts from any problems occurring on the system. As part of this work, one of the objectives is to provide mitigation techniques for impacts of cyber-physical attacks on the HP-FCS. As per the analysis of the impact assessment of cyber-physical attacks and referring to Figure 4-4 one potential mitigation technique can be related to the charging times of the EVs. As showed in sample microgrid, the V2G block consists of 100 EVs which will be charging at their respective times set by their profiles. Therefore, the mitigation technique can be suggested to change the charging times of the EVs to not overwhelm the microgrid with a peak power demand.

Additionally, as per the Figure 4-4 the V2G block also resembles the rated power of the charging stations to be 40kW as specified in [88] and the rated capacity of the typical EV vehicle battery or size to be 85 kWh as specified in [89]. Therefore, with a 40kW charger with a battery size of 85 kWh it takes 2.125hrs or 127.5 minutes to get a full charge assuming the battery is drained completely. This introduces another potential mitigation technique related to the rated power of the EV chargers. Since the V2G block is able to set the rated power of the chargers and the profiles for the EVs then changing the rated power of the chargers will reduce the power demand significantly.

Overall, the mitigation techniques can be utilized individually or together to reduce the impacts of the cyber-physical attacks. In the next chapter, a detail description on how the mitigation techniques will be utilized with what parameters will be explained based on the results of the impact assessment of cyber-physical attacks.

Chapter 5 Results & Discussion

5.1 Introduction

The purpose of this chapter is to analyze and present the results of the impacts of the cyber-attacks on the simulated microgrid vehicle to grid system. There are variety of impacts that occur when a cyber-attack is encountered on the system. The impacts can be physical or digital and the damages it creates can be short term or long term and may affect many parts of the microgrid. In this chapter the focus will be to study the impacts of the cyber-attacks on the transformer of the system. The transformer is a key element of any electrical substation and plays a very important role in delivering power from the generation to the distribution or transmit power from a higher voltage level to a lower distribution voltage level. Therefore, they are typically very important in terms of the smart grid but also, very important in a cost perspective as they are typically the most expensive equipment on the station overall.

5.2 Test System Description

For the analysis of the cyber-physical attack a test system has been developed, which will be used to simulate and test many different scenarios that can occur because of an electric vehicle and fast charging stations impacting the smart grid. The simulated test system consists of many different components required to make a microgrid. The system is designed to be a self-operating micro grid (isolated microgrid), which has no connection to the main grid or infinite bus as it is typically referred to in a power flow diagram. The key components of the system are a diesel generator, wind farm, PV farm, residential load, Vehicle-to-Grid (V2G), transformers, and the scopes & power measurement blocks as seen in Figure 5-1 below.

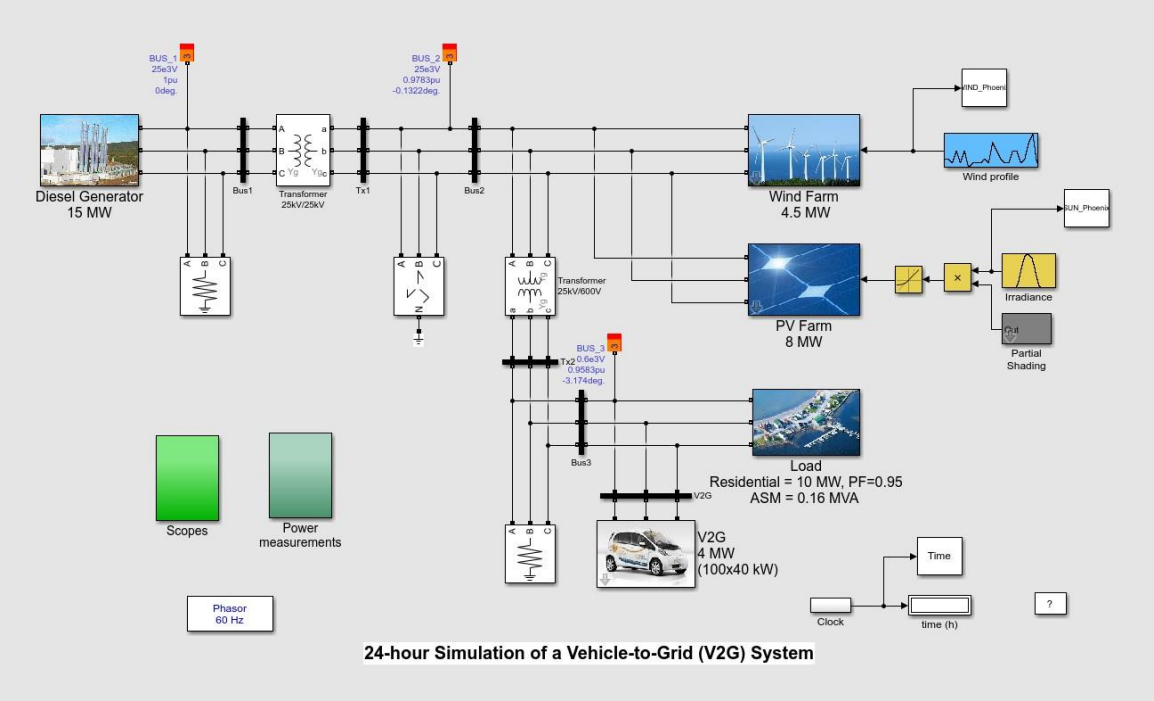

Figure 5-1 - Test System [88]

The system begins with a very key and important part of the micro grid, which is the diesel generator. This diesel generator acts as an infinite bus for the simulated micro grid when there is not enough renewable energy to supply all the loads in the grid. The diesel generator has a capacity of 15 MW, which is more than enough to supply all the loads in case of loss of renewable energy. The next two components are the wind farm and PV farm. The wind farm is modeled as a renewable resource that follows the wind profile of a typical day from whichever city is being used for the simulations. The wind farm can supply a maximum of 4.5 MW of power to the micro grid assuming max speed of the wind turbines according to the wind profiles. An example wind profile [90] for a city is shown in Figure 5-2 below. For safety reasons the wind turbines have a cut off speed at 15 m/s because in reality if the wind turbines are over speeding due to high winds, then they are kicked off the wind farm as it affects the frequency of the power inputted into the grid. If at any time

the wind turbine exceeds the max speed limit then automatically the wind farm is kicked off the grid which is simulated by showing the wind profile of 0 m/s to show the respective wind farm is contributing no power to the system.

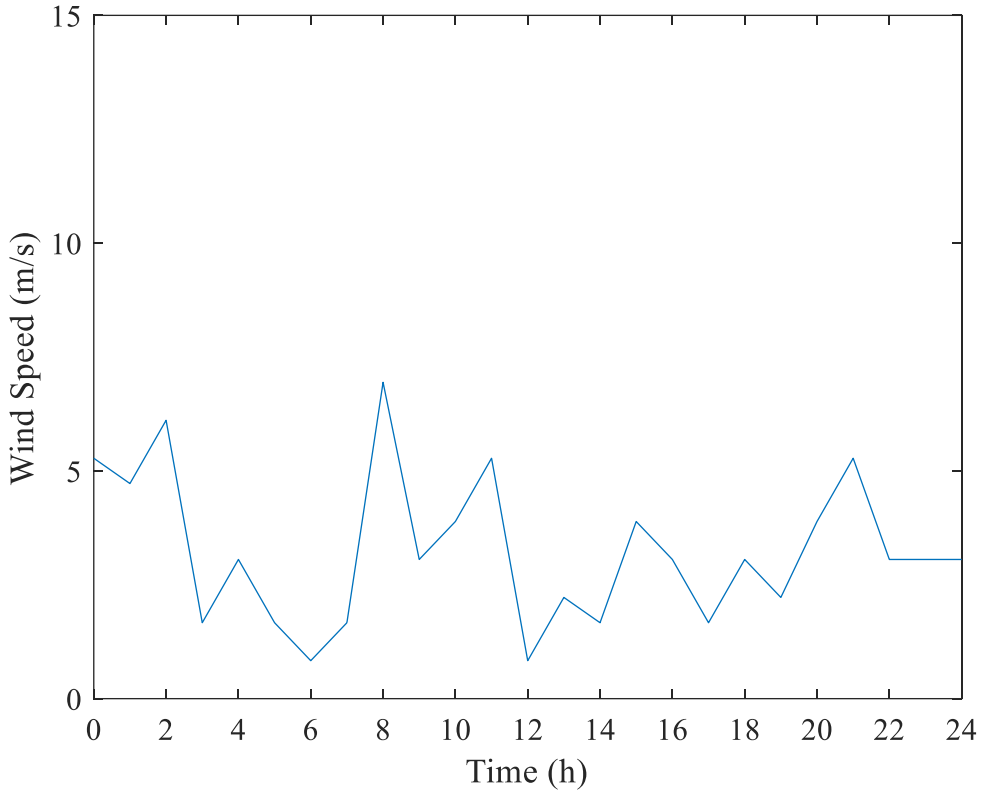

Figure 5-2 - Example Wind Profile

The PV farm generates power in forms of solar energy, which is harvested via solar panels in forms of solar farms. The solar farm also has a solar irradiance profile that it follows, which is based on data of that given city on that given day. The general irradiance profile suggests the highest amount of sunshine occurs during mid-day and therefore it results in providing the most amount of power at that given time. An example irradiance profile [91] can be seen in the Figure 5-3 below, which shows when the most of the solar power is generated. There is also a maximum capacity the solar farms can provide at a

given time is 8 MW to the system. Therefore, overall, the renewable resources can provide a maximum of 12.5 MW at a given time if both resources are at their maximum capacity for the micro grid.

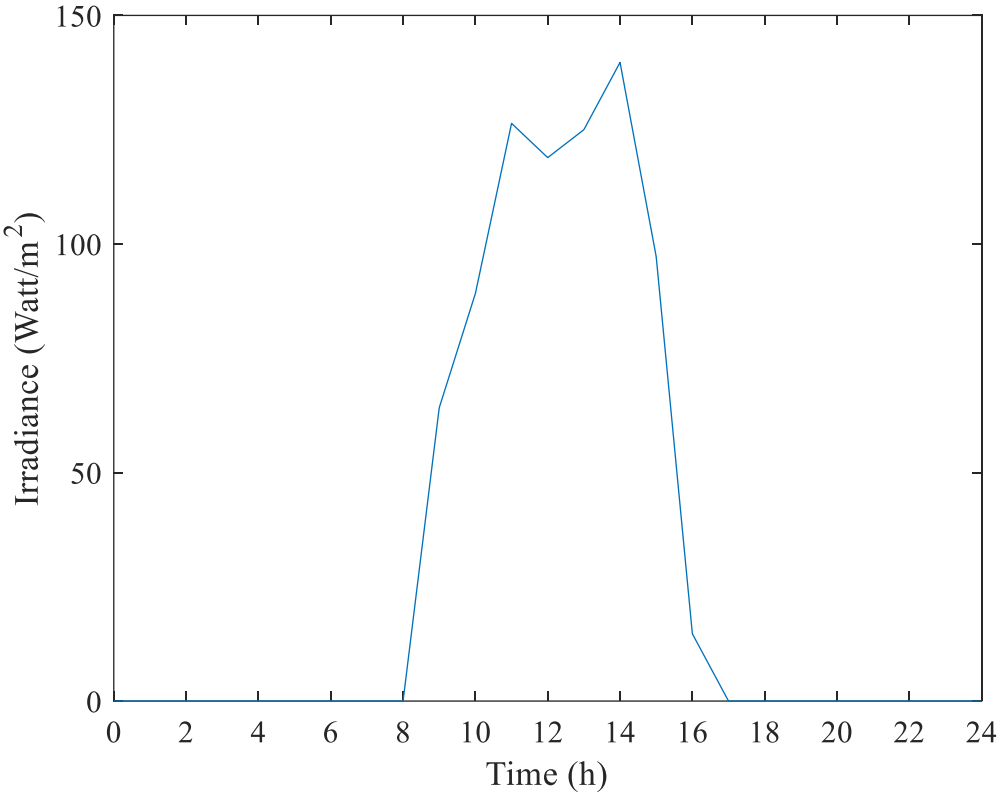

Figure 5-3 - Example Irradiance Profile

Additionally, the next components on the system are the residential load and the V2G system. The residential load follows load consumption profile, which is based on when people are home and the power demand by a typical home in a 24-hour period. The residential load is modelled to be a maximum of 10MW with a power factor of 0.95 and based on a typical home the maximum consumption that occurs during the evening time between 16 to 18 hours of the home when most people are home and most appliances are being used. The V2G is modelled on the same bus as the residential load indicating that the

electric vehicles are being charged at the customer's home. The V2G has an interesting mode, which basically allows the EVs to consume power to charge the batteries but also allows the vehicles that are connected for charging to provide regulation of the micro grid in case of any disturbances. For the purpose of the analysis the V2G mode will be kept on to help regulate any faults or disturbances that may occur but will not affect the outcome of the cyberattacks. Furthermore, the V2G is designed originally to take a default of 100 vehicles, which can be further increased to see the effect later on. Also, the charger information of the V2G is as follows: the rated power of the chargers is at 40kW with a rated capacity of 85kWh and an overall system efficiency of 90%. Another important idea of the V2G is the way the vehicles are separated into 5 different vehicle driving profiles. Since everyone does not drive the vehicle the same way or follow the same route or drive the same distances therefore these vehicle profiles will help determining the number of vehicles and how to split them into the different vehicle profiles. The vehicle profiles are as follows:

- **Vehicle Profile #1**: People going to work with a possibility to charge their vehicle at work
- **Vehicle Profile #2**: People going to work with no possibility to charge their vehicle at work
- **Vehicle Profile #3**: People going to work with a possibility to charge their vehicle at work but with a longer ride
- **Vehicle Profile #4**: People staying at home
- **Vehicle Profile #5**: People working on a night shift

Finally, the components are the buses, transformers, and the monitoring scopes that are used to connect the entire microgrid and monitor all the data flowing in and out of the system. There are three buses that are modelled where the bus 1 is at rated at 25 kV, which connects the diesel generator to the transformer 1, where transformer 1 simply maintains the voltage from the primary side to the secondary side at 25kV. Then, bus 2 is from the transformer 1 to the wind and PV farms that were connected by transformer 2, which drops the voltage from 25kV on its primary side to 600V on its secondary side. At the end is bus 3, which is connected from the secondary side of the transformer 2 to the residential load and the V2G system. The measurement and monitoring scopes are placed on each bus, which measures the voltage and current of each of the three buses. Then, monitoring tools also measure the power of each transformer and measure the voltage and current on both the primary and secondary sides of both transformers. Finally, the measurement tools measure the power generation of the renewable and non-renewable resources, and power consumption of all the loads in the system.

5.3 Test System Scenarios and its parameters

The test system consists of many different types of scenarios with different EV State of Charge (SOC), rated power, cyber-physical attacks, and no attacks as well. The goal of the test system was to try to look at many different aspects of the microgrid system and test whether or not different control parameters makes a difference when there is not an attack versus when there is a cyber-physical attack.

To begin, lets define what is a scenario with no attack. A system with no attack refers to ideal conditions on the microgrid system, where the consumers drive their EVs have normal operation and charging both at work and at home. The components of the microgrid

system respond in normal conditions like voltage of bus is controlled within a nominal range, the power of the transformer does not exceed its max rated capacity, and the diesel generator supplies power to the system within its rated parameters. Therefore, in a no attack scenario all operations are normal within specified parameters and no influence is occurring to modify or change any existing parameters on the system.

Now let's define a system, which is experiencing a cyber-physical attack. This is a system where the microgrid system is not acting under normal parameters and it is causing inconvenience to the consumers as they may or may not be able to charge their EVs. During an attack scenario the consumer who is traveling to work either from a short or long-distance commute may experience a denial of charging at their work place forcing them to charge when they get home. This may affect the consumers EVs battery life as it may result in dangerously not enough power to reach back home if having a longer commute. This sort of attack may occur when targeting only one group of EVs or two groups or all of the EVs that are modelling in the microgrid system. These different groups are referring to the vehicle profiles that are created to break up the EVs down. Additionally, when referring to an attack scenario, there may be other problems that may be occurring with the components of the microgrid system. The overloading of the transformer may occur as more power is demanded for a much higher time as EVs are much more depleted then in the normal scenario. There may be undervoltage that can occur as well from the high demand of charging when the EVs return back home from an unsuccessful charging session at work. Therefore, we can see multiple differences when we compare an attack scenario versus a no attack scenario. Below are the different types of attacks that were implemented on the test system.

- **Attack #1** – This attack will target the vehicles in profile 1, which is all the people going to work with a possibility to charge at work.
- **Attack #2** – This attack will target the vehicles in profile 3, which is all the people going to work with a possibility to charge at work with a longer ride
- **Attack #3** – This attack will target the vehicles in profile 1, 2, and 3, which is all the people going to work with or without a possibility to charge at work with a shorter and longer duration of the commute respectively

The impact of these three types of attacks was investigated by using different parameters to modify the test system. These parameters include what occurs if comparing the EV's SOC level when the vehicle reaches the workplace or back at home, the rated power used on the EV chargers, and increasing the penetration of EVs in the system. These parameters may very well affect the impact of the cyber-attacks on the system either for the better or worse.

The EV's SOC level is the battery percentage of the vehicle's battery that is remaining after the driver has driven the vehicle. The SOC when the vehicle arrives at work will be dependent on the length of the commute either a short commute vs a longer commute. The test system will also show what occurs if the driver chooses to have a longer commute and arrives the workplace with a more depleted battery and has to drive back home as they are unable to charge their vehicle work. Additionally, a similar impact will also be seen in the shorter commute as well where the driver is driving to the workplace and unable to charge at work and has to return home on the remaining SOC of the EV. Both are impactful cases but the longer commute driver is the one worried as they may be reaching home with only with about 10% SOC.

The rated power of the EV chargers is also a very important concept of the test system as it will determine how much power needs to be supplied to charge the EVs at a given time. The default rated power that will be used in the V2G model of the EVs is 40kW which allows the user to charge their vehicle much faster. Additional rated power of the EV chargers will also be investigated to see what is the impact of those on the test system.

Lastly, the penetration levels of the EVs will be investigated in the system by keeping the default number of vehicles at 100. If each vehicle was charging at a given time using the default charging rate at 40kW then there would be a max of 4MW power required to charge all the 100 vehicles at once. Additionally, to see the impact of the penetration levels of EVs in the test system with the cyber-physical attacks, the penetration level is increased from 100 vehicles to 200 vehicles with an increment of 50 vehicles at a time. This will help assessing the impact of increasing EVs on the test system as it shows an upcoming future where more and more EVs will be introduced in the households. Additionally, it will show the impact on the test system it will have enough if there is no cyber-physical attack the increasing number of vehicles should impact the system and with an attack it will go for the worse end.

5.4 Impacts of cyber-physical attacks on the components of the microgrid system

The impacts on the transformer can be seen by the characteristics of the transformer itself in terms of voltage, current, and power. Firstly, the significant impact on the transformer would be the overload it may experience. This occurs when the supplied power exceeds the rated power of the transformer. Secondly, the next impact can be seen as the aftermath of the overload of the transformer, which is the temperature of the oil in the transformer. This can be analyzed by the theta H curve of the oil in the transformer. Finally,

the third impact that will be discussed will be the undervoltage of the transformer. This occurs when the voltage of the transformer goes below the rated voltage limits. The consequences of such an impact are the transformer's pre-mature replacement and the power outages to the customers.

5.4.1 Transformer Overload

Firstly, the significant impact of the cyber-physical attacks can be seen by looking at the overload of the transformer of the microgrid vehicle to grid simulated system. Since the transformer is a key component, which houses the renewable (solar and wind) and non-renewable (diesel) sources at the primary side and connecting to the residential load and the V2G load on the secondary side. Any power flow that occurs will end up going through the transformer to supply the demand in terms of loads from homes or charging the EVs. When the cyber-physical attack occurs, the EVs are not allowed to charge during the morning time (depending on the attack of reference) and due to that the EVs have a lower state of charge when they come home. Therefore, this increases the time required to charge the EVs when they arrive home. The longer charging times puts a higher demand on the transformer by increasing power flow, which could cause the transformer to overload by going over its rated power level.

The simulations results will show how each cyber-attack can individually be analyzed to show the impact of that specific cyber-attack. First of all, the graph indicates a dotted red line, which shows the maximum rated power of the transformer as 1 pu, which equals to a base of 20MVA. Then, looking at the different bar of the bar graph, the figure reveals the increasing EV penetration from 100% to 200% with an increment by 50% each time. Before analyzing the attack, cases and understanding the impact of those on the

transformer overload, lets focus on the no attack case. Referring to Figure 5-4, the transformer demand for the no attack scenario is used as a reference for comparison when analyzing the impact of the attack cases. Even as the EV penetration increases from 100% to 200%, an impact on the transformer overload can be seen as it increases as well. But even at maximum EV penetration level, the transformer demand does not exceed the maximum rated capacity of 1 pu at the 18th and 19th hour when the highest demand occurs.

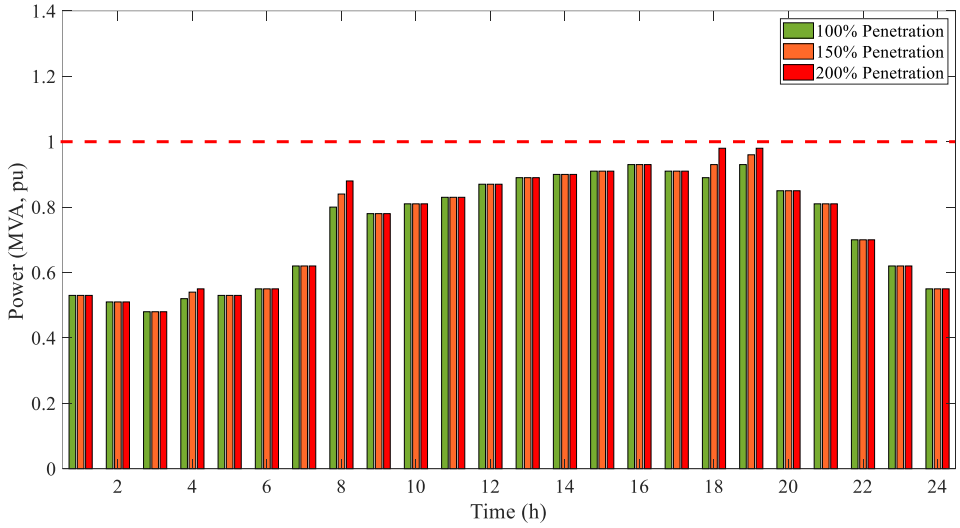

Figure 5-4 - Transformer Demand at different EV Penetration in case of no attack

On the other hand, the attack cases will show a different impact on the transformer demand profile versus the no attack case. Referring to Figure 5-5, the impact of attack 1 on the transformer profile for 24-hour period can be seen. Referring back to the previous section, attack 1 refers to when all the vehicles in profile 1 are unable to charge. These are the vehicles that travel a short distance and previously had the ability to charge the vehicle at work but due to the cyber-physical attack they were unable to charge their vehicle at work. The remaining of the profiles were able to charge the vehicle and followed the

profiles normally. The indication that other vehicles were not affected can be seen by the small changes in peaks at 8th and 9th hour where the vehicles that reached worked are getting plugged in and able to recharge their batteries prior to returning back home. The impact of the cyber-physical attack can be clearly seen during the evening time at 18hr and 19hr where the transformer overload exceeds the maximum rated power. Additionally, the impact also shows as the EV penetration increases so does the transformer overload as well. A clear comparison with the no attack scenario that results in no overload of the transformer demand profile for any of the EV penetration levels can also be seen.

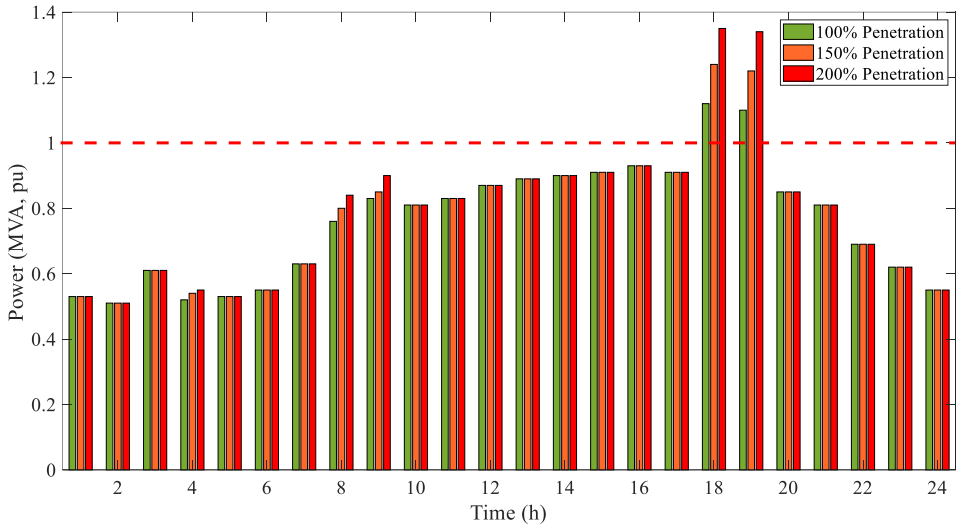

Figure 5-5 - Transformer Demand at different EV Penetration in case of attack case #1

Furthermore, the simulations result for attack 2 can be seen in Figure 5-6 respectively. For the cyber-physical attack 2, referring from the previous section, this is the attack where the vehicle that travel the longer distance are targeted. Since the simulation is broken into profiles that travel a shorter distance versus longer distance, the attack 2 targets only the vehicle traveling the longer distance. The simulation results show that for both

18th and 19th hour the transformer overload is 1.35 pu for both respectively. But comparing this to attack 1, the transformer overload was 1.35 pu for 18hr and 1.34 pu for 19hr. The difference is quite small but it helps revealing that for attack even at 20hr the longer distance vehicles were targeted so their battery was almost drained completely so hours of charging can also be seen for a whole additional hour. Compared to attack 1, there is no impact in transformer overload at 20hr as all the vehicles completely finished their charging within the 2 hours.

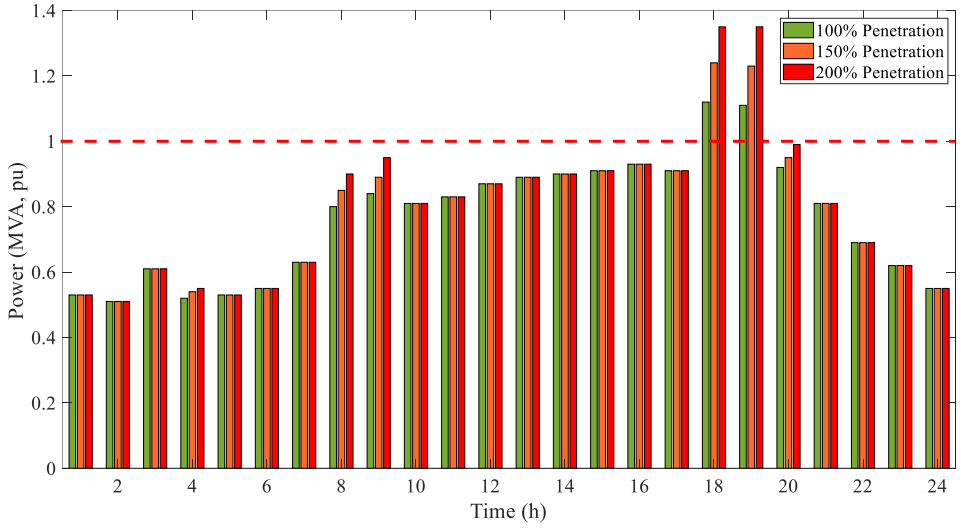

Figure 5-6 - Transformer Demand at different EV Penetration in case of attack case #2

Finally, the simulation results for attack 3 can be seen in Figure 5-7 respectively. For the cyber-physical attack 3, recall from the methodology, this is the attack that targets all the vehicles in profiles 1 to 3, which means all the shorter and longer distance vehicles are targeted. The graph shows very clearly that since the fast-charging station is under attack and none of the vehicles can charge can be clearly seen by the smooth peaks increases during the morning time. The morning time clearly shows that no charging is taking place,

which means the cyber-attack has impacted the transformer overload significantly. Therefore, all the impact can be seen between 18th to 20th hour and the peak of the overload is almost as high as attack 2 but the duration in attack 3 is longer because the amount of charging required is higher in attack 3 versus attack 2. Also, as the EV penetration increases to 200%, the peak gets very close to the rated power. It can be inferred that if the system is not upgraded or mitigation techniques are not implemented, then the future growth of system will also come under influence of transformer overload.

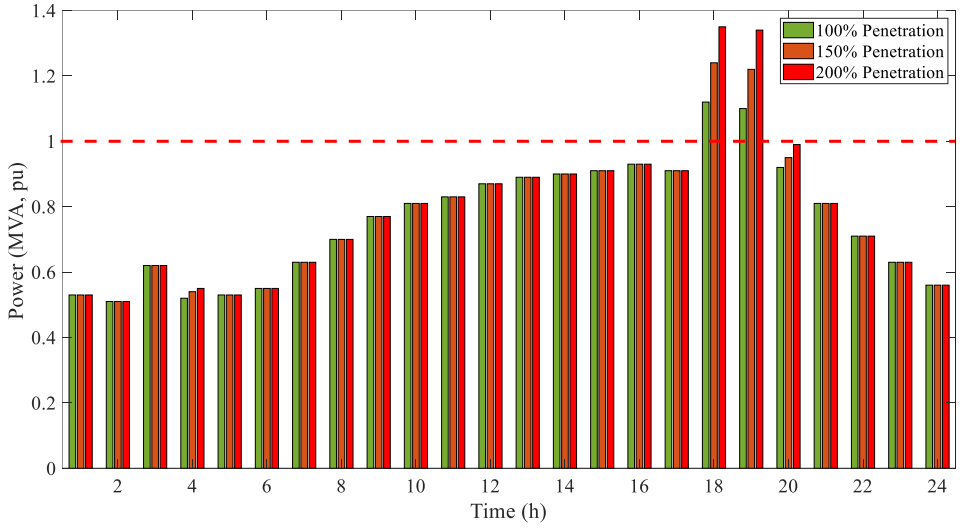

Figure 5-7 - Transformer Demand at different EV Penetration in case of attack case #3

To compare with the cyber-physical attacks, consider the worst-case scenario of each attack, which will occur at the 200% EV penetration level and plot them with respect to the Attack Type 1, 2, and 3. This can be seen in Figure 5-8 respectively, where the x-axis is shows the attack type (attack 1, attack 2, and attack 3) all at 200% EV penetration level and the difference can be seen at 8th hour versus 18th hour. At 8th hour the first two attacks have some charging going on but at 18th hour the transformer overloading occurring no

matter what type of cyber-physical attack has been implemented, can be seen. This allows to analyze that since the attacks are related, they are not drastically different from each other but still shows a consistent form of results where they affect the transformer overload from anywhere from 2 hours to 3 hours of overload duration.

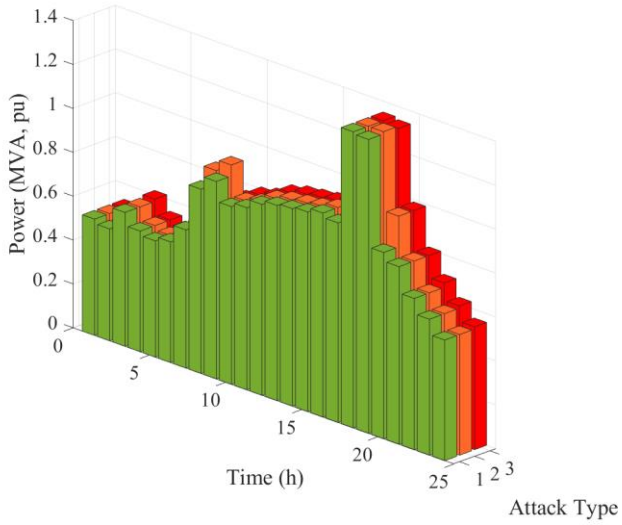

Figure 5-8 - 24-hour Transformer Demand Profile for all three attack cases at 200% penetration

To conclude, the impacts of different cyber-physical attacks on transformer overload profile along with the no attack scenario were analyzed to verify the impacts of the transformer demand profile. Referring back to the no attack scenario, it can be observed that even if the EV penetration changes from 100% to 200%, the transformer demand profile remains below the maximum rated power of the transformer. The transformer does not result in an overload thus exceeding the rated power of the transformer. This verifies that if the system is not under attack, then the transformer will operate in the specified conditions as per the electrical standards. However, in the presence of a cyber-physical

attack, the impact of the overload is quite devastating because the transformer demand is over the rated power for many hours at a given time. This will in the end affect the life of the transformer as it will cause the insulation to breakdown and result in the transformer being out of service much quicker when compared to in normal operation. Since the life of the transformer decreases, then the impact of cyber-physical attacks could be in the millions of dollars as the typical price of transformers in the market today.

5.4.2 Theta H Curve

Secondly, the next significant impact of cyber-physical attacks can be seen by looking at the temperature curve of the transformer of the microgrid vehicle to grid simulated system. The temperature curve can be referred as the Theta H (θ_H) curve of the transformer, which is the oil temperature in the transformer. The methodology chapter in this thesis provides the details on how this theta H temperature is calculated based on the thermal characteristics of the transformer. Since the transformer is a key component and all the resources and loads are on the secondary size makes them suspectable to failure if the transformer becomes overloaded therefore resulting in a higher temperature curve. The effects of this transformer theta H curve can be seen by looking at the no attack and attack scenarios to see what is the impact of them on the transformer.

The simulations results will show how each of the cyber-physical attack affects the theta H curve and will be compared to the reference case of the no attack case. The graphs will indicate a dotted red line, which shows the maximum rated thermal capacity limit of the transformer at 110 ℃. Referring to Figure 5-9, the temperature curve of the transformer for the no attack scenario is use as a reference for comparison when analyzing the impact of the attack cases. It can be seen that as the EV penetration increases from 100% to 200%

with an increment of 50% each time, the transformer temperature does not reach the maximum thermal rated capacity limit of 110 ℃. Even at the maximum power consumption at 18th and 19th hour, the theta H curve is much lower than the rated limit. This can be verified when referring back to the transformer demand profile to match that at no attack the demand also does not cross the rated maximum power of the transformer as well as the theta H temperature too. The temperature curve does follow the same pattern and the curve as the demand profile but only reaches a maximum of 100 ℃, which is 10 degrees below the rated thermal limit of the transformer. Therefore, the no attack case can be used as a reference to compare to see the impact of the cyber-physical attacks.

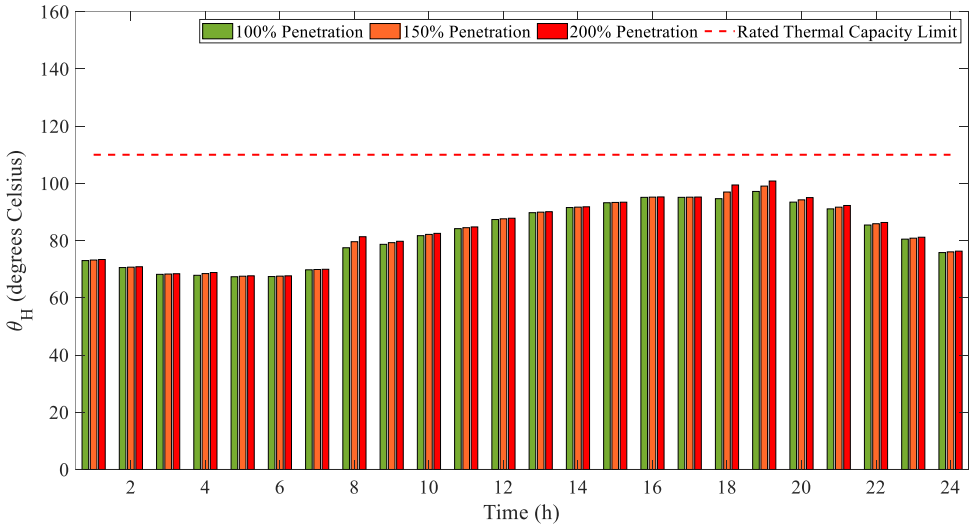

Figure 5-9 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of no attack

On the other hand, the attack cases definitely show a much different impact on the temperature curve of the transformer. To begin, referring to Figure 5-10 it can be seen that the attack case 1 of the theta H temperature curve for the 24-hour period simulation.

Recalling, that attack case 1 refers to the when all the vehicles in profile 1 are unable to charge their vehicle and they travel a short distance to work where they are unable to charge and charge when they arrive back home. From the graph, it can be seen that when the vehicles come back home, the theta H temperature curve definitely exceeds the rated thermal capacity limit of the transformer. Also, visual inspection reveals that at 100% EV penetration, the 18th hour does not exceed the rated limit, but at 19th it gets close to less than one degree to the rated limit. This reveals that even if the transformer demand profile might not exceed the rated power the transformer is getting close to the max limit thus, causing the thermal characteristics of the transformer to start breaking up by significantly increase the oil temperature for the higher EV penetration levels. When considering the no attack case as a clear comparison, the no attack scenario results never exceeded the thermal characteristics of the transformer for any of the EV penetration levels.

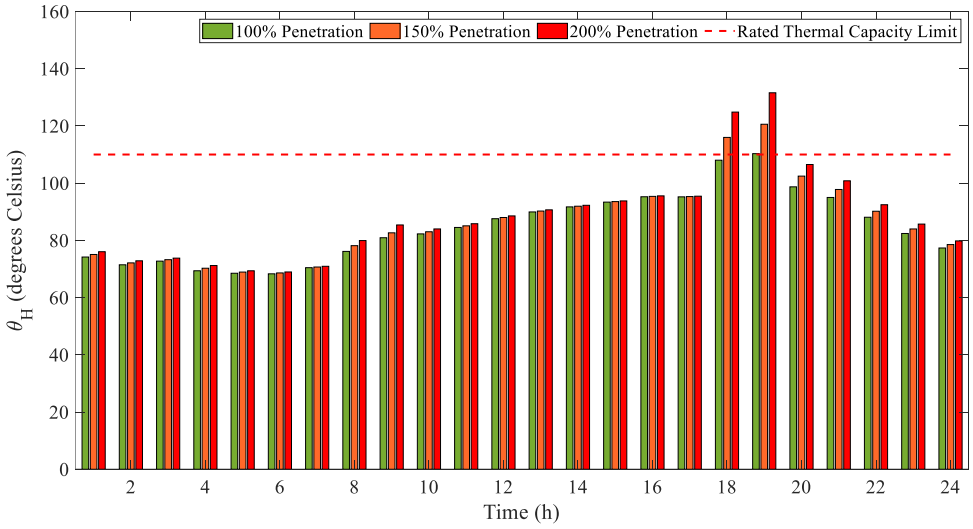

Figure 5-10 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of attack case #1

Furthermore, the simulation results for attack case 2 can be seen in Figure 5-11 below. For the cyber-physical attack case 2, let's recall that this attack targets the vehicles in profile 3, which commute a longer distance. The simulation results clearly show that the temperature theta H curve exceeds at 18th and 19th hour when the vehicles are back home to charge. Comparing to the transformer demand profile for attack case 2, it can be seen that the longer distance vehicles have their batteries more depleted therefore, they will require a much higher time to charge. Therefore, for the 200% EV penetration for the transformer demand profile it can be seen that the demand reaches the rated maximum power. Similarly, for the temperature curve, there is no violation of the thermal limit at the 20th hour but both attack case 1 and 2 are close to the rated thermal capacity limit. Comparing both attacks 1 and 2 reveals much or similarity in the theta H curve among them and clearly see a good comparison with the no attack scenario.

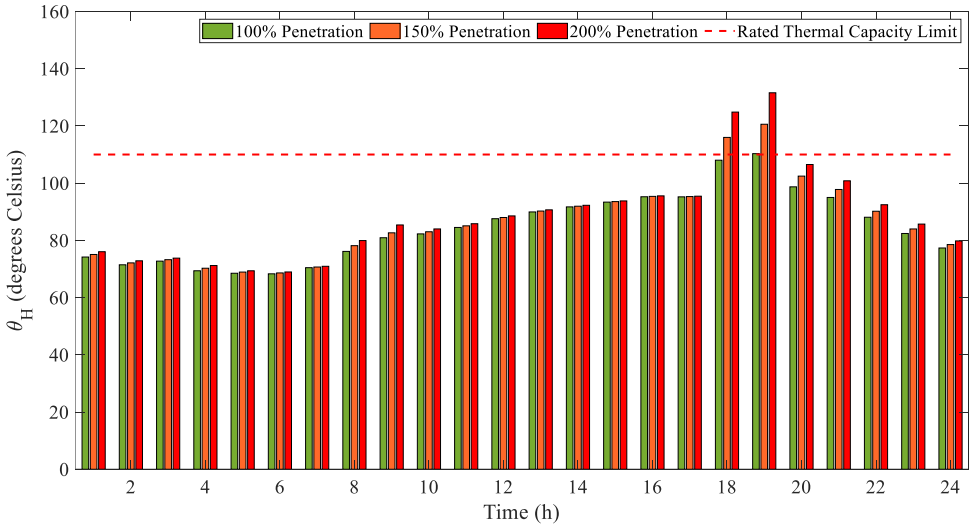

Figure 5-11 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of attack case #2

Finally, the simulation results for the attack case 3 can be seen in Figure 5-12 with the EV penetrations levels from 100% to 200%. To recall, attack 3 occurs when both the short and long-distance commute EVs are targeted therefore affecting vehicle profiles 1 and 3. The graph reveals a very similarity between the attack 1 and 2 cases as well because the temperature curve follows very closely to the same as seen in the other attacks. The reason for the temperature curve theta H to remain very similar between the three types of attacks deals with the fact that this is based on the overload of the transformer and the temperature of the oil. When the oil temperature is below the thermal rated limit, then it will require a drastic increase in the demand profile to make it exceed the thermal limit. But once it reaches the limit or cross it, then the temperature starts increasing much faster than when it under the thermal limit. This refers to the life of the transformer and the degrading of the insulation in the transformer will drastically reduce the life of the transformer. The main impact that occurs due to the high transformer demand is the loss of life which is evaluated through the theta H curve of the different attack cases.

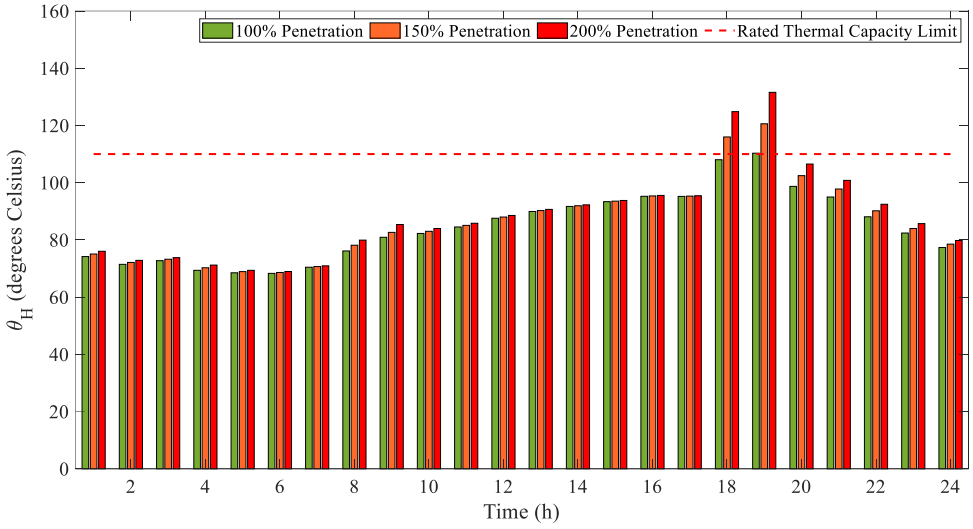

Figure 5-12 - Transformer Temperature Curve (Theta H) at different EV Penetration in case of attack case #3

Additionally, comparing the worst-case scenarios of all the attack cases can be seen when referring to the 200% EV penetration levels and plotting them with respect to the different attack types. Referring to Figure 5-13 respectively, the y-axis represents the attack type (attack 1, attack 2, and attack 3), which are all 200% EV penetration level and the difference can be seen at the 8th versus 18th hour similar to the transformer demand profile. Since impact of the theta H curve is not the same as the transformer overload and does not respond quickly, therefore it can be seen that the plots are almost the same between the three types of attack cases. The only clear difference occurs at 20th hour between the attack 1 versus the attack 2 and 3 case type as in attack 1 only the short distance vehicles are targeting leading to a shorter battery charging requirement. For both the attack 2 and 3 cases, the longer distance vehicles are targeted, which means that some portions of the vehicles will require a much longer charge due to the longer commute. This can be clearly seen at the 20th hour as the difference in the temperature curve between attacks 1, which

has a much lower temperature versus attack 2 and 3, which has a higher temperature curve. This allows to show similarity as the transformer demand profile was closer to 3 hours of overload and here the temperature curve also exceeds the limit to about 3 hours as well in the case of the longer distance EVs.

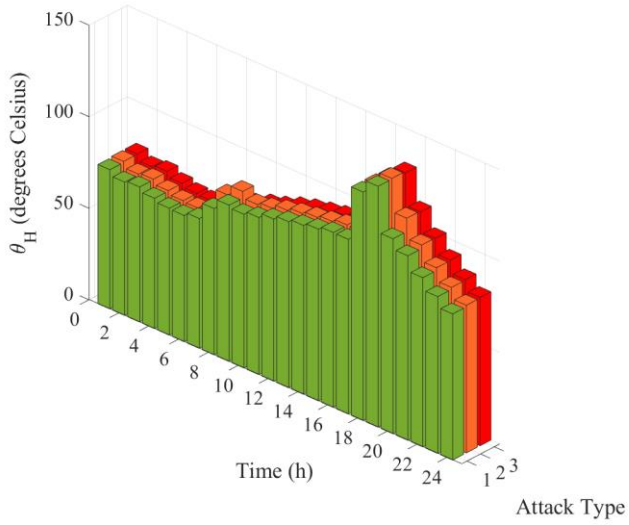

Figure 5-13- 24-hour Transformer Temperature Curve (Theta H) for all three attack cases at 200% penetration

To conclude, the impacts of the different cyber-physical attacks on the transformer temperature curve for theta H have been assessed. The work investigated the impacts on the no attack scenario versus the attack scenarios to see the impacts cyber-physical attacks had on the theta H curve of the transformer. It was concluded and verified that each of the cyber-physical attack case was compared to the no attack case to show that no impact was seen when an attack was not present. Additionally, whenever an attack was present no matter which type of attack case it may be always resulted in at least 2 hours where the theta H curved exceeded the thermal rated capacity limit of the transformer. This helps

concluding that whenever the transformer exceeds the thermal capacity it will end up affecting the life of the transformer. This occurs as the insulation inside the transformer will reach end of life quicker and will result in financial loss to replace a transformer ahead of its end of life.

5.4.3 Undervoltage

Thirdly, the last impact that will be analyzed will be the voltage of the bus, which is on the secondary side of the transformer. This is the same transformer that has been considered previously for the overload and temperature theta H. The impacts on the voltage are also harmful to the not just the transformer but other components in the microgrid as well. Most importantly it will affect the customers in the residential load who will feel the impacts of the under voltage which occurs when the voltage level is much lower than the rated voltage levels of the given bus. In the simulation results the system that was utilized has the bus designation as bus 3 and the rated voltage level of bus 3 is 600 V or 1 pu. Refer to the Figure 5-14 to reference the designation and location of bus 3 within the microgrid simulated system.

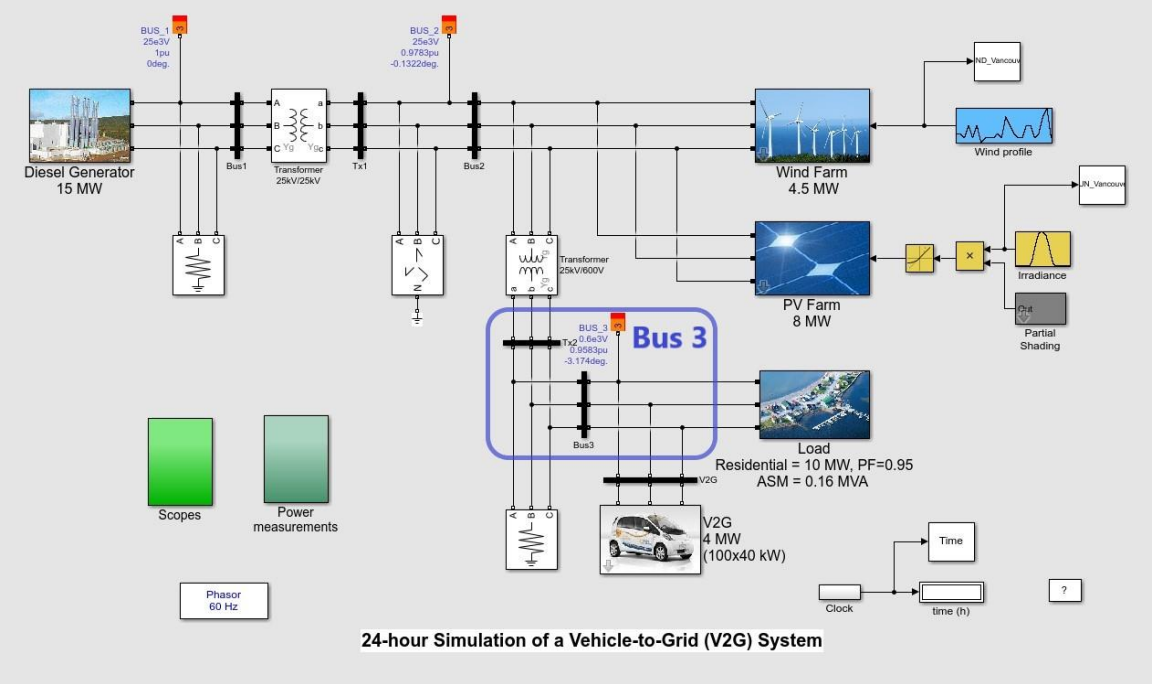

Figure 5-14 - Highlighted portion identifies Bus 3 in the microgrid system

According the American National Standards Institute (ANSI), referring to standard ANSI C84.1-2020 shows the rated service voltage levels that can be used on the user end to successfully meet the voltage requirements. Additionally, the service voltage levels are classified into Range A and Range B. Range A provides the normal voltage level fluctuations that can occur to make sure the expected service voltage is within the +5% to -5% of the rated voltage level. Range B provides the tolerances that occur when the system is not operating under normal circumstances and the voltage limits are occurring in very limited frequency and duration of the rated voltage level. The service voltage range for Range B is +5.8% to -8.3% of the rated voltage level. Therefore, since the cyber-physical attacks are a scenario that occurs on an infrequent or limited time based, the work utilize Range B to show if the operating voltage level of bus 3 experiences and undervoltage, which is lower than limits provided. Since the rated voltage level is 600V (1pu), which

translates the upper limit to 634.8V (1.058pu) or the lower limit to 550.2V (0.917pu). The results that show the undervoltage in this section will refer to a dotted red line on the graphs, which show the lower limit of the undervoltage operating voltage level as a comparison to see if the bus 3 is violating the undervoltage limits or not.

Figure 5-15 shows the voltage profile for bus 3. The no attack case shows very clearly that at no time within the 24-hour time period does the voltage go below the lower limit as set by Range B which is 0.917 pu. Using the no attack case, a comparison for the attack cases, the no attack is used to show the impacts of the undervoltage when a cyber-physical attack is present. Also, the no attack scenario also shows that even when EV penetration increases from 100% to 200% in 50% increments, at any of increments the voltage does not dip below the lower voltage limit.

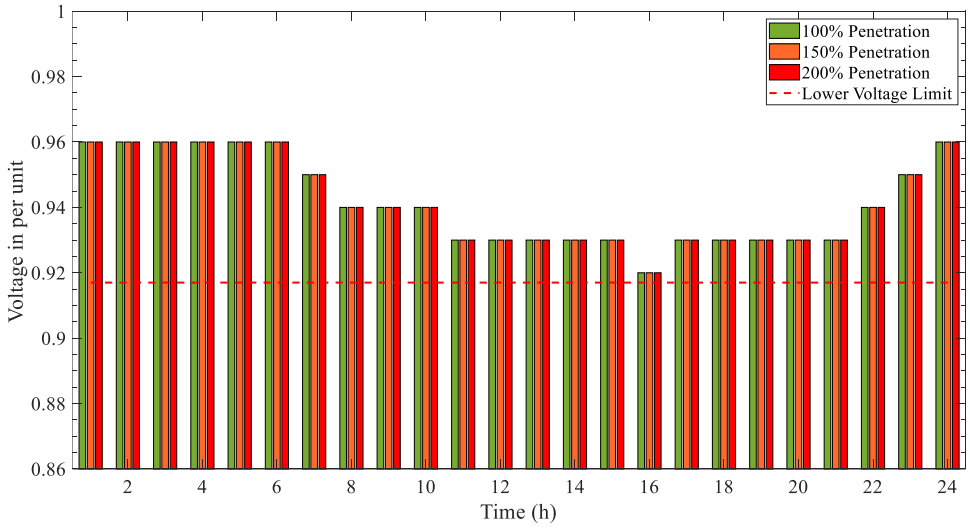

Figure 5-15 - 24-hour Voltage Profile of Bus 3 in case of no attack case

Furthermore, start with attack 1 and the simulation results of increasing EV penetration to see the effects of undervoltage of bus 3 in our microgrid simulated system. The results can be referred to Figure 5-16 below, which shows the undervoltage in per unit when attack 1 was implemented on the system. Just overall observation is that the voltage level throughout the 24-hour time period is above the lower limit of Range B, which shows that the service voltage is operating within the variations defined in Range A of the standard. As the transformer overload, the bus 3 voltage also experiences an undervoltage for 2 hours at 18hr and 19hr when the vehicles come back home to charge. This correlates with the overload confirming that when the power demand drastically increases above the rated capacity, then the voltage of the system will experience an undervoltage as seen in the results.

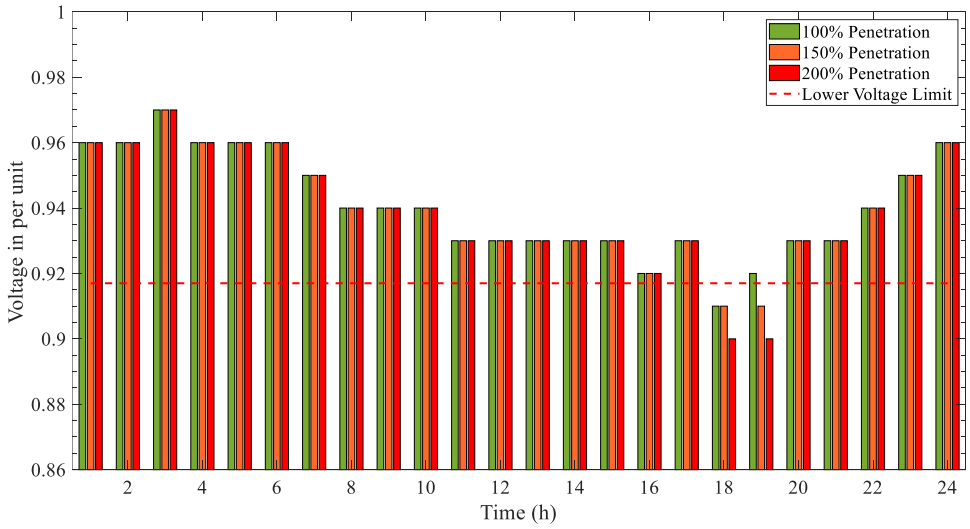

Figure 5-16 - 24-hour Voltage Profile of Bus 3 in case of attack case #1

Secondly, looking at the results of attack 2 (refer to Figure 5-17) we see a very similar pattern in undervoltage as expected to attack 1. In attack 1 at 19hr the EV penetration of 100% does not experience an undervoltage but in attack 2 when we target the longer distance vehicles, we see the power demand is much higher in attack 2 versus attack 1 therefore all the EV penetration levels will experience an undervoltage. Also, since the voltage change is not as drastic as transformer overload, we also observe that when the EV penetration increases by 50% from 100% to 150%, the voltage level does not really change. This shows us that you need a significant increase in load demand to see an effect from the voltage levels of bus 3 within the system.

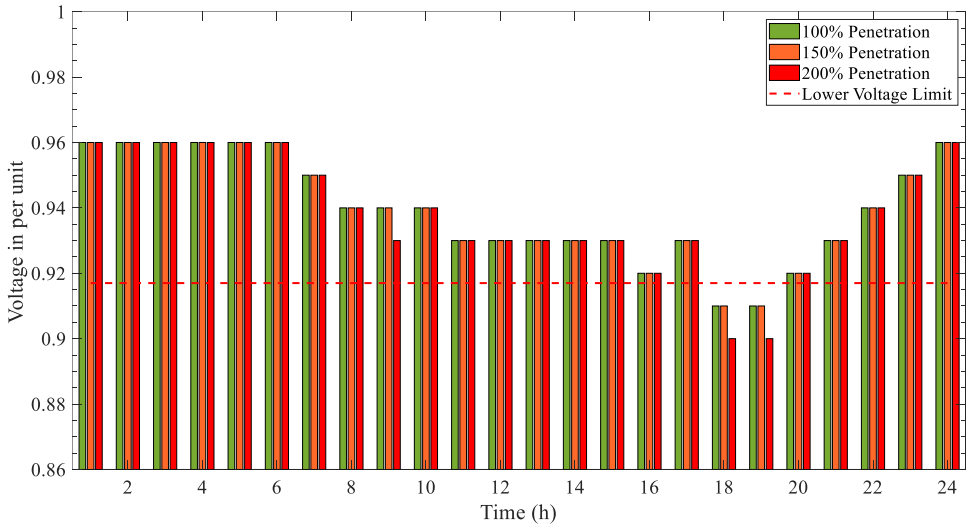

Figure 5-17 - 24-hour Voltage Profile of Bus 3 in case of attack case #2

Looking at the results for attack 3 (refer to Figure 5-18) we see three distinct voltage levels for each the 100%, 150% and 200% EV penetration levels, which was not visible in attacks 1 or 2. Either way, the results correlate with what we expected as the attack targets all the vehicles in profiles 1 to 3, the charging duration for some vehicle extend up to 3

hours. In results for attack 3 we can see 2 hours of clear undervoltage but the third hours at 20hr we see that for the 200% EV penetration the operating voltage is almost on the lower limit of the operating voltage. It is above the limit but still signifies and shows the potential impacts it can have if the cyber-attack intensity was increased or another factor may cause the third hour to also experience under voltage as well.

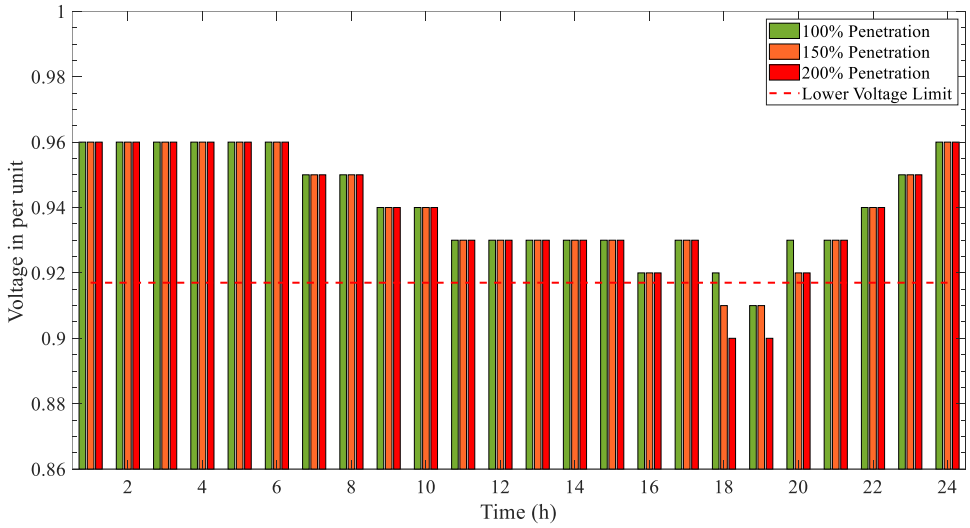

Figure 5-18 - 24-hour Voltage Profile of Bus 3 in case of attack case #3

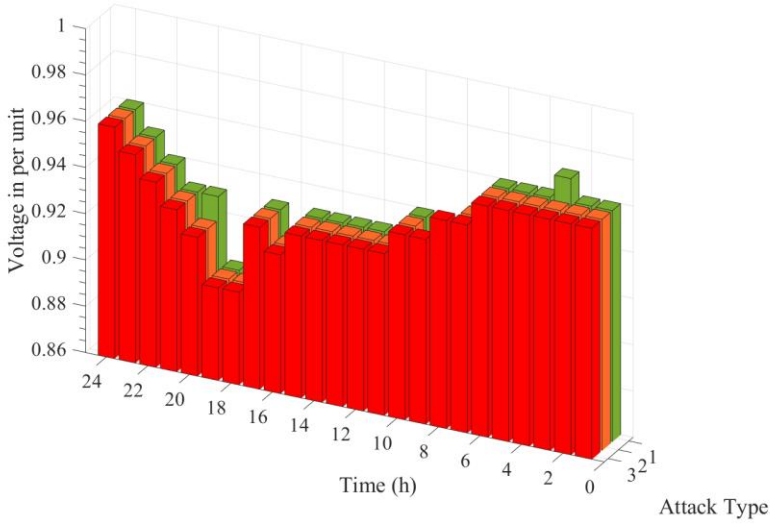

Figure 5-19 - 24-hour Voltage Profile of Bus 3 for all the attacks at 200% penetration

Finally, in Figure 5-19 we see the voltage profiles of all the three attack types at their worst-case scenarios which is at 200% EV penetration level. Overall, the results are the same but we can clearly see the attack 3 and attack 2 bars in the graph dipping below and lower limit or behind the bars shown in attack 1 in blue. Typically, in attack cases we saw voltage deviations for 2-3 hours but for no attack we see no deviation occurring for no hours. The only downside is that since at 18hr the voltage level is somewhat close to lower limit of Range B of the standard but it is operating within the limits of Range of the standard. This shows us if any further expansion of EVs or different residential load may result in our no attack scenario to have experience undervoltage as well.

5.5 Vulnerabilities of the OCPP and Cyber-Physical Attacks on the test system

As we analyzed the Open Charge Point Protocol, the vulnerability of OCPP was mentioned regarding the minimum status duration. Now if we investigate what occurs

when we take the vulnerabilities of the OCPP and pair it with cyberattacks on the system. The impacts of the cyberattacks as seen by the results can clearly show that there are devasting circumstances that will take place due to the those cyberattacks. But how are they able to occur from the vulnerabilities of the OCPP? The answer is the types of attacks that were tested in this research shows how those vulnerabilities can be explained.

Recalling the parameters of the three types of the attacks:

- **Attack #1** – This attack will target the vehicles in profile 1, which is all the people going to work with a possibility to charge at work.
- **Attack #2** – This attack will target the vehicles in profile 3, which is all the people going to work with a possibility to charge at work with a longer ride
- **Attack #3** – This attack will target the vehicles in profile 1, 2, and 3, which is all the people going to work with or without a possibility to charge at work with a shorter and longer duration of the commute respectively

As we recall, since the minimum status duration time is the where the Charge Point updates the Central System regarding the status of the Charge Point. Understanding Attack #1, where the people who are going to work who have the ability to charge their vehicle at work but due to the DoS attack, they are unable to charge. The same applies to Attack #2, where the people who are going to work with a longer commute has the ability to charge their vehicle at work but again due to DoS attack, they are also not able to charge as well. Finally, the last Attack #3, targets both people who drive to work with a short or long commute and make them unable to charge their vehicle at work. For the consumer, this may not be clear at the moment that their inability to charge occurred due to a cyberattack and possibly occurred from their devices communicated with the charge points. The

impacts for the consumer occur as they may not have enough charge to reach back home or the inconvenience of not able to charge.

On a larger scale, the cyberattack that took place during the morning time via the OCPP protocol actually starts impacting the smart grid when these consumers get home and all start to charge their vehicle at the same time. As mentioned, earlier that the consumers themselves could have been responsible of allowing the intruder access to the charge point via their connection to enable the charge point to charge their vehicles. But the long-term impacts on the smart grid does not start until they get home. Then the smart grid experiences the impacts like transformer overload, high Theta H curve for the transformer, and undervoltage for several hours as shown by the results in the previous sections. This allows to examine the effects of vulnerability of the OCPP protocol has when cyberattacks have occurred on the smart grid as seen by the results of the test microgrid system.

5.6 Mitigation Techniques

The analysis showed three significant impacts on the smart grid, as seen in the microgrid test system simulation model. The results showed that when we simulated a cyberattack as Attack #1, Attack #2, or Attack #3, each showed impacts on the smart grid. Each of the three attacks contributed to the smart grid's impacts in various ways. Some attack was more harmful vs. other, but overall, there were significant impacts that occurred to the cyberattacks. Therefore, when considering a mitigation technique, an intelligent approach is to design the mitigation to target the worst of the three cyberattacks possible. Upon which that mitigation technique will be tested and simulated on all three attacks to verify its effectiveness across all the simulated cyberattacks. From the results, Attack #3

showed the most harm towards the simulated test system compared to the other two attacks. Since Attack #3 can be seen as a combination of Attack #1 and Attack #2, it targets all the EVs traveling for a short or long duration and forces them to charge at home. Since this occurs, more vehicles require charging for a more extended period of time as they have drained their battery more compared to any of the other two attack scenarios. Therefore, if we can find a mitigation technique that can target Attack #3 and shows an improvement in the impacts towards the smart grid, then a mitigation technique that can be effective for the other two cyberattacks as well will be tested and simulated on them as well.

The results showed that since the EV charger demand is very high within the two-hour period, this causes the increased demand as seen in the transformer overload, temperature curve, and undervoltage between the times of 18^{th} hour to the 20^{th} hour. This means that any mitigation technique that is targeted shows to be able to reduce these impacts of the cyberattack in this time frame. Additionally, all mitigation techniques will analyze all the results from the mitigation with respect to the impacts of the smart grid. The impacts of the transformer overload, the transformer's temperature curve, and the bus's undervoltage will be analyzed for each mitigation technique for each type of attack. The goal of this will help in understanding the mitigation technique towards all the components for the cyberattacks and their respective impacts on the smart grid.

5.6.1 Mitigation Technique #1 – Changing the Charging Times

Since the proposed mitigation technique in this work targets the worst attack, which is Attack #3, then one of the options that may be used is to change the charging times. This refers to the different vehicle profiles implemented in the simulated test model. Since the users in the longer commute or duration vehicle profile and under a cyberattack cannot

charge their vehicle at work, it will result in a more significant battery depletion when they reach home. Since their duration is longer, it can be anticipated that they will arrive home later if everyone leaves work at the same time.

Therefore, with this thought in mind and separating the charging times, we will move the charging times of all the vehicles in profile #3 that drive longer and cannot charge at work due to a cyberattack. The default start charging time for all the vehicle profiles who returned from work was the 18^{th} hour, which can be seen by the sudden peak in any of the graphs in the results, such as Figure 5-8, showing the power demand changing suddenly from the 17^{th} to the 18^{th} hour. For the vehicles in profile 3, let's change the start charging time to the 19^{th} hour, which is one full hour after the short-duration vehicles have started charging. According to our data, a car takes approximately 2 hours to charge if drained completely. But since the commuters with a shorter duration should complete charging in 1 to 1.5 hours should impact the smart grid in some manner. In addition, to develop a very future proof mitigation technique, the EV penetration will be set at 200%, which refers to the 200 vehicles as the microgrid test model. As identified in the results, each attack was conducted for three EV penetration levels ranging from 100% to 200% (max) with an increment of 50%, and by default, 100% penetration referred to 100 vehicles in the model. Therefore, to consider a future proof mitigation technique, it is best to use a 200% penetration level in the simulated mitigation techniques shown.

For the following mitigation technique, the terminology 'SAME' will refer to charging time of all the vehicles will be 18^{th} hour when they come home and plug in for charge. The 'SAME' charging time is the default charging time that was used when conducting the testing on the microgrid system with attack and no attack scenarios. The

mitigation technique will focus on the 'SEPARATE' charging times, which refers to the charging times during the evening hours of 18th to 20th hour to lower the impact from the cyberattacks. The 'SEPARATE' charging times will refer to allowing the vehicles that commute a longer distance to start their charging at 19th hour rather than the 18th hour, which will reduce the amount power required at a specified given hour and reduce the impacts on the smart grid.

5.6.1.1 Mitigation Technique #1 – Transformer Overload

According to Figure 5-20, Figure 5-21, and Figure 5-22, the transformer demand can be seen using the same specifications for the V2G where the rated power remains the same at 40kW for the FCS and only the charging times have been changed to identify a mitigation technique. From the figures, it can be clearly seen in green, which is the separate charging time does make an impact as it reduces the transformer demand. The impact may not be substantial as it is still above the maximum rated transformer capacity limit but definitely lowers the enormous peak.

Additionally, for all three attacks, the mitigation technique is effective to reduce the initial peak at 18th hour, which was causing the greatest hour of overload but still remains above maximum rated transformer capacity. Since the charging does not all occur at the same time, it can be seen in green a higher peak during the 21st hour as the vehicles is still charging, which is higher than the same charging time. This is still better than the same charging as even with a higher peak, the peak is still located well under the maximum transformer capacity limit. Rather than pushing all the vehicles to charge at once, instead the vehicles become a spread out allowing the transformer to supply power at different times which reduces the overload for a given period of time. Finally, the greatest reduction

in overload between same and separate charging can be seen for Attack #3 in Figure 5-22 during the 18th to 20th hours.

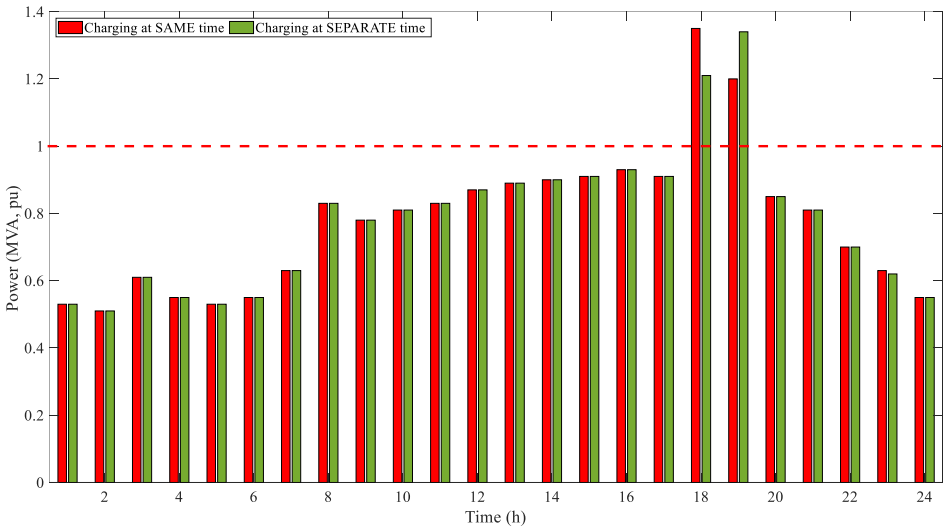

Figure 5-20 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times according to Mitigation Technique #1

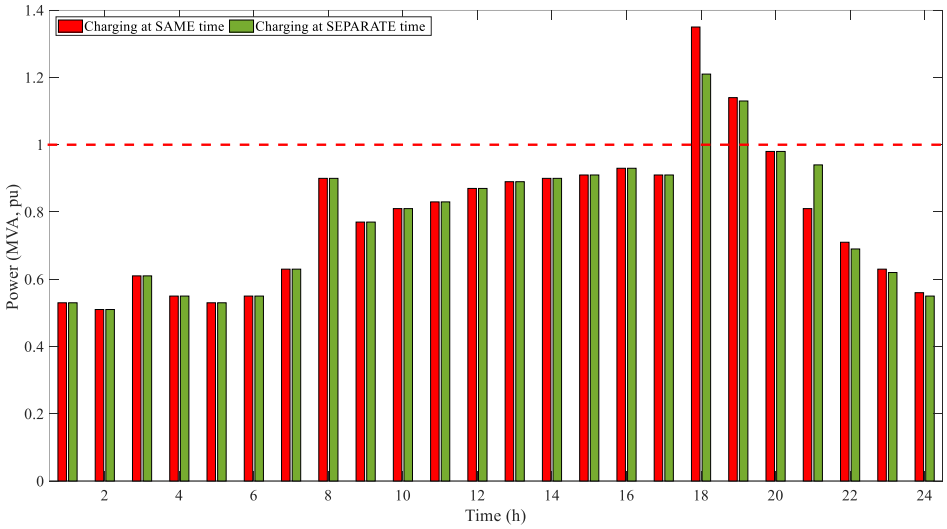

Figure 5-21 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times according to Mitigation Technique #1

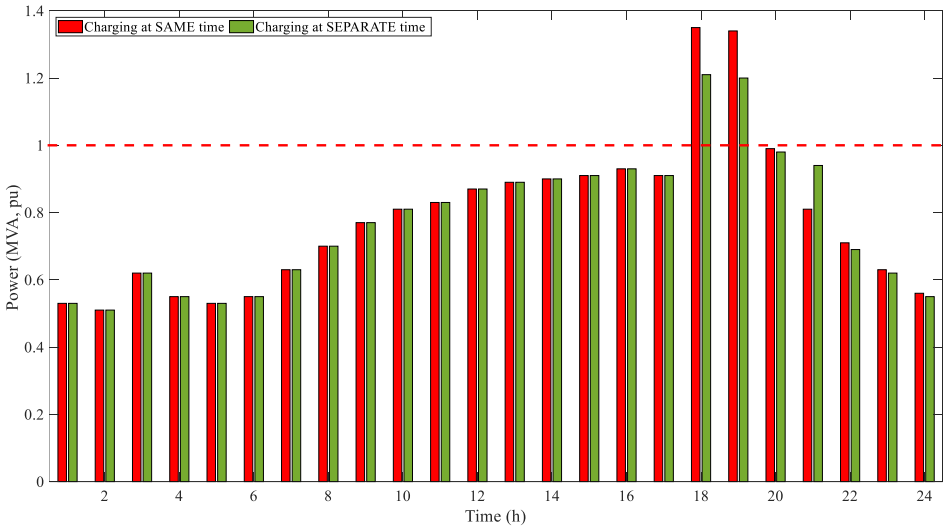

Figure 5-22 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times according to Mitigation Technique #1

5.6.1.2 Mitigation Technique #1 – Theta H Curve

For the Theta H Curve, the results are similar to what was seen for the transformer overload. Since the mitigation for Theta H curve depends on the oil temperature of the transformer, it will behave similarly the overload trend for mitigation technique #1. Figure 5-23, Figure 5-24, and Figure 5-25 represents the transformer temperature curve for Attack #1, Attack #2, and Attack #3 respectively. Similar to the transformer overload, the peak that is seen for the same charging at 18th hour is decreased significantly but not enough when mitigation technique #1 of separating the charging times is applied. For each of the three attack cases, even with the separate charging technique, the rated thermal capacity limit for each attack along with mitigation technique is violated. Therefore, the mitigation technique helps reducing the overall temperature but it is not enough to where it below the rated thermal operating limit of the transformer.

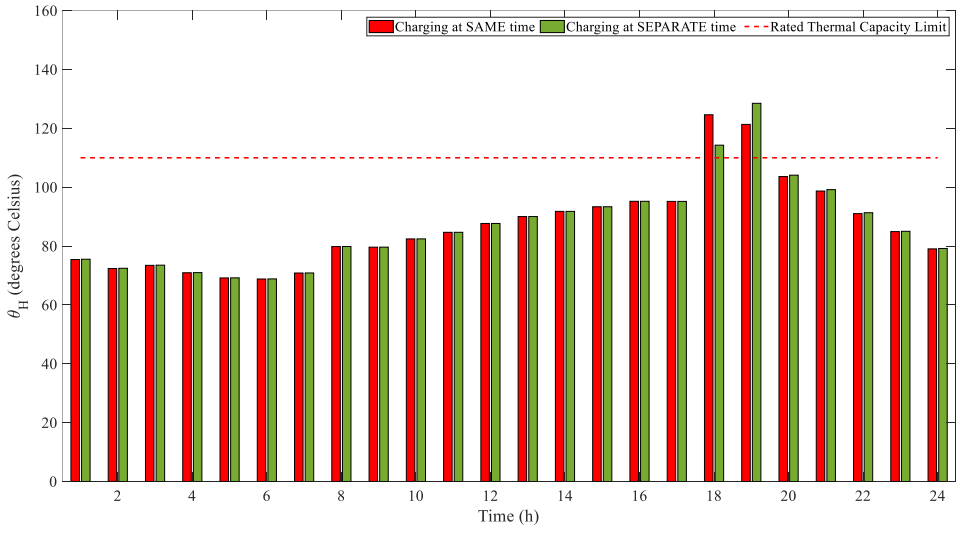

Figure 5-23 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times according to Mitigation Technique #1

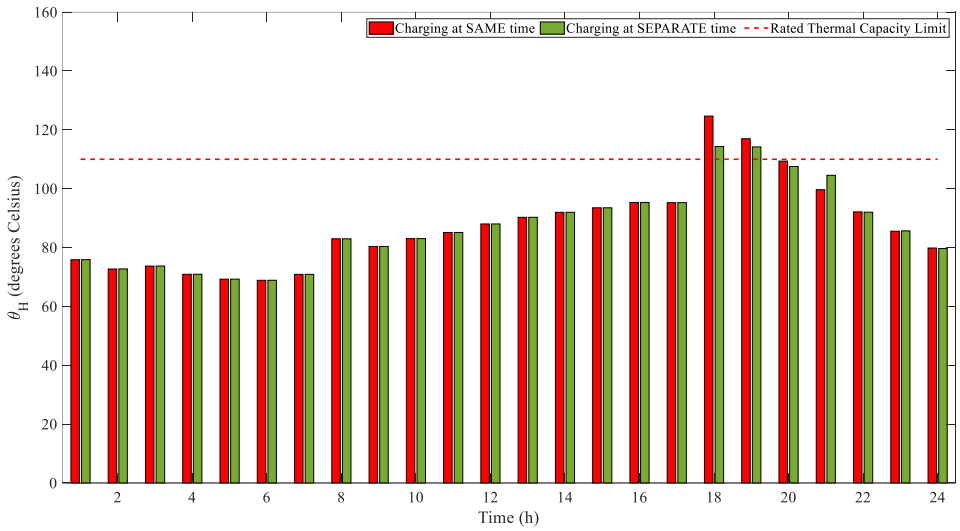

Figure 5-24 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times according to Mitigation Technique #1

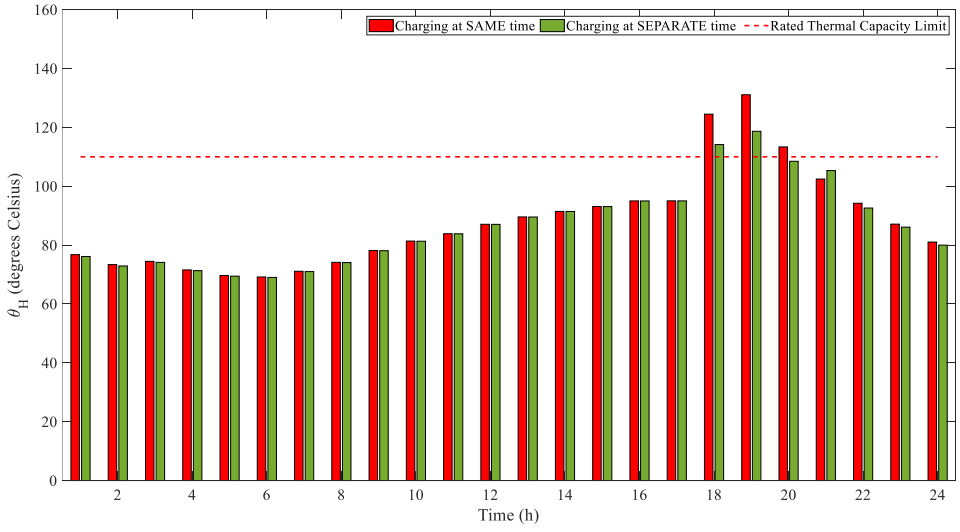

Figure 5-25 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times according to Mitigation Technique #1

Similarly, to the transformer overload in terms of the mitigation technique, Attack #3, shows the significant reduction in the transformer temperature curve between the 18th to 20th hour. In addition to the reduction, if compared the same and separate charging times at the 20th hour, then it can be seen that from Figure 5-25 the separate charging in green is actually below the rated thermal limit. This shows that the mitigation technique is effective to lower the impact at a given hour and may be useful to implementation during a cyberattack. In addition, for the other two attacks, at 20th hour both charging times are below rated thermal limit as the impacts of those attack does not last as long as third attack. Either way, when compared the values at all three attacks, the separate charging times has a lower temperature than the same charging time scenario.

5.6.1.3 Mitigation Technique #1 – Undervoltage

To begin, the impacts of undervoltage on the smart grid has been the most minimal compared to the other two impacts of transformer overload and the temperature curve of the transformer. Since undervoltage only occurs when a problem persists in a system for a longer period of time therefore, focusing on the same 18th to 20th hour time frame the system is affected by undervoltage as seen in the results sections. Therefore, the mitigation technique should target the impact of undervoltage as well to reduce the overall impact to the smart grid.

According to Figure 5-26, Figure 5-27, and Figure 5-28, the voltage profile for Attack #1, Attack #2, and Attack #3 are shown respectively by utilizing the same and separate

charging times mitigation technique. The results of the mitigation techniques lead to separate charging resulting it not causing an undervoltage when utilized in the Attack #1 and Attack #3 scenarios at the 18th hour. This shows that the separate charging works in removing the undervoltage in the system voltage at 18th hour for two of the attacks while Attack #2 remains unaffected and experience an undervoltage. Additionally, the separate charging also try and change the impact at the 19th hour as well but does not completely satisfy all the three attack cases and ends up showing an undervoltage during that time.

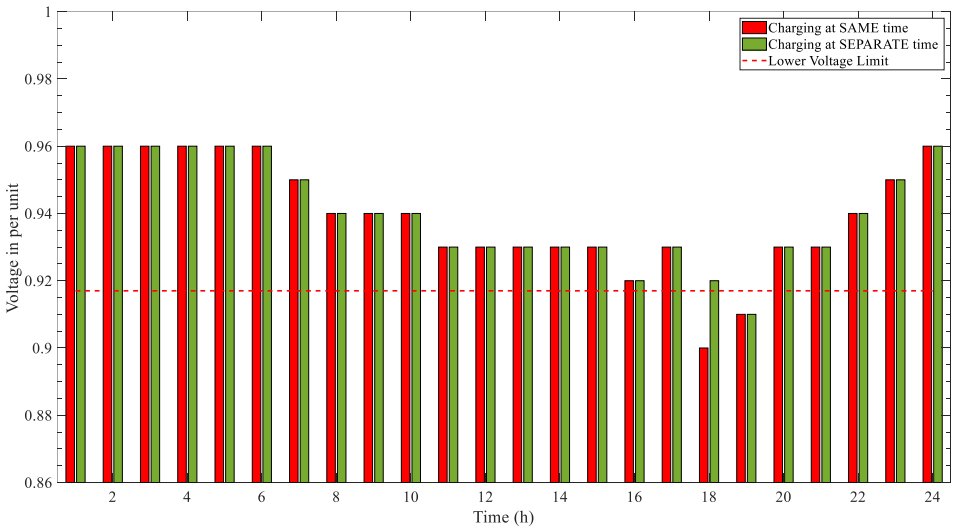

Figure 5-26 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times according to Mitigation Technique #1

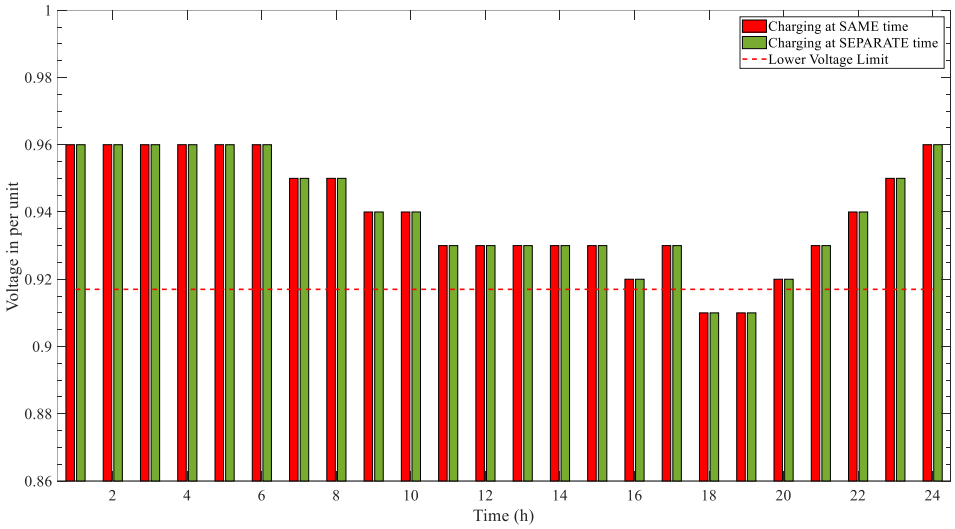

Figure 5-27 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times according to Mitigation Technique #1

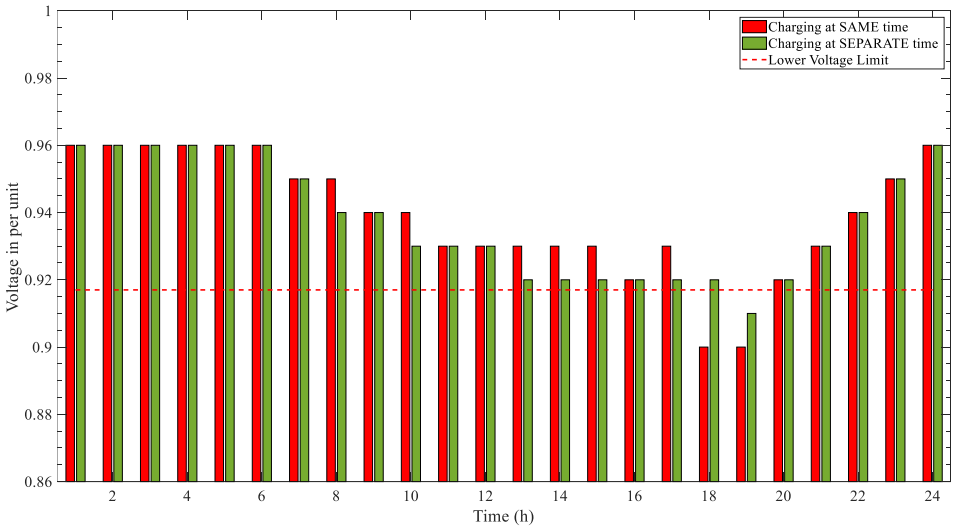

Figure 5-28 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times according to Mitigation Technique #1

5.6.2 Mitigation Technique #2 – Changing the Charging Times & the Rated Power

According to the results of the mitigation technique #1, the results of separate charging times definitely show some improvements in relieving the impacts when compared to the same charging times. Also, for many cases the separate charging reduced the impacts but completely therefore another mitigation technique needs to be considered. Mitigation Technique #2, focus on the idea that since these vehicles come home to charge when they are affected by the cyberattacks, the charging levels available at home may not be the same for everyone. According to Tesla [92], the company describes the type of wall connectors that are available to install at home EV charging. Some of the charging levels identified from the list are 11.5kW, 9.6kW, and 7.7kW. These were the top three charging levels closest the FCS charging levels utilized in the microgrid simulation.

Since changing the charging times alone did not mitigate the problem completely, then in addition to the changing charging times, Mitigation Technique #2 will also implement changing the charging rates of the EV chargers at home. In Mitigation Technique #1, the EV chargers rates were specified to be 40kW and battery size to 85kWh as per [88, 89]. By changing only, the charging rates, it will decrease the amount of power required at given time by a charger and extend the charging time but reduce the peak power demand. The mitigation will be tested for each of the three cyberattacks and will be tested at the three top charging rates acquired for possible home charging levels. The goal behind using these charging rates specifically provides the closest rates possible for homes to reduce the charging times as performed by a typical FCS utilized for quick charging. Additionally, for each of these cases, the impacts on the smart grid will be analyzed to see

how the mitigation technique improves and provide an appropriate mitigation to cyberattacks.

5.6.2.1 Mitigation Technique #2 – Transformer Overload

To begin, this subsection starts with the first impact of the cyberattacks of Transformer Overload and identify how it can be mitigated using Mitigation Technique #2. The aim is to analyze different charging rates ranging from 11.5kW to 7.7kW to see the what impacts it has on the Transformer Overload when it is under the three cyberattacks analyzed in the results. Therefore, each charging rate will have three corresponding graphs which corresponds to the three cyberattacks.

5.6.2.2 Mitigation Technique #2 – Transformer Overload at 11.5kW Charging Rate

The transformer overload impact was one of the three major impacts on the microgrid from the cyberattacks. Upon analyzing the data and utilizing the separate charging time mitigation technique #1, the technique was not able to reduce the transformer overload under the maximum rated power. According to Figure 5-29, Figure 5-30, and Figure 5-31, corresponding to Attack #1, Attack #2, and Attack #3 respectively, the utilization of Mitigation Technique #2 can be seen where the rated power of the chargers was reduced to 11.5kW. From the graphs, a significant decrease in the transformer overload can be observed for both the SAME and SEPARATE charging times. The impacts of reducing the power of the chargers have shown to be effective in removing the overload and for all the attacks between 18^{th} hour to 20^{th} hour.

Additionally, the positive impacts of this mitigation technique can be seen but for the 18^{th} hour the SAME charging time still is above the maximum rated power. Also, at the 19^{th} hour the transformer overload is reaching the maximum rated power limit meaning the

transformer is working at 100% capacity limit. This problem still will be addressed with the other two charging rates of 9.6kW and 7.7kW.

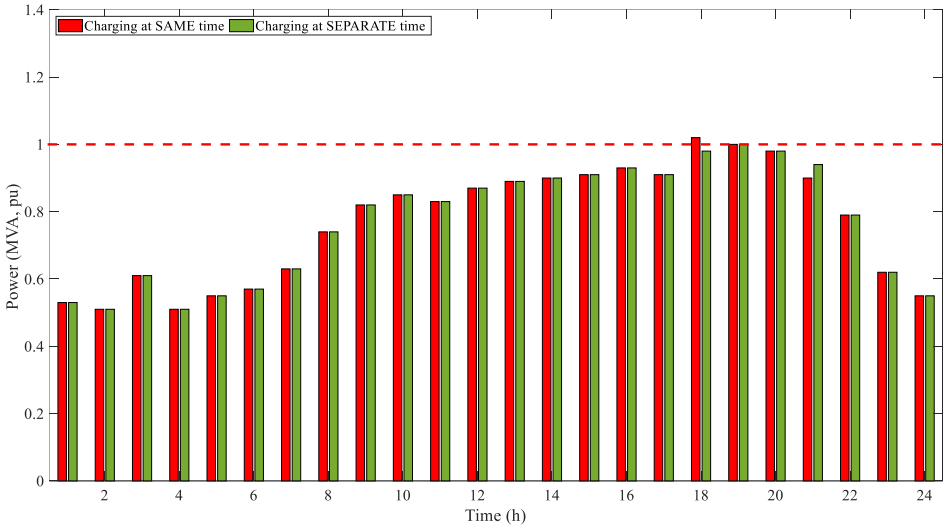

Figure 5-29 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

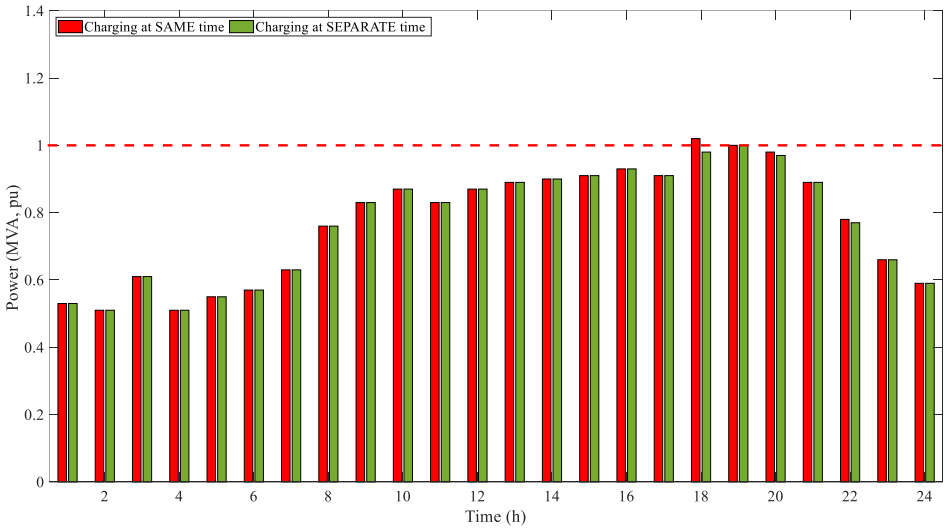

Figure 5-30 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

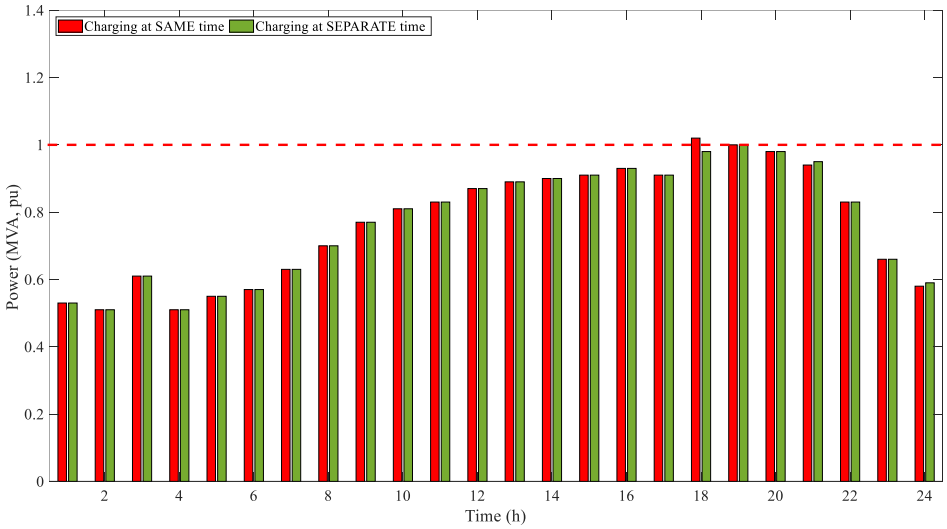

Figure 5-31 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

5.6.2.3 Mitigation Technique #2 – Transformer Overload at 9.6kW Charging Rate

The effect of the charging rate of 9.6kW for the chargers can be seen in Figure 5-32, Figure 5-33, and Figure 5-34, for Attack #1, Attack #2, and Attack #3 respectively. As shown in the 11.5kW mitigation, the transformer overload significantly decreased when the charging rates were decreased from 40kW to 11.5kW. Now the charging rates in the mitigation technique decreased from 11.5kW to 9.6kW shows a much smaller drop but significant enough that brings the transformer overload either at the maximum rated power limit or under it. Compared to the 11.5kW charging rate no attacks cases for 9.6kW have the transformer overload above the maximum rated capacity of the transformer.

The transformer overload has decreased for the SAME charging time at 18th hour from being above the limit to being on the limit when compared to the 11.5kW charging rate. Although, this still needs to be addressed as at the 18th hour the transformer will be

running at 100% capacity for the entire hour. On the other hand, at the 19th hour the transformer overload has decreased and is well below the maximum rated capacity limit when compared to the 11.5kW charging rate. Since the transformer overload has not been completely eliminated with the two charging rates for the mitigation technique #2, then further decrease in charging time is required to the next available rate of 7.7kW.

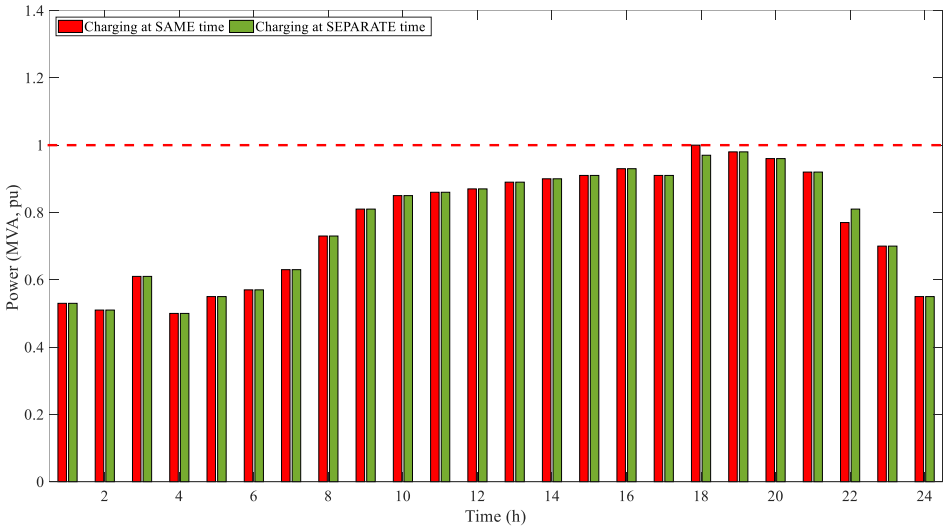

Figure 5-32 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2

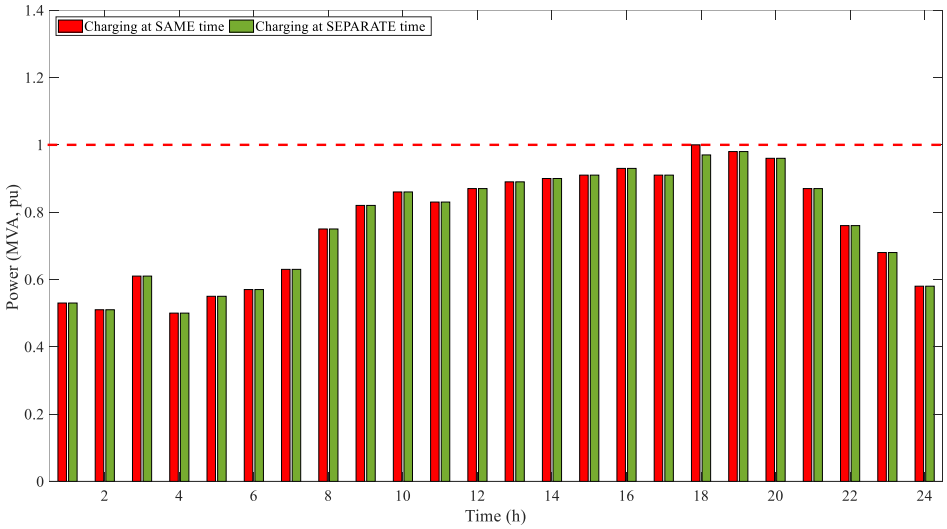

Figure 5-33 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2

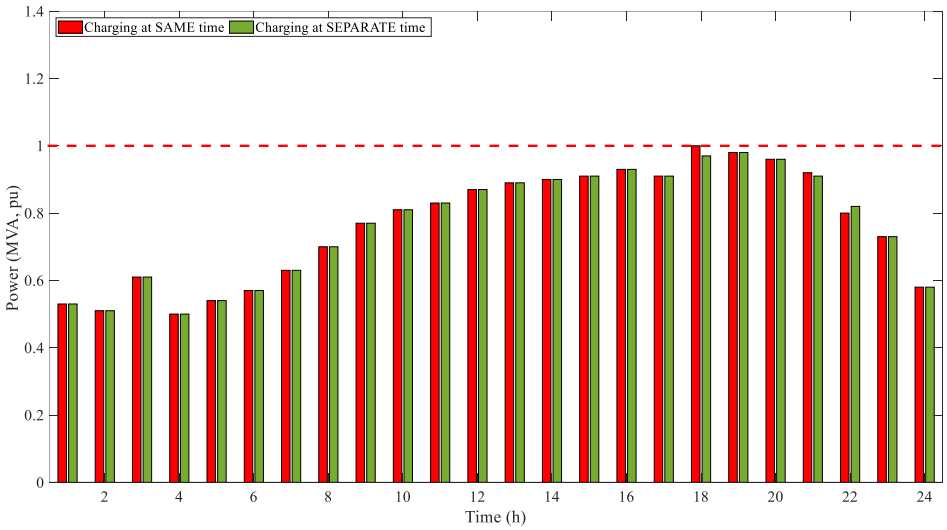

Figure 5-34 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2

5.6.2.4 Mitigation Technique #2 – Transformer Overload at 7.7kW Charging Rate

At last, the third charging rate of 7.7kW is used to address the impact of transformer overload as seen in Figure 5-35, Figure 5-36, and Figure 5-37 for Attack #1, Attack #2, and Attack #3 respectively. Upon analyzing all three attacks with the mitigation technique of applying the 7.7kW as the charging rate and utilizing both SAME and SEPARATE charging times, it can be concluded that no transformer overload is occurring for any hour for any attack. Therefore, with the utilization of Mitigation Technique #2 at 7.7kW both the SAME and SEPARATE charging times from Mitigation Technique #1, at all hours the transformer overload is below the maximum rated transformer capacity.

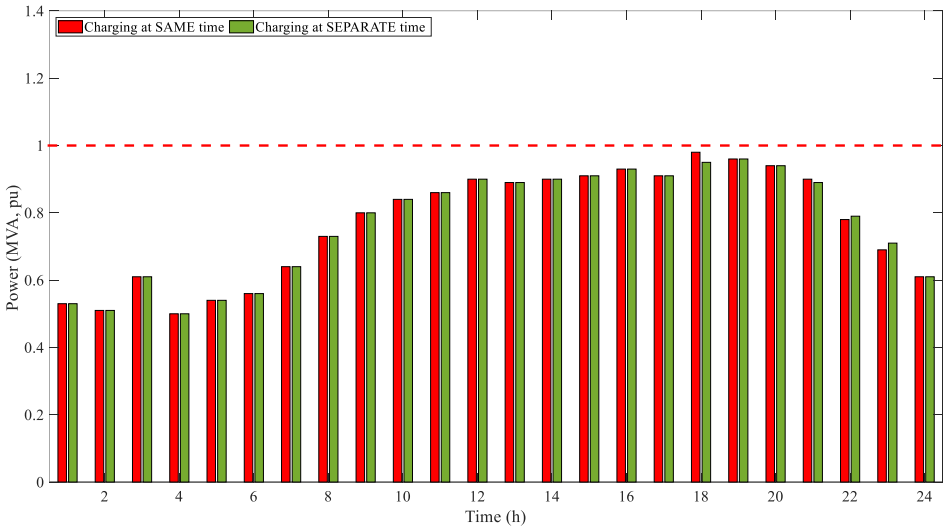

Figure 5-35 - Transformer Demand for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

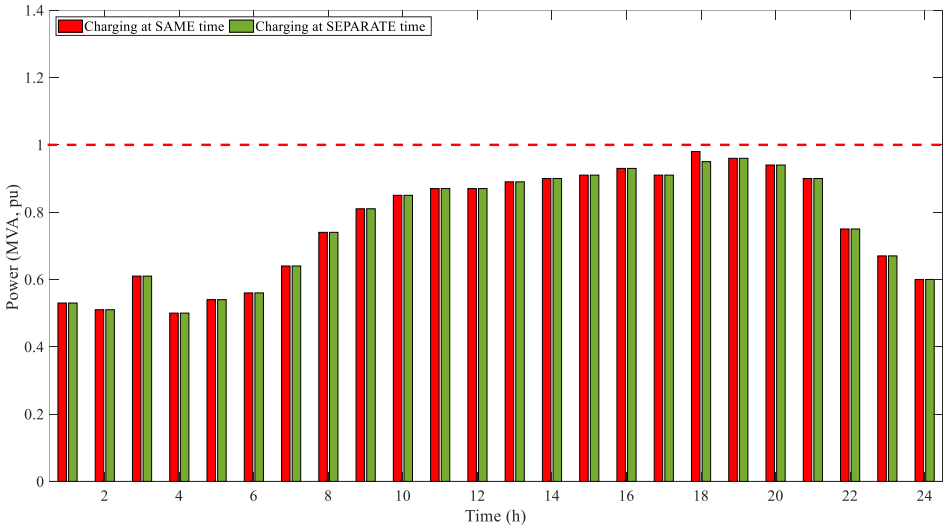

Figure 5-36 - Transformer Demand for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

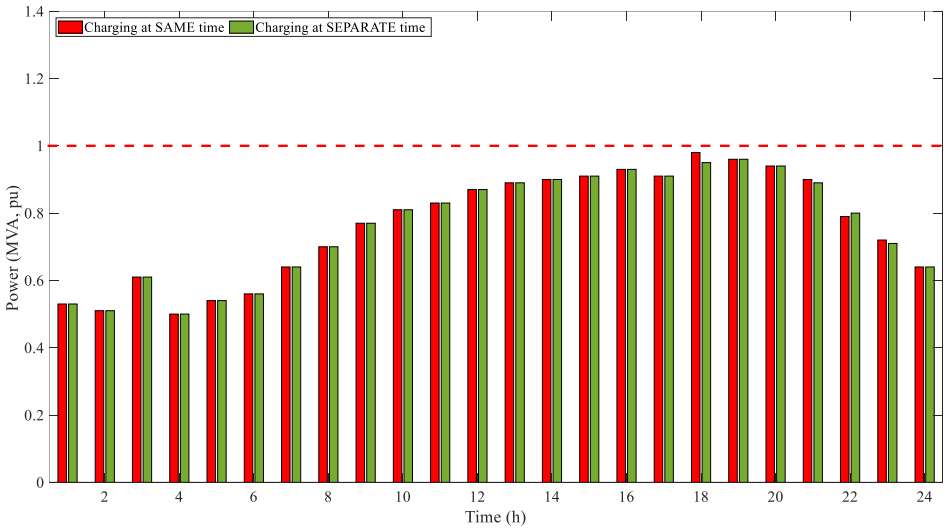

Figure 5-37 - Transformer Demand for Attack #3 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

5.6.2.5 Mitigation Technique #2 – Theta H Curve

Secondly, the impact of the Temperature Curve of the transformer or Theta H curve is the next impact that needs to be addressed when analyzing Mitigation Technique #2. Similarly, to the transformer overload, the mitigation will be assessed for all three cyberattacks with three charging rates of 11.5kW, 9.6kW and 7.7kW as stated by the home charging limits. Since the transformer overload required the use of the all three charging times to mitigate the overload, the same idea will be applied to the temperature curve as well. The effect can be similar or different as the temperature curve is largely dependent on the overload and may experience mitigation at an earlier or later charging rate. There will be three graphs for each charging rate for each of the three corresponding cyberattacks to analyze the impacts of Theta H curve. Then, those three graphs will be tested for the remaining two charging rates resulting in nine graphs showing mitigation technique for the Theta H curve with all possible combinations between charging times and attacks.

For each charging rate, the mitigation technique will focus on reducing the temperature from the rated thermal capacity limit of 110 (degrees Celsius) to increase the life of the transformer. When Mitigation Technique #1 was utilized the separate charging time reduced the Theta H close the rated thermal limit but still resulted in exceeding the limit. The goal of building with mitigation technique #2 will be see how the SAME and SEPARATE charging times will impact the Theta H curve when we change the rated power of the chargers for the EVs.

5.6.2.6 Mitigation Technique #2 – Theta H Curve at 11.5kW Charging Rate

According to Figure 5-38, Figure 5-39, and Figure 5-40, corresponding to Attack #1, Attack #2, and Attack #3 respectively, the mitigation of Theta H curve given at the 11.5kW

charging rate can be seen. From the three graphs it can be observed that for each of the three attacks the rated thermal limit of the Theta H has been exceeded instead is about 10 degrees lower than the limit. Therefore, the Theta H curve sees the impact of the mitigation technique the quickest when the charging rate is reduced from 40kW to 11.5kW for all three attacks. This shows the largest changes for the impact on the transformer as even though the transformer is experiencing an overload at the given charging rate of 11.5kW but the Theta H curve is well below the limit for the same charging rate. This concludes that the mitigation technique is definitely having a positive impact in reducing the temperature of the transformer and lower the Theta H curve well below the rated thermal limits as per the standard.

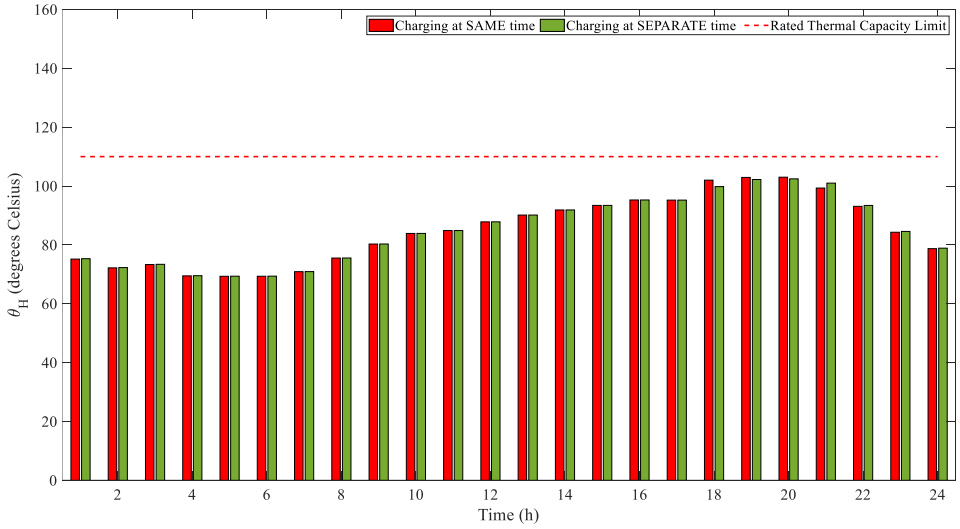

Figure 5-38 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

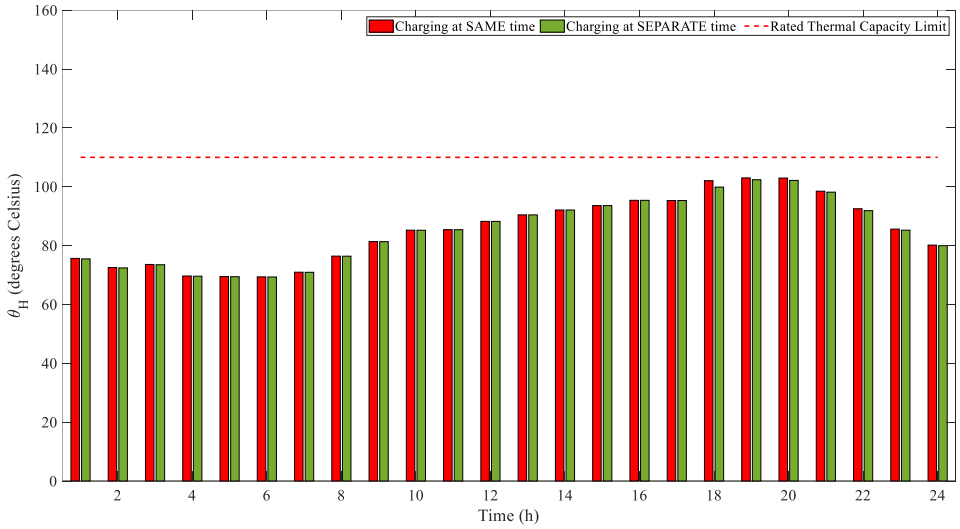

Figure 5-39 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

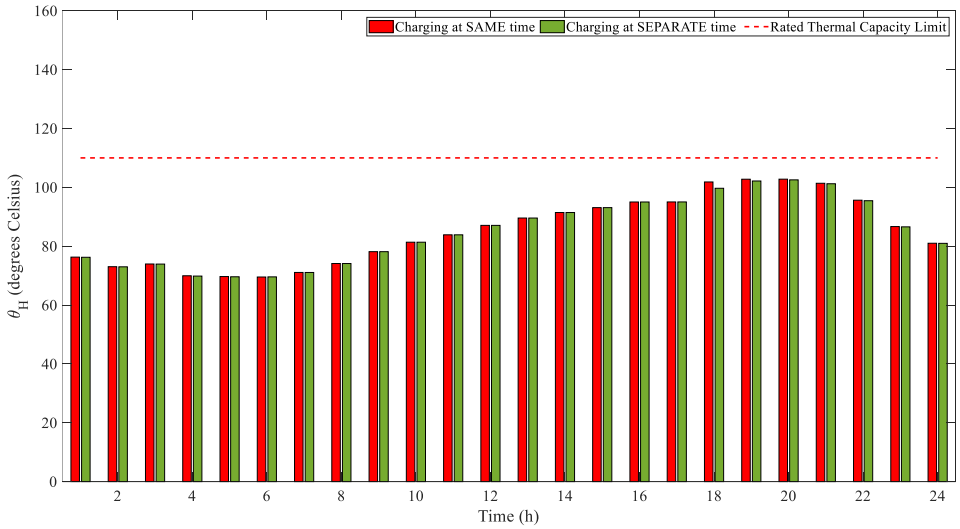

Figure 5-40 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

5.6.2.7 Mitigation Technique #2 – Theta H Curve at 9.6kW Charging Rate

Continuing on to the next charging rate of 9.6kW for the impact on the Theta H curve for the transformer. As it was seen in the previous section, the Theta H curve was successfully mitigated for all the three cyberattacks at the 11.5kW charging rate that was tested. Therefore, this charging rate of 9.6kW for sure will also mitigate as well but for consistency and other factors that may impact the Theta H curve, all testing for the mitigation techniques will be done for all three charging rates. Since it took transformer overload a charging rate of 7.7kW to mitigate the overload all impacts will be tested until 7.7kW or further until the mitigation is successfully under the limits provided for home charging levels.

According the Figure 5-41, Figure 5-42, and Figure 5-43, corresponds to the Attack #1, Attack #2, and Attack #3 for the mitigation technique #2 utilizing the 9.6kW charging rate for both SAME and SEPARATE charging times. Overall, the mitigation is successful and the Theta H values as slightly lower than what was seen in the 11.5kW charging rate in the previous section. The rated thermal capacity limit is never exceeded for any of the attacks under the 9.6kW charging rate for both charging times as well.

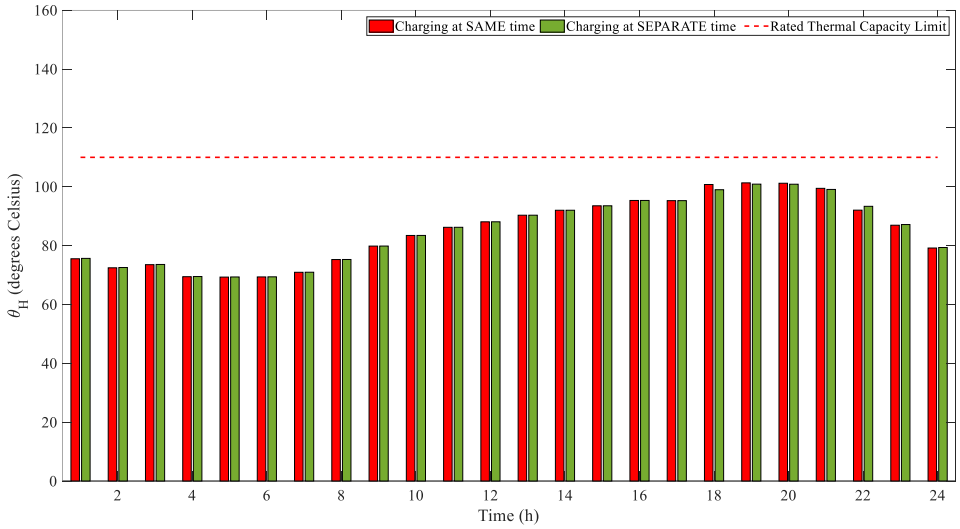

Figure 5-41 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

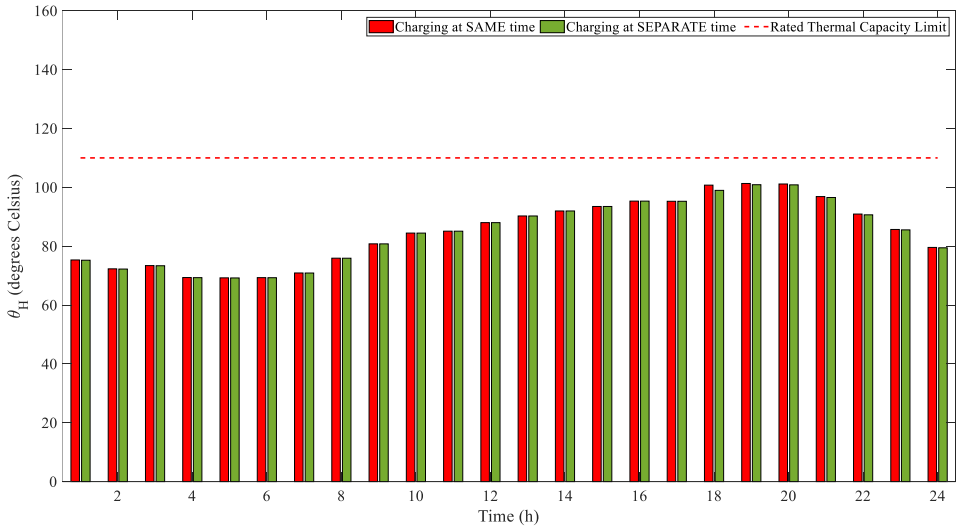

Figure 5-42 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

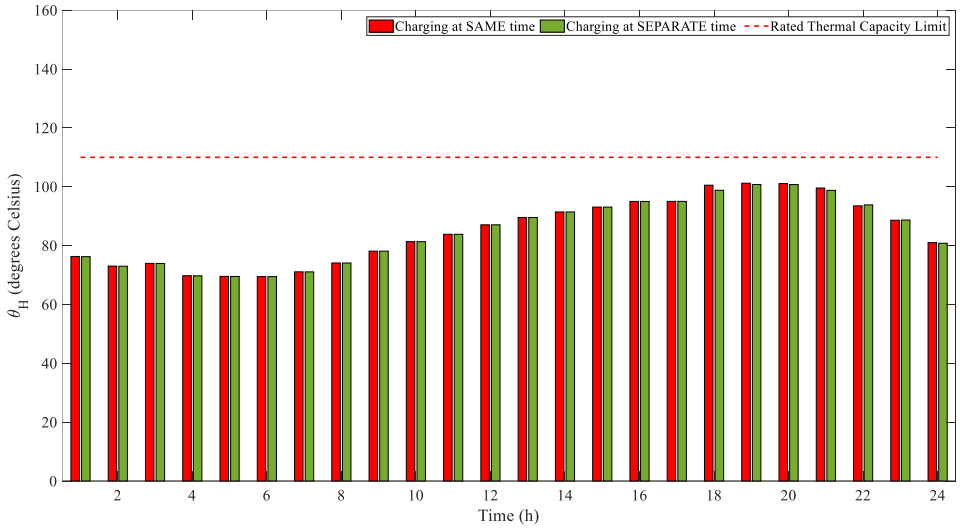

Figure 5-43 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2

5.6.2.8 Mitigation Technique #2 – Theta H Curve at 7.7kW Charging Rate

According to Figure 5-44, Figure 5-45, and Figure 5-46 corresponds to the Attack #1, Attack #2, and Attack #3 for the mitigation technique #2 utilizing the 7.7kW charging rate for both SAME and SEPARATE charging times. Overall, the mitigation is successful and the Theta H values as slightly lower than what was seen in the 11.5kW and the 9.6kW charging rates in the previous sections. The rated thermal capacity limit is never exceeded for any of the attacks under the 7.7kW charging rate for both charging times as well.

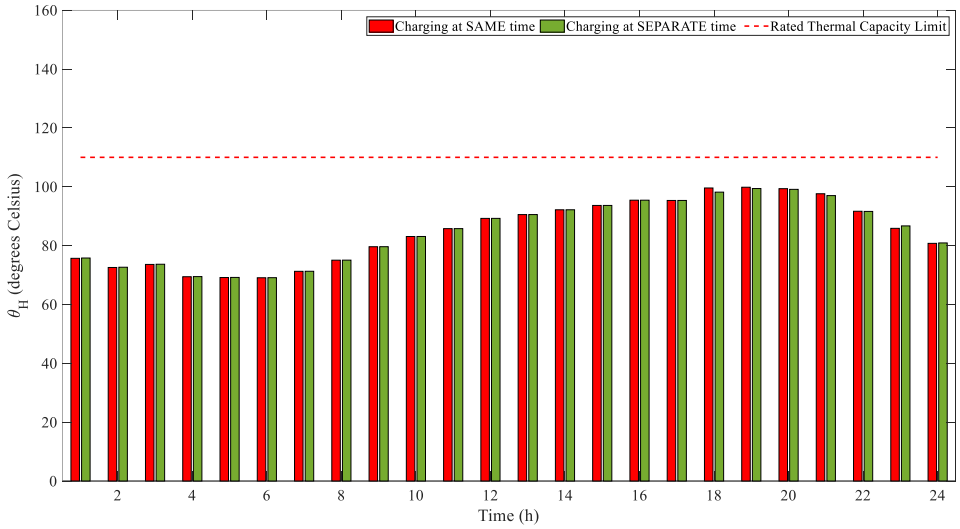

Figure 5-44 - Transformer Temperature Curve (Theta H) for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

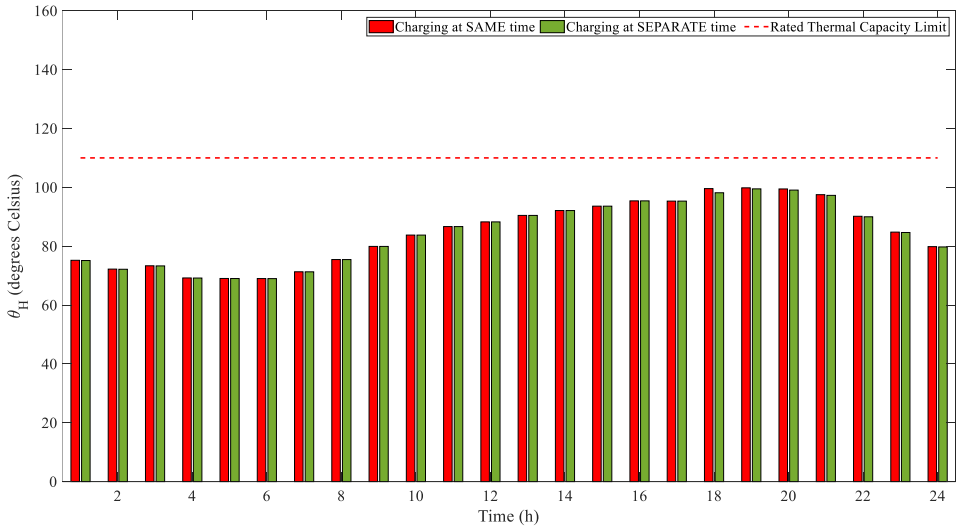

Figure 5-45 - Transformer Temperature Curve (Theta H) for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

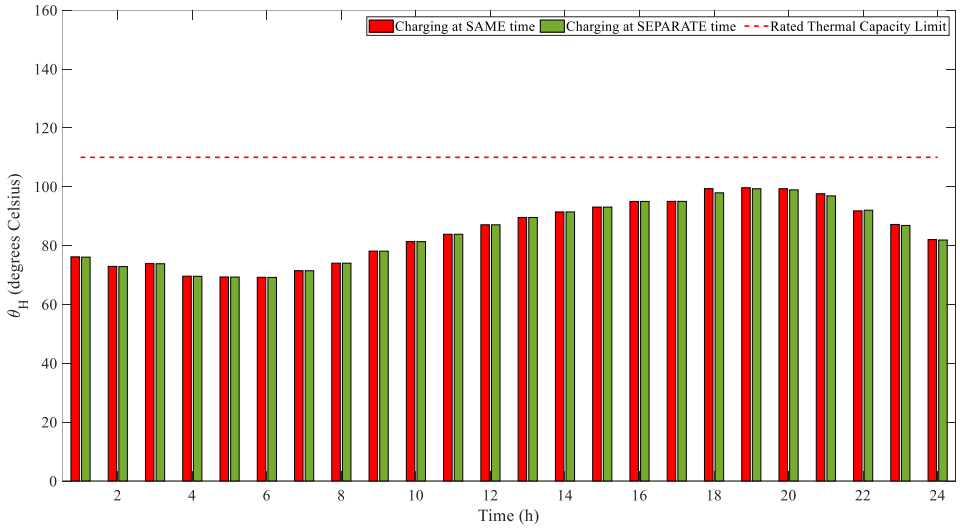

Figure 5-46 - Transformer Temperature Curve (Theta H) for Attack #3 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

5.6.2.9 Mitigation Technique #2 – Undervoltage

Lastly, the last impact on the microgrid from the cyberattacks is the Undervoltage of the bus 3 that was analyzed in the results. Due to the undervoltage, many disruptions such as power outages or discontinuity in power can occur for the consumer who are downstream and will impact the smart grid as well. Therefore, the importance of mitigation is crucial to lower the overall impacts on the smart grid. The mitigation technique #1, showed that the undervoltage improved and the voltage profile was impacted slightly from the SEPARATE charging time vs, the SAME charging time method. But overall, still experienced an undervoltage during the 18th to 20th hour of the voltage profile.

Therefore, with Mitigation Technique #2, the same approach will be taken as it was for transformer overload and Theta H curve where there the voltage profile will be tested against three charging rates at 11.5kW, 9.6kW, and 7.7kW. As seen in the Theta H curve,

the mitigation occurred at the very beginning with the 11.5kW but still the other two charging rates were tested for consistency and open if any other factors affected the impact. The same approach is followed for the undervoltage and all three charging rates will be assessed for all three cyberattacks resulting in three graphs for each charging rate for a total of nine graphs overall. This will identify all the possible combinations for providing mitigation towards the undervoltage in the smart grid.

For each charging rate, the mitigation technique will focus on staying above the lower voltage limit of the bus voltage at 550.2 V or 0.917 voltage per unit. When Mitigation Technique #1 was utilized, the separate charging time has some impact on the undervoltage but overall, still experienced an undervoltage which resulted in exceeded in the lower voltage limit. The goal of building with mitigation technique #2 will be see how the SAME and SEPARATE charging times will impact the undervoltage when we change the rated power of the chargers for the EVs.

5.6.2.10 Mitigation Technique #2 – Undervoltage at 11.5kW Charging Rate

According to Figure 5-47, Figure 5-48, and Figure 5-49, corresponding to Attack #1, Attack #2, and Attack #3 respectively, identifies the Mitigation Technique #2 utilized with the charging rate of 11.5kW for both SAME and SEPARATE charging times. From the result of the mitigation, it can be concluded that the 11.5kW along with the different charging times successfully mitigated all the impacts of the cyberattacks for all three attacks for the undervoltage in the smart grid. All results identify the voltage profile to be above the lower voltage limit and therefore is not violating the voltage level set by the standards. Since undervoltage requires a longer time to show impact as seen in the 40kW

charging time in mitigation technique #1, by dropping the charging time to 11.5kW it was successfully above the voltage limit.

Similar to the Theta H curve, even though mitigation was successful at 11.5kW charging rate, the other two charging rates will also be tested to show the impacts on the undervoltage. This will keep consistency throughout the impacts on the smart grid and allow comparison to occur between them.

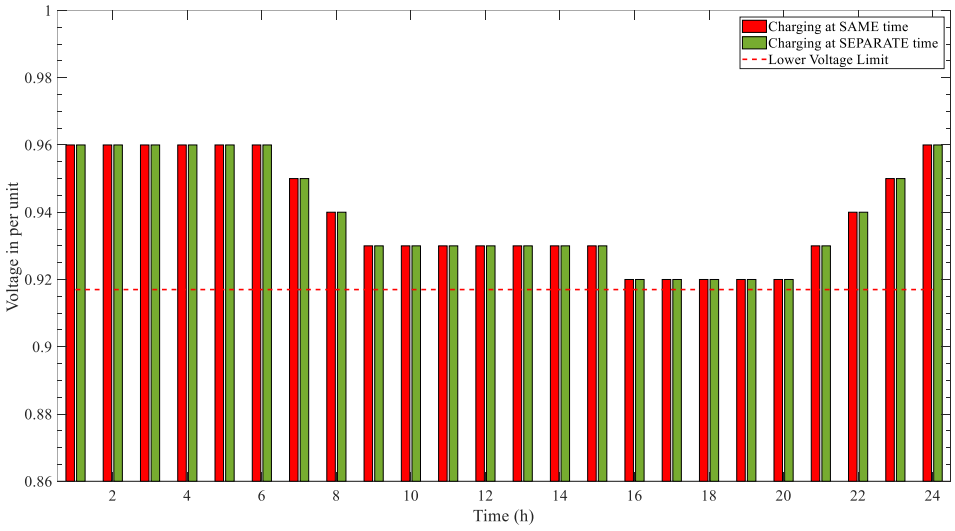

Figure 5-47 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

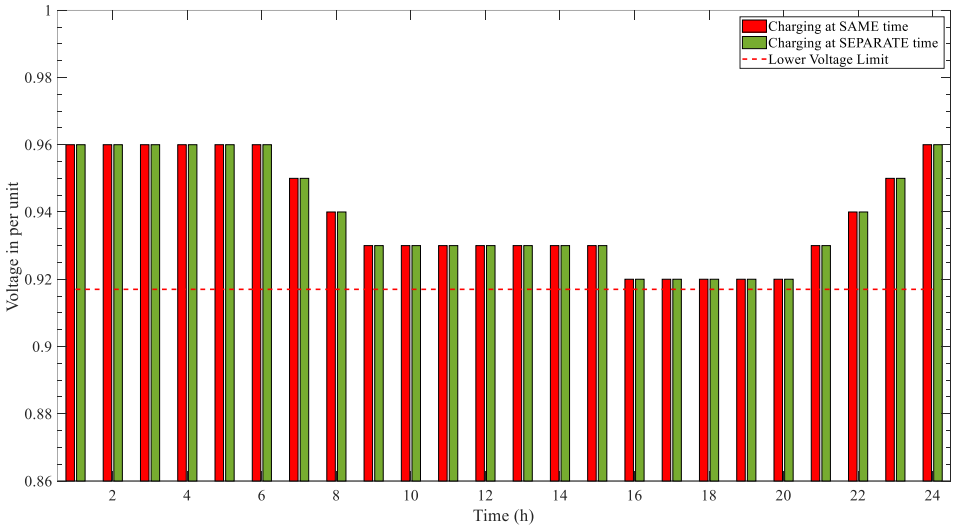

Figure 5-48 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

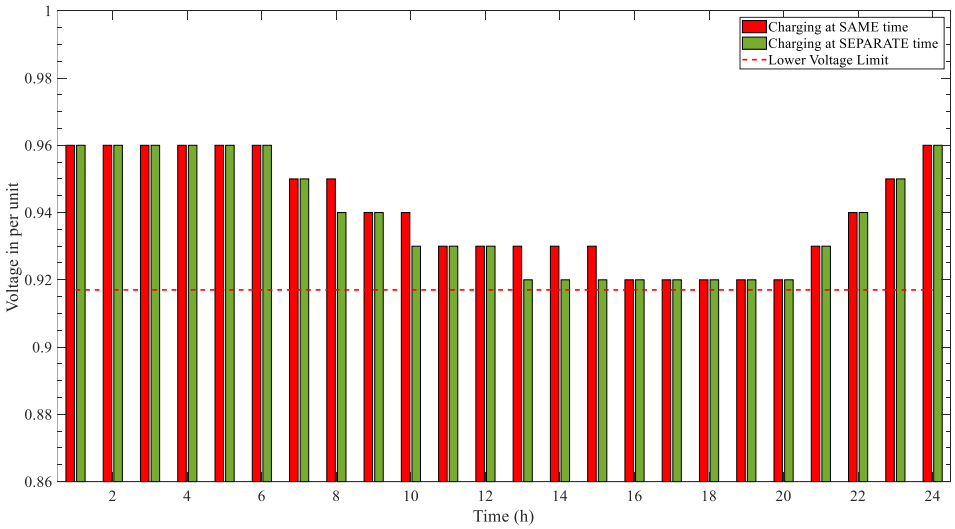

Figure 5-49 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times at 11.5kW rated power according to Mitigation Technique #2

5.6.2.11 Mitigation Technique #2 – Undervoltage at 9.6kW Charging Rate

According to Figure 5-50, Figure 5-51, and Figure 5-52, corresponding to Attack #1, Attack #2, and Attack #3 respectively, identifies the Mitigation Technique #2 utilized with the charging rate of 9.6kW for both SAME and SEPARATE charging times. From the result of the mitigation, it can be concluded that the 9.6kW along with the different charging times successfully mitigated all the impacts of the cyberattacks for all three attacks for the undervoltage in the smart grid. All results identify the voltage profile to be above the lower voltage limit and therefore is not violating the voltage level set by the standards. Comparing to the 11.5kW charging rate, the voltage profile remains the same and no change can be observed between them as the transformer is still running near to maximum rated capacity.

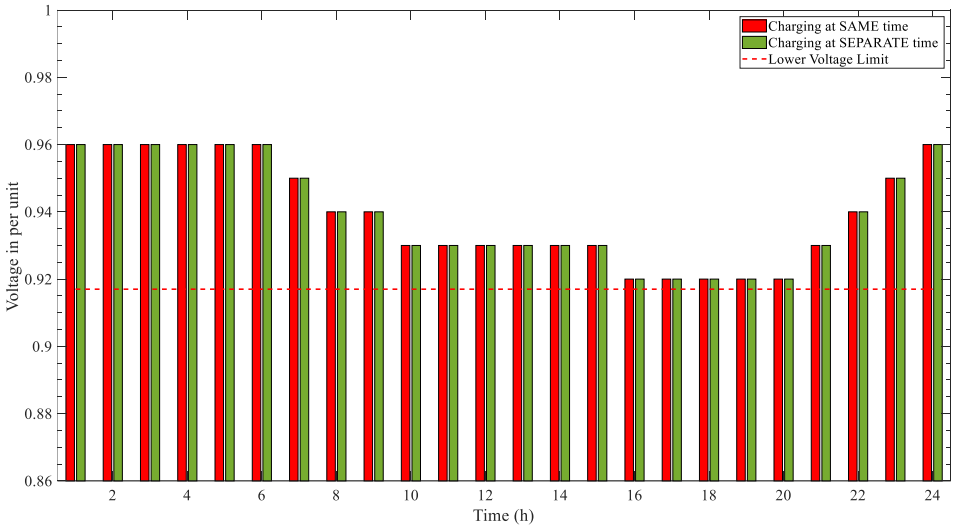

Figure 5-50 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2

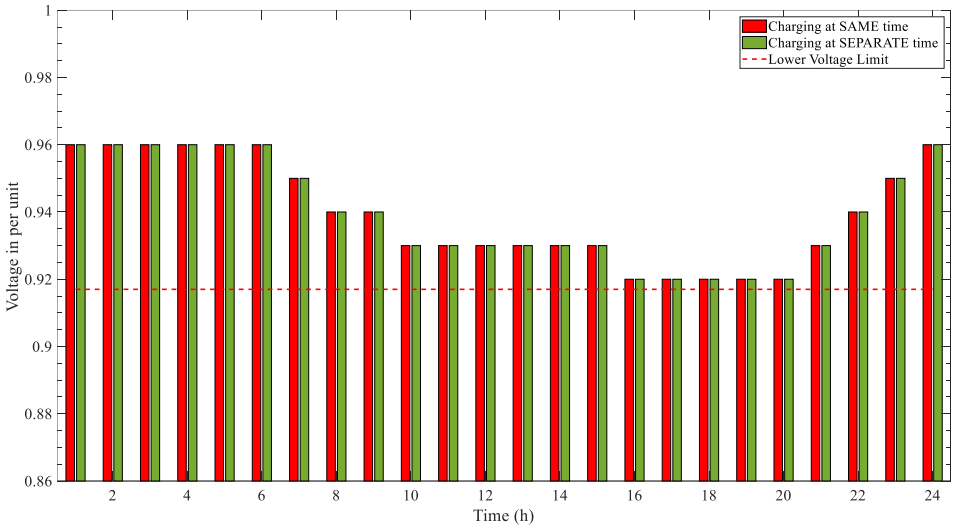

Figure 5-51 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2

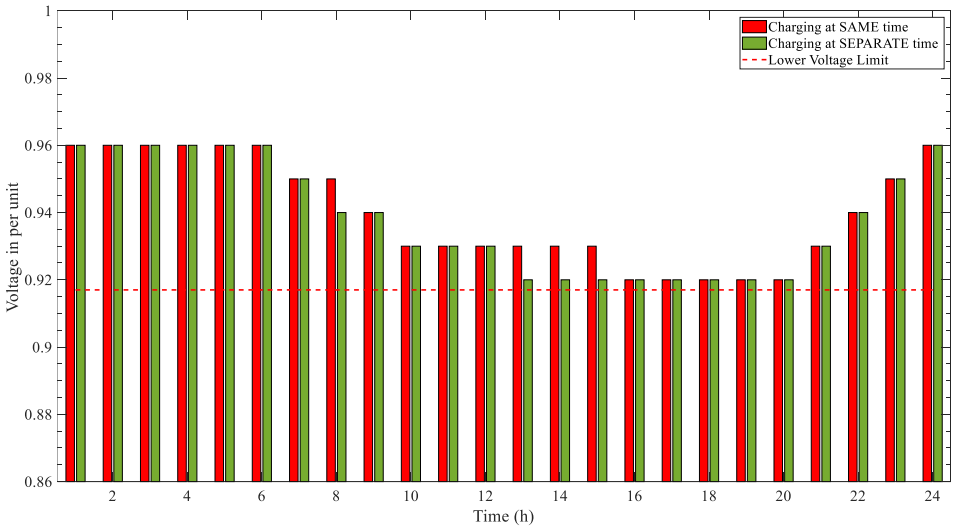

Figure 5-52 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times at 9.6kW rated power according to Mitigation Technique #2

5.6.2.12 Mitigation Technique #2 – Undervoltage at 7.7kW Charging Rate

According to Figure 5-53, Figure 5-54, and Figure 5-55, corresponding to Attack #1, Attack #2, and Attack #3 respectively, identifies the Mitigation Technique #2 utilized with the charging rate of 7.7kW for both SAME and SEPARATE charging times. From the result of the mitigation, it can be concluded that the 7.7kW along with the different charging times successfully mitigated all the impacts of the cyberattacks for all three attacks for the undervoltage in the smart grid. All results identify the voltage profile to be above the lower voltage limit and therefore is not violating the voltage level set by the standards. Comparing to the 11.5kW and 9.6kW charging rate, the voltage profile remains the same and no change can be observed during the 18th to 20th hours.

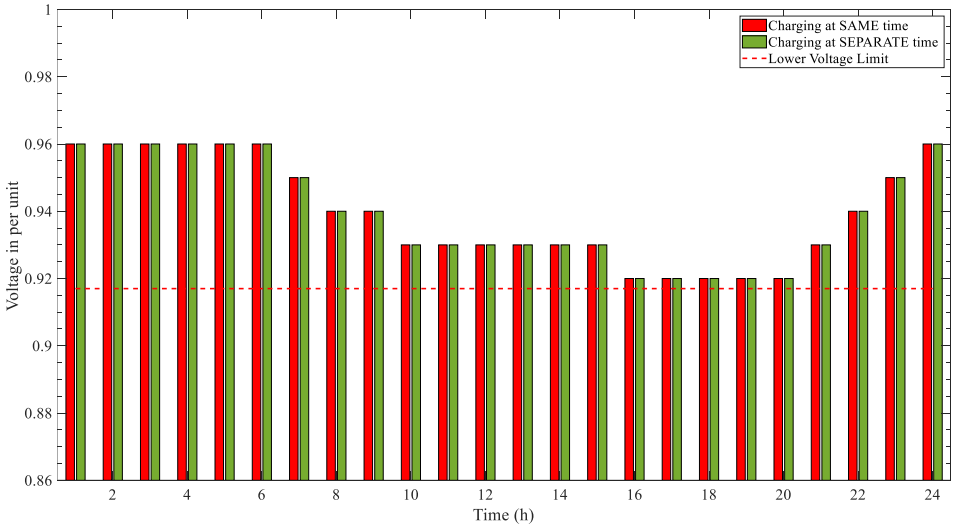

Figure 5-53 - 24-hour Voltage Profile for Attack #1 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

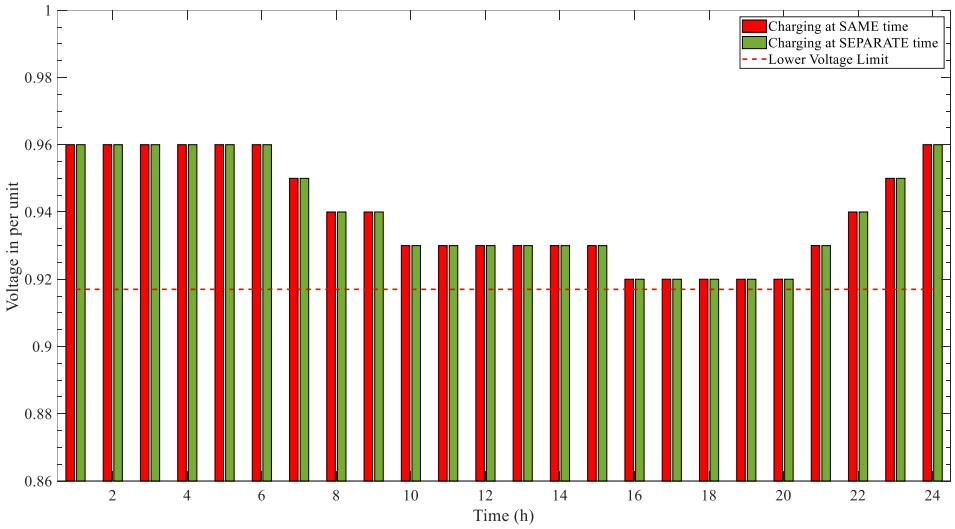

Figure 5-54 - 24-hour Voltage Profile for Attack #2 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

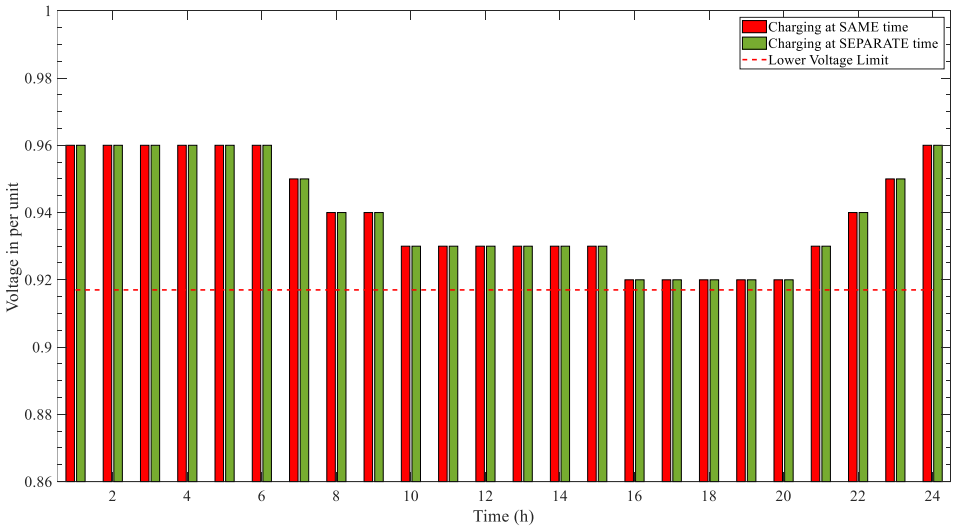

Figure 5-55 - 24-hour Voltage Profile for Attack #3 with SAME and SEPARATE charging times at 7.7kW rated power according to Mitigation Technique #2

Chapter 6 Conclusion

Electric Vehicles and Fast Charging Stations have grown tremendously over the upcoming years in the new era of electrification. This new era in electrification comes with many benefits toward the environment as it provides enormous benefits towards global climate change and reducing the greenhouse gasses. On the other hand, it also comes with many challenges toward the smart grid. With the large-scale growth on EVs, there has been a greater demand for the FCS of HP-FCS as well. The more EVs that can be seen on the roads result in a similar trend and growth in charging infrastructure to keep up with consumer demands. The concept of cybersecurity is introduced because, in this new era of electrification, the traditional grid is evolving into a smart grid. The introduction of the smart grid allows for much better communication between all the assets and components in the grid and allows for much more robust monitoring. This also brings challenges, and cyber threats can impact the smart grid directly or indirectly via other assets, components, or consumers who may unknowingly compromise the network.

Cybersecurity has become a much-needed priority in this new era of electric vehicles, and methods need to be developed to detect, target, and mitigate the threats to the smart grid. Cyber threats come in various forms of cyber-physical attacks, but this thesis focuses on Denial-of-Service attacks. Since the lack of charging also impacts the smart grid as the power that is expected to be consumed at a given time does not happen, then it leads to other situations during other times. If the allocation of power is high for a given period of time and a cyber threat manages to block that power demand from being transferred, then that excess power leads to many problems in the grid on both the consumer and provider end.

Therefore, this research focuses on the DoS-based attack on the isolated microgrid, which is one of the critical components of the smart grid. The isolated microgrid test system was modeled in MATLAB SIMSCAPE to act as a standalone system. The DoS attacks were grouped into three categories based on the driving patterns of people from home to work and comparing them to the charging times and patterns. The simulated cyberattacks targeted different groups of people on a short or long commute to see the impacts of the EVs on the microgrid and its components. Focusing on the microgrid system, the timing when charging EVs occurs, and for how long is very important as during a certain time, you expect a higher power output versus other times in the day. Therefore, if a DoS occurs, the power that needs support later on may not be physically available in the system at that given time. This results in a power imbalance and causes several problems in the microgrid, such as affecting the consumers who are trying to charge their vehicle and the system components are affected.

This research showed that when a cyber-physical attack took place under the three attack types, Attack #1, Attack #2, and Attack #3, there were impacts to the smart grid. The impact started with the transformer overload in the microgrid, which supplied power to the microgrid and its components. The transformer overload became the most significant impact because when the cyberattack targeted the vehicles by denying them to charge in the morning at work (both short or longer-duration cases), the impact was seen during the evening. The impact of the cyberattack didn't result in a transformer overload instantaneously; instead, it created a major overload occurring from the 18^{th} to the 20^{th} hour of the evening when everyone got home and plugged their vehicles to charge. Since certain vehicles were affected by the cyberattacks and could not charge during the morning, it

required them to charge for a lot longer during the evening, which created an unnecessary overload on the transformer. Also, projecting the growth of EVs, multiple EV penetration levels were targeted to make the research applicable in the future in terms of cybersecurity. The impacts of the transformer overload doubled when the EV penetration levels were doubled in the simulated microgrid. The impact of the transformer overload was measured when the maximum rated capacity limit of the transformer exceeded during a certain hour.

The second impact related to the transformer was the temperature curve of the transformer (*Theta H* curve), which was a direct result of the transformer overload. Since the temperature of the transformer has certain requirements, which are based on the current transformer load profile, it is in direct relation to the transformer overload. As the overload increases, the temperature does as well. For each of the cyberattacks that were simulated, the results showed that the Theta H curve resulted in a similar trend of increasing the transformer overload. The one differentiation factor is the temperature in the transformer does not rise or drop instantaneously, which was clearly seen in the results as the impact of temperature lasted even after the overload had ended.

The third impact was related to the bus voltage and the voltage profile experienced by the components of the microgrid. The bus voltage showed an effect of undervoltage after the effects of cyberattacks. The undervoltage also occurred during the 18^{th} to 20^{th} hour of the evening when the power demand rose drastically; it caused the voltage to drop below the rated lower limit as per the ANSI standards. The undervoltage may not be a noticeable issue at first. When it lasts for longer durations, consumers are affected as homes, devices, and all power-consuming equipment require a certain voltage level to operate. If the voltage level deviates from the norm it is still acceptable. But when the voltage deviation occurs

very significantly for a longer duration then you are experiencing an undervoltage since is way below the recommend and rated lower limit of the bus voltage.

All these impacts of the smart grid are very serious when it comes to cybersecurity in the smart grid. These cyber-physical attacks cause long term damage when it come to the transformer for example. Since the transformer experiences an overload and an increase in the Theta H curve for a significant period of time, then this impacts the loss of the life of the transformer. This is the value that determines the life of a transformer based on the average load it handles every day and the amount of overload it sustains as well. When several years are quickly removed from the transformer's life then it will result in millions of dollars of damages as you will need to change it much earlier than expected. These costs will endure more costs for the consumers and the providers as well. The undervoltage situation can affect homes but in commercial plants, voltage levels are crucial for manufacturing for example. If system experiences multiple hours of undervoltage it will result in loss of the consumer and commercial business who will turn to the utility provider to pay for the damages. Overall, the impacts of the cyberattacks are important and should not be taken lightly as it comes with many impacts as time passes.

On the other hand, keeping these impacts in mind, mitigation techniques were discussed on how to best handle the cyberattacks and lower the impacts it causes on the smart grid. The research showed two mitigation techniques where the first focused on the breaking the charging times to multiple hours to lower the initial peak that system endured when the consumers got home to charge their vehicle after a cyberattack. The idea of same charging where all vehicles come in and start charging at 18^{th} hour was compared to the idea of separate charging where shorter duration vehicles charge at 18^{th} hour and longer

duration vehicles start charging at 19th hour. The mitigation technique showed that the separate charging definitely reduced the initial peak that occurred in all the impacts identified of the cyberattacks but it did not complete eliminate or remove the impacts at all. Therefore, a second mitigation technique was utilized where using the idea of same versus separate charging times, another factor was added on, which was the charging power of the EV chargers. In this mitigation, the original charging occurred at 40kW chargers but by reducing the charging power to 11.5kW, 9.6kW and 7.7kW respectively and hence it was able to eliminate the impacts of the cyberattacks on the microgrid. The impact of the transformer overload was not completed eliminated until the charging power was reduced completely to 7.7kW where the Theta H curve and the undervoltage were able to be mitigated at the 11.5kW charging power. There are direct connections between the impacts of but some impacts take a longer time to manifest versus some are instantaneous.

In conclusion, the research shows the impacts of cyberattacks on the security of the smart grid. The thesis focused on the electric vehicles and the fast-charging stations utilized for charging EVs and its impacts from the cyberattacks on them. The thesis also focused on how the intruder was able to gain access to this by utilizing the OCPP protocol between the EVs and the FCS. The research showed from start to finish the path of the cyberattack its impact on the smart grid and its components. The results were clear and showed the relationship between the impacts on the microgrid and cyberattacks. At last, cybersecurity needs an upcoming new research topic that needs to be address with electrification of the EVs and FCS everywhere.

References

[1] "The EV revolution is here," 2021. [Online]. Available: https://www.theclimategroup.org/media/7946/download

[2] IEA, "Trends in charging infrastruture," in "The Internation Energy Agency (IEA)," 2022. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2022/trends-in-charging-infrastructure

[3] "New motor vehicle registrations, 2021," Statistics Canada, 2022. [Online]. Available: https://www.statcan.gc.ca/en/topics-start/automotive

[4] F. Richter. "Global Electric Car Sales Doubled in 2021." https://www.statista.com/chart/26845/global-electric-car-sales/ (accessed 2022).

[5] L. McDonald, "Comparing the Ratio of EV Charging Stations Versus Gas Stations." [Online]. Available: https://evadoption.com/stat-of-the-week-comparing-the-ratio-of-ev-charging-stations-versus-gas-stations-evs-win/

[6] O. V. N. Manji, and E. Fusaro. "Accelerating Canada's electric vehicle transition." PwC. https://www.pwc.com/ca/en/industries/automotive/publications/accelerating-canadas-electric-vehicle-transition.html (accessed 2022).

[7] N. R. Canada. "Zero Emission Vehicle Infrastructure Program." Government of Canada. https://www.nrcan.gc.ca/energy-efficiency/transportation-alternative-fuels/zero-emission-vehicle-infrastructure-program/21876 (accessed 2022).

[8] "Ontario Boosting Electric Vehicle Charging Availability," ed: news.ontario.ca, 2021.

[9] "Ivy Charging Network." Canadian Electricity Association. https://electricity.ca/lead/centre-of-excellence/ivy-charging-network/ (accessed 2022).

[10] M. Rabson, "Canada needs to build millions — not thousands — of EV charging stations, industry group says," in *The Canadian Press*, ed: CBC, 2021.

[11] G. Angelov, M. Andreev, and N. Hinov, "Modelling of Electric Vehicle Charging Station for DC Fast Charging," in *2018 41st International Spring Seminar on Electronics Technology (ISSE)*, 16-20 May 2018 2018, pp. 1-5, doi: 10.1109/ISSE.2018.8443663.

[12] IEA, "Charging points per EV and kW per electric LDV in selected countries, 2021," ed. Paris: IEA, 2021.

[13] G. P. d. Azevedo, P. C. Pellanda, and M. B. Campos, "Addressing the Cybersecurity Challenges of Electrical Power Systems of the Future," in *2020 12th International Conference on Cyber Conflict (CyCon)*, 26-29 May 2020 2020, vol. 1300, pp. 293-308, doi: 10.23919/CyCon49761.2020.9131732.

[14] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1-29, 2016.

[15] S. Acharya, Y. Dvorkin, H. Pand, x017E, x, and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol. 8, pp. 214434-214453, 2020, doi: 10.1109/ACCESS.2020.3041074.

[16] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications,* vol. 1, no. 1, pp. 13-27, 2016.

[17] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "'Cyber-attack against Ukrainian critical infrastructure'." [Online]. Available: https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01

[18] M. Zeller, "Common Questions and Answers Addressing the Aurora Vulnerability," Schweitzer Engineering Laboratories, Inc, 2011.

[19] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Transactions on Smart Grid,* vol. 4, no. 1, pp. 235-244, 2013.

[20] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580-591, 2014.

[21] B. V. Solanki, K. Bhattacharya, and C. A. Cañizares, "A Sustainable Energy Management System for Isolated Microgrids," *IEEE Transactions on Sustainable Energy*, vol. 8, no. 4, pp. 1507-1517, 2017, doi: 10.1109/TSTE.2017.2692754.

[22] Natural Resources Canada, "The First Canadian Smart Remote Microgrid: Hartley Bay, BC." [Online]. Available: https://www.nrcan.gc.ca/maps-tools-publications/publications/energy-publications/technology-research-publications/first-canadian-smart-remote-microgrid-hartley-bay-bc/14421

[23] Natural Resources Canada, "Microgrids in Canada Overview." [Online]. Available: http://microgrid-symposiums.org/

[24] Electricity Canada. "Microgrid." https://www.electricity.ca/programs/centre-of-excellence/the-lac-megantic-microgrid/ (accessed 2022).

[25] M. o. E.-. Ontario. "Microgrids." https://www.ontario.ca/document/projects-funded-smart-grid-fund/microgrids (accessed 2022).

[26] S. Pullins, "Why microgrids are becoming an important part of the energy infrastructure," *The Electricity Journal*, vol. 32, no. 5, pp. 17-21, 2019/06/01/ 2019, doi: https://doi.org/10.1016/j.tej.2019.05.003.

[27] C. Huang, S. Thareja, and Y. Shin, "Wavelet-based Real Time Detection of Network Traffic Anomalies," in *2006 Securecomm and Workshops*, 28 Aug.-1 Sept. 2006 2006, pp. 1-7, doi: 10.1109/SECCOMW.2006.359584.

[28] C. M. Akujuobi, N. K. Ampah, and M. N. O. Sadiku, "Application of Wavelets and Self-similarity to Enterprise Network Intrusion Detection and Prevention Systems," in *2007 IEEE International Symposium on Consumer Electronics*, 20-23 June 2007 2007, pp. 1-6, doi: 10.1109/ISCE.2007.4382163.

[29] W. Lu, M. Tavallaee, and A. A. Ghorbani, "Detecting Network Anomalies Using Different Wavelet Basis Functions," in *6th Annual Communication Networks and Services Research Conference (cnsr 2008)*, 5-8 May 2008 2008, pp. 149-156, doi: 10.1109/CNSR.2008.75.

[30] M. L. Laboratory. *1999 DARPA INTRUSION DETECTION EVALUATION DATASET*.

[31] H. Wu and S. S. Huang, "Performance of Neural Networks in Stepping-Stone Intrusion Detection," in *2008 IEEE International Conference on Networking, Sensing and Control*, 6-8 April 2008 2008, pp. 608-613, doi: 10.1109/ICNSC.2008.4525290.

[32] R. Renk, L. Saganowski, W. Holubowicz, and M. Choras, "Intrusion Detection System Based on Matching Pursuit," in *2008 First International Conference on Intelligent Networks and Intelligent Systems*, 1-3 Nov. 2008 2008, pp. 213-216, doi: 10.1109/ICINIS.2008.68.

[33] G. Kaur, V. Saxena, and J. P. Gupta, "Anomaly Detection in network traffic and role of wavelets," in *2010 2nd International Conference on Computer Engineering and Technology*, 16-18 April 2010 2010, vol. 7, pp. V7-46-V7-51, doi: 10.1109/ICCET.2010.5485392.

[34] M. Salagean and I. Firoiu, "Anomaly detection of network traffic based on Analytical Discrete Wavelet Transform," in *2010 8th International Conference on Communications*, 10-12 June 2010 2010, pp. 49-52, doi: 10.1109/ICCOMM.2010.5509071.

[35] M. Salagean, "Real network traffic anomaly detection based on Analytical Discrete Wavelet Transform," in *2010 12th International Conference on Optimization of Electrical and Electronic Equipment*, 20-22 May 2010 2010, pp. 926-931, doi: 10.1109/OPTIM.2010.5510445.

[36] R. P. d. Azevedo, B. Mozzaquatro, A. Kozakevicius, R. C. Nunes, C. Cappo, and C. Schaerer, "DoS attack detection using a two dimensional wavelet transform," in *2012 XXXVIII Conferencia Latinoamericana En Informatica (CLEI)*, 1-5 Oct. 2012 2012, pp. 1-8, doi: 10.1109/CLEI.2012.6427250.

[37] S. Pukkawanna, H. Hazeyama, Y. Kadobayashi, and S. Yamaguchi, "Investigating the utility of S-transform for detecting Denial-of-Service and probe attacks," in *The*

International Conference on Information Networking 2014 (ICOIN2014), 10-12 Feb. 2014 2014, pp. 282-287, doi: 10.1109/ICOIN.2014.6799482.

[38] Z. Chen, C. K. Yeo, B. S. L. Francis, and C. T. Lau, "A MSPCA based intrusion detection algorithm tor detection of DDoS attack," in *2015 IEEE/CIC International Conference on Communications in China (ICCC)*, 2-4 Nov. 2015 2015, pp. 1-5, doi: 10.1109/ICCChina.2015.7448617.

[39] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Frequency based DDoS attack detection approach using naive Bayes classification," in *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*, 27-29 June 2016 2016, pp. 104-107, doi: 10.1109/TSP.2016.7760838.

[40] C. Callegari, S. Giordano, and M. Pagano, "Anomaly detection: An overview of selected methods," in *2017 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, 18-22 Sept. 2017 2017, pp. 52-57, doi: 10.1109/SIBIRCON.2017.8109836.

[41] Z. Pan, J. Pacheco, and S. Hariri, "Anomaly behavior analysis for building automation systems," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 29 Nov.-2 Dec. 2016 2016, pp. 1-8, doi: 10.1109/AICCSA.2016.7945692.

[42] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469-482, 2018.

[43] Y. Wadhawan, A. AlMajali, and C. Neuman, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, no. 10, p. 249, 2018.

[44] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847-855, 2013, doi: 10.1109/TSG.2012.2226919.

[45] B. Li, R. Lu, W. Wang, and K. R. Choo, "DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415-2425, 2016, doi: 10.1109/TIFS.2016.2576898.

[46] P. Jokar, "Model-based intrusion detection for home area networks in smart grids," *University of Bristol*, pp. 1-19, 2012.

[47] F. M. Tabrizi and K. Pattabiraman, "A Model-Based Intrusion Detection System for Smart Meters," in *2014 IEEE 15th International Symposium on High-Assurance Systems Engineering*, 9-11 Jan. 2014 2014, pp. 17-24, doi: 10.1109/HASE.2014.12.

[48] "Smart Energy Group." https://www.smart-energygroup.com/ (accessed 2022).

[49] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452-2459, 2017, doi: 10.1109/TSG.2017.2669647.

[50] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the

Open Charge Point Protocol (OCPP)," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1504-1533, 2022, doi: 10.1109/COMST.2022.3184448.

[51] O. C. Alliance, "Open Charge Point Protocol 1.6," *Open Charge Alliance*, September 28, 2017.

[52] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 26-28 Feb. 2018 2018, pp. 1-5, doi: 10.1109/NTMS.2018.8328675.

[53] *IEC 62351 – Cyber Security Series for the Smart Grid*, IEC, 2022. [Online]. Available: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/

[54] B. Vaidya and H. T. Mouftah, "Deployment of Secure EV Charging System Using Open Charge Point Protocol," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 25-29 June 2018 2018, pp. 922-927, doi: 10.1109/IWCMC.2018.8450489.

[55] D. Devendra, S. Malkurthi, A. Navnit, and A. M. Hussain, "Compact Electric Vehicle Charging Station using Open Charge Point Protocol (OCPP) for E-Scooters," in *2021 International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*, 21-23 Jan. 2021 2021, pp. 1-5, doi: 10.1109/SeFet48154.2021.9375812.

[56] S. Misra, P. K. Panigrahi, and S. Ghosh, "Smart Battery Management Scheme for V2G Based EV Smart Charger – A Better approach of Allocation of EV Based Distributed Generation," in *2020 IEEE International Symposium on Sustainable*

Energy, Signal Processing and Cyber Security (iSSSC), 16-17 Dec. 2020 2020, pp. 1-6, doi: 10.1109/iSSSC50941.2020.9358817.

[57] C. D. Parker, "APPLICATIONS – STATIONARY | Energy Storage Systems: Batteries," in *Encyclopedia of Electrochemical Power Sources*, J. Garche Ed. Amsterdam: Elsevier, 2009, pp. 53-64.

[58] N. Bhusal, M. Gautam, and M. Benidris, "Cybersecurity of Electric Vehicle Smart Charging Management Systems," in *2020 52nd North American Power Symposium (NAPS)*, 11-13 April 2021 2021, pp. 1-6, doi: 10.1109/NAPS50074.2021.9449758.

[59] S. Dey and M. Khanra, "Cybersecurity of Plug-In Electric Vehicles: Cyberattack Detection During Charging," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 1, pp. 478-487, 2021, doi: 10.1109/TIE.2020.2965497.

[60] S. Acharya, Y. Dvorkin, and R. Karri, "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099-5113, 2020, doi: 10.1109/TSG.2020.2994177.

[61] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet-Based Vehicle-to-Grid Technology Framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4425-4435, 2020, doi: 10.1109/TIA.2020.2966160.

[62] L. Guo *et al.*, "Systematic Assessment of Cyber-Physical Security of Energy Management System for Connected and Automated Electric Vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3335-3347, 2021, doi: 10.1109/TII.2020.3011821.

[63] D. Reeh, F. C. Tapia, Y. W. Chung, B. Khaki, C. Chu, and R. Gadh, "Vulnerability Analysis and Risk Assessment of EV Charging System under Cyber-Physical Threats," in *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*, 19-21 June 2019 2019, pp. 1-6, doi: 10.1109/ITEC.2019.8790593.

[64] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform," *IEEE Access*, vol. 9, pp. 29429-29440, 2021, doi: 10.1109/ACCESS.2021.3059042.

[65] K. Kaur, G. Kaddoum, and S. Zeadally, "Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5178-5189, 2021, doi: 10.1109/TITS.2021.3068092.

[66] Z. Pourmirza and A. Srivastava, "Cybersecurity Analysis for the Communication Protocol in Smart Grids," in *2020 IEEE 8th International Conference on Smart Energy Grid Engineering (SEGE)*, 12-14 Aug. 2020 2020, pp. 58-63, doi: 10.1109/SEGE49949.2020.9182015.

[67] O. C. Alliance, "OPEN SMART CHARGING PROTOCOL 1.0," *Open Charge Alliance*. [Online]. Available: https://www.openchargealliance.org/protocols/oscp-10/

[68] E. Foundation, "Open Charge Point Interface." [Online]. Available: https://evroaming.org/

[69] *SteVe*. (2007). RWTH Aachen University. [Online]. Available: https://github.com/RWTH-i5-IDSG/steve

[70] A. Lantero, "How Microgrids Work." [Online]. Available: https://www.energy.gov/articles/how-microgrids-work

[71] "The Role of Microgrids in Helping to Advance the Nation's Energy System." [Online]. Available: https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/role-microgrids-helping

[72] National Cyber Security Centre. (2020). *Denial of Service (DoS) guidance*. [Online] Available: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

[73] M. E. Hariri, T. A. Youssef, A. Hariri, and O. A. Mohammed, "Microgids on Wheels: Not to Leave Security Behind," *IEEE Newsletter*. [Online]. Available: https://tec.ieee.org/newsletter/june-2016/microgids-on-wheels-not-to-leave-security-behind

[74] G. S. Morrison, "Threats and mitigation of DDoS cyberattacks against the US power grid via EV charging," Wright State University, 2018.

[75] "Tools for electric vehicle drivers in North America | ChargeHub." https://chargehub.com/en/ (accessed 2022).

[76] "EVSE | Electric Vehicle (EV) Charging Stations - ChargePoint." https://www.chargepoint.com/en-ca (accessed 2022).

[77] "Chargeway." https://www.chargeway.net/ (accessed 2022).

[78] "Evgo." https://www.evgo.com/ (accessed 2022).

[79] "PlugShare - EV Charging Station Map - Find a place to charge." https://www.plugshare.com/ (accessed 2022).

[80] "Open Charge Map, 2022." https://openchargemap.org/site (accessed 2022).

[81] Tesla. "Supercharger | Tesla." https://www.tesla.com/en_ca/supercharger (accessed 2022).

[82] M. Stadler and A. Nasle, "Planning and implementation of bankable microgrids," *The Electricity Journal*, vol. 32, 05/01 2019, doi: 10.1016/j.tej.2019.05.004.

[83] "IEEE Guide for Loading Mineral-Oil-Immersed Transformers and Step-Voltage Regulators," *IEEE Std C57.91-2011 (Revision of IEEE Std C57.91-1995)*, pp. 1-123, 2012, doi: 10.1109/IEEESTD.2012.6166928.

[84] *Temperature change in Canada*. [Online] Available: https://www.canada.ca/en/environment-climate-change/services/environmental-indicators/temperature-change.html

[85] T. Gonen, *Electric Power Distribution Engineering*. CRC Press, 2015.

[86] *American National Standard for Electric Power Systems and Equipment—Voltage Ratings (60 Hz)*, ANSI C84.1-2020, N. E. M. Association, 2020.

[87] "VOLTAGE TOLERANCE STANDARD – ANSI C84.1." [Online]. Available: https://voltage-disturbance.com/voltage-quality/voltage-tolerance-standard-ansi-c84-1/.

[88] MathWorks, "24-hour Simulation of a Vehicle-to-Grid (V2G) System." [Online]. Available: https://www.mathworks.com/help/physmod/sps/ug/24-hour-simulation-of-a-vehicle-to-grid-v2g-system.html;jsessionid=74cb6bdbf8be8c435dd9eb2d889d

[89] T. M. Inc, "Tesla Model S Electric Vehicle Catalog." [Online]. Available: https://www.tesla.com/sites/default/files/tesla-model-s.pdf

[90] *Environment Canada, Canadian Weather Energy Engineering Datasets (CWEEDS)*. [Online]. Available: http://climate.weather.gc.ca/prods_servs/engineering_e.html

[91] *NSRDB: National Solar Radiation Database*. [Online]. Available: https://nsrdb.nrel.gov/

[92] Tesla. "Home Charging Installation - Wall Connector." https://www.tesla.com/en_CA/support/home-charging-installation/wall-connector (accessed 2022).