# Congestion Management in Active Distribution Networks and its Cyber Security

by

Omniyah Gul M Khan

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2023

© Omniyah Gul M Khan 2023

**Examining Committee Membership**

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

| | |
|---|---|
| Supervisor: | Ehab El-Saadany<br>Professor |
| Co-Supervisor: | Magdy Salama<br>Professor |
| Internal Examiner: | Fakhri Karray<br>Professor |
| Internal Examiner: | Ramadan ElShatshat<br>Lecturer |
| Internal-External Examiner: | Kumaraswamy Ponnambalam<br>Professor |
| External Member: | Bala Venkatesh<br>Professor |

## Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

## Abstract

The evolution of the Traditional Power Grid (TPG) to the digital smart grid is expected to improve the operation of the power system. The smart grids' capability to support various distributed generation technologies, self-healing capacity, and ability to minimize operational costs are some of its benefits. However, distribution networks are facing congestion challenges due to the increased number of flexible loads and Distributed Energy Resources (DER)s being used. Moreover, the dependence of such technologies on uncontrollable factors, such as temperature, wind speed, solar radiation, etc., may result in potential congestion problems which were not of concern in the past within the distribution network. This is due to the high power consumption of active loads and the weakening correlation between electricity prices and demand resulting from the increased penetration level of intermittent Renewable Energy Source (RES)s. Such congestion results in voltage violations and/or thermal overloading as a result of the power flow exceeding a network asset's transfer capability, possibly damaging devices such as distribution transformers and feeders. Rather than incurring a huge cost to reinforce the network assets, the Distribution Network Operator (DNO) can use Demand Side Management (DSM) to motivate consumers to shift their load from peak to off-peak times. However, congestion management methods based on DSM rely on communication between DNO, aggregators, and consumers meters to encourage customers to make some corrective actions, such as peak shifting, peak clipping, and valley filling, to relieve congestion. Cyber attacks against aggregators can compromise the operation of DSM-based congestion management methods, and hence, affect the security and reliability of electrical networks. The congestion management schemes become useless in the event of a cyber attack and can instead result in increase in network congestion. The vulnerability of DSM-based congestion management methods to Load Altering Attack (LAA)s is hence studied to determine the cyber weaknesses in the DSM protocols. An optimization algorithm is developed to determine which aggregators a cyber attacker would compromise in order to cause congestion by minimally altering their load profiles. The impact of such attacks on congestion and consumers' electricity bill is then studied. A mitigation scheme is formulated to determine the most critical aggregators in the network. The security of these aggregators is then reinforced to mitigate such cyber attacks. Also, a detection technique is proposed using Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN)s. By securing the aggregators, the DSM congestion management schemes can be effective in alleviating congestion in the distribution network.

Given a cyber secure network, to minimize consumers' electricity cost and decrease the Peak to Average Ratio (PAR) of the load curve to a required level that alleviates existing

congestion, a multi-objective optimization is proposed to schedule flexible loads. This results in a consumer load schedule that is economical and does not require the imposition of congestion tariffs. However, the success of the proposed congestion management scheme relies on the accuracy of the consumer load consumption. Hence, uncertainty analysis of consumers' flexible load schedule is executed to ensure the desired robustness of the power flowing in the distribution network to changes in uncertain variables. The results obtained are compared with the existing congestion management scheme demonstrating the advantage of the proposed multi-objective framework in terms of decreasing price and flattening the load curve while alleviating congestion. However, it should be noted that modeling distributed energy resources is not an easy task as they rely on uncertain factors which are hard to predict. It is very challenging to design a congestion management scheme given the uncertainty of such flexible loads consumption and electricity prices. Obtaining stochastic models for such loads may not be easily available in practice. To overcome this challenge, a Deep Deterministic Policy Gradient (DDPG) Reinforcement Learning (RL) scheme is proposed to alleviate congestion. DDPG RL is a model-free technique that does not require explicit probabilistic models of the controllable loads to determine the change in electricity prices needed, in the form of tariffs and/or subsidies. The DDPG RL technique is compared with the existing model-based congestion management scheme and the results obtained demonstrate the outperformance of the proposed technique in terms of electricity cost and PAR of the load profiles.

Aggregators load schedules utilizing the day-ahead congestion management schemes are used in the real-time market. However, this does not eliminate the possibility of having congestion in the real-time market. The electrification of the transportation system is double-edged for the smart grid. Although it is green and eco-friendly, uncontrolled charging of electric vehicles (EV) could cause not only distribution network congestion, but also long queues at the charging stations. Hence, it is necessary to ensure existing charging resources are efficiently utilized. An algorithm is hence developed that assigns EVs to charge stations such that distribution network congestion and time spent by the user from requesting a charging service to accessing it is minimized. The Lyapunov function is utilized for developing an EV assignment algorithm to manage a dynamic population of EVs ensuring queuing stability. Moreover, as the EV assignment algorithm relies on the communication network, an intrusion cyber-attack can occur resulting in an unstable queuing system. An intrusion detection technique is, hence, proposed which utilizes existing transportation network sensor data with the EV charging stations operator information to detect such attacks.

IEEE 33 bus system is used as a case study to demonstrate the effectiveness of all the proposed techniques compared to the existing models.

**Acknowledgements**

Praise be to Allah, the most Gracious and Merciful, for providing me the strength and perseverance to complete this thesis successfully. I would like to express my sincere gratitude and appreciation to several people who have been instrumental, either directly or indirectly, to make this work possible. Thanks to my supervisors Dr. Ehab El Saadany and Dr. Magdy Salama, as well as my collaborator Dr. Amr Youssef, who generously shared their time, experience, wisdom, knowledge, and most importantly, their advice with me.

It is difficult to overstate my gratitude to my mentor, Dr. Ehab El Saadany, who took the biggest risk in accepting me as a Ph.D. student though I came from a different field. Dr. Ehab would always treat me like one of his daughters and would ensure that I have his complete support when life brought its ups and downs. I still remember when I was out of babysitting options and I had to bring my 2-year-old son to our weekly meetings. Dr. Ehab went on playing with my son while I presented my progress to him. Throughout these years, he provided encouragement, sound advice, valuable teaching, and lots of great ideas. He taught me how to push myself to the maximum and was always ready to discuss any of my absurd ideas. I would have been lost without him.

Special thanks go to my co-advisor, Dr. Magdy Salama, for making this thesis possible. Meetings with him would inspire and motivate me to do better. He taught me how to be a better speaker and had confidence in me when I doubted myself.

Furthermore, I would like to thank my collaborator, Dr. Amr Youssef, for simply everything. He was always there to meet and talk about everything and anything and to proofread my work. He taught me how to push myself to the maximum and was always ready to discuss any of my absurd ideas. His support, dedication, and tendency to ask mind-boggling questions to help me think through my problems were invaluable assets. Besides my advisors, I would like to thank my thesis examiners, Dr.Fakhri Karray, Dr. Ramadan ElShatshat, Dr. Kumaraswamy Ponnambalam, and Dr. Bala Venkatesh for their time, effort, and valuable comments. Surely, I could have never seen the completion of this thesis without the constant support of my friends. Special thanks to my friend, Shereen Helal, who had played a pivotal role in supporting me from the beginning. Her cheerfulness in those long research days, her provocations throughout the day, and her ability to get me out of depression made my years memorable and unforgettable. I would like to thank also Maria Ossama, my so called "bump buddy" for her continuous believe that a day will come in which we will graduate. Just being able to pick up the phone and complain about work stress to her was a daily blessing. Also, I would like to thank Nancy Alaa Eldeen for her friendship and support. Just having people to talk to openly without

feeling judged or feeling stupid is a great gift. Thank you girls for being there and making UWaterloo amazing.

Last but not the least, no words can express my indebtedness to my family without whom none of this would have even been possible. To my amazing husband who encouraged me to sign and commit to a Ph.D. and got himself stuck in a fly-in and out job to make this a possibility: Thank you. To my lovely kids, Ibrahim and Taliyah: you were my stability point after a long hard day. Just looking at both of you re-energized me to face the next day. To my brother, Mohammed Ishaque, for encouraging me to be the first Ph.D. graduate in the family. It is you who inspired me to get into the program and it is you who indirectly motivated me to graduate. To my sister, Badria, for being an amazing role model for all of us: I don't think I can ever be like you. To my sister Abeer, your constant support with my responsibilities was invaluable, so thank you. To my youngest sibling, Yaquob: I will never forget the famous sentence that you use to encourage me when I used to get scared "if they can do it you can also do it and in fact excel in it". To mom, thanks for always being there, for being so understanding, so patient with my negligence and so loving. Lastly and most importantly, to my father, who devoted his entire life to making this a possibility. Without you dad, I would not be what I am today. I really wished you could have shared this success with me. This is dedicated to you, dear father, from your forever grateful daughter.

## Dedication

*This is dedicated to the memory of my father, Gul Mohammed Khan Noory. Though you never got to see this but you are the main reason every page of this thesis was ever written.*

# Table of Contents

**List of Tables** xiv

**List of Figures** xv

**List of Abbreviations** xviii

**1 Introduction** 1

1.1 Research Motivation . . . . . 2

1.2 Research Contribution and Objectives . . . . . 5

1.3 Dissertation Outline . . . . . 8

**2 Background and Literature Review** 11

2.1 Congestion Management in Distribution Networks . . . . . 12

2.1.1 Existing Indirect Control Congestion Management Schemes . . . . . 16

2.1.2 Congestion Management Using Valley-filling Schemes . . . . . 19

2.1.3 Limitations of Model-based Congestion Management Schemes . . . 20

2.2 Comparison Technique: Distributed Dynamic Tariff (DDT) . . . . . 22

2.2.1 Optimal Flexible Load Scheduling by Aggregators . . . . . 22

2.2.2 Calculation of Distributed Dynamic Tariff (DDT) by Network Operator 23

2.3 Cyber-Security of Congestion Management Schemes . . . . . 24

2.3.1 Smart Meters and their Cybersecurity . . . . . 26

2.4 Aggregators and their Cybersecurity . . . 29
2.4.1 Cyber-Attack Mitigation Schemes . . . 31
2.4.2 Cybersecurity Detection Schemes . . . 32

**3 Cyber Security of Market-based Congestion Management Methods in Power Distribution Systems 33**

3.1 Introduction . . . 33
3.2 Modeling of a Load Altering Cyber Attack . . . 36
3.2.1 Attack Model . . . 36
3.2.2 Load Altering Attacks (LAA) . . . 37
3.3 Case Study . . . 41
3.3.1 Choice of maximum scaling factor, $\gamma$ . . . 43
3.3.2 Creating and/or Increasing Congestion . . . 44
3.3.3 Hiding Congestion . . . 46
3.3.4 Computational Scalability . . . 50
3.4 Conclusions . . . 51

**4 Load Altering Attacks Mitigation Scheme 52**

4.1 Introduction . . . 52
4.2 Modeling of Mitigation Scheme . . . 53
4.2.1 Optimization Problem Formulation . . . 53
4.2.2 Linearization of the product of two variables . . . 54
4.2.3 Power Flow Equations Relaxation . . . 55
4.2.4 Using Generalized Bender Decomposition (Generalized Benders Decomposition (GBD)) . . . 57
4.3 Case Study . . . 61
4.3.1 Computational Scalability . . . 62
4.3.2 Discussion . . . 62
4.4 Conclusion . . . 63

**5 LSTM-based approach to detect cyber attacks on market-based congestion management methods** **64**

5.1 Introduction . . . 64

5.2 Case Study System Details . . . 65

5.3 Detection of LAA . . . 66

5.3.1 LSTM . . . 67

5.3.2 Data Preprocessing . . . 69

5.3.3 Results and Discussion . . . 70

5.4 Conclusions . . . 71

**6 Robust Multi-Objective Congestion Management in Distribution Network** **72**

6.1 Introduction . . . 72

6.2 Deterministic Multi-Objective Congestion Management Scheme . . . 74

6.2.1 Modeling Assumptions . . . 75

6.2.2 Flexible Loads . . . 75

6.2.3 Problem Formulation . . . 78

6.2.4 Determining Optimal Pareto Solution . . . 79

6.3 Developing a Robust Solution for the Proposed Congestion Management Scheme . . . 81

6.3.1 Identification of Uncertain Variables . . . 83

6.3.2 Sensitivity Analysis . . . 85

6.3.3 Robustness Enhancement of Proposed Scheme through Uncertainty Propagation . . . 87

6.4 Case Study, Results and Discussion . . . 88

6.4.1 Deterministic Multi-Objective Flexible Load Scheduling . . . 91

6.4.2 Robustness of the Proposed Multi-Objective Congestion Management Scheme . . . 95

6.5 Conclusions . . . 97

**7 Congestion Management in Distribution Networks Using Reinforcement Learning** **99**

7.1 Introduction . . . 99

7.2 Consumer Load Scheduling and Aggregation . . . 103

7.2.1 Consumer Flexible Load Scheduling . . . 103

7.2.2 Additive Secret Sharing Consumer Data Aggregation . . . 104

7.3 Reinforcement Learning Congestion Management System Design . . . 104

7.3.1 Formulation of the Markov Decision Process . . . 105

7.3.2 Training the DNO RL Agent . . . 107

7.4 Case Study . . . 109

7.4.1 Distribution Network . . . 109

7.4.2 Comparison Algorithm . . . 111

7.4.3 RL Training . . . 112

7.4.4 Testing Performance . . . 113

7.5 Conclusions . . . 119

**8 A Cyber-Secure Congestion-Aware Charging Station Assignment for EVs** **122**

8.1 Introduction . . . 122

8.2 System Model . . . 125

8.2.1 Distribution Network . . . 125

8.2.2 Transportation Network . . . 127

8.3 Problem formulation . . . 127

8.4 Solution methodology . . . 131

8.4.1 Day-ahead Residential Load Scheduling . . . 132

8.4.2 Linear Regression . . . 132

8.4.3 Real-time Electric Vehicle (EV) Assignment Algorithm . . . 133

8.5 Cyber Security of the Proposed Real-time EV Charging Assignment to False Data Injection Attack (FDIA) . . . 134

8.5.1 EV Assignment Model under FDIA . . . . . 136
8.5.2 Cyber Attack Intrusion Detection . . . . . 137
8.6 Case Study and Results . . . . . 137
8.6.1 Performance Comparison . . . . . 138
8.6.2 Results and Performance evaluation . . . . . 138
8.6.3 Impact of False Data Injection Cyber Attack . . . . . 140
8.6.4 Intrusion Detection . . . . . 141
8.7 Conclusions . . . . . 141

**9 Contributions and Conclusions** **154**
9.1 Summary and Conclusions . . . . . 154
9.2 Direction for Future Work . . . . . 156

**Bibliography** **158**

# List of Tables


2.1 Literature review of cyber security of consumers meters . . . . . 29

3.1 Residential Bus Loading . . . . . 43
3.2 Case Study parameters . . . . . 44
3.3 Effect of $\gamma$ on convergence time . . . . . 44
3.4 Aggregators compromised due to a LAA creating/increasing congestion . . 45
3.5 Aggregators compromised due to a LAA hiding congestion . . . . . 48
3.6 Computational Scalability of LAA . . . . . 51

4.1 Computational Scalability of Mitigation Scheme . . . . . 62

5.1 Confusion Matrix of LSTM-RNN Results . . . . . 70

6.1 Arrival and Departure Time Probability Density Function (PDF) Properties 85
6.2 Case study parameters . . . . . 89

8.1 Mean sensitivity, $\zeta_s$, of congestion (8.6) to changes in the load. . . . . 140

# List of Figures


1.1 Power and information flow under the (a) TPG, and (b) smart grid environments. . . . 3

1.2 Flowchart of the dissertation contributions. . . . 7

2.1 Power transfer between two voltage buses . . . 12

2.2 DSM Strategies: (a) Peak Clipping, (b) Load Shifting, and (c) Valley-Filling. 14

2.3 Comparison between the different existing congestion management schemes in the distribution network (a) Dynamic Tariff (DT), (b) DDT, and (c) Subsidy-based method. . . . 19

2.4 General RL Model . . . 21

2.5 Representation of DSM-based congestion management methods . . . 24

2.6 Operation of Advanced Metering Infrastructure (AMI) and customer control technologies [1] . . . 28

3.1 General representation of existing DSM-based congestion management methods . . . 34

3.2 Flowchart of cyber attack on DDT-congestion management method . . . 41

3.3 IEEE 33 bus system [1] . . . 42

3.4 Impact of a LAA on the loading of line 0-1 . . . 46

3.5 Impact of a positive attack value LAA on the electricity price . . . 47

3.6 Impact of a LAA aiming to hide congestion on line 0-1 . . . 49

3.7 Impact of LAA aiming to hide congestion on the electricity price . . . 50

4.1 High level flowchart of inputs and outputs of mitigation scheme . . . . . 55
4.2 Generalized Bender Decomposition Flowchart . . . . . 60

5.1 IEEE 33 bus system involving nine aggregators [1] . . . . . 66
5.2 Structure of an LSTM-RNN block . . . . . 68
5.3 Architecture of an unrolled LSTM-RNN . . . . . 69

6.1 Operation of (a) Air Source Heat Pumps (HPs) [2] and (b) Ground Source HPs [3] as a heater and cooler. . . . . 76
6.2 Flowchart for determining multi-objective Pareto weight and optimal consumer load schedule . . . . . 82
6.3 PDF of EV (a) arrival, and (b) departure times . . . . . 84
6.4 Day-ahead electricity price. . . . . 91
6.5 Pareto optimal front, ideal and nadir points . . . . . 92
6.6 Effect of varying multi-objective function weight, $\alpha$, on power flowing in main feeder . . . . . 93
6.7 Percentage congestion in the network versus electricity cost as a function of Pareto weight . . . . . 94
6.8 Comparison using proposed multi-objective load scheduling versus DDT congestion management scheme . . . . . 95
6.9 Sensitivity of the IEEE 33 bus system main feeder line loading to changes in EV power required . . . . . 96
6.10 Comparison between the robust and deterministic schemes in terms of power flowing in the main feeder . . . . . 97

7.1 Congestion Management in the Distribution Network using Reinforcement Learning . . . . . 115
7.2 Consumer Load Scheduling and Additive Secret Sharing Aggregation . . . 116
7.3 Reinforcement Learning Network Model . . . . . 116
7.4 IEEE 33 bus system [1] . . . . . 117
7.5 Episode Reward on Training RL+/- Agent using the combined tariff and subsidy action space . . . . . 117

7.6 Comparison of proposed congestion management scheme with existing DDT scheme in terms of (a) Electricity Cost, and (b) Peak-to-Average Ratio . . 118
7.7 Comparison of power flow without any congestion management versus implementing the proposed RL+/- model or the DDT scheme . . . . . 119
7.8 Comparison of electricity prices without any congestion management versus implementing the proposed RL+/- model or the DDT scheme . . . . . 120
7.9 Boxplot of the power flowing in the main feeder on testing the trained RL+/- model . . . . . 121

8.1 Proposed EV queuing model . . . . . 128
8.2 Cyber vulnerabilities in the EV charging process. . . . . 136
8.3 Architecture of Proposed Intrusion Detection System . . . . . 142
8.4 IEEE 33-bus system . . . . . 143
8.5 Mean assignment delay time . . . . . 143
8.6 Mean travelling time versus trade off parameter $w^d$ for various $w^l$ . . . . . 144
8.7 Power Flowing in Main Feeder of IEEE 33 bus system of proposed framework versus using nearest charging station assignment policy . . . . . 145
8.8 IEEE 33 load bus voltages for NCS versus proposed EV charging assignment model. . . . . 146
8.9 Comparison of average congestion, $\bar{c}$ . . . . . 147
8.10 Number of EVs charging in (a) Fast Charging Station (FCS) 1 and (b) FCS 4.148
8.11 Boxplot representation of queuing time in charging station for different rates of charging requests . . . . . 149
8.12 Comparison of Power Flowing in Main Feeder of IEEE 33 bus system of proposed framework in the presence and absence of FDIA . . . . . 150
8.13 Comparison of number of EVs charging in real time in (a) FCS 1 and (b) FCS 4 for FDIA scenario and not attacked scenario. . . . . 151
8.14 Boxplot representation of queuing time in charging station for different rates of charging requests . . . . . 152
8.15 Intrusion detector raising an alarm alerting the possibility of FDIA . . . . 153

# List of Abbreviations

**AMI** Advanced Metering Infrastructure xv, 26–28

**DDPG** Deep Deterministic Policy Gradient v, 6, 9, 20, 101, 102, 107, 109, 111, 120, 156

**DDT** Distributed Dynamic Tariff ix, xv, xvii, 16, 17, 19, 22, 23, 35, 36, 41, 43, 45, 46, 48, 65, 74, 92, 93, 100, 111, 113, 114, 118–120, 122, 155

**DER** Distributed Energy Resources iv, 31, 34, 64

**DNO** Distribution Network Operator iv, xii, 5, 13, 15–17, 19, 21–24, 26, 27, 30–37, 39, 42–45, 47, 48, 51, 53, 63–67, 70, 71, 78–81, 90, 100–102, 104, 105, 107, 109, 113, 122, 139, 140

**DoS** Denial of Service 25, 27, 29

**DSM** Demand Side Management iv, xv, 2, 4–6, 8, 9, 13, 15, 16, 24, 27, 30, 31, 33–35, 38, 63, 64, 72–74, 98, 100, 102, 119, 155–157

**DT** Dynamic Tariff xv, 16, 17, 19, 22, 30, 100, 122

**EV** Electric Vehicle xii, xiii, xvi, xvii, 1, 2, 6, 9, 11, 15, 19, 21, 30, 42, 44, 50, 63, 65, 66, 72, 73, 75, 77–79, 83–90, 93, 95, 96, 99, 100, 102, 104, 110, 111, 114, 122–129, 131–141, 146, 148, 151, 156, 157

**FCS** Fast Charging Station xvii, 123, 125, 127–129, 131–133, 136, 137, 139–141, 148, 151, 156

**FDI** False Data Injection 25, 27, 29, 31, 32, 35, 52

**FDIA** False Data Injection Attack xii, xiii, xvii, 125, 134, 136, 137, 140, 150, 151, 153, 156

**GBD** Generalized Benders Decomposition x, 31, 52, 53, 57, 59, 61, 62

**HAN** Home Area Network 36

**HEMS** Home Energy Management System 102, 103, 105

**HP** Heat Pump xvi, 2, 11, 42, 50, 65, 72, 73, 75–79, 85–88, 110, 112, 114, 122, 126, 137, 155

**ICT** Information and Communication Technology 1, 11

**ISOs** Independent System Operators 16

**LAA** Load Altering Attack iv, x, xi, xiv, xv, 9, 25–27, 29, 31, 35–38, 43–48, 50–53, 61–63, 65, 66, 155

**LMP** Locational Marginal Price 16

**LRA** Load Replay Attacks 26

**LRDA** Load Redistribution Attacks 25, 27

**LSTM** Long Short-Term Memory iv, xi, xiv, xvi, 6, 66–71, 155

**MINLP** Mixed Integer Non-Linear Programming 31, 37, 39, 40, 46, 52–54, 56, 57, 61, 62

**MSP** Mobility Service Provider 127, 133, 134, 136, 137, 139–141

**NAN** Neighborhood Area Network 15, 36

**NIST** National Institute of Standards and Technology 11, 24

**PAR** Peak to Average Ratio iv, v, 19, 73, 74, 92, 94, 111, 113, 114, 119, 120

**PDF** Probability Density Function xiv, xvi, 81, 83–85, 90, 96

**PV** Photovoltaic 2

**RES** Renewable Energy Source iv, 1, 2, 4, 11, 12, 21, 72, 156

**RL** Reinforcement Learning v, xii, xv–xvii, 6, 9, 20, 21, 101, 102, 104–109, 111–114, 117, 119–121, 156

**RNN** Recurrent Neural Network iv, xiv, xvi, 6, 66–70, 155

**SDP** Semi-definite Programming 55, 56

**SG** Smart Grid 4, 5

**SOC** State of Charge 66, 83, 85, 86

**SOCP** Second-Order Conic Programming 55, 56

**TPG** Traditional Power Grid iv, xv, 1, 3, 5, 11, 154

**TSO** Transmission System Operator 13

**WAN** Wide Area Network 36

# Chapter 1

# Introduction

For decades, consumers' electricity needs have been provided by the Traditional Power Grid (TPG) composed of generation, transmission, distribution, and consumption. However, the significant changes the TPG has undergone lately affects power system operation and reliability. The TPG is mainly reliant on fossil fuels which have variable costs impacted by world events. Such sources of electricity are responsible for the greenhouse gas emissions harming our environments. The increased penetration of Renewable Energy Sources (RESs) in the grid, which are considered as unstable energy sources as their effectiveness is dependent on weather conditions, can potentially cause serious grid imbalances without an advanced management system. Moreover, the increased amount of heavy flexible loads such as, Electric Vehicles (EVs), are resulting in increased demand. EV charging represents a heavy flexible load consuming an immense amount of energy. The TPG, as illustrated in Figure 1.1a, cannot meet these needs as it relies on unidirectional power flow generated from centralized bulk sources of coal and natural gas. Moreover, the TPG suffer from significant losses through its lines due to its centralized topology as energy is transferred from the sources to the consumers. Hence, more energy needs to be generated than is required to overcome these losses, resulting in additional costs and additional environmental damage. Moreover, TPGs allows very little participation of consumers in the market to enable their energy usage management and reduction. All of these reasons resulted in subjecting the TPG to huge changes transforming them to a smart grid. A smart grid integrates the electrical infrastructure with the Information and Communication Technology (ICT) resulting in an improvement in the efficiency and reliability of electricity services [4]. It supports the bi-directional flow of power and information, as illustrated in Figure 1.1b. Moreover, the smart grid enables the integration of RESs reducing the pollution of the environment. Energy can be injected into the grid by RESs that are located near loads they serve. Also,

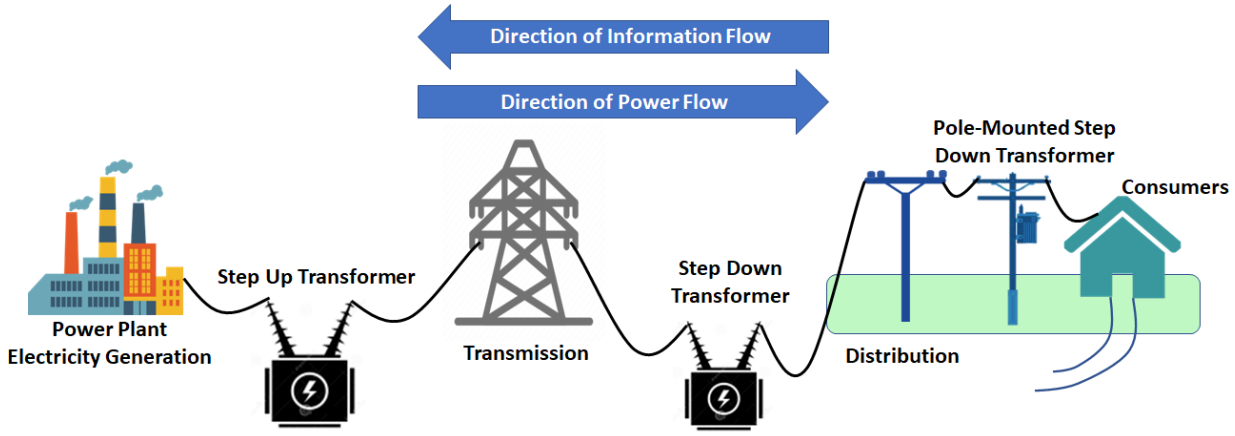
Demand Side Management (DSM) programs of the smart grid increases customers control of their electricity consumption and increases consumer market participation [5].

## 1.1 Research Motivation

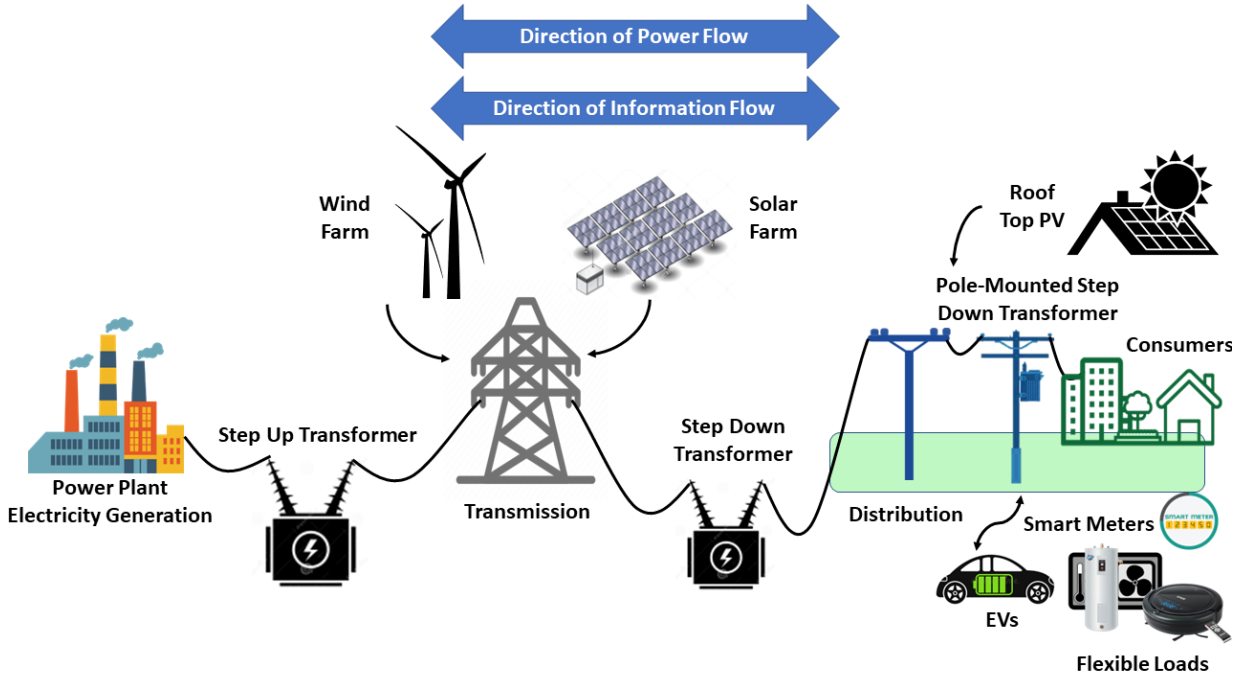
As smart grid technology continues to advance, many countries in the world are exploring grid improvements. In its climate leadership and community protection act [6], the city of New York committed to a decrease of greenhouse gas emissions by 85% by 2050. Thailand aims to generate a third of its energy needs by RESs by 2037. Similarly, Austria aims to reach net-zero carbon emissions by 2040, and clean electricity by 2030. In 2021, Canada adopted the net-zero emissions accountability act which creates carbon targets and plans to meet them every five years. This is continued until 2050 when the net-zero target is achieved. China promised to achieve carbon neutrality by 2060. Similarly, Denmark, France, Fiji, Hungary, Japan, and Ireland are some of the countries which aim to achieve carbon neutrality by 2050 [7].

To accomplish carbon neutrality, heavy penetration of renewable resources, such as solar and wind, are expected to contribute significantly to generation and help with peak demands. However, RESs do not only add bidirectional power flow to the grid but also introduce uncertainty due to their intermittent nature. Hence, balancing supply and demand in a smart grid is complex. In California, on May 13, 2018, an oversupply event happened as a result of renewable generation exceeding the load. The system was forced to curtail 12,000MWh of Photovoltaic (PV) output to clear the congestion [8]. Moreover, Germany being the leader among the European countries in terms of installed PVs, had about 49,170MW at the end of 2019. However, grid congestion resulted in 74% of renewable curtailment in 2018 [9].

To decrease greenhouse gas emissions, the smart grid drives towards the electrification of the transportation system, via EVs, and space heating, via Heat Pumps (HPs). This has increased the usage of such heavy flexible loads and changed the operating conditions of the distribution system [10]. As of 2022, the United States had more than 2.64 million EVs sold [11] and 1.34 million shipments of HPs [12]. The demand for electricity appears to be increasing as HPs are replacing many traditional heating/cooling units in order to reduce oil consumption and heating costs, and EVs are replacing combustion engine vehicles to reduce harmful exhaust emissions. For example, an average Danish family consumes 4000kWh/year. However, this may increase by 5000-10000kWh if HPs are installed. Using EVs would further increase the consumption by another 2000-3000kWh/year [13]. Moreover, the dependence of such technologies on uncontrollable factors, such as temperature,




(a)




(b)

Figure 1.1: Power and information flow under the (a) TPG, and (b) smart grid environments.

wind speed, solar radiation, etc., may result in potential congestion problems which were not of concern in the past in the distribution network. This is due to the high power consumption of active loads and the weakening correlation between electricity prices and demand resulting from the increased penetration level of intermittent RESs [14] - [15]. Typically, demand responds to electricity prices. So, at peak times, when demand is high, electricity prices rises. This motivates heavy flexible load users to shift their demand to off peak times. However, as a consequence of RESs, if during peak hours the RES output is high, electricity prices decreases. This causes flexible load demand to increase in response to the price decrease causing congestion in the network [15]. Such congestion results in voltage violations and/or thermal overloading as a result of the power flow exceeding a network asset's transfer capability, possibly damaging devices such as distribution transformers and feeders [16]. Hence, reinforcement of overloaded network assets is required incurring costs [17] that may seem redundant as peak load generally appears only for a few hours. To avoid or postpone such costs, this dissertation aims to utilize smart grid's DSM feature to alleviate congestions in the distribution network.

DSM refers to programs involving consumers having the flexibility to change (reduce or shift) their electric consumption pattern to gain an economic advantage in terms of reduced electricity bills and help the network operator in managing peak loads. Hence, DSM has been utilized by utilities to manage power system efficiently, reducing the need to reinforce the network. To decrease peak demand, distribution network operators have installed millions of smart meters in the distribution network. In fact, in 2019, 94.8 million smart meters were installed in the United States representing a total advanced meter penetration rate of 60.3% [18]. This paved the way for the New York Independent system operator to activate emergency demand response for several hours in New York city acquiring approximately 495MW of electricity due to an extended heat wave in the city and a sudden outage of a transmission line on 2nd of July, 2018. Also, the mid-continent independent system operator was recorded to have activated an emergency demand response on January 17, 2018, due to unusually cold temperatures [18].

The Smart Grid (SG) introduces bidirectional communication between different network entities to enhance the efficiency, reliability, and fault-tolerance of the grid. Data transmission is executed through either wired communication technologies, such as fiber optic communications or power line communications, or wireless communication technologies, such as wireless mesh network, cellular communication systems or communications based on IEEE 802.15.4 (ZigBee and microwave communications). The smart grid's DSM feature relies on the grid's communication network for exchanging customers preferences, price tariffs, and load schedules between the involved entities to shift demand from peak to off-peak times. However, this reliance on the communication network introduces a

significant vulnerability to the SG if information is not secured. Hence, the success of DSM relies on its *cybersecurity*. Cybersecurity refers to protection of processes, systems, networks, and information from cyber attacks aiming to prevent damage to the authentication, authorization, confidentiality, integrity, and availability of information assets in the SG. The CIA triad of a network can get compromised by cyber attackers through usage of vulnerabilities that exists in the SG. A cyber attacker in an attempt to gain unauthorized access is capable of compromising the consumers' smart meters, the aggregators' system, the Distribution Network Operator (DNO) system, or the communication link connecting all these three entities. Various participants in the grid are at risk of compromising the privacy and integrity of data transmitted between them through false data injection attacks, denial of service attacks, man-in-the middle attacks, etc. Such cyber attacks can cause an overloaded grid, faults, damaged lines, or blackouts resulting in compromising the security, and reliability of the SG. For example, on December 23, 2015, the Ukrainian power grid was cyber-attacked by hackers who manipulated the information systems of three regional power distribution companies. This resulted in power outages impacting nearly 225,000 clients for a couple of hours [19]. Hence, given the criticality of the SG system, the establishment of cyber-secure programs is essential, else it can pose significant threats to the smart grid if security vulnerabilities are not addressed [20].

The evolution of the TPG to the digital smart grid creates opportunities for improving the operation of the power system. The smart grids' capability to support various power generation technologies, self-healing capacity, and ability to minimize operational costs are some of its benefits. However, to enjoy the operational benefits associated with the smart grid, the overloading problem of network assets as a result of the uncertainty associated with the penetration of renewable technologies and heavy flexible loads, and the cyber security of the grid needs to be tackled and their impacts minimized. This is the main objective of this thesis.

## 1.2 Research Contribution and Objectives

Motivated by the above-mentioned smart grid problems, this dissertation aims to develop a cyber secure DSM-based system that accounts for flexible load uncertainties to manage congestion in the distribution network. The thesis utilizes existing smart grid technologies, specifically secured DSM with the communication layer, without incurring any costs associated with the reinforcement of network assets, to alleviate network congestion. As illustrated in Figure 1.2, achieving this contribution will be attained by fulfilling the following milestones:

- In the day-ahead market:
  - Study the vulnerability of existing DSM-based congestion management techniques to cyber attacks and develop an attack model that achieves various adversary objectives in compromising aggregators.
  - From a planning perspective, develop a load altering mitigation scheme to determine the critical aggregators in the network to secure. The mitigation scheme is prepared from the network operator's perspective, assuming the worst case scenario, to secure the aggregators in the network which if compromised would result in a stealthy attack.
  - From an operational planning perspective, utilize Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) as a detection scheme that determines the presence or absence of a load altering cyber attack compromising aggregators in the distribution network.
  - Develop a robust multi-objective congestion management framework using valley filling to flatten the load curve to an optimal level that alleviates congestion in the network while maintaining minimum consumer electricity costs and not imposing any tariffs. The robustness of the proposed multi-objective congestion management model to uncertainties in consumer load scheduling is investigated.
  - Utilize Deep Deterministic Policy Gradient (DDPG) Reinforcement Learning (RL) as a model-free machine learning approach that does not need prior knowledge of the system to manage congestion, minimize electricity cost, and improve the utilization of feeders in the distribution network.
- In the real-time market: develop a cyber-secure and efficient EV assignment model to appoint EVs to charge stations, during grid operation, minimizing queuing time and managing congestion in the electrical network.

The publications completed during the Ph.D. study are as follows:

1. **Gul M Khan, O.**, El-Saadany, E., Youssef, A. and Shaaban, M. F. *Cyber Security of Market-Based Congestion Management Methods in Power Distribution Systems.* IEEE Transactions on Industrial Informatics, vol. 17, no. 12, pp. 8142-8153, Dec 2021, doi: 10.1109/TII.2021.3065714.
2. **Gul M Khan, O.**, Youssef, A., Salama, M. and El Saadany, E. *Robust Multi-Objective Congestion Management in Distribution Networks.* IEEE Transactions on Smart Grid Power Systems, 2022, doi: 10.1109/TPWRS.2022.3200838.

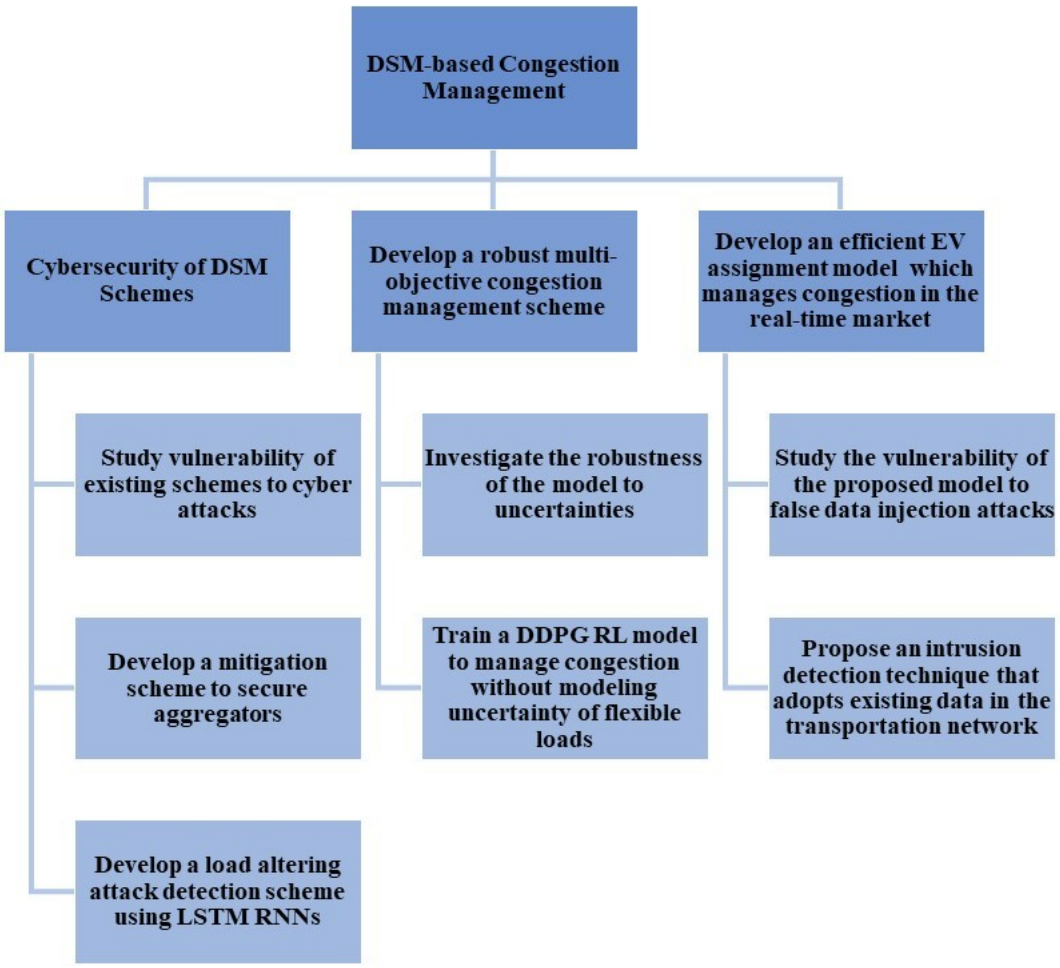



Figure 1.2: Flowchart of the dissertation contributions.

3. **Gul M Khan, O.**, Youssef, A., Salama, M. and El Saadany, E. *Congestion Management in Distribution Networks using Reinforcement Learning.* IEEE Systems Journal, 2022 (Article Submitted on 29th July 2022, article resubmitted for revision on 5th January 2023).

4. **Gul M Khan, O.**, Elghitani, F., Youssef, A., Salama, M. and El Saadany, E. *A Congestion-Aware Charging Station Assignment for EVs.* IEEE Transactions on Smart Grid, 2022 (Article Submitted on 19th July 2022, article resubmitted for revision of 15th December 2022)

5. **Gul M Khan, O.**, Youssef, A., El Saadany, E. and Salama, M. *LSTM-based approach to detect cyber attacks on market-based congestion management methods.* 2021 IEEE Power & Energy Society General Meeting (PESGM), 2021, pp. 1-5, doi: 10.1109/PESGM46819.2021.9637976.

6. **Gul M Khan, O.**, El Saadany, E., Youssef, A. and Shaaban, M. *Impact of Electric Vehicles Botnets on the Power Grid.* 2019 IEEE Electrical Power Energy Conference (EPEC), 2019, pp. 1-5, doi: 10.1109/EPEC47565.2019.9074822.

7. **Gul M Khan, O.**, El Saadany, E., Saleh K., Shaaban, M. and Youssef, A. *Cyber Attacks On Distributed Congestion Management Methods*, 2019 IEEE Power Energy Society General Meeting (PESGM), 2019, pp. 1-5, doi: 10.1109/PESGM40551.2019.8973458.

Publications 1-3, 5, and 7 are incorporated in this thesis. The rest are cited as references whenever needed.

## 1.3 Dissertation Outline

The chapters in this dissertation are organized as follows:

*Chapter 2* provides the required background on DSM and the various entities involved. Moreover, it presents a thorough literature review of congestion in the distribution network and existing congestion management methods studied in the literature and lists their shortcomings. Additionally, it provides an overview of a cyber secure smart grid, details main types of cyber attacks that could compromise the grid, and provides existing literature studying cyber attack mitigation and detection techniques to secure the grid.

*Chapter 3* studies the vulnerability of existing DSM-based congestion management methods to cyber attacks, specifically Load Altering Attacks (LAAs). A stealthy attack model is then developed compromising aggregators in the distribution network increasing/hiding existing congestions. The impact of such stealthy attacks on congestion and consumers' electricity bill is then studied.

*Chapter 4* formulates a mitigation scheme to determine the most critical aggregators in the distribution network. The security of these aggregators is then reinforced to mitigate load-altering cyber attacks.

*Chapter 5* develops a detection scheme that would determine the presence or absence of a load-altering cyber-attack compromising aggregators in the distribution network. The detection scheme is to be executed by the network operator in the day-ahead market on receiving aggregators' load profiles before computing the congestion tariff.

*Chapter 6* proposes multi-objective optimization to schedule flexible load to alleviate potential congestions in the distribution network. The proposed scheme minimizes consumers' electricity costs and decreases the peak to average ratio of the load curve to a required level that alleviates existing congestion. However, the success of the proposed congestion management scheme relies on the accuracy of the consumer load consumption. Hence, uncertainty analysis of consumers' flexible load schedule is executed to ensure the desired robustness of the power flowing in the distribution network to changes in uncertain variables.

*Chapter 7* adopts a machine learning approach where a DDPG RL scheme is proposed to determine the change in electricity prices needed, in the form of tariffs and/or subsidies, to alleviate congestion. The proposed solution aims to overcome the reliance of existing congestion management techniques on consumer behavior forecasts and/or requires multiple iterations between the network operator and the aggregators to determine the needed tariff to alleviate existing congestions.

*Chapter 8* develops an algorithm that assigns EVs to charge stations such that distribution network congestion and time spent by the user from requesting a charging service to accessing it is minimized. The Lyapunov function is utilized for developing an EV assignment algorithm to manage a dynamic population of EVs ensuring queuing stability. Moreover, as the EV assignment algorithm relies on the communication network, an intrusion cyber-attack can occur resulting in an unstable queuing system. An intrusion detection technique is, hence, proposed which utilizes existing transportation network sensor data with the EV charging stations operator information to detect such attacks.

*Chapter 9* concludes this dissertation, outlines its completed work, and articulates topics for future research work.

# Chapter 2

# Background and Literature Review

The Traditional Power Grid (TPG) is uni-directional transporting electrical energy from the generating power plants to the end users for consumption. However, the increased usage of fossil fuels to provide for the increase in electricity demand has caused an increase in carbon emission into the atmosphere. This increase in greenhouse gas emissions and the increase in electricity cost as a result of depletion of such sources in the near future has encouraged bringing about a change in the grid. The new grid proposes changing the TPG to a low-carbon, reliable, and sustainable smart grid. The smart grid integrates new Renewable Energy Sources (RESs), to decrease the carbon footprint, and utilizes advanced Information and Communication Technology (ICT), to improve real-time control, grid resilience, and operational efficiency, in the existing system. The National Institute of Standards and Technology (NIST) defined the smart grid as [21],

> *"A modernized grid that enables bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications."*

However, the increased penetration of RESs and power-hungry flexible loads, such as Electric Vehicles (EVs) and Heat Pumps (HPs), have changed the operating conditions of the distribution system. Congestion, a condition caused as a result of the power flow exceeding a network asset's transfer capability, which was not of concern in the past in the distribution network, might now occur [22], impacting network devices such as distribution transformers and feeders [10]. Moreover, the coupled nature of the smart grid between cyber and physical components has introduced new security vulnerabilities in the distribution network which have become the primary target of cyber attackers. Governments, industry, and academia have hence, focused on identifying the smart grid cyber vulnerabilities and

addressing them for a reliable, efficient and stable operation of the grid.

On this basis, Section 2.1 briefly discusses existing congestion management techniques in the distribution network in the literature. Afterward, Section 2.2 describes cyber-security of the smart grid in terms of defining a cyber secure system, and existing literature securing smart meters and aggregators in Section 2.3. Section 2.4 describes an existing congestion management technique that will be utilized in this thesis to evaluate and compare the performance of the proposed models.

## 2.1 Congestion Management in Distribution Networks

Congestion has been defined in [23] as,

*"A condition that occurs when the traffic exceeds the capacity of the network".*

Given a two bus system, as illustrated in Figure 2.1, the power flowing between bus A and B, $P$, is measured as follows,

$$P = \frac{V_A V_B sin\delta}{X} \tag{2.1}$$

where $V_A$ and $V_B$ refers to voltages of bus A and B, $\delta$ is the phase difference between $V_A$

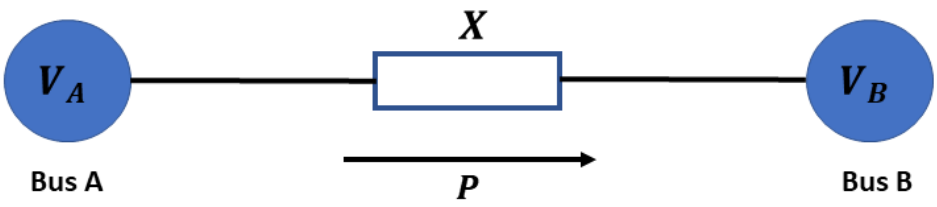



Figure 2.1: Power transfer between two voltage buses

and $V_B$, and $X$ is the reactance of the line. Hence, to increase the power flow in the line, an increase in the bus voltage, increase in load, or a decrease in impedance of the line is required. Congestion is a phenomenon that occurs when the power flowing in the line, $P$, exceeds the line's capacity, $P^{max}$. This is caused as a result of:

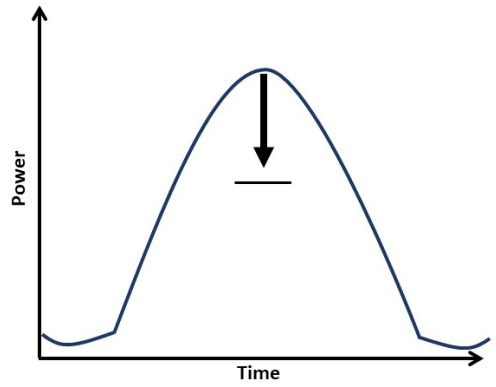
- Voltage Violation: This refers to an increase in bus voltage beyond its limits of $\pm 10\%$ of nominal voltage. Voltage violation occurs in the distribution network as a result of real power injection due to the increased penetration of RESs.

- Current Violation: An increase in the loads in the distribution network causes an increase in the current flowing in the line. Current violation happens when the current flow exceeds the ampacity of the line resulting in congestion.
- Change in line impedance: Reduction of the line impedance due to a fault in the network can result in congestion in the distribution network.

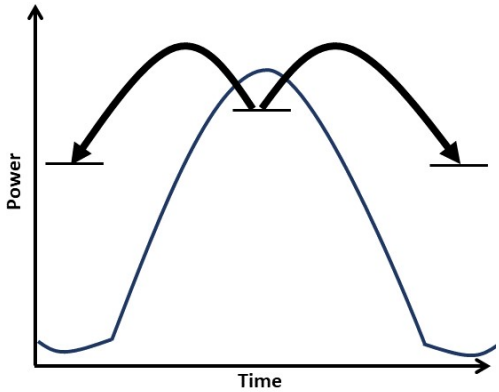
However, as distribution networks are majorly radial represented by a supply providing the connected loads, congestion in this thesis represents a state in which the electricity lines are not capable of accommodating the load during peak periods. Congestion has always been observed in the transmission system and has been treated by the Transmission System Operators (TSOs). However, the bidirectional flow of electricity and the high penetration of power-hungry flexible loads, have changed the operating conditions of the distribution system [10]. Potential congestion problems, which were not of concern in the past, might now occur in the distribution network. Such congestions can possibly damage devices such as distribution transformers and feeders [16]. To avoid congestion, conventionally, network assets are reinforced, incurring huge costs although peak load generally appears only for a few hours as renewable sources are inherently variable in nature [17]. To avoid or postpone such costs, the following congestion management methods have been developed,

- Direct Control Methods: These are methods in which the Distribution Network Operator (DNO) can directly control power system components. Congestion management can be achieved through network reconfiguration, reactive power control, and active power control.
- Indirect Control Methods: These techniques, also known as market-based methods, refer to motivating consumers to change their flexible demand through the usage of price signals, from peak to off-peak times. Indirect methods include dynamic tariffs, subsidy-based methods, and flexibility service market.

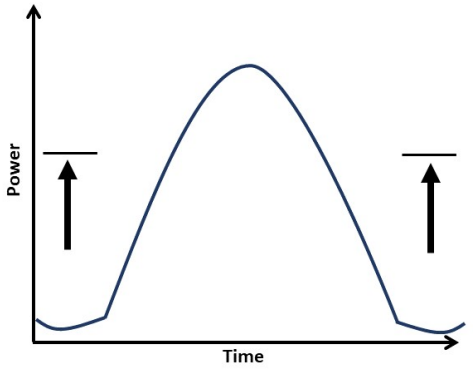
The focus of this thesis is the utilization of existing smart grid resources without causing user discomfort to manage congestion in the distribution network through indirect/market-based methods. These methods have been developed using Demand Side Management (DSM) to motivate consumers to decrease or shift their demand using appropriate prices or incentives. DSM are utility load control strategies and programs that are designed to encourage consumers to modify their demand through economic signals. DSM mainly aims to achieve peak clipping, valley-filling, and load shifting. Peak clipping refers to reduction of demand at peak load periods. Valley-filling refers to increasing load during off peak




(a)




(b)




(c)

Figure 2.2: DSM Strategies: (a) Peak Clipping, (b) Load Shifting, and (c) Valley-Filling.

hours while load shifting refers to shifting the load to off peak hours. These three DSM strategies are illustrated in Figure 2.2.

All of these methods rely on the communication between the DNO, aggregators, and consumers' smart meters, which provide the connecting link between the flexible loads and the aggregators. The characteristics and responsibilities of each of the involved entities are as follows:

- Distribution Network Operator (DNO): The DNO is responsible for distributing and managing energy to end-users. It is responsible for ensuring smooth energy flow between suppliers and consumers and for confirming that there is no congestion in the distribution network.

- Aggregators: Aggregators are load-serving entities responsible for scheduling their consumers' loads. Aggregators have contracts with end-consumers to control their flexible loads or to indirectly motivate them to change their consumption. Consumption preferences, such as the charging behavior of EVs and indoor temperature requirements, have to be communicated, via the Neighborhood Area Network (NAN), to aggregators to minimize consumers' costs and to schedule their loads optimally. Aggregators are responsible for forecasting the non-flexible electricity needed by their consumers and acquiring it in the day-ahead market. Aggregators are also responsible for optimally scheduling their flexible loads either directly or indirectly such that the electricity bill of the users is minimized while maintaining the comfort levels specified by the user. As aggregators are purely economic units that are not responsible of considering any network constraints, they will prefer to schedule the maximum power demand of the flexible loads when the price is lower to maximize consumer welfare. However, this might lead to congestion in the distribution network.

- Consumers Smart Meters: Consumers are the owners of flexible and non-flexible loads and they are represented in the electricity market through the aggregators. The amount of electricity consumed is recorded by the consumers' smart meters at 5-, 15-, 30-, or 60-minute intervals. Local distribution companies receive this information automatically. The utilities can re-communicate with consumers for billing, energy feedback, and time-based rates. Consumers can also view their energy usage information for monitoring and control purposes. Moreover, smart meters are capable of sending signals to home appliances and controlling them given that the flexible loads are smart meter-connected devices or through the home energy management systems.

DSM-based congestion management techniques rely on the Independent System Operators (ISOs) operating both day-ahead and real-time markets. In the day-ahead market, majority of market sales and purchase of electricity occurs based on market participants forecasted load. This protects purchasers of electricity against changes in price that might occur in real-time. PJM and ERCOT are examples of ISOs that operate day-ahead markets. On the other hand, real-time markets manage sales and purchase of electricity based on participants real-time demand. Real-time markets accounts for any changes between the proposed day-ahead schedule and real demand. It should be noted that prices of real-time market can change every minute. PJM and ERCOT also represent examples of ISOs that operate real-time markets.

### 2.1.1 Existing Indirect Control Congestion Management Schemes

Indirect control methods, or market-based congestion management schemes, rely on DSM to motivate consumers to shift their flexible loads from congested times to non-peak times. These schemes are either price-based or incentive-based. Price-based DSM methods include day-ahead Dynamic Tariff (DT) [24] - [25], and day-ahead Distributed Dynamic Tariff (DDT) (also referred to as distributed capacity market) [26]. On the other hand, incentive-based DSM methods include subsidy-based method [27] and peak time rebate [28]. A short description of the modeling of existing price-based and incentive-based congestion management schemes is explained as follows [29]:

- Dynamic Tariff (DT): This is a price-based method in which flexible demand is assumed to be price sensitive. The congestion component of the Locational Marginal Price (LMP) concept from the transmission networks is utilized by the network operator as DTs to alleviate congestion in the distribution network. Using optimization, the DNO is responsible for finding the minimum day-ahead DT that would cause the demand not to congest the distribution lines while being within the network constraints. The DNO is responsible for forecasting the electricity prices and the flexible load in the network. However, if the DNO's forecast is inaccurate then the DT imposed by the DNO would not be an effective solution for congestion mitigation [24, 25, 30].

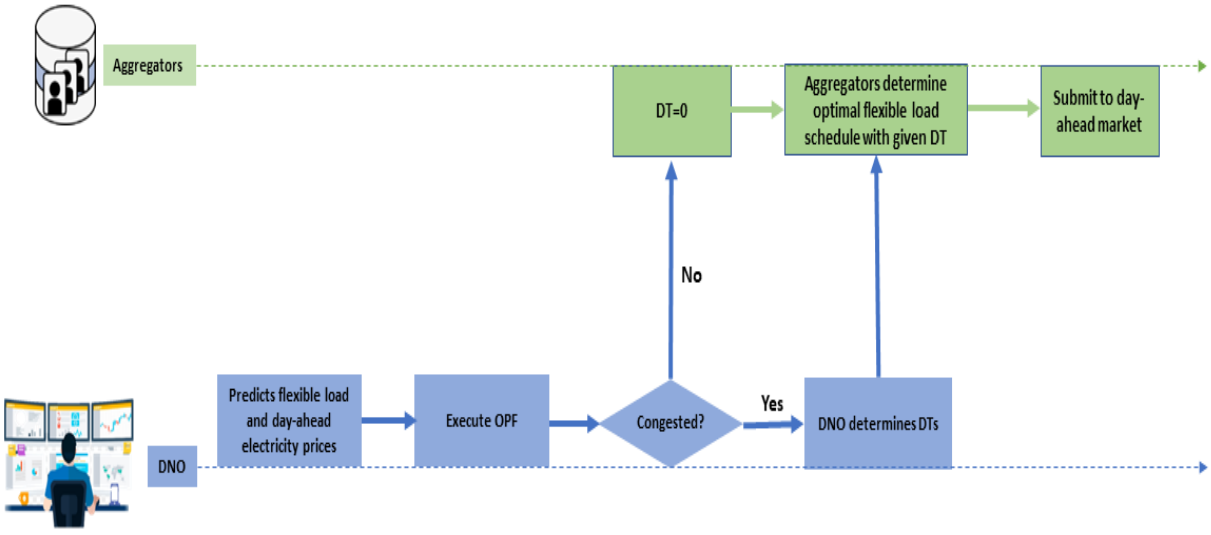
- Distributed Dynamic Tariff (DDT): This is a more distributed form of the DT method in which aggregators are responsible for providing their load schedules to the DNO for determining the congestion tariff. Aggregators in [31] utilized linear programming to determine an optimal flexible load schedule. However, this may result in multiple solutions causing the congestion management scheme to fail. To overcome this, aggregators in [32] utilized quadratic optimization to schedule consumers' flexible loads

prior to forwarding the schedule to the network operator. Load flow analysis is then used by the DNO to determine the voltage level of each bus and the power flowing in each line in the network. The results obtained are compared with the network limits to determine the extent to which the branch thermal limit and the node voltage limits have been violated. Capacity violation of a branch and bus voltage limit violations are represented using marginal prices to determine the DDT congestion tariff for each bus. This tariff is then communicated to the aggregators who re-optimize their load schedules accordingly. The process is repeated until congestion is relieved [26].

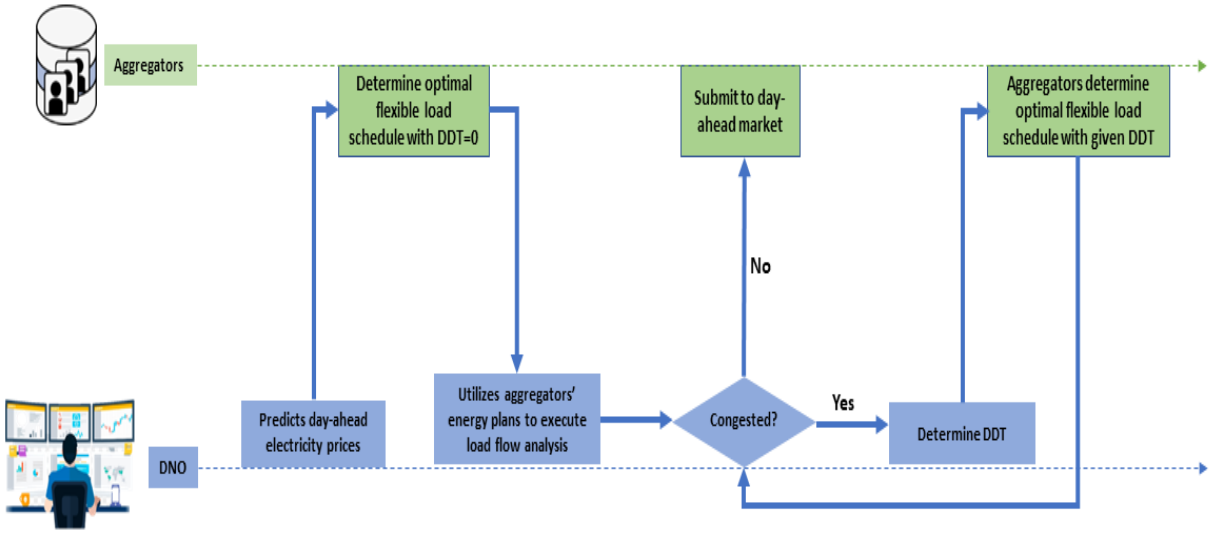
- Subsidy-based Method: To motivate consumers to shift their loads from peak time to off-peak hours, a dynamic subsidy is paid by the DNO in the form of a locational price. In contrast to the DT and DDT methods, where a tariff is collected from the consumers by the DNO, the dynamic subsidy is paid to the consumers without any rebound effect. To determine the subsidy to motivate consumers to shift their flexible demand depends on each consumer's income, location, and flexible load control preferences. Aggregators need to study their consumers to successfully determine the incentives they need to shift their demand. In [27], a two-level optimization formulation is used initially to determine the optimal load of the aggregator and then to determine the subsidy while maintaining network constraints [27]. In [33], voluntary incentives are implemented to customers iteratively such that aggregators' profit is maximized. However, once the aggregators' profit no longer increases, the incentives given to the consumers to shift their demand stop. Thus, alleviation of congestion is not guaranteed.

- Peak-time Rebate: Fenrick [28] proposed a peak-time rebate incentive-based program in which the network operator identifies peak hours in the day-ahead market. The customers then can get a rebate for reducing their load at these peak hours alleviating congestion in the distribution network. However, this method requires an accurate estimation of the base load of consumers to result in the correct calculation of the reduction of the flexible load and the corresponding rebate incentive. Moreover, the calculation of the rebate rate is dependent on the price elasticity of the demand which is difficult to estimate.

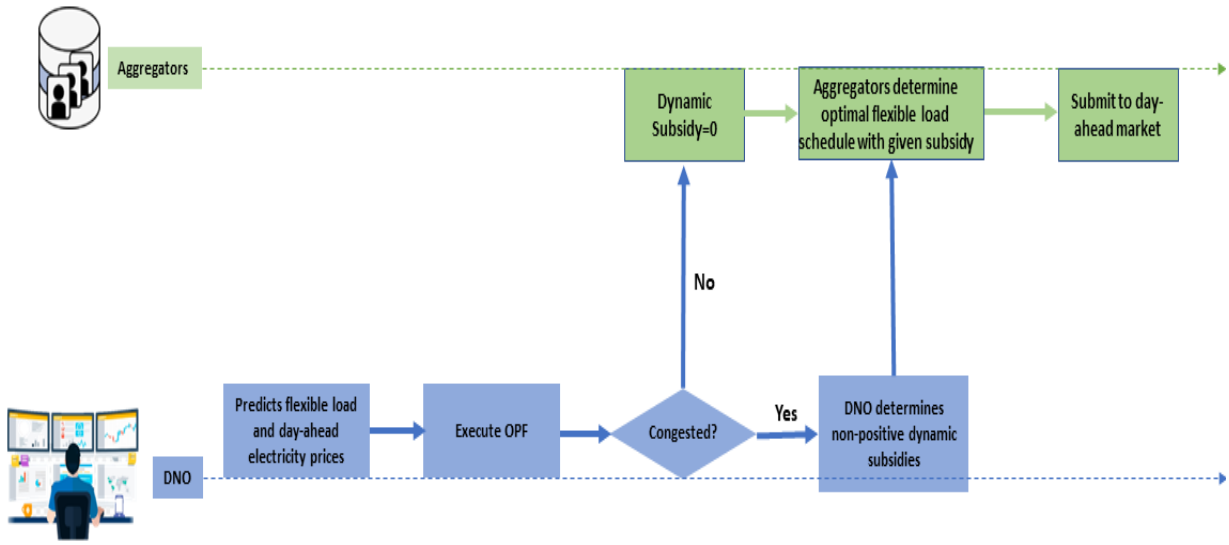
Figure 2.3 illustrates the different existing congestion management schemes and the communication between aggregators and DNO.


Aggregators
DT=0
Aggregators determine optimal flexible load schedule with given DT
Submit to day-ahead market
No
Predicts flexible load and day-ahead electricity prices
Execute OPF
Congested?
Yes
DNO determines DTs
DNO

(a)


Aggregators
Determine optimal flexible load schedule with DDT=0
Submit to day-ahead market
Aggregators determine optimal flexible load schedule with given DDT
No
Predicts day-ahead electricity prices
Utilizes aggregators' energy plans to execute load flow analysis
Congested?
Yes
Determine DDT
DNO

(b)




(c)

Figure 2.3: Comparison between the different existing congestion management schemes in the distribution network (a) DT, (b) DDT, and (c) Subsidy-based method.

### 2.1.2 Congestion Management Using Valley-filling Schemes

The existing price and incentive-based congestion management methods [24] - [33] aims to alleviate congestion using an electricity cost minimization objective function. However, this may result in new peaks as loads are scheduled at times when prices are low. Moreover, the Peak to Average Ratio (PAR) of load curves in such modeling is high. On the other hand, valley filling techniques [34] - [35] result in flattening the load curve by filling the valleys in the load profiles, as illustrated in Figure 2.2(c), which is advantageous in terms of PAR. In [34], predetermined demand forecast information was utilized to schedule flexible loads probabilistically. This resulted in almost a flat power consumption curve. Moreover, in [36], grid power valley-filling and peak shaving were proposed through the utilization of EVs by minimizing the load difference between the predicted load curve and that of the target. Similarly, a decentralized valley-filling-based network-aware charging model for EVs was proposed in [37]. Chen et al. [38] determined optimal EV charging schedule according to the valley level of the grid determined by the DNO. The proposed time-dependent problem jointly optimized the operation of the grid as well as the charging of EVs. On the other hand, [35] proposed a decentralized water-filling-based approach to solve the EV charging problem. Based on the stochasticity of the base load forecast and the random arrival of EVs to charging stations, a moving horizon approach was used.

However, the price is not taken into consideration in the valley-filling literature resulting in consumers paying more compared to load shifting methods. To gain the advantage of both worlds, multi-objective optimization is proposed in this thesis as a contribution in Chapter 3 to schedule flexible loads by merging load shifting and valley filling methods. As defined in [39], multi-objective optimization refers to

> *"an area of multiple criteria decision making that is concerned with mathematical optimization problems involving more than one objective function to be optimized simultaneously"*

This would result in consumers minimizing their electricity costs as well as flattening the curve enough to alleviate any existing congestion in the network.

### 2.1.3 Limitations of Model-based Congestion Management Schemes

Existing congestion management techniques [24]- [28] are defined as model-based methods, requiring an optimization model for aggregator scheduling and for determining congestion tariff by the network operator. The model-based methods, however, require prior knowledge of the exact load models. However, flexible load models are stochastic and are affected by factors such as temperature, location, etc. Obtaining stochastic models for such loads may not be easily available in practice. Moreover, these model-based schemes rely on the accuracy of uncertain parameters, such as consumers' energy price sensitivity. This step is a difficult task considering the heterogeneity of consumers and their behavioral differences [40]. Moreover, the models require back and forth iterations between the network operator and aggregators via the communication network to determine the needed tariff to alleviate network congestions. There is no guarantee that the iterations will be complete as consumers' comfort preferences might not be met causing the persistence of peak load and congestion not being managed in the day-ahead market.

Given the discussed limitations of the existing congestion management techniques, a method needs to be developed to determine an appropriate congestion tariff that relieves network congestion. As the problem requires decision-making in an uncertain environment and given the large volume of data available in the smart grid, a data-driven machine learning model is proposed in Chapter 4 of this thesis as a congestion management model in the distribution network. Proven the high accuracy of deep learning-based models in other applications in power systems, and their capability to learn patterns unsupervised, they are ideal for determining the required tariffs and/or subsidies to alleviate congestion. Specifically, Deep Deterministic Policy Gradient (DDPG) Reinforcement Learning (RL) is utilized as a model-free technique that does not require explicit probabilistic models of the controllable loads to determine the congestion tariff that would alleviate congestion.

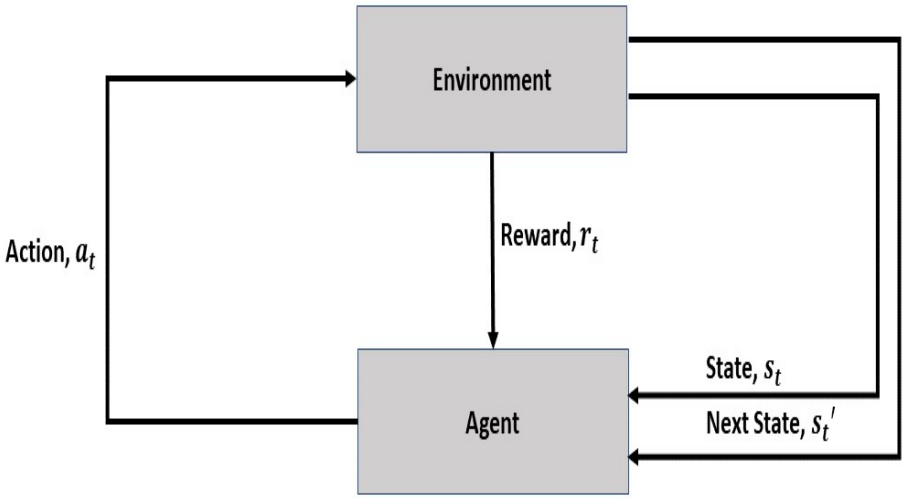



Figure 2.4: General RL Model

Instead, RL is adopted to train an agent to take appropriate actions in a dynamic environment to maximize long-term reward [41]. The DNO represents the agent that senses the state of the environment and determines, accordingly, the action needed to manage congestion. The overall aim of RL techniques is to train an agent that maximizes a numerical reward signal calculated as a consequence of actions taken on the environment, as illustrated in Figure 2.4. In the event that the action taken causes the updated environment state to diverge from the objective, a reward in the form of a negative penalty is imposed. However, if the action taken results in an updated state that is closer to achieving the objective of the problem, a positive reward is imposed by the model. This cycle is repeated until the objective of the problem is achieved.

RL has been utilized in the literature to manage congestion through reconfiguration of the distribution network. [41] utilized a RL-assisted multi-objective bacterial foraging optimization algorithm to solve its many-objective distribution network reconfiguration model. The model aims to improve the accommodation of RESs while maintaining the stability of network operations. Similarly, [42] developed a data-driven batch constrained RL model for dynamic distribution network reconfiguration to improve the system's performance. Bahrami et al. [43] proposed a RL algorithm to remotely control flexible loads in the distribution network considering network constraints. A two-stage voltage control model adopting RL was developed in [44] to mitigate voltage violations caused by the increased penetration of EVs in the network. However, to our knowledge, RL has not been

adopted to determine congestion tariffs and/or incentives to motivate consumers to shift their loads from peak to off-peak times managing distribution network congestion.

## 2.2 Comparison Technique: Distributed Dynamic Tariff (DDT)

The DDT method, proposed in [26], is adopted in this thesis as a comparison technique. Being the most generalized congestion management technique and due to its distributed nature compared to the centralized DT method, the DDT congestion management technique was adopted. In DT [24], the DNO is responsible for forecasting the electricity prices and the flexible load in the network. However, if the DNO's forecast is inaccurate, then the DT imposed by the DNO would not be an effective solution for congestion mitigation. On the other hand, the DDT congestion management method makes the aggregators responsible for providing their load forecast to the DNO and hence, the DNO is not solely responsible for determining the DDT. This distributed calculation of the DDT increases the certainty and transparency of the model.

The DDT method mainly involves two steps: first, aggregators are responsible for determining their customers optimal load schedule meeting their customers' preferences and minimizing cost. Second, the DNO is responsible for determining the DDT on receipt of the optimal load schedules from all the aggregators in the distribution network. The DNO forwards the DDT to the aggregators and the cycle is repeated a number of times until congestion is cleared in the network. The following sub-sections explain the details of the two steps involved and the specifications of the IEEE 33 bus system which is used as a case study to represent the DDT congestion management method.

### 2.2.1 Optimal Flexible Load Scheduling by Aggregators

Using quadratic optimization, consumers preferences, and day-ahead electricity prices, aggregators can schedule their consumers flexible loads [26]. Aggregators define their optimal load schedules as follows,

$$P^{a}_{i,t} = E_{a,i}(P^{nf}_{t} + P^{f}_{t}), \forall i \in \mathbb{K}_a, \mathbb{K}_a \subset \mathbb{I}, a \in \mathbb{A}, t \in \mathbb{T} \tag{2.2}$$

where $P^{a}_{i,t}$ is aggregator's $a$ customers load schedule for all aggregators, $N_a$. $E_{a,i}$ is a matrix that represents aggregator's $a$ customers to bus mapping matrix. $P^{nf}_{t}$ and $P^{f}_{t}$ are the non-flexible and flexible loads at time $t$, where $t$ is an hour in the set of next day

planning periods, $N_T$, respectively. Moreover, $\mathbb{I}$ is the set of buses, $1...N_{bus}$, $\mathbb{T}$ is the set of time slots, $1...N_T$, and $\mathbb{A}$ is the set of aggregators $1...N_a$ respectively. Each aggregator, $a$ is responsible of an explicit subset of buses. The optimal load schedule of the aggregators, $P_{i,a}$, are then forwarded to the DNO who is responsible for determining the DDT.

### 2.2.2 Calculation of DDT by Network Operator

On receiving the aggregated load schedule from all the aggregators, $P_{i,t}$, the DNO determines the total complex power, $S_{i,t}$, for each bus using both the flexible, $P_t^f$, and non-flexible, $P_t^{nf}$, load demands of the consumers. Load flow analysis is then used to determine the voltage level, $V$, of each bus and the power flow in each line, $F_{i,j}$. The results obtained are compared with the network limits to determine the extent to which the branch thermal limit and the node voltage limits have been violated. Capacity violation of a branch is represented using marginal price $\lambda_t$, while the violation of voltage limits is represented using marginal price $w_t$. Consequently, DDT, $r_t$, is determined for each bus.

Initially, the DDT, $r_t$, is initialized to zero and sent to the aggregators. The aggregators then optimize their customers' flexible demand and resend their optimal load schedules, $P_{i,t}$, defined in (2.2), to the DNO who determines $S_{i,t}^{(k)}$, where $k$ is the iteration number, and the corresponding DDT, $r_t^{(k)}$, as shown in (2.3)-(2.5).

$$\lambda_{i,j,t}^{(k+1)} = \lambda_{i,j,t}^{(k)} + \alpha(F_{i,j,t} - F_{i,j}^{max}), t \in \mathbb{T} \tag{2.3}$$

$$w_{i,t}^{(k+1)} = w_{i,t}^{(k)} + \alpha(-1 + \frac{1}{V_0^2} Re(Z\overline{s_t^{(k)}}) + \frac{V}{V_0}), t \in \mathbb{T} \tag{2.4}$$

$$r_{i,t}^{(k+1)} = D^T \lambda_{i,j,t}^{(k+1)} + \frac{Re(Z^T)}{V_0^2} w_{i,t}^{(k+1)}, t \in \mathbb{T} \tag{2.5}$$

where $\lambda_{i,j,t}^{(k+1)}$ is the updated marginal price based on how much the power flowing, $F_{i,j,t}$, at time, $t$, has exceeded branch $(i,j)$ maximum power flow limit, $F_{i,j}^{max}$. $w_{i,t}^{(k+1)}$ is the updated marginal price, $\underline{V}$ is the lower voltage limit, $V_0$ is the voltage at node 0, $\alpha$ represents the step size, $Z$ is the partial nodal impedance matrix and $D$ represents the bus and branch mapping matrix. Since the DDT method imposes tariffs to decrease demand, the marginal prices are required to be non-negative. This iteration continues between the DNO and the aggregators who would re-optimize their flexible demand using the imposed DDT and communicate it back to the DNO until $\mid r_{i,t}^{(k+1)} - r_{i,t}^{(k)} \mid$ converges to a small value.

## 2.3 Cyber-Security of Congestion Management Schemes

All DSM-based congestion management methods rely on the communication between the DNO, aggregators, and consumers' meters in exchanging customers' preferences, price tariffs, and load schedules to relieve congestion [45], as illustrated in Figure 2.5. This reliance on the two-way flow of information between the different involved entities makes them prone to cyber-attacks. Any theft or alteration of data could violate consumer privacy, cause economical damage, or even electrical outages. Hence, studying the vulnerability of indirect congestion management methods to cyber-attacks is vital.

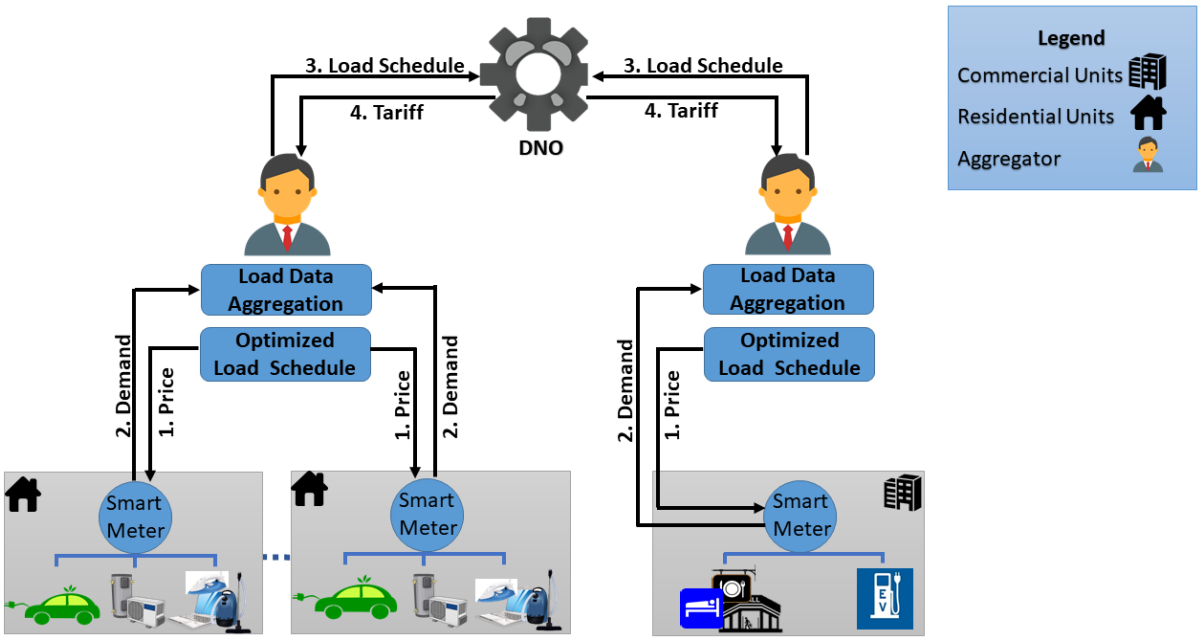



Figure 2.5: Representation of DSM-based congestion management methods

The success of market-based congestion management methods relies on its cyber-security which needs to satisfy the *CIA* triad as defined by the NIST to maintain the security of the smart grid [46] [47]. The CIA triad symbolizes the following three security objectives:

- **Confidentiality**: Confidentiality preserves restricted and authorized access to private and propriety information. Cyber attacks targeting confidentiality include stealing information exchanged between smart meters and various entities and manipu-

lating it, modifying it, or using it for other malicious reasons.

- **Integrity**: Integrity refers to the assurance that information, such as price signals sent to consumers' meters, is authentic and not corrupted. Attacks targeting integrity refer to unauthorized alteration or destruction of information exchanged within the smart grid. Example of such an attack is false data injection attacks, replay attacks, and man-in-the-middle attacks.

- **Availability**: Availability is the guarantee that authorized users have reliable access to required information and services at all times. For example, aggregators should be able to communicate their load demand readily with the network operator. Attacks targeting availability aim to deny users access to their data disturbing the operation of the control system. An example of such an attack is Denial of Service.

Besides the CIA triad, a cybersecure system needs to have an authentication and authorization process [48]. Authentication refers to the process through which a data owner is verified. Circuit shifting, key exchange protocols, and symmetric-key cryptography are some of the existing authentication techniques. Authorization, on the other hand, refers to data owner validation once correct credentials are provided. This can be executed through digital certificates, or usernames and passwords.

Different types of cyber attacks exist that can impact the operation of the smart grid as follows,

- False Data Injection (FDI): FDI attacks refers to an attacker stealthily compromising measurements to lead the system to execute a wrong control action [49]. Load Redistribution Attacks (LRDA) is a form of FDI attack in which the sum of the change in load measurements due to an attack is zero making the attack hard to detect. Moreover, LRDA restricts deviations of load measurements to be within a certain threshold value [50].

- Load Altering Attack (LAA): A LAA is a cyber-physical attack aimed against demand-side management programs. It attempts to gain access to flexible loads and change their demand to damage the grid by causing circuit overflow or unbalancing supply and demand [51].

- Denial of Service (DoS): DoS attacks impact the availability of a network or a system by flooding communications or resources, such as memory, and bandwidth, to that network [52]. For example, a consumer smart meter not capable of communicating with its aggregator as a result of DoS attack.

- Man-in-the-Middle Attack: It is a type of eavesdropping attack in which a cyber attacker intercepts communication between two parties and relays messages between them instead. Load Replay Attacks (LRA) is a form of man-in-the-middle attack that is hard to detect since they do not cause direct damage to the system. An attacker compromises certain entities, monitors and records their output, and repeats the output at a later time affecting the operation of the power system [53]. The Stuxnet virus that attacked the SCADA system in Iran's nuclear facilities was a form of a replay attack that was able to execute malicious commands succeeding in destroying the nuclear centrifuges [54].
- Relay Setting Attack: This is a type of cyberattack in which an attacker compromises a transmission line to trip a second line [55].
- Spoofing Attacks: These are attacks that aims to disguise a user as another user through data falsification so that the user appears to be an authorized source. When the corrupt user is authenticated and granted access, the user can use this access for damaging the grid [48].

In this research, we are focusing on LAA targeting integrity. Mohsenian et al. [56] studied static LAA in which the load was abruptly increased. [57] used false data injection and false command injection attacks to manipulate direct-controlled load and disturb the grid. A frequency response model is also proposed which describes the effect of the injected false commands on frequency. On the other hand, Amini et al. [51] studied the effect of a closed loop dynamic LAAs on the power system's stability when the attacker changes the load control signal of vulnerable loads based on the system frequency.

The main involved entities in the congestion management schemes are the DNO, aggregators, smart meters, and the communication lines connecting them all. Attacking the DNO is not easy since its the main control center and hence, is highly secure due to its significant role in the grid. Attacks on consumers' meters and their communication links have been studied in the literature, a summary of which is detailed in the next subsection. Attacking aggregators or their communication link with the DNO is another aspect that can be utilized by a cyber attacker to affect congestion. This is the main focus of this thesis as it has not been studied in the literature and will be explained in the following subsections.

### 2.3.1 Smart Meters and their Cybersecurity

One of the essential components of the smart grid is the Advanced Metering Infrastructure (AMI) which comprises of smart meters, communication systems, and data manage-

ment systems enabling two-way communication between utilities and customers. Wireless mesh networks are one of the key communication technologies used in the AMI network [58]. This system provides customers the ability to automatically and remotely measure electricity usage, monitor voltage, connect or disconnect service, and provide time-based electricity rates for customers taking part in DSM programs. [59] reports a 30% decrease in peak demand as a result of customers responding to the critical peak pricing program and a 29% decrease in peak demand as a result of customers responding to critical peak rebates. Home area networks and energy management systems that utilize programmable communicating thermostats are installed to automatically control appliances for customers taking part in DSM programs. Figure 2.6 illustrates the operation of AMIs and customer control technologies to manage demand-side consumption.

Due to its increased deployment and its cyber-physical nature, cyber security of AMIs needs to be studied. A summary of the literature studying attacks on consumers' meters and their communication links is illustrated in Table 2.1. In [60] and [61], the impact of FDI attacks on price and load signals in a distribution system was studied. DoS and FDI attacks were adopted in [62] to compromise Home Energy Management Systems or its communication link with the DNO. LAA were studied in [63] and [51]. Static LAA resulted in causing damage to network equipment as a result of circuit overflow [63] while closed-loop dynamic LAA had an impact on power system stability [51]. LRDAs were simulated in [64]. Different scenarios were simulated, representing various levels of network information possessed by an attacker.

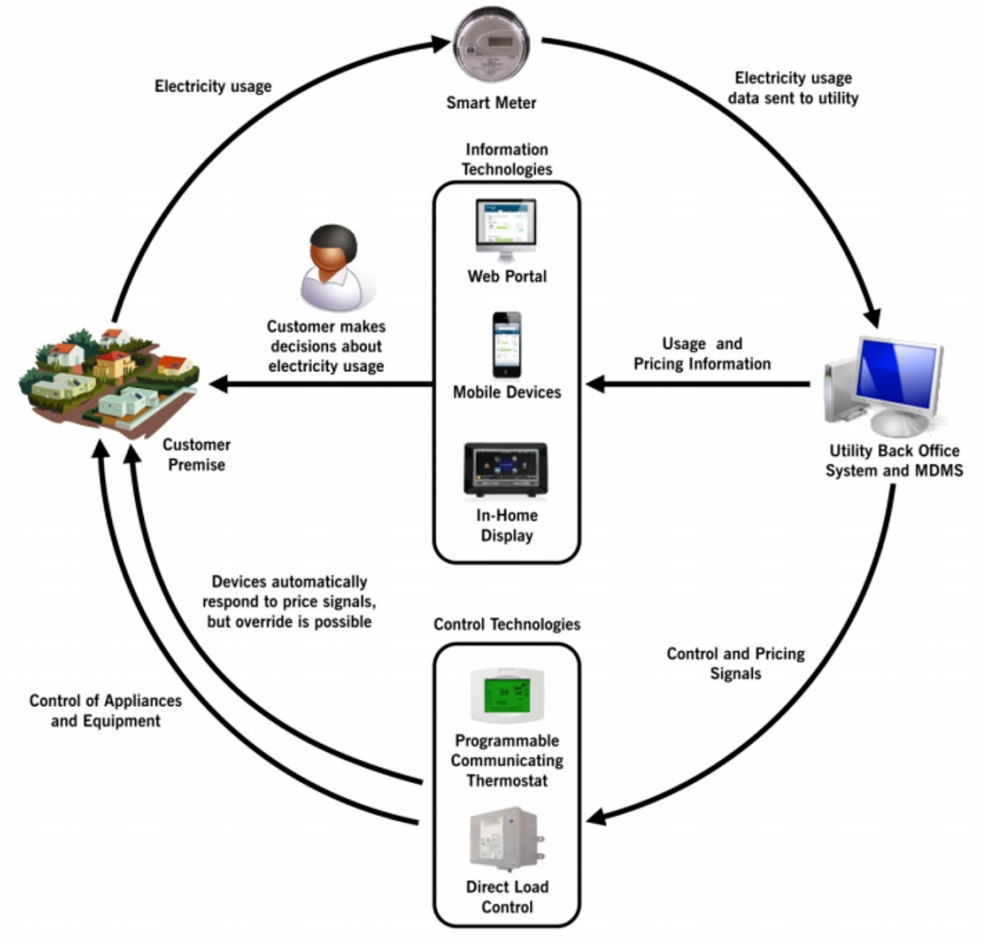



Figure 2.6: Operation of AMI and customer control technologies [1]

Table 2.1: Literature review of cyber security of consumers meters

| Ref. | Attack | Compromises | Impact |
|---|---|---|---|
| [60] | FDI | Price signal and load data | Price attack causes change in demand resulting in price change. Load attack results in wrong demand causing price change. |
| [61] | FDI | Price received by consumers | Change in demand causing instability, fluctuation in real-time pricing or voltage violations. |
| [62] | DoS and FDI | Price signal and load data | DoS causes load scheduling to temporarily become ineffective. FDI results in random load schedules not reflecting market. |
| [63] | LAA | Internet connected loads | Circuit overflow causing damage to the utility and/or equipment. |
| [51] | Dynamic LAA | Vulnerable loads | Power system stability. |
| [64] | LRDA | Smart Meters | Circuit overflow causing damage to the utility and/or equipment |

## 2.4 Aggregators and their Cybersecurity

In a deregulated market, residential consumers are usually not allowed to directly procure electricity from a wholesale market. Instead, consumers are aggregated and represented by aggregators in the market. Aggregators have been defined in [65] as

> *"the act of grouping distinct agents in a power system (i.e. consumers, producers, prosumers, or any mix thereof) to act as a single entity when engaging in power system markets or selling services to the system operator(s)."*

Aggregators' aim is the commercial successful operation of their client by creating automated controls for consumer flexible loads while taking into consideration preferences and behavioral patterns. Aggregators, hence, can provide network operators with a cost-effective mechanism for reducing the need for grid infrastructure. The control actions that they are capable of imposing on their customer loads can influence the load flows and line loading of distribution networks.

Aggregators can manage congestion through the management of flexible loads. They have the capability of providing system capacity by managing loads during peak demand times or shifting their operation to times at which electricity cost is lower. The development of home energy management systems enables effective control of consumer loads and provides communication ability between the aggregator and the end-users. Aggregators can engage with owners of flexible loads such as ?? devices and EVs to manage congestion. [65] utilizes aggregators to implement direct load control on residential heating and cooling loads. Consumers submit their flexible load preferences to their respective aggregators. The aggregator schedules the operation of the flexible loads for each resident and forms optimal demand-price bidding curves which it submits to the day-ahead market to procure electricity. [66] proposes a hierarchical day-ahead DSM model integrating renewable energy courses. The utility aims to minimize its operation cost by providing part of its revenue to the aggregators as an incentive. The aggregators provide an incentive to their respective customers to encourage them to modify their load schedules. To achieve this, a multi-objective problem is formulated that is not biased towards any particular participant to ensure overall fairness.

Aggregators can also be used for controlled EV charging to prevent congestion of the network. EVs are considered heavy flexible loads that are capable of influencing wholesale electricity prices and causing congestion in the distribution network. When EVs react to wholesale prices and shift their charging times until the electricity price is low, a rebound effect may be created resulting in new peak demand. However, controlled EV charging includes a feedback mechanism that considers the rebound effect and causes EV demand to spread to some extent. [67] proposed an EV charging model in which aggregators have an objective of minimizing the charging costs of their fleet of EVs. The model is simulated with wind penetration to observe the effect of wind energy influencing the electricity price and the resulting EV load's response to price. Dynamic grid tariff, capacity allocation, and distribution grid capacity market are then utilized as congestion management mechanisms to evaluate their performances. [68] proposes a novel controlled charging method that takes electricity grid constraints under consideration. A specific charging plan for each EV is established meeting the EV owners charging preferences and avoiding grid congestion by solving an optimization function that aims to minimize charging costs. Connell et al. [69] studied the effect of dynamic day-ahead grid tariff for managing congestion in the distribution network caused due to the charging of electric vehicles. The DNO is responsible for predicting day-ahead congestion and publishing DT congestion prices which the EV fleet aggregators have to include optimizing their EV charging schedules.

Aggregators' utilization of the communication infrastructure to receive DNO prices or customer preferences makes it prone to cyber-attacks. [70] establishes the unique position

of aggregators in the network based on their connection to Distributed Energy Resources (DER) equipment and DNO. Hence, the importance of studying aggregators' cyber security as their actions, if attacked, could have a considerable risk on the security of the grid. A state-sponsored adversary can cause economic disruptions in the country as a result of hiding existing congestions which could result in load shedding. Competitors could also hire attackers to impose high tariffs on consumers due to unreal congestion, causing them to switch utilities. Competitors could also hire attackers to impose high tariffs on consumers due to unreal congestion, causing them to switch utilities. However, to date, the impact of cyber-attacking aggregators on market-based congestion management techniques has not been studied. Chapter 5 in this thesis will study the vulnerability of DSM-based congestion management schemes to LAAs resulting in creating or hiding congestion in the distribution network.

### 2.4.1 Cyber-Attack Mitigation Schemes

A mitigation scheme should be modeled to protect the electrical network from cyber attacks. Until recently, many studies have come up with mitigation schemes to defend against FDI attacks in the smart grid. In [71], a graphical approach was proposed to detect the most critical meters in the network and mitigate against FDI attacks. Optimization techniques were utilized in [72] and [73] to develop its optimal mitigation scheme determining the least number of sensor measurements that need to be protected. Game theory has also been used to study data injection attacks involving multiple adversaries [74]. A Stackelberg Game was used to model the strategic interactions between the defender and attackers aiming to identify the main network components that need to be secured. It should be noted that FDI attacks are dependent on an adversary's knowledge of the system. Hence, proactive methods attempting to change system characteristics, either via changing topology or impedance perturbation, have been developed in the literature. This adds an extra layer of protection against FDI. In [75], strategic switching of network topology has been proposed as a mechanism to mitigate FDI attacks. In [76], an algorithm is modeled to determine branches that need to be perturbed using Distributed Flexible AC Transmission System (D-FACTS) devices to minimize the possibility of stealthy FDI attacks. Feasibility and limitations of proactive FDI detection scheme through branch impedance perturbation were studied in [77]. However, existing literature has not determined the critical aggregators in the distribution network that needs to be secured against cyber attacks. Chapter 6 in this thesis proposes a Mixed Integer Non-Linear Programming (MINLP) to model the mitigation scheme for single- and multiple-point load altering attacks. The optimization problem is solved using the Generalized Benders Decomposition (GBD) approach to determine the critical aggregators in the network. In order to make the grid more resilient

to cyber attacks, these aggregators are secured by the network operator.

### 2.4.2 Cybersecurity Detection Schemes

Detection of attacks on consumers' smart meters and their communication links have been studied in the literature. The impact of closed-loop load-altering attacks compromising the stability of the power system was studied in [51], where single and multi-point attacks were simulated to alter the victim's load based on power system frequency. A protection scheme was then formulated to determine the minimum load that must be secured at each bus by solving a non-convex pole placement optimization problem. In [78], three types of attackers were studied, with varying cyber attacking capabilities, that aim to steal electricity using FDI by tampering with the smart meters. Thus, based on the attacker type, false data could modify consumption data in the memory of the meter. A collaborative intrusion detection mechanism was then proposed to decide if the physical memory of the smart meter has been tampered with. In [79], a support vector machine-based classifier was adopted to detect energy theft attacks as a result of hacking smart meters. On the other hand, in [80], cyber attackers manipulated the readings of meters responsible for monitoring renewable units to overcharge the utility. A detection scheme was then proposed utilizing deep machine learning, specifically deep convolutional-recurrent neural networks to detect such malicious activity.

In the existing literature, up to the author's knowledge, no work exists on the detection of cyber attacks that compromises aggregators. Chapter 7 in this thesis is focused on developing a detection scheme that would determine the presence or absence of a load-altering cyber attack compromising aggregators in the distribution network. The detection scheme is to be executed by the DNO in the day-ahead market on receiving aggregators' load profiles before computing the congestion tariff.

# Chapter 3

# Cyber Security of Market-based Congestion Management Methods in Power Distribution Systems

## 3.1 Introduction

All existing Demand Side Management (DSM)-based congestion management methods rely on the communication between the Distribution Network Operator (DNO), aggregators, and consumers' meters in exchanging customers' preferences, price tariffs, and load schedules to relieve congestion [45], as illustrated in Figure 3.1. This reliance on the two-way flow of information between the different involved entities makes them prone to cyber attacks. Any theft or alteration of data could violate consumer privacy, cause economical damage, or even electrical outages. Hence, studying the vulnerability of indirect congestion management methods to cyber-attacks is vital.

The success of market-based congestion management methods relies on its cyber-security which needs to satisfy the *CIA* triad. The CIA triad symbolizes the Confidentiality, Integrity, and Availability of the cyber network which can pose significant threats to the grid if security vulnerabilities are not addressed. Confidentiality is needed to ensure authorized access to sensitive information, such as consumers' electricity demand. Integrity refers to the assurance that information, such as price signals sent to consumers meters, is authentic and not corrupted. Finally, availability is the guarantee that authorized users have access to the required services at all times. For example, aggregators should be able to communicate their load demand readily with the network operator [81].

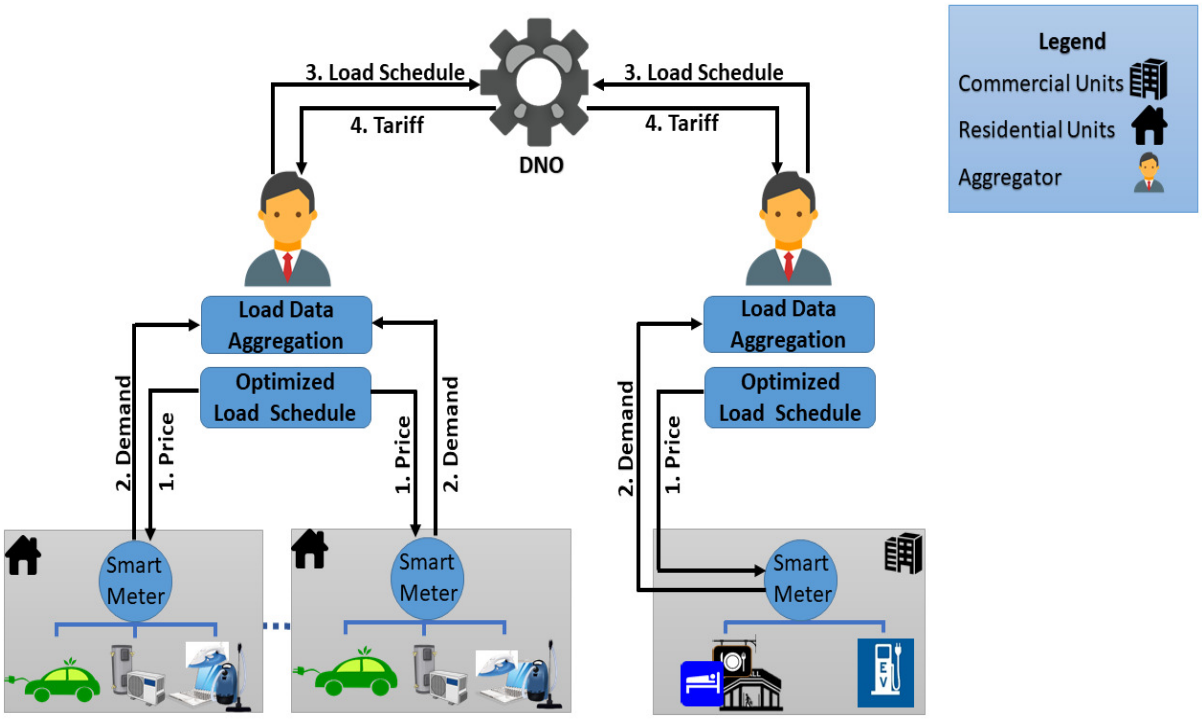



Figure 3.1: General representation of existing DSM-based congestion management methods

Attacking the DNO is not easy since its control center is highly secure due to its significant role in the grid. Attacks on consumers' meters and their communication links have been studied in the literature, a summary of which was described in Chapter 2. Attacking aggregators or their communication link with the DNO is another aspect that can be utilized by a cyber attacker to affect congestion. The unique position of aggregators in the network, in terms of its connection to its Distributed Energy Resources (DER) equipment and the DNO, has been established in [70]. Hence, the importance of studying aggregators' cyber security as their actions, if attacked, could have a considerable risk on the security of the grid. A state-sponsored adversary can cause economic disruptions in the country as a result of hiding existing congestions which could result in load shedding. Attackers could also be hired by competitors to cause high tariffs to be imposed on the consumers due to unreal congestions encouraging them to change their utility provider. However, to date, the impact of cyber-attacking aggregators on market-based congestion management techniques has not been studied.

Motivated by the research gap, the effect of compromising aggregators and their communication link to the DNO on market-based congestion management techniques is studied in this chapter. Load Altering Attack (LAA) are modeled in the day-ahead market to modify cyber attacked aggregators' load profiles to cause or hide congestion in the distribution network. LAAs, which is a type of False Data Injection (FDI), has been previously studied in the literature [51] - [63]. However, the impact of LAAs on the power system level was studied aiming to alter a certain volume of flexible loads in the network to cause frequency instability and circuit overflow in power systems. Hence, consumers smart meters and the DSM-signals received were altered. However, in this chapter, the attack is assumed to target the day-ahead market making the network operator not capable of using bad-data detection techniques to detect the attack. The impact of such a cyber attack in terms of congestion and congestion tariffs is evaluated.

The main contribution of this chapter is, hence, to identify cyber vulnerabilities of DSM-based congestion management methods as a result of a LAA on aggregators. This contribution is achieved by fulfilling the following objectives:

- Distributed and centralized market-based congestion management techniques are studied. Vulnerability of Distributed Dynamic Tariff (DDT) congestion management methods to cyber attacks is then assessed.
- Develop an attack model that achieves various adversary objectives in compromising aggregators. The attack model is formulated from the attacker's perspective minimizing the number of aggregators needed to be compromised in the network.
- Verify the effectiveness of the proposed models by simulating the IEEE 33 bus network to evaluate a cyber attack's impact on congestion and congestion tariffs.

The remainder of the chapter is organized as follows: Section 3.2 formulates the LAA model. The IEEE 33 bus system is illustrated as a case study in section 3.3 to demonstrate the effect of attacks on the network, followed by the conclusions in Section 3.4.

## 3.2 Modeling of a Load Altering Cyber Attack

To study the vulnerability of congestion management methods to cyber attacks, the DDT technique, proposed in [26], is initially simulated. The DDT method is adopted in this chapter due to its distributed nature compared to the centralized dynamic tariff method [24] in which the network operator is responsible for forecasting the electricity prices and the flexible load in the network. However, if the DNO's forecast is inaccurate, then the congestion tariff imposed would not be an effective solution for congestion mitigation. On the other hand, in the DDT method, aggregators are responsible for providing their load forecast to the network operator, and hence, the DNO is not solely responsible for determining the congestion tariff. This distributed calculation of the congestion tariff increases the certainty and transparency of the model. In this section, LAA are modeled to determine the aggregators that require minimum scaling of their load portfolio to compromise to achieve the objective of the cyber attacker.

### 3.2.1 Attack Model

For the DNO to determine the congestion tariff, consumers need to submit their flexible load utilization preferences to their respective aggregators. In turn, the aggregators need to determine their consumers' load profiles and submit their day-ahead load schedules to the DNO. Hence, the communication network of the smart grid forms the basis of information exchange between the consumers' smart meters, the aggregators, and the network operator. As illustrated in Figure 3.1, Home Area Network (HAN) are deployed at the lowest level, within residential and commercial units, to connect the various flexible and non-flexible loads of the consumers to the smart meters. The Neighborhood Area Network (NAN) is utilized to connect the aggregators to their customers' smart meters. And finally, Wide Area Network (WAN)s are utilized to facilitate communication between the aggregators and the utility operator. Aggregators, hence, can communicate their optimal load schedules to the DNO, which in turn, computes and conveys the congestion tariff to them. Congestion management methods' cyber reliance on the DNO's control center, the aggregators' management systems, the consumers' smart meters, and the communication infrastructure makes these points vulnerable to a cyber attack if not secured properly.

In this chapter, the vulnerability of indirect congestion management methods to cyber attacking aggregators or their communication link with the DNO, affecting the integrity of aggregators load profiles is studied. The attack model involves the following assumptions:

- The attacker has knowledge of subnetwork, $\mathbb{S}$, of the distribution system's topology [82] [83].

- The attacker is assumed to have been eavesdropping on $\mathbb{S}$ and hence, has knowledge of its historical load data [82].
- The attacker is capable of performing load flow analysis to predict which aggregator to attack [84] [82].
- All aggregators are assumed to have no incentive to lie.
- All aggregators are equally prone to be attacked.

The main objectives of the attacker for compromising aggregators can be summarized as follows:

- Create fake congestions causing the distribution network operator to impose high congestion tariffs.
- Alter aggregators' response to a congestion tariff imposed resulting in fake congestion.
- Hide congestion from being detected in the day-ahead market causing unresolved congestion in real-time.

Based on the aforementioned attack assumptions and objectives, the following section explains the modeling of load altering attacks compromising aggregators in the network.

### 3.2.2 Load Altering Attacks (LAA)

To determine possible congestions and calculate the congestion tariff, the DNO relies on the load profiles, $P^a_{i,t}$ (2.2), received from the aggregators in the network. In a LAA, an attacker compromises $N_c$ aggregators of the existing $N_a$ aggregators and changes their load profiles, $P^a_{i,t}$, that is sent to the DNO. The attacker is assumed to have been eavesdropping on $\mathbb{S}$ and has collected enough historical data to determine when a specific feeder is near congestion. The attacker then formulates an optimal attack to minimize the number of aggregators, $N_c$, needed to be compromised by solving the following Mixed Integer Non-Linear Programming (MINLP):

$$\min \sum_{a \in N_a} A^a \tag{3.1}$$

$A^a$ is a binary variable equal to 1 if aggregator $a$ or it's link with the DNO is attacked and 0 otherwise. Moreover, assuming a worst-case scenario in which an attacker has knowledge of $\mathbb{S}$ and historical load forecast (e.g. a disgruntled employee at the utility who has access

to such information), the attacker uses equality constraint (3.2) to perform power flow analysis and compute the power flowing in each branch.

$$\begin{aligned} P^G_{i,a} - P^L_{i,a}(1+\Delta^a_i) &= V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\cos\delta_{ij} + B_{ij}\sin\delta_{ij}) \\ Q^G_{i,a} - Q^L_{i,a}(1+\Delta^a_i) &= V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\sin\delta_{ij} - B_{ij}\cos\delta_{ij}) \end{aligned} \tag{3.2}$$

where $\{P^G_{i,a}, Q^G_{i,a}\}$ are the generated real and reactive power at bus $i$ of aggregator $a$, $\{P^L_{i,a}, Q^L_{i,a}\}$ are the load real and reactive power, $\Delta^a_i$ is the change in aggregator's $a$ bus $i$ load demand due to a cyber attack, $V_i$ is the voltage at bus i, $\{G_{ij}, B_{ij}\}$ are the conductance and susceptance of the $(i,j)$ element of the admittance matrix, and $\delta_{ij}$ is the difference between voltage angles of bus $i$ and $j$. Moreover, equality constraint (3.3) is used to optimally attack the load profiles of the buses as follows,

$$\Delta^a_i = A^a X^a_i, \forall i \in N_d, \forall a \in N_a \tag{3.3}$$

where $X^a_i$ is the attack value for bus $i$. Since DSM-based congestion management is performed day-ahead, the network operator cannot use bad data detection and compare the power flows with a real-time estimate or measurement to know if it's false data or not. Instead, to make sure that it does not raise any alarms, constraints (3.4) and (3.5) are used as follows,

$$-\gamma \leq X^a_i \leq \gamma, \forall i \in N_d, \forall a \in N_a \tag{3.4}$$

$$0.95 \leq V_i \leq 1.05, i \in N_d \tag{3.5}$$

where $\gamma$ is the maximum scaling factor of the compromised aggregators' load schedule. LAA causes congestion to increase or decrease compared to reality based on the objective of the attacker to increase or hide existing congestion. The formulation of these two attack models is explained next.

### Creating and/or Increasing Congestion

To cause and/or increase congestion in a feeder connecting buses $x$ and $y$ in the distribution network, constraint (3.6) is imposed to ensure that the power flowing in branch $(x,y)$ is larger than its maximum power flow limit $P^{max}_{i,j}$.

$$P_{i,j} > P^{max}_{i,j}, \text{for } i = x \text{ and } j = y \tag{3.6}$$

Moreover, the lower limit of constraint (3.4) is set to zero to have only positive scaling factors, $X_i^a$. This ensures that the attack is increasing the existing load profile, $P_{i,t}^a$, of the compromised aggregator causing or creating congestion in branch $(x, y)$.

Hence, MINLP (3.7) needs to be solved using peak time data to obtain the minimum number of $N_c$ aggregators to compromise and their respective attack vectors, $X_i^a$, for different maximum scaling factors, $\gamma$.

$$\min \sum_{a \in \mathbb{A}} A^a \tag{3.7a}$$

$$\text{s.t. } 0.95 \leq V_i \leq 1.05, i \in N_d \tag{3.7b}$$

$$P_{i,j} > P_{i,j}^{max}, \text{for } i = x \text{ and } j = y \tag{3.7c}$$

$$0 \leq X_i^a \leq \gamma, \forall i \in N_d, \forall a \in N_a \tag{3.7d}$$

$$\Delta_i^a = A^a X_i^a, \forall i \in N_d, \forall a \in N_a \tag{3.7e}$$

$$P_{i,a}^G - P_{i,a}^L(1 + \Delta_i^a) = V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\text{cos}\delta_{ij} + B_{ij}\text{sin}\delta_{ij}) \tag{3.7f}$$

$$Q_{i,a}^G - Q_{i,a}^L(1 + \Delta_i^a) = V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\text{sin}\delta_{ij} - B_{ij}\text{cos}\delta_{ij}) \tag{3.7g}$$

The binary variable, $A^a$ and the power flow constraints, causes the non-convexity of (3.7). Hence, the results obtained can represent a local optimal solution. However, a local optimal solution is sufficient to achieve the objective of the attacker to create a fake congestion impacting congestion tariffs. The attacker hence compromises the resulting aggregators, $N_c$, and scales their load profiles, $P_{i,a}^a$, using their corresponding attack values obtained by solving (3.7). These load profiles are then received by the DNO who then attempts to relieve the increase in congestion seen as a result of the cyber attack by imposing larger congestion tariffs, $r_{i,t}$.

### Hiding Congestion

An attacker is also capable of compromising aggregators' load profiles such that congestion is masked. This would result in the DNO not to take any corrective actions to resolve existing congestion. No tariff is imposed to decrease demand at peak times. Eventually, congestion needs to be dealt with in real-time otherwise the network assets would be affected. To perform such an attack, the attacker uses historical data obtained from

eavesdropping to determine the typical time in which congestion is seen. The attacker determines the optimal minimum number of aggregators to attack, $N_c$, solving the following,

$$\min \sum_{a \in \mathbb{A}} A^a \tag{3.8}$$

$$\text{s.t. } P_{i,j}^{max} - \beta < P_{i,j} < P_{i,j}^{max} \tag{3.8a}$$

$$-\gamma \leq X_i^a \leq 0, \forall i \in N_d, \forall a \in N_a \tag{3.8b}$$

$$0.95 \leq V_i \leq 1.05, i \in N_d \tag{3.8c}$$

$$\Delta_i^a = A^a X_i^a, \forall i \in N_d, \forall a \in N_a \tag{3.8d}$$

$$P_{i,a}^G - P_{i,a}^L(1 + \Delta_i^a) = V_i \sum_j^{N_{bus}} V_j(G_{ij}\cos\delta_{ij} + B_{ij}\sin\delta_{ij}) \tag{3.8e}$$

$$Q_{i,a}^G - Q_{i,a}^L(1 + \Delta_i^a) = V_i \sum_j^{N_{bus}} V_j(G_{ij}\sin\delta_{ij} - B_{ij}\cos\delta_{ij}) \tag{3.8f}$$

Inequality constraint (3.8a) has been added to obtain the attack values for the compromised buses such that the power flowing in the feeder of interest is less than its maximum limit ensuring that congestion is not detected by the congestion management program. However, to avoid the optimization algorithm setting the power flowing in the main branch to zero, parameter $\beta$ is added as a very small number to ensure the stealthiness of the attack. Moreover, the attack value, $X_i^a$ is limited to negative values to decrease the compromised aggregators' load profiles using (3.8b).

Solving MINLP (3.8), the resulting attack vectors, $X_i^a$, are used to modify the load profiles of the $N_c$ aggregators. Being a non-convex problem, the results can represent a local optimum solution. However, a locally optimal solution suffices to achieve the objective of the attacker to hide existing congestion affecting the effectiveness of the technique in relieving congestion in the day-ahead market.

Figure 3.2 summarizes the process involved in calculating congestion tariff. It also demonstrates the parallel work of the attacker in compromising aggregators' load profiles to achieve its objective of faking or hiding congestion.

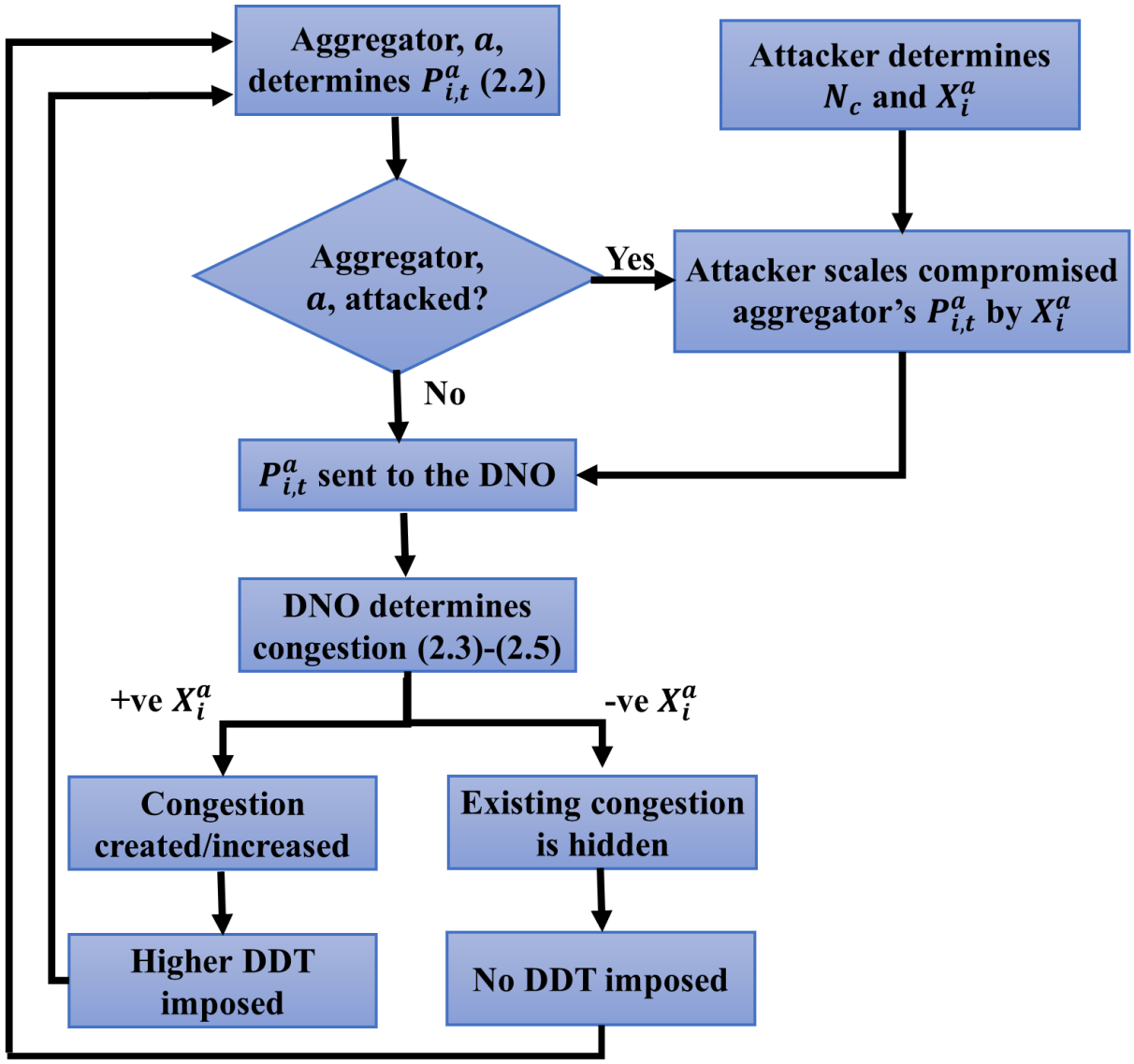



Figure 3.2: Flowchart of cyber attack on DDT-congestion management method

## 3.3 Case Study

To simulate the DDT congestion management method, the IEEE 33 bus system [1], illustrated in Figure 3.3, is utilized. Having 32 load buses, the IEEE 33 bus system is represented by nine aggregators having comparable loads. All the load buses, except bus

23 and 24, are assumed to be residential, having both flexible and non-flexible loads. Residential base load profiles are designed to have a maximum load equivalent to the default loading of the IEEE 33 test bus system. Table 3.1 represents the base load of the residential buses of the IEEE 33 bus system and the number of houses per bus. On the other hand, residential flexible loads are represented by one Electric Vehicle (EV) and one Heat Pump (HP) per house. Having the largest base load, load bus 23 and 24 were utilized as commercial buses consisting of Fast Charging Direct Current (FCDC) EV charging parking lots. These buses are represented by aggregators 6 and 7 respectively. Table 3.2 illustrates the various parameters needed for simulating the operation of the HPs and EVs. Data obtained from Toronto Parking Authority (TPA) [85] representing the daily hourly arrival and departure times of combustion engine cars in a commercial area parking lot in Toronto was used to simulate the availability of EVs in the commercial lots. In the absence of an EV from the lot, the EV was assumed to be at home. A subset of the TPA data was utilized such that the minimum parking duration exceeds the charging time required. The initial state of charge (SOC) of each EV is randomized to be uniformly distributed between 20% and 30% and is assumed that the EV needs to be completely charged on departure. GAMS [86] was used for executing the optimizations, and MATLAB was used for determining the congestion tariff imposed by the DNO to relieve congestion.

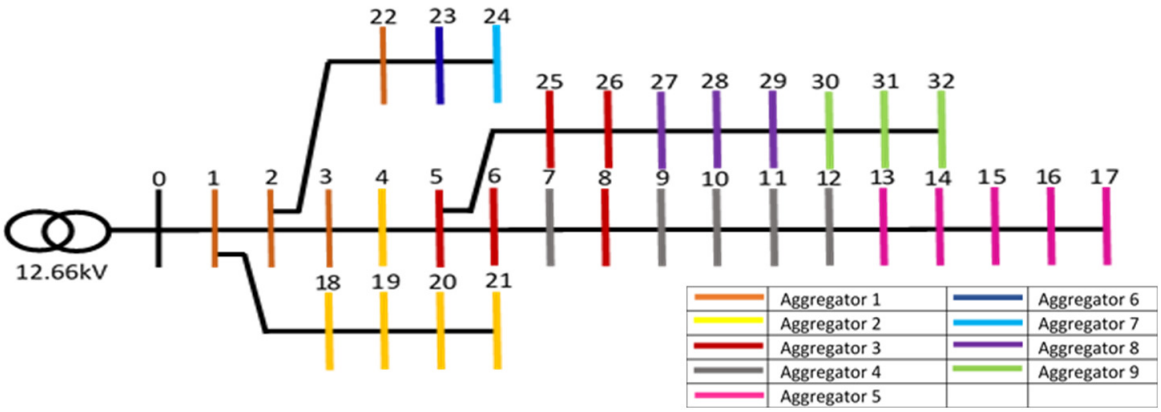



Figure 3.3: IEEE 33 bus system [1]

Table 3.1: Residential Bus Loading

| Bus # | No. of Houses | Load (kW) | Bus # | No. of Houses | Load (kW) | Bus # | No. of Houses | Load (kW) |
|---|---|---|---|---|---|---|---|---|
| 2 | 25 | 100 | 12 | 16 | 60 | 22 | 23 | 90 |
| 3 | 23 | 90 | 13 | 16 | 60 | 25 | 22 | 90 |
| 4 | 31 | 120 | 14 | 29 | 120 | 26 | 15 | 60 |
| 5 | 16 | 60 | 15 | 15 | 60 | 27 | 15 | 60 |
| 6 | 15 | 60 | 16 | 15 | 60 | 28 | 15 | 60 |
| 7 | 50 | 200 | 17 | 15 | 60 | 29 | 30 | 120 |
| 8 | 51 | 200 | 18 | 23 | 90 | 30 | 50 | 200 |
| 9 | 15 | 60 | 19 | 23 | 90 | 31 | 38 | 150 |
| 10 | 15 | 60 | 20 | 23 | 90 | 32 | 53 | 210 |
| 11 | 12 | 45 | 21 | 23 | 90 | 33 | 16 | 60 |

### 3.3.1 Choice of maximum scaling factor, $\gamma$

Scaling factor, $\gamma$ (3.4), was used to limit the maximum change in the load portfolio, $P^a_{i,t}$, of the compromised aggregators. Simulations were carried out in MATLAB R2018a using a PC with an Intel Core(TM) i7-4790 CPU, 3.6 GHz, and 8 GB RAM to study the effect of $\gamma$ on the convergence time of the DDT congestion management method. As illustrated in Table 3.3, $\gamma = 0$ represents a system that is not compromised. Time needed to determine congestion tariff was observed to increase from 286 seconds, for $\gamma = 0$, by 168% for $\gamma = 1$, and by 573.6% for $\gamma = 2$. This increase is as a result of requiring more iterations to shift the flexible demand of consumers to other times while meeting their preferences. However, the attacker only needed to compromise one aggregator to achieve its objective. Larger values of scaling factors, ($\gamma > 1$), would result in larger attack values that would increase the chances of being detected by the DNO. A scaling factor, $\gamma$, less than 0.05 was observed to not cause congestion while a $\gamma$ larger than 2 was observed to cause non-convergence of the congestion management optimization problem. This results in the congestion not being relieved from the network. To avoid risking the stealthiness of LAA, the attack implemented should not cause the loads to largely deviate from their original values as it will raise alarms. Hence, $\gamma$ of 0.1 and 2 were chosen to study the impact of a stealthy attack versus an extreme attack on congestion in the network.

Table 3.2: Case Study parameters

| Variable | Value | Variable | Value |
|---|---|---|---|
| COP | 2.2 | Residential Areas | 1500-2500 sq.ft |
| Residential Height | 8.2 ft. | Temperature Range | 18-24°C |
| EV battery size | 36 kWh | Residential EV power | 11 kW |
| FCDC EV power | 50 kW | Initial SOC of EV | 0.2-0.3 |
| Power flow limit | 7.91 MW | Voltage limits | 0.95-1.05 pu |

### 3.3.2 Creating and/or Increasing Congestion

Using historical data, the attacker is aware that the main branch is near congestion at peak time. Utilizing peak time data, (3.7) is solved, for $\gamma = 0.1$, to obtain the minimum number of aggregators, $N_c$, to compromise and their respective attack vectors, $X_i^a$. Aggregators 3, 6, and 7 were identified as optimal aggregators to be compromised and Table 3.4 illustrates the optimal aggregators that a cyber attacker should compromise and their optimal attack vectors resulting from solving optimization problem (3.7) when $\gamma = 0.1$. However, on changing $\gamma$ to 2, (3.7) resulted in compromising only aggregator 7 with an attack value of 1.9981. These attack values are then utilized to alter the load profiles of the aggregators by $\Delta_i^a$ (3.3) before being sent to the DNO to determine the congestion tariff using (2.3)-(2.5).

Figure 3.4 depicts the effect of the LAA on the power flow in branch $(0-1)$ of the IEEE 33 bus system. As observed, in the absence of an attack, the power flow in the main feeder is already congested at time 12 as it is peak time and demand for FCDC charging is high. For $\gamma = 0.1$, the optimal attack values, $X_i^a$, determined from solving (3.7), increases

Table 3.3: Effect of $\gamma$ on convergence time

| $\gamma$ | Convergence time (sec) | % Increase in time | No. of compromised aggregators |
|---|---|---|---|
| 0 | 285.843877 | - | - |
| 0.1 | 422.279258 | 47.73% | 3 |
| 0.5 | 509.393095 | 78.21% | 1 |
| 1 | 766.977701 | 168.32% | 1 |
| 2 | 1925.429139 | 573.6% | 1 |

Table 3.4: Aggregators compromised due to a LAA creating/increasing congestion

| **Aggregtor No.** | **Bus Number** | **Attack Value** |
|---|---|---|
| 3 | 5 | 0.0536 |
| | 6 | 0.0579 |
| | 8 | 0.0568 |
| | 25 | 0.0683 |
| | 26 | 0.0550 |
| 6 | 23 | 0.0856 |
| 7 | 24 | 0.0964 |

the aggregators load profiles. Consequently, the power flow in branch $(0-1)$ increases, and the impact of the attack is significantly observed between times 10 to 12 since the commercial bus is most active at that time. As observed in Figure 3.4, congestion at $t = 12$ is observed to increase, and a fake congestion is created at $t = 10$ and 11 though the main feeder, in reality, is not congested. This fake congestion would then be attempted to be redistributed to other times using the congestion tariff imposed. The aggregators would attempt to encourage the consumers to shift their demand to other times. However, when $\gamma = 2$, altering the load profile of aggregator 7 by 1.9981 (the attack value obtained solving (3.7)), resulted in a fake increase in congestion at times 9 to 12. This unreal congestion has to be dealt with by the DNO in the day-ahead market. Moreover, at $t = 12$, the existing congestion increased drastically causing the network operator to impose a much higher tariff if the attack goes undetected. However, since the DNO would have historical data and would perform short term load forecast, the chances of such an attack being detected are high.

Figure 3.5 demonstrates the effect of the LAA on congestion tariff, $r_{i,t}$, imposed by the DNO. In the absence of an attack, the imposed tariff increases the price of electricity at $t = 12$ by 16.6% to clear the congestion. Also, no tariff was imposed at $t = 10$ and 11 since there was no congestion. However, a LAA results in a higher DDT at congestion times to alleviate the increased levels of feeder overload. A LAA, with $\gamma = 0.2$, increases the imposed tariff by an unnecessary 14.4% at $t = 12$. Customers, hence, have to pay a higher DDT of $0.028\$/kW$ instead of $0.015\$/kW$. Also, as a result of the unreal congestion being created at $t = 10$ and 11, a needless tariff is imposed by the DNO to solve the fake congestion. Customers who cannot change their demand from those times now have to pay 8.82% and 10% more at $t = 10$ and 11 respectively. This corresponds to approximately an increase of $0.01\$/kW$. Customers are, otherwise, inconvenienced in changing their demands

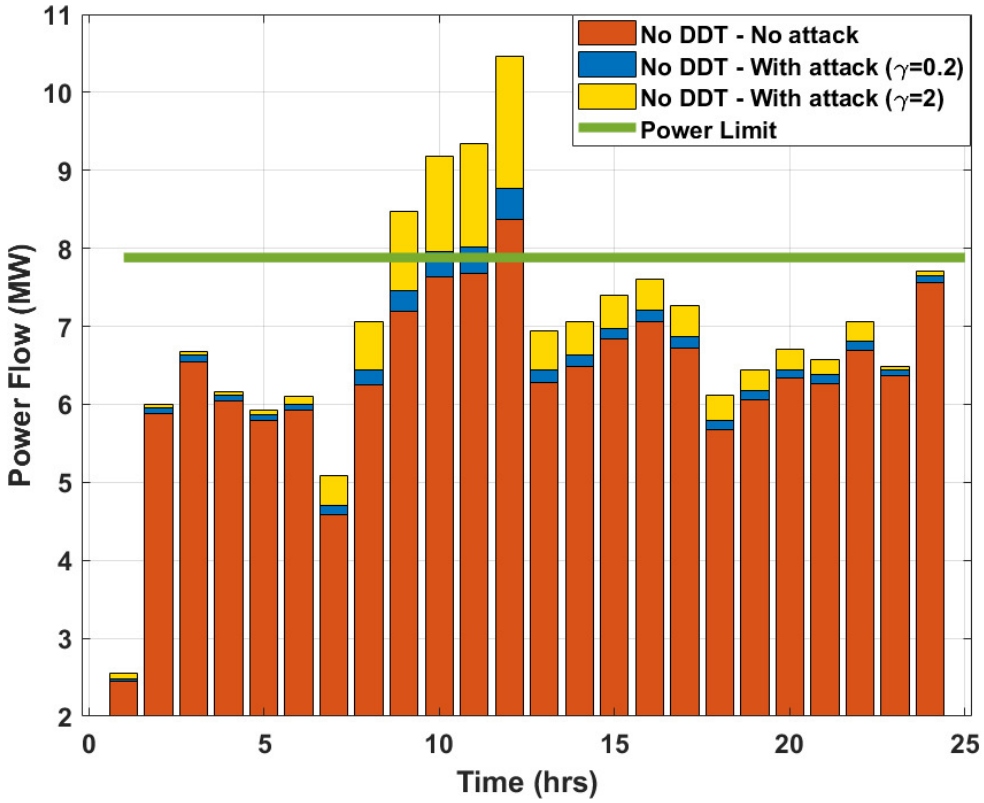



Figure 3.4: Impact of a LAA on the loading of line 0-1

to other times which in reality is unnecessary. On the other hand, for a LAA with a $\gamma = 2$, the imposed DDT at $t = 12$, increases the price by a needless 237%. Customers, hence, have to pay a higher DDT of $0.3053\$/kW$ instead of $0.1063\$/kW$. Also, as a result of fake congestion being created at $t = 10$ and 11, an unnecessary tariff is imposed by the network operator. Customers now have to pay approximately 170% more at $t = 10$ and 11, which corresponds to an increase of approximately $0.195\$/kW$. Moreover, at $t = 9$, customers should now pay 142% more for their demand which corresponds to an increase of $0.181\$/kW$.

### 3.3.3 Hiding Congestion

Using historical data, the attacker is assumed to be aware that the main branch is congested at peak time corresponding to $t = 12$. Hence, using peak time data, MINLP (3.8) is solved to obtain the minimum number of aggregators to compromise and their respective attack vectors, $X_i^a$. Note that in this case scenario, negative $\gamma$ values are adopted

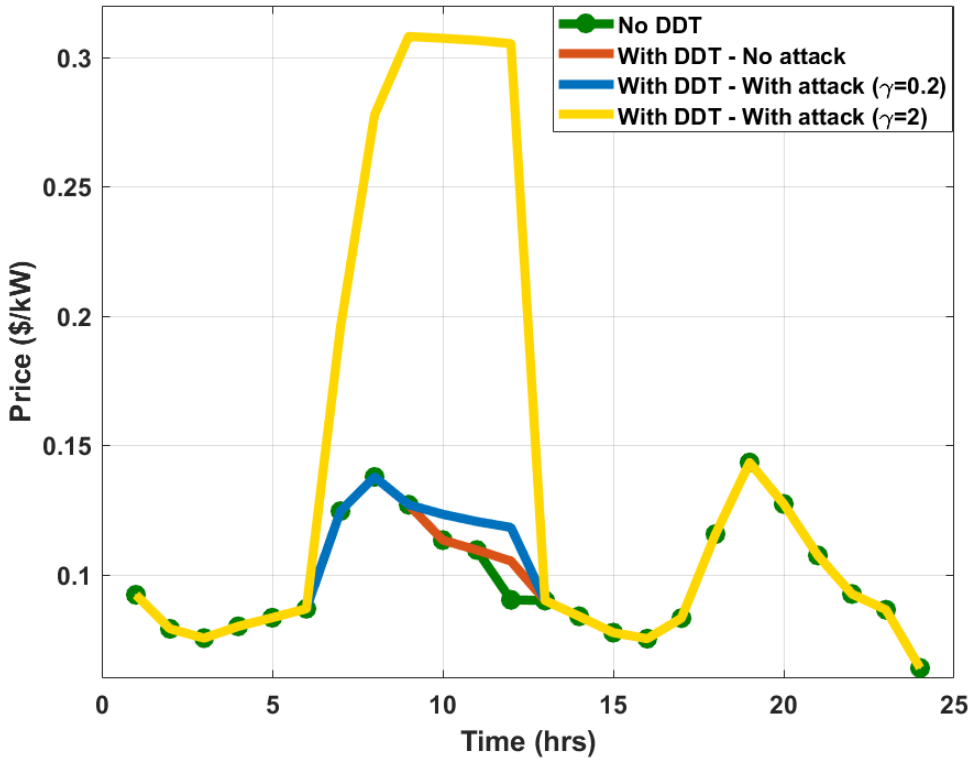



Figure 3.5: Impact of a positive attack value LAA on the electricity price

to ensure that the compromised aggregators' load is lower than reality causing congestion to be masked. In our simulation, $\gamma = 0.1$ is chosen to avoid large differences from the original load profile and not raise any alarms, ensuring the stealthiness of the attack.

Table 3.5 illustrates the optimal aggregators to compromise, $N_c$, and their respective attack vectors, $X_i^a$, that an attacker utilizes to hide congestion. As observed, solving (3.8) for $\gamma = 0.1$ results in identifying aggregators 3, 6, 7, and 9 that an attacker should compromise to hide congestion. The maximum attack values, $X_i^a$, for the four aggregators were determined as $-0.0876$, $-0.0983$, $-0.0999$, and $-0.0820$ for aggregators 3, 6, 7, and 9 respectively. These attack values are then utilized by the attacker to compromise the aggregators' load profiles by $\Delta_i^a$ (3.3) for $a = 3, 6, 7$, and 9 to mask the existing congestion. All aggregators in the network send their load profiles to the DNO who determines the congestion tariff using (2.3)-(2.5). However, as a consequence of the attack which decreased the compromised aggregators load profiles, congestion of branch $(0 - 1)$ of the IEEE 33 bus system at $t = 12$ was successfully masked, as illustrated in figure 3.6. To hide the

congestion happening at $t = 12$, the $N_c$ aggregators' load profiles determined by solving (3.8) are compromised with attack values illustrated in Table 3.5. Since the attack values are negative, the load profiles of the compromised aggregators, $N_c$, decrease causing the congestion at $t = 12$ not to be detected by the DNO as observed in Figure 3.6. Moreover, nearly congested times are observed to be less congested than actual. The network operator, seeing no congestion, does not impose any tariff, as observed in Figure 3.7. In reality, a DDT of 16.6% of the electricity price should have been imposed by the DNO to relieve the congestion that was masked. Moreover, branch $0 - 1$ was near congestion at $t = 10 - 11$. But, as a result of the LAA, the line is observed to be less congested than reality. This will cause a problem in real-time as customers have not been motivated to shift their demand to off-peak times. The DNO has to then try to solve the congestion otherwise network assets will get affected.

Table 3.5: Aggregators compromised due to a LAA hiding congestion

| **Aggregator No.** | **Bus Number** | **Attack Value** |
|---|---|---|
| 3 | 5 | -0.0647 |
| | 6 | -0.0780 |
| | 8 | -0.0748 |
| | 25 | -0.0876 |
| | 26 | -0.0743 |
| 6 | 23 | -0.0983 |
| 7 | 24 | -0.0999 |
| 9 | 30 | -0.0807 |
| | 31 | -0.0820 |
| | 32 | -0.0757 |

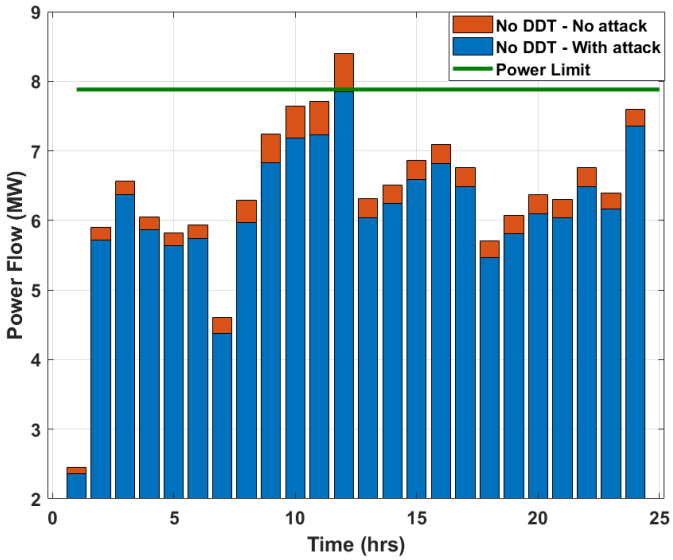



Figure 3.6: Impact of a LAA aiming to hide congestion on line 0-1

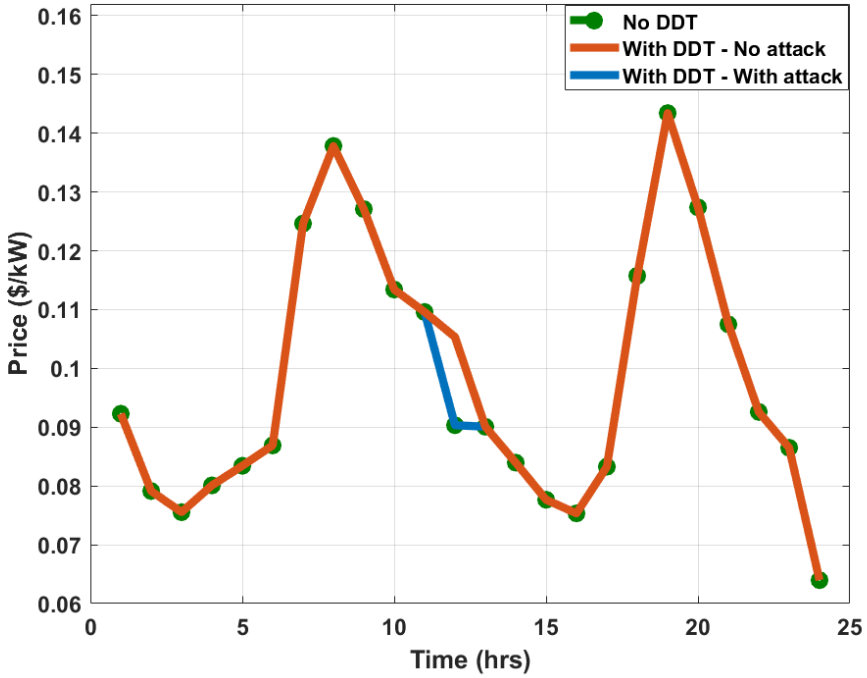



Figure 3.7: Impact of LAA aiming to hide congestion on the electricity price

### 3.3.4 Computational Scalability

To test the effect of LAA on congestion management in terms of scalability, the IEEE 70 bus system [87] was simulated. The IEEE 70 bus system is an 11-kV radial distribution system having 70 nodes and 79 branches. Similar to the case study adopted, the system is represented using nine aggregators responsible for comparable loads. All the load buses except bus 57 are assumed to be residential, having both flexible and non-flexible loads. Residential non-flexible base load profiles are designed to have a maximum load equivalent to the IEEE 70 bus system default loading. Residential flexible loads are represented by one EV and one HP per house. Having the largest base load, bus 57 is utilized as a commercial bus consisting of FCDC EV charging parking lot with a maximum capacity of 150 EVs. Table 3.6 illustrates the scalability study of an attacker determining the optimal aggregators to attack in the IEEE 70 bus system versus that of the 33 bus system. The case studies were implemented on a PC with an Intel Core(TM) i7-4790 CPU, 3.6 GHz, and 8 GB RAM. As the number of variables and constraints needed to be solved increased,

Table 3.6: Computational Scalability of LAA

| Description | IEEE 33 | IEEE 70 |
|---|---|---|
| No. of variables in (3.7) | 4647 | 19623 |
| No. of constraints in (3.7) | 4582 | 19486 |
| Execution time to determine aggregators to attack | 2.936 sec | 4.581 sec |

the time required by the attacker to determine the critical aggregators in the network increased. However, since this computation is executed offline in the day-ahead market, this increase in time would not cause a problem to the attacker.

## 3.4 Conclusions

Congestion management techniques dependence on the communication infrastructure makes them vulnerable to cyber attacks. A LAA can create or hide congestion. In the event of a cyber attack compromising aggregators causing fake congestion, congestion tariffs are imposed on consumers increasing their expenditure on purchasing electricity. If the cyber attack continues without it being detected, consumers would be motivated to change their aggregator representative to decrease their cost. On the other hand, a LAA that results in not managing congestion in the day-ahead market, would force the DNO to use active power control in the real-time market. This results in shedding unnecessary loads to prevent activation of protection devices, following National Electric Code article 240 [88]. Load is disconnected from overloaded buses at times when electricity demand is maximum, resulting in dissatisfied customers [89]. Other attacks, such as denial-of-service attacks and load replay attacks can compromise the performance of such congestion management techniques. However, due to limited space, vulnerability of congestion management methods was demonstrated using only LAA.

[1]

[1]This chapter has been published in: Gul M Khan, O., El-Saadany, E., Youssef, A. and Shaaban, M. F. *Cyber Security of Market-Based Congestion Management Methods in Power Distribution Systems.* IEEE Transactions on Industrial Informatics, vol. 17, no. 12, pp. 8142-8153, Dec 2021, doi: 10.1109/TII.2021.3065714.

# Chapter 4

# Load Altering Attacks Mitigation Scheme

## 4.1 Introduction

The impact of cyber attacks, specifically Load Altering Attacks (LAAs), on the efficiency of the congestion management schemes has been demonstrated in Chapter 3. To defend the congestion management schemes against such cyber attacks, a mitigation scheme is required. Until recently, many studies have come up with mitigation schemes to defend against False Data Injection (FDI) attacks in the smart grid as described in Chapter 2. However, existing literature have not determined the critical aggregators in the distribution network that needs to be secured against cyber attacks. In this chapter, Mixed Integer Non-Linear Programming (MINLP) is used to model the mitigation scheme for single- and multiple-point load altering attacks. The optimization problem is solved using the Generalized Benders Decomposition (GBD) approach to determine the critical aggregators in the network. These aggregators are secured by the network operator to make the grid more resilient to such cyber attacks.

The main contribution of this chapter is, hence, to develop a mitigation scheme against LAAs that target aggregators in the distribution network. This contribution is achieved by fulfilling the following objectives:

- Develop a mitigation scheme to determine the critical aggregators in the network to secure against LAAs. The mitigation scheme is prepared from the network operator's perspective, assuming the worst case scenario, to secure the aggregators in

the network which if compromised would result in a stealthy attack. The problem is formulated as a MINLP and is solved using a decomposition technique.

- Verify the effectiveness of the proposed mitigation scheme by simulating the IEEE 33 bus network.

The remainder of the chapter is organized as follows: in Section 4.2 a mitigation scheme is proposed to determine the critical aggregators that need to be secured in the network. Section 4.3 tests the proposed mitigation scheme in an IEEE 33 bus system followed by the conclusions.

## 4.2 Modeling of Mitigation Scheme

In the previous chapter, load altering attacks impacting congestion management methods were introduced, modeled, and simulated. In this section, a mitigation scheme, executed by the Distribution Network Operator (DNO), is proposed to determine the impact that different adversaries with varying intrusion capabilities can have on congestion. An attack that can compromise only one aggregator would require a higher attack value to achieve its objective risking the stealthiness of the attack. However, to compromise multiple aggregators using low attack values, strong cyber intrusion capabilities, as well as a larger effort, is needed to avoid being detected. The LAA mitigation scheme proposed in this chapter identifies the critical aggregators in the network that would be the first choice for an adversary to attack. The term "critical aggregator" refers to aggregators that can be compromised using minimal attack values to achieve the objective of a cyber attacker while evading detection. A MINLP is proposed to determine the attack-prone aggregators in the network. GBD algorithm is then utilized to solve the problem. The DNO would then increase the security enforcement of the resulting critical aggregators and their communication links preventing them from being compromised.

### 4.2.1 Optimization Problem Formulation

MINLP is used to determine the critical aggregators that would be the first point of attack by an adversary aiming to minimize attack values. Besides the constraints considered in (3.7), equality constraint (4.1) is enforced to ensure that the total number of compromised aggregators is equal to $N_c$.

$$\sum_{a \in N_a} A^a = N_c \tag{4.1}$$

Hence, to determine the critical aggregators which would be the first point of attack by an attacker that aims to create and/or increase congestion, the following MINLP needs to be solved:

$$\min \sum_{a \in N_a} \sum_{i \in N_d} X_i^a \tag{4.2a}$$

$$\text{s.t.} \sum_{a \in N_a} A^a = N_c \tag{4.2b}$$

$$P_{i,j} > P_{i,j}^{max}, \text{for } i = x \text{ and } j = y \tag{4.2c}$$

$$\Delta_i^a = A^a X_i^a, \forall i \in N_d, \forall a \in N_a \tag{4.2d}$$

$$-\gamma \leq X_i^a \leq \gamma, \forall i \in N_d, \forall a \in N_a \tag{4.2e}$$

$$0.95 \leq V_i \leq 1.05, i \in N_d \tag{4.2f}$$

$$P_{i,a}^G - P_{i,a}^L(1 + \Delta_i^a) = V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\text{cos}\delta_{ij} + B_{ij}\text{sin}\delta_{ij}) \tag{4.2g}$$

$$Q_{i,a}^G - Q_{i,a}^L(1 + \Delta_i^a) = V_i \sum_{j}^{N_{bus}} V_j(G_{ij}\text{sin}\delta_{ij} - B_{ij}\text{cos}\delta_{ij}) \tag{4.2h}$$

where the lower limit of $\gamma$ (4.2(e)) is set to 0 to ensure the increase in the load of the compromised aggregator. On the other hand, to hide existing congestion, MINLP (4.2) is solved with the upper limit of $\gamma$ (4.2(e)) set to 0. This is done to ensure the decrease in the profile, $P_{i,t}^a$, of the compromised aggregator. Moreover, the power flow inequality constraint is changed to ensure that the power flow in the branch being attacked is lesser than its maximum limit, $P_{i,j}^{max}$. Figure 4.1 summarizes MINLP (4.2) used to determine the critical aggregators in the network and their corresponding attack values.

MINLP (4.2) is a non-linear and non-convex problem due to: (i) non-linearity of equality constraint (4.2(d)), (ii) non-linearity and non-convexity of power flow equations (4.2(g-h)), and (iii) non-convexity caused by the binary variable, $A^a$. This causes the determination of a global solution for the optimization problem difficult. These problems were tackled to succeed in obtaining a global solution for the mitigation scheme proposed.

### 4.2.2 Linearization of the product of two variables

The equality constraint (4.2(d)) is nonlinear due to it being the product of a binary variable, $A^a$, and a continuous bounded variable, $X_i^a$. To linearize (4.2(d)), the following constraints were added to our MINLP formulation [90],

$$X_i^a - (1 - A^a)\overline{X_i^a} \leq \Delta_i^a \leq X_i^a - (1 - A^a)\underline{X_i^a} \tag{4.3}$$

$$A^a \underline{X_i^a} \leq \Delta_i^a \leq A^a \overline{X_i^a} \tag{4.4}$$

where $\overline{X_i^a}$ and $\underline{X_i^a}$ represents the upper and lower limits of the attack value, $X_i^a$. Hence, if the binary variable $A^a = 1$, then equation (4.3) makes $\Delta_i^a = X_i^a$, and (4.4) enforces that $\Delta_i^a$ is bounded within its limits. However, if the binary variable $A^a = 0$, then equation (4.4) makes $\Delta_i^a = 0$, and (4.3) enforces the limits on $X_i^a$. Thus, $\Delta_i^a = X_i^a A^a$. It should be noted that, given $\gamma$ is a constant, for mitigating an attack that aims to create congestion, $\overline{X_i^a}$ represents $\gamma$ while $\underline{X_i^a} = 0$. On the other hand, for mitigating an attack that aims to hide an existing congestion, $\overline{X_i^a} = 0$, while $\underline{X_i^a}$ represents negative $\gamma$.

### 4.2.3 Power Flow Equations Relaxation

Researchers have proposed numerous relaxation and approximation methods to convexify power flow equations. Convex relaxations increase the feasible space to include the non-convex feasible space, providing a lower bound solution to the non-convex problem (for a minimization) [91]. Moreover, convex relaxations can be exact for certain optimization problems making their solution globally optimal. However, the feasible region of power flow approximations does not enclose the feasible space of the non-convex problem. Hence, the global optimality of an approximated power flow problem solution cannot be guaranteed [92]. Semi-definite Programming (SDP) Relaxation and Second-Order Conic Programming (SOCP) Relaxations are the main methods utilized in the literature. SOCP was utilized in this chapter to convexify the power flow equations due to the limited guarantee of the exactness of SDP to only a certain class of problems with certain assumptions. Moreover, SOCP has been demonstrated in the literature to have a computational advan-

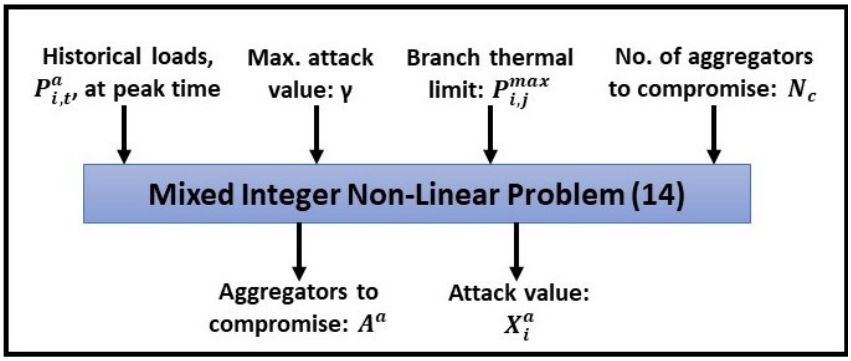



Figure 4.1: High level flowchart of inputs and outputs of mitigation scheme

tage over SDP [93].

SOCP relaxation of the power flow equations involves the introduction of new variables representing the product of voltages. Given voltage at bus $i$ is represented in rectangular coordinates as $V_i = V_{di} + jV_{qi}$, $\forall i \in N_d$, the squared voltage magnitude is represented by $c_{ii}$. Hence, $c_{ii} = |V_i|^2 = V_{di}^2 + V_{qi}^2$. New variables $c_{ij}$, where $c_{ij} = |V_i||V_j|cos(\theta_i - \theta_j) = V_{di}V_{dj} + V_{qi}V_{qj}$, and $s_{ij}$, where $s_{ij} = -|V_i||V_j|sin(\theta_i - \theta_j) = V_{di}V_{qj} - V_{qi}V_{dj}$, are introduced to represent the real and imaginary parts of the product of voltages at bus $i$ and its conjugate at bus $j$ respectively, $\forall\{i,j\} \in N_d$. Using these new variables, the power flow equations (4.2(g-h)) are changed as,

$$\begin{aligned} P_i^G - P_i^L &= c_{ii}G_{i,i} + \sum_{j\neq i}^{N_{bus}} \Big( c_{ij}G_{i,j} - s_{ij}B_{i,j} \Big) \\ Q_i^G - Q_i^L &= -c_{ii}B_{i,i} + \sum_{j\neq i}^{N_{bus}} \Big( -c_{ij}B_{i,j} - s_{ij}G_{i,j} \Big) \end{aligned} \tag{4.5}$$

The following constraints need to be added to the MINLP (4.2),

$$c_{ij} = c_{ji} \text{ and } s_{ij} = -s_{ij}, \forall\{i,j\} \in B \tag{4.6}$$

$$c_{ij}{}^2 + s_{ij}^2 = c_{ii}c_{jj}, \forall\{i,j\} \in B \tag{4.7}$$

where $B$ is the set of lines in the sub-network. However, constraint (4.7) is non-convex. Hence, a convex relaxation is formed by replacing the equality constraint (4.7) to an inequality as illustrated in (4.8),

$$c_{ij}{}^2 + s_{ij}{}^2 \leq c_{ii}c_{jj}, \forall\{i,j\} \in B \tag{4.8}$$

The power flow equations are now a form of SOCP and are convex. Hence, replacing (4.2(g-h)) with (4.5-4.6) and inequality constraint (4.8) results in MINLP (4.9) that needs to be solved and checked for exactness. If the solution for (4.9) satisfies (4.7) then the solution is global.

$$\min \sum_{a \in N_a} \sum_{i \in N_d} X_i^a \tag{4.9a}$$

$$\text{s.t.} \sum_{a \in N_a} A^a = N_c \tag{4.9b}$$

$$0.95 \leq V_i \leq 1.05, i \in N_d \tag{4.9c}$$

$$A^a \underline{X_i^a} \leq \Delta_i^a \leq A^a \overline{X_i^a} \tag{4.9d}$$

$$c_{ij} = c_{ji} \text{ and } s_{ij} = -s_{ij}, \forall \{i,j\} \in B \tag{4.9e}$$

$${c_{ij}}^2 + {s_{ij}}^2 \leq c_{ii} c_{jj}, \forall \{i,j\} \in B \tag{4.9f}$$

$$X_i^a - (1 - A^a)\overline{X_i^a} \leq \Delta_i^a \leq X_i^a - (1 - A^a)\underline{X_i^a} \tag{4.9g}$$

$$P_i^G - P_i^L = c_{ii} G_{i,i} + \sum_{j \neq i}^{N_{bus}} \Big( c_{ij} G_{i,j} - s_{ij} B_{i,j} \Big) \tag{4.9h}$$

$$Q_i^G - Q_i^L = -c_{ii} B_{i,i} + \sum_{j \neq i}^{N_{bus}} \Big( - c_{ij} B_{i,j} - s_{ij} G_{i,j} \Big) \tag{4.9i}$$

### 4.2.4 Using Generalized Bender Decomposition (GBD)

To solve the MINLP (4.9), GBD [94] was utilized. The basic idea in GBD is dividing the MINLP into two parts: the primal and the master problem. The primal problem involves fixing the $y^k$ binary variables, where $k$ is the iteration number, such that the problem is now only in the x-space. $y$ represents $A^a$ which is an array of $N_a$ binary variables. $x$ represents the $n$ continuous variables in our optimization problem. Hence, $x = \{P_i^G, Q_i^G, P_{i,j}, \Delta_i^a, X_i^a, c_{ij}, s_{ij}\}$. The MINLP is reduced now to a nonlinear problem that can be solved using any of the commercial solvers to determine the $x^k$ continuous variables. The solution obtained from the primal problem represents the upper bound, $UB$, solution for MINLP (4.9). The master problem then utilizes the obtained Lagrange multipliers and the $x^k$ variables solution from the primal problem to change the problem to a MIP determining $y^{k+1}$. The solution for the master problem would then represent the lower bound, $LB$, of the global solution. The process is repeated between the primal and the master problem until the sequence of upper bounds are non-increasing and the sequence of lower bounds are non-decreasing, hence, the problem converges. The theoretical development of the primal and master problems are discussed next.

**Primal Problem**

The main MINLP can be defined in standard form as follows,

$$\begin{aligned} &\min_{x,y} f(x,y) \\ &\text{s.t. } h(x,y) = 0 \\ &\quad g(x,y) \leq 0 \end{aligned} \tag{4.10}$$

where $x \in X$ is a non-empty convex set, $y \in Y$ and $Y$ is binary $\{0,1\}$. The complicating binary variable, $y^k$, is fixed to obtain the primal problem at iteration $k$ as follows,

$$\begin{aligned} &\min_{x} f(x,y^k) \\ &\text{s.t. } h(x,y^k) = 0 \\ &\quad g(x,y^k) \leq 0 \end{aligned} \tag{4.11}$$

If the primal problem (4.11) at iteration $k$ is feasible, then the solution for (4.11) results in $x^k$, the upper bound, $z_{nlp}$, solution $f(x^k,y^k)$, and the Lagrange multipliers $\lambda^k$ and $\mu^k$ for the equality and inequality constraints. Hence, the Lagrange function is formulated as,

$$L(x^k,y^k,\lambda^k,\mu^k)^k = f(x,y) + {\lambda^k}^T h(x,y) + {\mu^k}^T g(x,y) \tag{4.12}$$

If the primal problem (4.11) at iteration $k$ is infeasible, then to identify a feasible point an l1 minimization problem is formulated using only the constraints of the primal problem as follows,

$$\begin{aligned} &\min_{x} \sum_{i=1}^{p} \alpha_i \\ &\text{s.t. } h(x,y^k) = 0 \\ &\quad g_i(x,y^k) \leq \alpha_i, \text{ i=1,2,...p} \\ &\quad \alpha_i \geq 0, \text{ i=1,2,...p} \end{aligned} \tag{4.13}$$

The solution for (4.13) results in obtaining the Lagrange multipliers, $\bar{\lambda}^k$ and $\bar{\mu}^k$, for the equality and inequality constraints. The resulting Lagrange function for the infeasible primal problem is hence as follows,

$$\bar{L}(x^k,y^k,\bar{\lambda}^k,\bar{\mu}^k)^k = \bar{\lambda}^{kT} h(x,y) + \bar{\mu}^{kT} g(x,y) \tag{4.14}$$

### Master Problem

To formulate the master problem, $v(y)$ is defined as follows,

$$\begin{aligned} v(y) = \inf_x \; & f(x,y) \\ \text{s.t. } & h(x,y) = 0 \\ & g(x,y) \leq 0 \end{aligned} \tag{4.15}$$

Set $V$ is then defined as,

$$V = \{y : h(x,y) = 0, g(x,y) \leq 0 \text{ for some x } \in X\} \tag{4.16}$$

Hence, to project (4.10) into the $y$-space, (4.10) is rewritten as,

$$\begin{aligned} \min_y \; & v(y) \\ \text{s.t. } & y \in Y \cap V \end{aligned} \tag{4.17}$$

To determine the region that contains $V$ for the infeasible primal problem, the dual of $V$ is determined as follows,

$$0 \geq inf \; \bar{L}(x,y,\bar{\lambda},\bar{\mu}), \forall \bar{\lambda},\bar{\mu} \in \psi \tag{4.18}$$

Similarly, for the feasible primal problem scenario, the dual representation of $v(y)$ is determined as follows,

$$v(y) = \sup_{\lambda,\mu} \inf_x L(x,y,\lambda,\mu) \tag{4.19}$$

Substituting (4.19) and (4.18) into (4.17) results in the following master problem,

$$\min_{y,\theta} \; \theta \tag{4.20a}$$

$$\text{s.t. } \theta \geq \inf_x L(x,y,\lambda,\mu) \tag{4.20b}$$

$$0 \geq inf \bar{L}(x,y,\bar{\lambda},\bar{\mu}) \tag{4.20c}$$

where inequality constraint (4.20(b)) is referred to as the optimality cut, and (4.20(c)) is known as the feasibility cut. The solution for (4.20) results in determining a lower bound, $LB$, solution for (4.10). Figure 4.2 illustrates the steps involved in executing the GBD algorithm to solve the optimization problem.

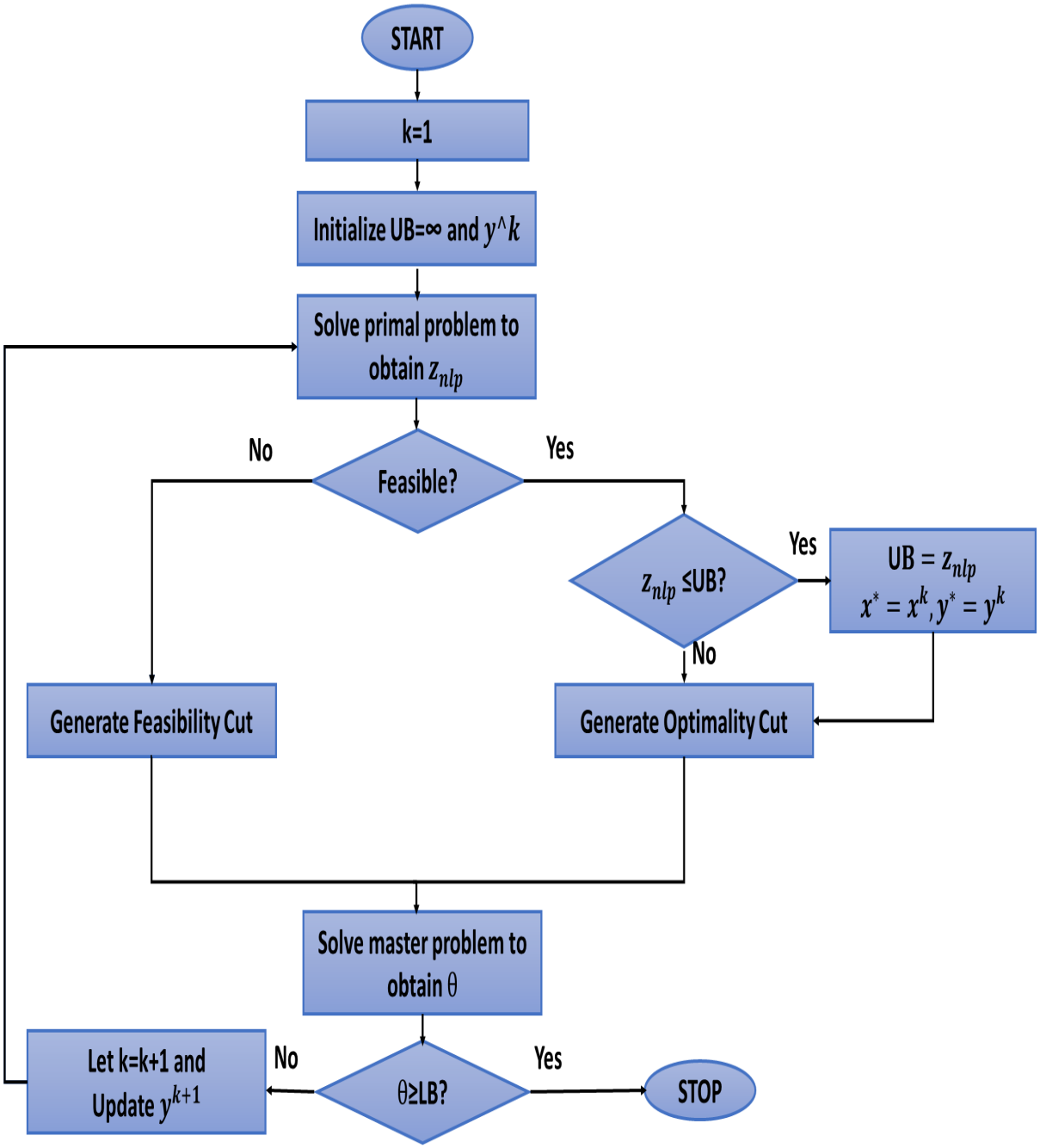



Figure 4.2: Generalized Bender Decomposition Flowchart

## 4.3 Case Study

The proposed mitigation scheme was tested on the IEEE 33 case study, modeled in Chapter 3 section 3.3, which was assumed to be compromised using LAAs. For identifying the most critical aggregator in the network, $N_c$ (4.1) was set to 1. GBD resulted in identifying aggregator 7 as the optimal aggregator to attack with a minimal attack value, $X_i^a$, of 0.1762. Thus, to ensure a stealthy attack, an adversary's first choice of attack to cause congestion during peak time is to attack aggregator 7. This is a realistic choice since commercial bus 7 is at peak load at that time, having an FCDC parking lot, compared to the other buses. Hence, the security of aggregator 7 needs to be reinforced. For a multi-point attack, where multiple aggregators are compromised, $N_c$ (4.1) was set to 2. The GBD problem resulted in identifying aggregators 6 and 7 as the optimal choice for being compromised with a maximum attack value, $X_i^a$, of 0.095. On the other hand, for a multi-point attack where $N_c = 3$, aggregators 3, 6, and 7 were identified as critical aggregators that would require the minimum amount of load scaling of 0.054 to achieve a stealthy attack. All the solutions obtained were observed to be exact on testing using the equality constraint (4.7). As expected, as the number of critical aggregators increased, the attack value obtained by solving the GBD problem was lower. Hence, security reinforcement of aggregators 3, 6, and 7 would mitigate a LAA that aims to create congestion in the network.

For an adversary that aims to hide congestion, the GBD algorithm was executed on MINLP (4.9) with negative $\gamma$. Also, the power flow in the branch is ensured to be lesser than its maximum limit. For identifying the most critical aggregator in the network, $N_c$ (4.1) was varied between 1 to 3. The optimization problem resulted in identifying aggregator 7 as the critical aggregator that needs to be secured in the event of a single point attack. On the other hand, for a multi-point attack, the optimization problem resulted in identifying aggregators 3, 6, and 7 as the three most critical aggregators in the network. These aggregators are capable of achieving the objective of the cyber attackers with an attack value, $X_i^a$, as low as $-0.17$. All the solutions obtained were observed to be also exact on testing using the equality constraint (4.7). Hence, security reinforcement of aggregators 3, 6, and 7 would mitigate a load altering cyber attack that aims to create congestion, increase existing congestion, or hide congestion in the network.

### 4.3.1 Computational Scalability

To test the scalability of the proposed mitigation scheme, the performance of the algorithm was tested on the IEEE 70 bus system [87]. As illustrated in Table 4.1, using GBD to determine the critical aggregator in the network that needs to be secured, the number of variables in the master problem depends on the number of aggregators. In the current case scenario, 9 aggregators were used to represent both networks. Also, the number of variables and constraints in the primal problem of the IEEE 70 system is nearly double that of the IEEE 33 bus system. This, however, did not have a large effect on the time required to determine the critical aggregators.

### 4.3.2 Discussion

To decrease the attack value, $X_i^a$, required to create or hide congestion while ensuring its stealthiness, a multi-point attack is more effective than a single point attack. In a multi-point attack, the attacker is capable of distributing the change in load needed to achieve its objective to more aggregators. However, as the number of aggregators compromised increases, the complexity of performing the attack without being detected also increases. Hence, $N_c$ was restricted to only determining the first three critical aggregators. Moreover, for a single point attack, as the security of the first critical aggregator was reinforced, $X_i^a$ required to compromise the second most critical aggregator increases risking the stealthiness of the attack. Aggregators 3, 6, and 7 were the adversary's first choices of attack. Hence, their security needs to be reinforced to prevent LAA. Compromising other aggregators would require the attacker to increase $X_i^a$ to larger values or increase the aggregators compromised risking the stealthiness of the attack. To simulate this scenario, a constraint was added to MINLP (21) preventing aggregators 3, 6 and 7 from being identified as critical. Instead, simulating a single-point attack, resulted in identifying aggregator 4 as the next critical aggregator with an attack value of 0.659. However, to compromise aggregator 7, an attack value of 0.1762 was needed to achieve the objective of the attacker. This

Table 4.1: Computational Scalability of Mitigation Scheme

| **Description** | **IEEE 33** | **IEEE 70** |
|---|---|---|
| No. of variables to solve primal subproblem | 398 | 818 |
| No. of constraints to the primal subproblem | 458 | 926 |
| No. of variables to solve master problem to | 9 | 9 |
| Execution time | 6.411 sec | 6.679 sec |

increase in attack value by more than 200% would affect the stealthiness of the attack. For a multi-point attack, aggregators 2, 3 and 4 were identified as the next set of critical aggregators with a maximum attack value of 0.09. Hence, the attack value increased by 66.67% which increases the chance of it being detected by the DNO. This mitigation scheme needs to be executed by the DNO whenever a new aggregator is introduced in the network, or when any of the aggregators have a major change in their loads (for example installation of Electric Vehicle (EV) charging parking lots).

## 4.4 Conclusion

Cyber security of various entities involved in indirect congestion management techniques is vital for congestion relief. A mitigation scheme was developed to determine the critical aggregators in the network that requires minimal attack values to either fake or hide congestion. Security for these critical aggregators needs to be reinforced to mitigate stealthy LAAs in the day-ahead market. Future work aims to study the effect of other attacks on Demand Side Management (DSM)-based congestion management methods and developing one mitigation scheme for all.

[1]

[1]This chapter has been published in: Gul M Khan, O., El-Saadany, E., Youssef, A. and Shaaban, M. F. *Cyber Security of Market-Based Congestion Management Methods in Power Distribution Systems.* IEEE Transactions on Industrial Informatics, vol. 17, no. 12, pp. 8142-8153, Dec 2021, doi: 10.1109/TII.2021.3065714.

# Chapter 5

# LSTM-based approach to detect cyber attacks on market-based congestion management methods

## 5.1 Introduction

Market-based congestion management methods [24] [25] employ the communication layer to relay consumer preferences to their respective aggregators, price tariffs from Distribution Network Operator (DNO) to aggregators, and load schedules from aggregators to the DNO to mitigate congestion. The success of such congestion management methods, as explained in Chapter 3, relies on the cyber security of all the entities involved and their communication links. Ensuring the confidentiality, integrity, and availability of the DNO, aggregators, consumers' meters, and the information exchanged is vital to resolve congestion using Demand Side Management (DSM).

The DNO is highly secure due to its significant role in the network, making it hard to be cyber attacked. On the other hand, consumers' smart meters and their communication lines are vulnerable to cyber attacks. Detection of attacks on consumers' smart meters and their communication links have been studied in the literature, as described in Chapter 2. Attacking aggregators or their communication links with the DNO is another aspect that can be utilized by a cyber attacker to affect the performance of market-based congestion management methods. The unique position of aggregators in the distribution network, in terms of their connection to their respective Distributed Energy Resources (DER) equipment and the DNO, has been established in [70]. Hence, it is critical to study the impact

of cyber attacks on aggregators and how to detect such attacks. Compromising the cyber security of aggregators could risk the overall security of the grid. Financial losses can be caused as a result of an adversary causing congestions not to be detected in the day-ahead market by the DNO. This would cause unnecessary load shedding that could be avoided if the attack was mitigated. Moreover, cyber attacks can be executed by DNO competitors to fake congestion resulting in higher congestion tariffs to be imposed on the consumers. This would encourage consumers to change their utility provider. Vulnerability of Distributed Dynamic Tariff (DDT) Congestion Management technique [26] to cyberattacks has been studied in [95]. The impact of compromising aggregators, as a result of Load Altering Attack (LAA), on congestion and congestion tariff has been evaluated. LAA were modeled to create fake congestion, cause a congestion increase, and to hide existing congestion. Faking congestion or increasing the level of existing congestion resulted in an unnecessary increase in the price of electricity, which has to be eventually paid by consumers. On the other, hiding existing congestion in the day-ahead market, resulted in no tariff being imposed by the DNO to plan for alleviating the congestion. The DNO, then, has to deal with the congestion in the real-time market using more expensive direct congestion management techniques. However, up to the author's knowledge, no literature exists on the detection of such attacks that compromises aggregators.

The main contribution of this chapter is focused on developing a detection scheme that would determine the presence or absence of a load altering cyber attack compromising aggregators in the distribution network. The detection scheme is to be executed by the DNO in the day-ahead market on receiving aggregators' load profiles prior to computing the congestion tariff. The chapter is organized as follows: Section 5.2 describes a case study using the IEEE 33 bus system which will be referred to in demonstrating LAAs on market-based congestion management techniques. Section 5.3 presents a quick overview of recurrent neural networks followed by cyber attack detection results. The chapter is then concluded in Section 5.4.

## 5.2 Case Study System Details

To simulate load altering attacks on market-based congestion management techniques and the proposed detection model, the IEEE 33 bus system [1], illustrated in Figure 5.1, is adopted. Having 32 load buses, residential consumers are represented using both flexible and base loads. Residential base load profiles are designed to have a maximum load equivalent to the default loading of the IEEE 33 test bus system. On the other hand, residential flexible loads consist of one Heat Pump (HP) and one Electric Vehicle (EV) with a battery

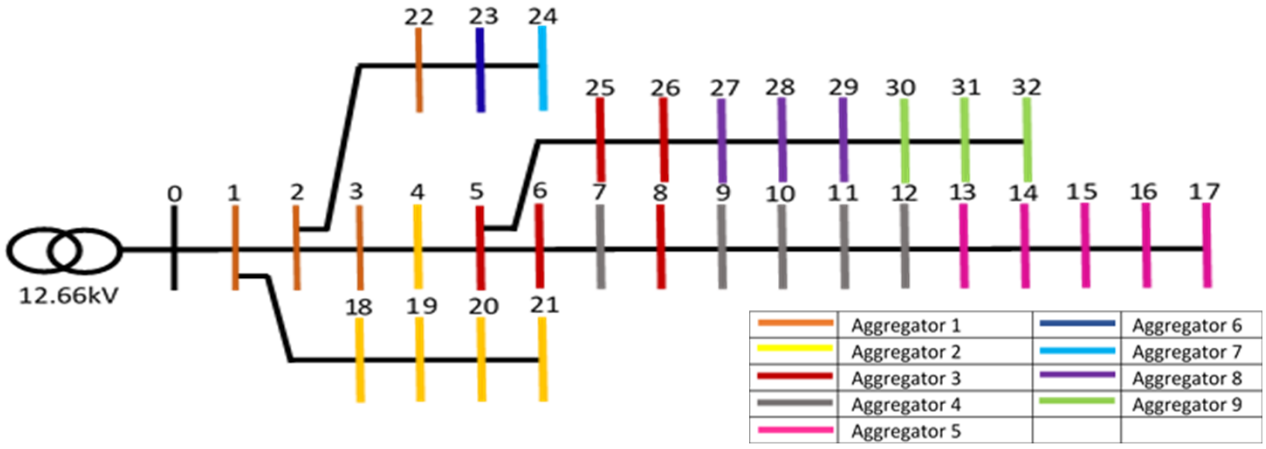



Figure 5.1: IEEE 33 bus system involving nine aggregators [1]

size of 36kWh, per residence. Consumers' preferences in terms of their comfortable indoor temperature range and initial State of Charge (SOC) of EV are randomized to be uniformly distributed between $18-24°C$ and $20-30\%$ respectively. The residential charging power of EVs was chosen as 11kW. All the load buses of the IEEE 33 bus system, are assumed to be residential, having both flexible and non-flexible loads, except bus 23 and 24. Having the largest base-load, load bus 23 and 24 were utilized as commercial buses consisting of Fast Charging Direct Current (FCDC) EV charging parking lots of 50kW. Arrival and departure of EVs from the FCDC parking lot were simulated using data obtained from Toronto parking authority [85]. The absence of an EV from the commercial parking lot was assumed to indicate its presence at its residence. All residential and commercial buses were represented by 9 aggregators having comparable loads, as illustrated in Figure 5.1. Aggregators 6 and 7 are used to represent commercial buses. GAMS [86] was used for executing the optimizations in this chapter. MATLAB was used for determining the congestion tariffs imposed by the DNO to relieve congestion and for implementing the proposed detection scheme.

## 5.3 Detection of LAA

To detect LAAs, Recurrent Neural Network (RNN), specifically Long Short-Term Memory (LSTM) RNN [96], is proposed in this chapter. RNNs fundamentally differ from neural networks being sequential-based models. They are capable of utilizing sequential information to establish a temporal relationship between past and present information. The net-

work, hence, develops a memory of past events and encodes it in its hidden state variables. RNNs are ideal for applications in which there is a temporal dependency in the data [97]. There are many types of RNNs based on their input and output data: sequence input (also known as many-to-one), sequence output (also known as one-to-many), sequence input and output (also known as many-to-many), or synced sequence inputs and outputs (also known as bidirectional many-to-many). Backpropagation through time is used to train RNN models in which a loss function that represents the difference between the output and the target is minimized. However, RNNs suffer from gradient vanishing and exploding problems making it difficult to be utilized for learning long data sequences [98]. Vanishing gradient refers to the gradient term for long term components going to zero exponentially fast making learning long sequence dependencies difficult. On the other hand, in the exploding gradient, the terms increases to infinity exponentially fast resulting in the weights not getting updated. To solve these problems, LSTM has been proposed as an improvement over RNNs. Being in the day-ahead market, and receiving the aggregators' load schedules as a full day sequence makes utilization of LSTM RNN as a classifier attractive for the DNO before computation of the congestion tariff.

### 5.3.1 LSTM

Let the input sequence to an LSTM be represented by $x_1, x_2, ..., x_T$. A single LSTM layer consists of three gates: an input gate, $i(t)$, an output gate, $o(t)$, and a forget gate, $f(t)$. It also maintains an internal memory cell state, $c(t)$, which is responsible for establishing temporal connections within the data [96]. The three gates are responsible for selecting and rejecting the information that passes through the network in its cell state. Initially, the LSTM needs to determine which information of the cell state, $c(t-1)$, should be updated or erased. This is done by the sigmoid layer forget gate, $f(t)$, which takes its previous cell output, $h(t-1)$, and the new cell input, $x(t)$, to output a number between 0 and 1 for $c(t-1)$. A 1 indicates retaining the contents of $c(t-1)$ while a 0 means deleting the contents.

$$f(t) = \delta(W_f[x(t), h(t-1)] + b_f) \tag{5.1}$$

A sigmoid layer input gate then takes the current input, $x(t)$, and previous cell output, $h(t-1)$, to determine which cell states to update. A tanh layer is responsible for creating an array of new updated values that would be added to the state.

$$i(t) = \delta(W_i[x(t), h(t-1)] + b_i) \tag{5.2}$$

$$\tilde{c}(t) = tanh(W_c[x(t) + h(t-1) + b_c) \tag{5.3}$$

The previous cell state, $c(t-1)$, is then updated through element-wise multiplication with $f(t)$ (5.1) to forget the contents that was decided to be forgotten. The result is added to the element wise multiplication of $i(t)$ (5.2) and $\tilde{c}(t)$ (7.3) to update the cell state values.

$$\tilde{c}(t) = f(t) * c(t-1) + i(t) * \tilde{c}(t) \tag{5.4}$$

The output gate, $o(t)$, utilizes the sigmoid activation function to decide which part of the current cell makes it to the output. These values are then filtered using a tanh function to be between -1 and 1.

$$o(t) = \delta(W_o[x(t), h(t-1)] + b_o) \tag{5.5}$$

$$h_t = o_t * tanh(c(t)) \tag{5.6}$$

$W_f, W_i$, and $W_c$ represents the weight of the forget, input and output gates. Figure 5.2 illustrates the structure of an LSTM block at a time time step, while Figure 5.3 demonstrates the unrolled LSTM architecture. It should be noted that the weights of all LSTM blocks are identical for the $T$ number of time steps.

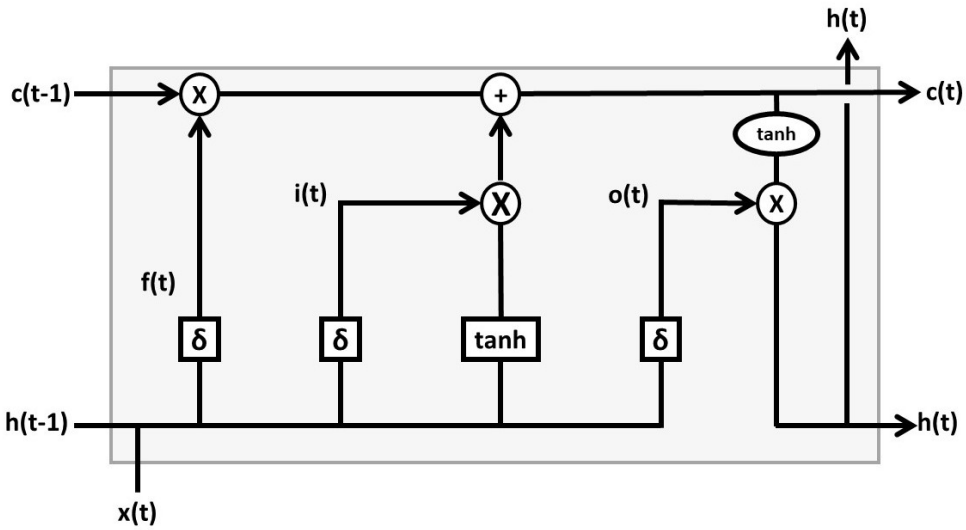



Figure 5.2: Structure of an LSTM-RNN block

The error between the output and the target, represented as the loss function, is returned via backpropagation through time. Weights are adjusted accordingly until they converge. The total error is determined as the summation of the error, $\eta_t$, for all time

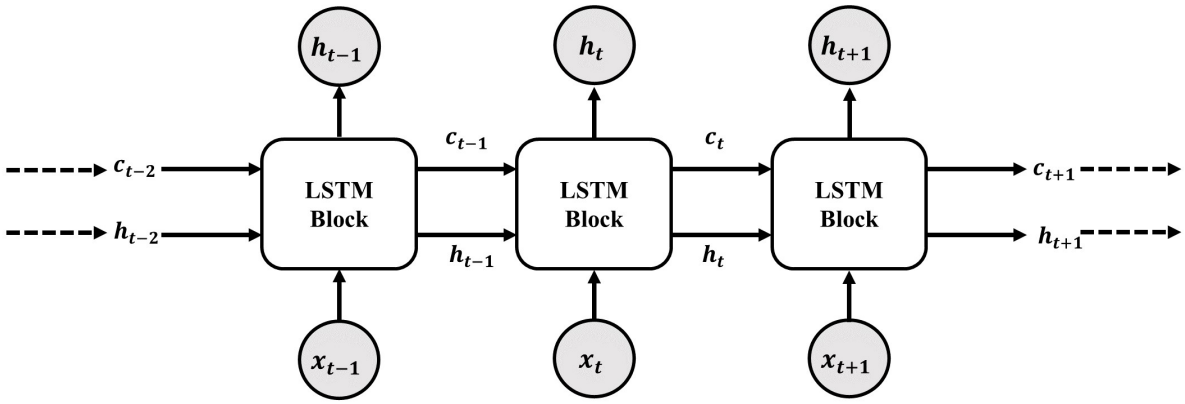



Figure 5.3: Architecture of an unrolled LSTM-RNN

steps as follows,

$$\frac{d\epsilon}{dw} = \sum_{t=1}^{t=T} \frac{d\epsilon_t}{dw} \tag{5.7}$$

### 5.3.2 Data Preprocessing

To model the many-to-one LSTM network, hourly customer real power load, electricity price, and weather data for Michigan, USA was utilized. Data was collected for random days in the months of November to March of 2015 to 2020. These winter months were chosen as the loads are at its peak, and there is a high chance of the network being congested. The real power load per bus in the distribution network is determined using the weather and day-ahead electricity prices to optimize aggregators' consumers' load. Hence, the four types of sequences that were chosen as input features are as follows:

- Historical daily weather data.
- Historical day-ahead electricity prices.
- Three days historical real power load per bus.
- Real power load per bus.
- Real power flow in the main feeder of the distribution network.

As LSTM is sensitive to data scale, all the input vectors were normalized between 0 to 1. 300 days of data were used to simulate stealthy load altering attacks, while another 300 days were chosen to simulate aggregators' load schedules if not compromised. An attacked day is labeled as 1, and 0 otherwise when training the model.

### 5.3.3 Results and Discussion

Utilizing the input data explained earlier, a 97% accuracy was obtained on testing 100 days of data. Table 5.1 illustrates the confusion matrix of the results obtained in terms of the number of false positives, false negatives, true positives, and true negatives on executing the LSTM network. False positives refer to the number of cases that were classified as attacked when in reality they were not attacked. On testing the trained LSTM-RNN model, only one out of the 100 scenarios came out as a false positive. On the other hand, a false negative refers to the number of cases that were not classified as attacked by the model. The simulation results had 2 such cases. On close examination of these two cases, the attack values, i.e. the change in the compromised aggregators' load profiles were very small and hence might have been missed by the model. True positives and true negatives refer to the case scenarios that represented attacked and not attacked days respectively and the model classified it correctly. The combination of these two values represents the model's accuracy of 97%.

Table 5.1: Confusion Matrix of LSTM-RNN Results

| **Actual** / **Predicted** | **Positive (1)** | **Negative (0)** |
|---|---|---|
| **Positive (1)** | 48 | 1 |
| **Negative (0)** | 2 | 49 |

In the day-ahead market, on receipt of the aggregators' load schedules, the DNO executes the proposed LSTM model to detect if an attack has occurred. If the LSTM classifier detects no attack, then the DNO would go ahead to compute the congestion tariffs. However, if an attack is detected the DNO would inform the aggregators that a cyber attack has occurred in the network so that the aggregators could check their cyber security. Until the cyber attack is eliminated, the DNO would rely on its historical data to determine if there is congestion in the network. Future work should incorporate the detection of the aggregator that is compromised in the network.

## 5.4 Conclusions

Cyber vulnerabilities of market-based congestion management techniques were studied in this chapter. The impact of load altering attacks that creates fake congestion was studied earlier in Chapter 3 in terms of congestion level and congestion tariffs. A detection technique using LSTM recurrent neural networks was proposed. On receiving aggregators' load schedules in the day-ahead market, the DNO would simulate the LSTM detection model to determine if any of the data received for each bus has been compromised. Distinctive sequences were chosen as features for the detection model to classify the presence or absence of an attack in the day-ahead market. Although the attacks simulated were made to be stealthy and hence hard to be detected, an accuracy of 97% was obtained reflecting the capability of the proposed model in detecting load altering cyber attacks that compromises aggregators in the network.

[1]

[1]This chapter has been published in: Gul M Khan, O., Youssef, A., El Saadany, E. and Salama, M. *LSTM-based approach to detect cyber attacks on market-based congestion management methods.* 2021 IEEE Power Energy Society General Meeting (PESGM), 2021, pp. 1-5, doi: 10.1109/PESGM46819.2021.9637976.

# Chapter 6

# Robust Multi-Objective Congestion Management in Distribution Network

## 6.1 Introduction

Lately, the smart grid has observed heavy penetration of Renewable Energy Sources (RESs), such as solar and wind, to help with peak demands. However, this causes bidirectional power flow in the grid and also introduces uncertainty due to their intermittent nature. Moreover, to decrease greenhouse gas emissions, the smart grid drives towards the electrification of the transportation system, via Electric Vehicles (EVs), and space heating, via Heat Pumps (HPs). This has increased the usage of such heavy flexible loads and changed the operating conditions of the distribution system [10]. Moreover, the dependence of such technologies on uncontrollable factors, such as temperature, wind speed, etc., may result in potential congestion problems in the distribution network which were not of concern in the past. Such congestion results in thermal overloading as a result of the power flow exceeding a network asset's transfer capability, possibly damaging devices such as distribution transformers and feeders [16]. Hence, reinforcement of overloaded network assets is required incurring costs [17] that may seem redundant as peak load generally appears only for a few hours. To avoid or postpone such costs, this chapter utilizes the grid's Demand Side Management (DSM) feature to alleviate congestion in the distribution network. Utilization of DSM [99] to schedule flexible loads helps in reducing these challenges.

To manage congested networks, DSM techniques, specifically load shifting and valley filling methods, have been developed. These techniques encourage consumers to adjust their electricity consumption profiles, as discussed in Chapter 2. The existing price and incentive-based congestion management methods [24] - [28] aims to alleviate congestion using an electricity cost minimization objective function. However, this may result in new peaks as loads are scheduled at times when prices are low. Moreover, the Peak to Average Ratio (PAR) of load curves in such modeling is high. On the other hand, valley filling techniques [34] - [35] results in flattening the load curve by filling the valleys in the load profiles which is advantageous. However, as the price is not taken into consideration, consumers end up paying more compared to load shifting methods. To gain the advantage of both worlds, multi-objective optimization is proposed to schedule flexible loads by merging load shifting and valley filling methods. This would result in consumers minimizing their electricity costs as well as flattening the curve enough to alleviate any existing congestion in the network.

Accuracy of the proposed multi-objective congestion management scheme, and any other existing technique, relies on the accuracy of the modeling parameters. However, the scheduling of flexible loads is generally reliant on uncertain data. For example, planning the day-ahead operation of HPs relies on uncertain ambient temperature. As a result of load uncertainty, the consumers' power profiles would deviate in real-time from the day-ahead load schedule impacting congestion in the network. Hence, it is essential that the sources of load uncertainty are identified and the propagation of uncertainty, reflected as the change in power flowing in the distribution network due to uncertain variables, is studied. To the authors' knowledge, [100] - [101] is the only work that has incorporated uncertainty in modeling a dynamic tariff-based congestion management model. However, the proposed model only considered EVs as stochastic flexible loads and is not distributed in nature, i.e. it relies on the network operator to forecast consumer flexibility and load requirements.

This chapter presents a robust multi-objective congestion management framework to alleviate congestions in the distribution network. The contributions of this chapter can be summarized as follows:

- A multi-objective congestion management model is developed using valley filling to flatten the load curve to an optimal level that alleviates congestion in the network while maintaining minimum consumer electricity costs. This would avoid the need for any extra congestion tariffs to be imposed to manage network congestions. Since the success of the proposed congestion management scheme in the real-time market depends on the accuracy of the consumer load consumption model in the

day-ahead market, the robustness of the proposed multi-objective congestion management model to uncertainties in consumer load scheduling is investigated. An iterative scheme is adopted to determine the multi-objective Pareto weight that ensures the robustness of the line loading despite uncertainties in consumer flexible load.

- The proposed method is tested using an IEEE 33 bus system and the results are compared to that of the Distributed Dynamic Tariff (DDT) congestion management scheme.

The rest of the chapter is organized as follows: section 6.2 explains the proposed deterministic multi-objective congestion management scheme. Sources of uncertainty in the proposed model are identified and a robust solution is developed in section 6.3. In section 6.4, the proposed multi-objective flexible load scheduling is tested in an IEEE 33 bus system. The obtained results are compared with price-based congestion management method prior to concluding the chapter.

## 6.2 Deterministic Multi-Objective Congestion Management Scheme

To schedule flexible loads, DSM methods, using either load shifting or valley filling, have been utilized in the literature. These methods have their advantages and disadvantages and can be compared in terms of electricity price paid by customers and PAR of the power flowing in the network feeder as follows:

- Electricity Price: Price-based optimization is based on determining the optimal schedule that minimizes the consumers' electricity cost. Hence, price-based optimization results in the most economic schedule. On the other hand, valley-filling schemes aim to flatten the load curve resulting in higher electricity costs for the consumer.
- PAR: Price-based optimization's advantage in terms of minimum electricity cost consumption can result in rebound peaks, and hence a higher PAR. Flexible load is scheduled in the early morning and late-night hours when the price of electricity is the lowest resulting in peaks in demand. On the other hand, flattening the load curve as a result of valley-filling optimization results in a lower PAR compared to price-based optimization.

In this chapter, to gain the advantage of minimizing consumers' bills and flattening the load curve to alleviate congestion, a multi-objective model is proposed.

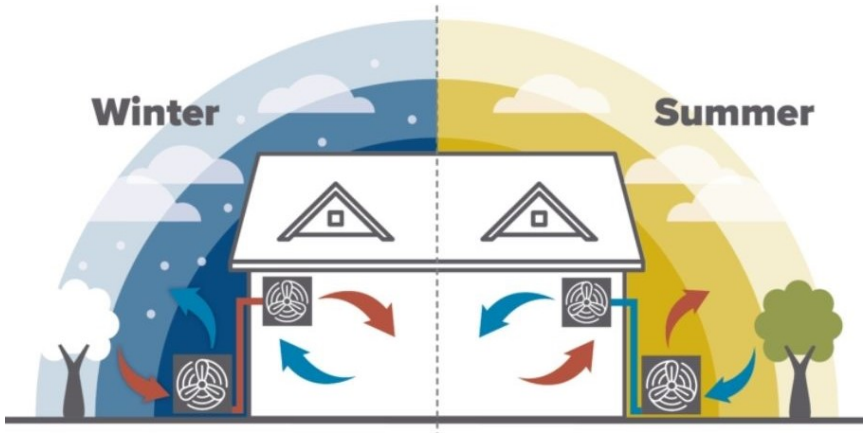
### 6.2.1 Modeling Assumptions

Prior to formulating the problem, the necessary assumptions adopted are listed and justified as follows:

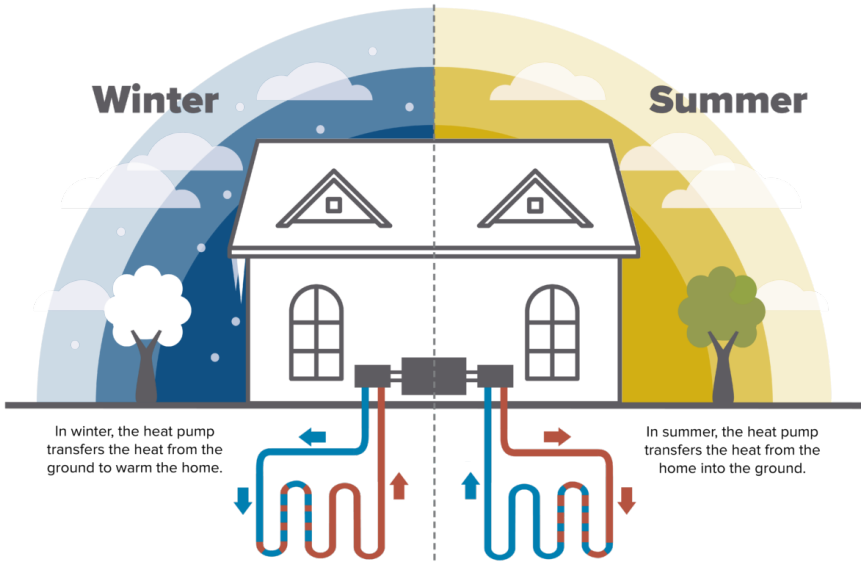
- Forecasted day-ahead prices, $p_t$, are determined by the market operator and forwarded to the grid operators who in turn sends them to the aggregators in the network [102].
- EVs and HPs are chosen as flexible loads. Not only do they represent the heaviest residential loads, but they represent shiftable and non-shiftable flexible loads [26].
- Aggregators are defined as entities that are not only responsible for adjusting consumers' demand to minimize their costs but are also the retailers of the consumers [103].
- Aggregators are assumed to be motivated to participate in the day-ahead market as they provide financially binding prices protecting consumers from unexpectedly high real-time prices [104].
- Aggregators have the option to not participate in the day-ahead market to schedule their flexible loads. The network operator, hence, utilizes its load forecasting tools to complete the missing aggregator's load information.
- Aggregators have no incentive to lie.

### 6.2.2 Flexible Loads

HPs utilize electrical energy to extract heat from a low-temperature region (referred to as a source) and transfer it to a warmer area (referred to as a sink) resulting in its usage to provide heating or cooling. Some of the commonly used sources of HPs are air and ground-source HPs. Air-source HPs extract heat from the external air for heating and pump heat outside for residential cooling, as illustrated in Figure 6.1(a). On the other hand, ground-source HPs use groundwater and/or the earth to extract heat for heating or pump heat into it for residential cooling, as illustrated in Figure 6.1(b). In this chapter, air-source HPs are utilized as flexible loads as they dominate global HP sales [105]. The thermal dynamics of HPs are modeled by the following constraints




(a)




(b)

Figure 6.1: Operation of (a) Air Source HPs [2] and (b) Ground Source HPs [3] as a heater and cooler.

$$T^i_{h,t} - T^i_{h,t-1} = \frac{1}{C^i_h}(P^{hp}_{h,t}C_h + R^{is}_h(T^s_{h,t} - T^i_{h,t}) + R^{ie}_h(T^e_t - T^i_{h,t})) \tag{6.1}$$

$$T^s_{h,t} - T^s_{h,t-1} = \frac{1}{C^s_h}(R^{is}_h(T^i_{h,t} - T^s_{h,t}) + R^{se}_h(T^e_t - T^s_{h,t})) \tag{6.2}$$

$$0 \leq P^{hp}_{h,t} \leq P^{hp}_{max} \tag{6.3}$$

$$T^{min}_h \leq T^i_{h,t} \leq T^{max}_h \tag{6.4}$$

where $C^i_h$ and $C^s_h$ represent the internal and surface heat capacity of house, $h$, respectively. $R^{is}$, $R^{ie}$, and $R^{se}$ represent thermal resistance between the interior and surface, interior and external, and surface and exterior respectively. $C_h$ symbolizes the coefficient of performance of the HP. $P^{hp}_{max}$ is the maximum heat output limit. $T^i_{h,t}$ is the internal temperature of house $h$ at time, $t$, and $T^{max}_h$ and $T^{min}_h$ are the maximum and minimum indoor temperature preferences of the consumers. $T^e_t$ is the external temperature and $T^s_{h,t}$ is the surface temperature of house $h$ at time $t$.

Similarly, the increased deployment of EVs has increased the need for public rapid charging stations. Currently, based on the SAE J1772 standard [106], the following three main charging methods are used either residentially, commercially or in public environments:

- Slow Charging-Level 1: It is mainly a residential charger that supplies AC energy to the EV on-board charger at a maximum rate of 16 amps at 120V. Depending on the EV's battery technology, level 1 charging takes 8 to 12 hours to fully charge an empty battery.
- Standard Charging-Level 2: It is typically found residentially or commercially supplying AC energy to the EV on-board charger at a maximum rate of 80 amps at 240V. Depending on the EV's battery technology, level 2 charging takes 4 to 6 hours to fully charge an empty battery.
- Fast Charging-Level 3: It is typically found commercially or on highways supplying DC energy from an off-board charger to the EV. Most common forms of level 3 chargers currently provide 50kW charge per hour. Tesla level 3 chargers, on the other hand, provides 120kW of charge per hour.

As EVs are becoming more popular day by day, they are becoming more affordable to middle and lower class households. However, not all EVs consumers own their own residential property to charge their cars. Instead, many of them may live in more dense environments that would require the installation of public level 2 or level 3 charging stations to satisfy their charging needs. Moreover, to attract more people into driving EVs, the future would see the deployment of a large scale fast charging Direct Current (FCDC) stations that provides speedy charging. EV charging is modeled by:

$$P_h^{req} \leq \sum_t P_{h,t}^{ev} \tag{6.5}$$

$$0 \leq P_{h,t}^{ev} \leq a_{h,t} P_h^{ev_{max}} \tag{6.6}$$

where $P_h^{req}$ is the total required battery charge for EV $h$, energy at time $t$, $P_h^{ev_{max}}$ is the maximum charging power, and $a_{h,t}$ is how the availability of EV $h$ at time $t$ for charging.

### 6.2.3 Problem Formulation

The Distribution Network Operator (DNO) is the entity responsible for ensuring the alleviation of any congestions in the distribution network. Price-based load shifting and valley-filling objective functions are combined into a single multi-objective optimization problem to schedule consumers' flexible loads. Since both objective functions are convex, the weighted-sum method is adopted by the aggregators as follows:

$$\begin{aligned} \min_{\mu_h, P_{h,t}^{ev}, P_{h,t}^{hp}} \alpha \sum_h \mu_h + (1-\alpha) \sum_{h,t} \Big( & P_{h,t}^{evT} \beta P_{h,t}^{ev} \\ & + P_{h,t}^{hpT} \beta P_{h,t}^{hp} + p_t (P_{h,t}^{ev} + P_{h,t}^{hp}) \Big) \end{aligned} \tag{6.7}$$

where weight, $\alpha \in [0, 1]$, is used to scalarize the objective functions proportional to the valley-filling level desired. A higher $\alpha$ represents a higher priority to flattening the load curve over minimizing the electricity cost for the consumers and vice versa. $P_{h,t}^{ev}$ and $P_{h,t}^{hp}$ represents the EV power and HP power for each house, $h$, at time $t$ respectively. It should be noted that $h \in N_h$ and $t \in N_T$, where $N_h$ and $N_T$ are the total number of houses and hours in a day respectively. $\beta \in R^{N_T \times N_T}$ represent the price sensitivity coefficient matrix. $\mu_h$, is referred to as the water level of consumer $h$ and it represents the summation of its flexible, $P_{h,t}^{f}$, and non-flexible, $P_{h,t}^{nf}$, load. The flexible load, $P_{h,t}^{f}$, is the summation of the

existing EV load, $P_{h,t}^{ev}$ and HP load $P_{h,t}^{hp}$ for house $h$ at time $t$. The valley-filling part of the multi-objective optimization problem, hence, aims to minimize the water level of the consumers and maximize the feeder's capacity using the following equality constraint:

$$\text{s.t. } P_{h,t}^{ev} + P_{h,t}^{hp} = (\mu_h - P_{h,t}^{nf})^+, h \in N_h \tag{6.8}$$

### 6.2.4 Determining Optimal Pareto Solution

Solving the multi-objective optimization problem (6.7) results in a set of optimal solutions referred to as the Pareto optimal front [107]. Neither point on the Pareto front is considered better than the other except in terms of the decision-makers objective. To determine the Pareto front, the two objective functions of (6.7) have to be initially normalized as they are not of the same type. The ideal point, $z^*$, and the nadir point, $z^{nadir}$, defined respectively as the lower and upper bound of the Pareto optimal set [108] are utilized to normalize the objective functions (6.7) as:

$$f_i^n = \frac{f_i - z_i^*}{z_i^{nadir} - z_i^*}, \text{for } i = 1, 2 \tag{6.9}$$

where,

$$\begin{aligned} f_1 &= \sum_h \mu_h \\ f_2 &= \sum_{h,t} P_{h,t}^{ev^T} \beta P_{h,t}^{ev} + P_{h,t}^{hp^T} \beta P_{h,t}^{hp} + p_t (P_{h,t}^{ev} + P_{h,t}^{hp}) \end{aligned} \tag{6.10}$$

$f_i^n$ is the $i^{th}$ normalized objective function, $f_i$ is the $i^{th}$ objective function, $z_i^*$ is the $i^{th}$ objective function ideal point, and $z_i^{nadir}$ is the $i^{th}$ objective function nadir point.

The multi-objective function (6.7) symbolizes a trade-off between total electricity price and feeder congestion level, as the weight, $\alpha$, varies. An increase in the weight, $\alpha$, increases, the importance of valley filling load scheduling. This results in a flexible load schedule that is more costly compared to that of lower weights where price-based scheduling is dominant. However, a higher weight indicates lower congestion levels. Hence, given the Pareto front, to determine the desired optimal Pareto solution, an interactive method is utilized in which the decision-maker is allowed to search for the optimal solution that achieves its desired objective [109]. In this chapter, the decision-maker is the DNO and the goal of clearing congestions in the day-ahead market would determine the desired optimal Pareto for solving (6.7). In the absence of congestion, the weight, $\alpha$, is chosen to be 0 to schedule the flexible loads using price-based optimization. This results in the most

economical flexible load schedule resulting in satisfied consumers. However, as the flexible load increases, the scheduling of the soft load is shifted from price-based to valley-filling optimization. This would result in flattening the curve to the level needed to alleviate the existing congestion. Using this method, congestion tariff is not imposed and hence the price paid by the consumers is lower compared to existing price-based congestion management schemes.

Initially, each aggregator schedules its flexible load using (6.7) and $\alpha^0$, where 0 represents the $k$ iteration number. Hence, the flexible loads are initially scheduled using economical price-based optimization to determine if there is congestion in the network or not. Aggregator $i$ consumers' total load requirement, $P_{i,t}$, is calculated as:

$$P_{i,t} = E(P_{h,t}^{i,nf} + P_{h,t}^{i,f}), \forall i \in N_a, \forall t \in N_T \tag{6.11}$$

Given that $N_a$ and $N_d$ are the set of aggregators and load buses in the network. $E$ represents the customer-to-bus mapping matrix where $E \in \mathbb{R}^{N_d \times N_h}$. $P_{h,t}^{i,nf}$ and $P_{h,t}^{i,f}$ are the non-flexible and flexible loads of customer, $h$, of aggregator $i$, where $\{P_{h,t}^{i,nf}, P_{h,t}^{i,f}\} \in \mathbb{R}^{N_h}$. Before day-ahead market closure, aggregators forward their consumers' load requirement, $P_{i,t}$, securely to the DNO. The network operator is responsible for determining the optimal Pareto weight that resolves congestion and minimizes consumers' costs. Hence, the DNO performs power flow analysis to determine if the power flowing in the branches, $F_t^b$, where branch $b \in N_b$, exceeds the branches maximum limits, $F_{max}^b$. The Pareto weight, $\alpha^k$, is then updated in proportion to the congestion level using,

$$\alpha^{k+1} = \alpha^k + D\theta \min(b, F_t^b - F_{max}^b) \tag{6.12}$$

where $\theta$ represents the step size and $D$ represents the power transfer distribution factor. $\alpha^{k+1}$ is updated in proportion to the most congested feeder in the network. As feeders that are not congested would result in negative $\alpha^{k+1}$,

$$\alpha^{k+1} = (\alpha^{k+1})^+ \tag{6.13}$$

all negative $\alpha^{k+1}$ are replaced by zeros. This iteration continues between the DNO and the aggregators until the network is not congested, and the difference between the Pareto weights in two consecutive iterations is less than a small constant, $\tau$. Figure 6.2 illustrates the flowchart of steps involved in determining the Pareto weight of the multi-objective optimization problem and the resulting consumers' optimal load schedules.

As an additional feature, to ensure the absence of manipulation of day-ahead load

schedules by the aggregators in the distribution network, an imbalance penalty factor (IPF) [110] is imposed by the utility operator in the real-time market. This penalty is initially zero for all aggregators in the network assuming they are all truthful. However, proportional to the deviation between their day-ahead load schedule and real-time consumption, IPF for each aggregator is adjusted accordingly. Once the IPF exceeds a certain threshold the aggregator would not be allowed to take part in the day-ahead market.

## 6.3 Developing a Robust Solution for the Proposed Congestion Management Scheme

The proposed congestion management scheme relies on the accuracy of the consumer load profiles submitted by the aggregators in the network, $P_{i,t}$, to the DNO. Despite the fact that congestion management is executed in the day-ahead market, if the proposed scheme is impacted by its flexible loads' uncertainties, the network can experience congestion in real-time. Hence, propagation of uncertainty as a consequent effect of EV and HP uncertainties on congestion in the distribution network needs to be studied. Uncertainty in the line loading of a distribution network can be quantified using the standard deviation, $\Delta F_t^b$. Hence, to consider a solution of the multi-objective optimization problem robust, the following constraint has to be met where the probability, $\mathbf{P}$, of the network line, $F_t^b$, not being congestion by $\delta$ (expressed in percentage) as a result of consumer load uncertainties, $U$, is larger than $\eta$, where $\eta$ represents the confidence level and is typically 0.9, 0.95 or 0.99,

$$\mathbf{P}(F_t^b \leq (1-\delta)F_{max}^b) \geq \eta \tag{6.14}$$

To fulfill the constraint (6.14) achieving the desired robustness, the classical uncertainty propagation theorem [100] is adopted. This is explained in the following subsections after identifying the uncertain variables, $U$, in the network and characterizing their stochastic nature using Probability Density Functions (PDFs).

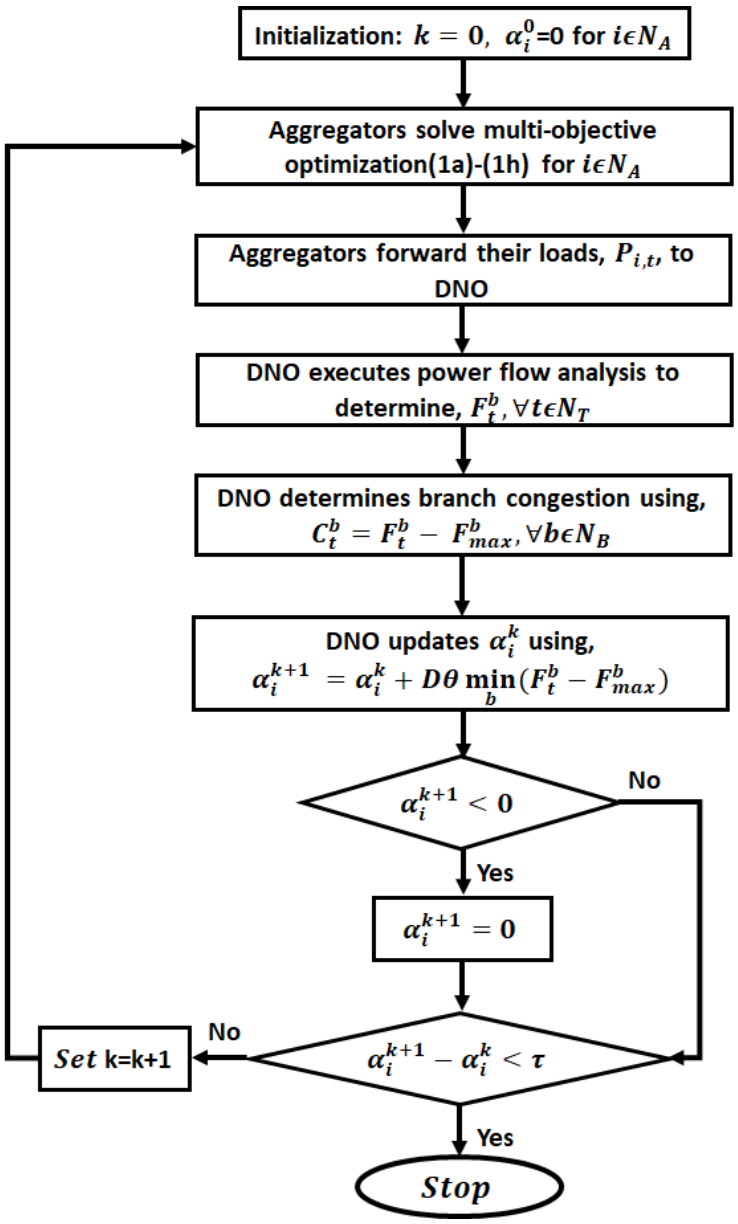



Figure 6.2: Flowchart for determining multi-objective Pareto weight and optimal consumer load schedule

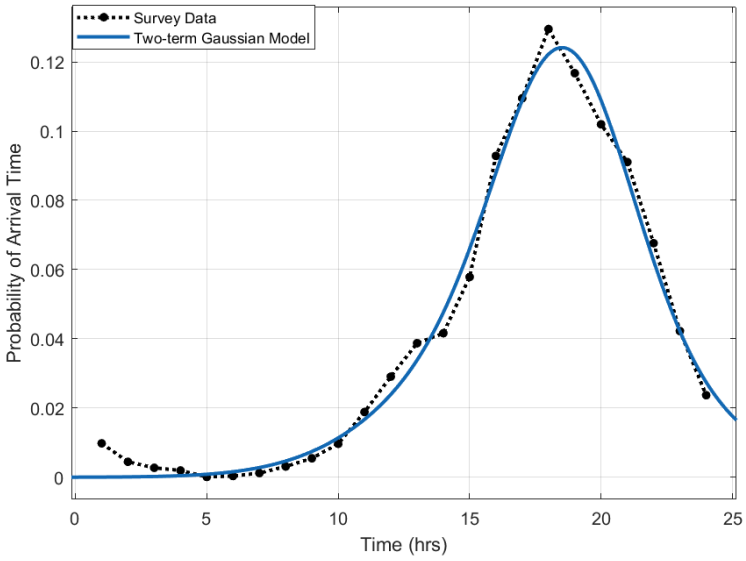
### 6.3.1 Identification of Uncertain Variables

To schedule their consumers' flexible load with higher accuracy, aggregators in the distribution network have to factor in any source of uncertainty in their optimal load scheduling. Assuming accurate day-ahead price forecast by the market operator, $p_t$, aggregators have to incorporate flexible load-related uncertainties, $U$. For example, the amount of charge EV consumers require on returning home, $P_h^{req}$, depends on their distance traveled during the day. In the occurrence of extra traffic or a road blockage, an EV driver would require to travel a larger distance and hence require more battery charge, $P_h^{req}$, than what was forecasted in the day-ahead schedule. These uncertainties are hence due to the stochastic nature of such flexible loads and it has to be identified, represented using PDFs, and included in the congestion management model. The sources of uncertainty, $U$, considered in this chapter and their respective modeling are as follows:

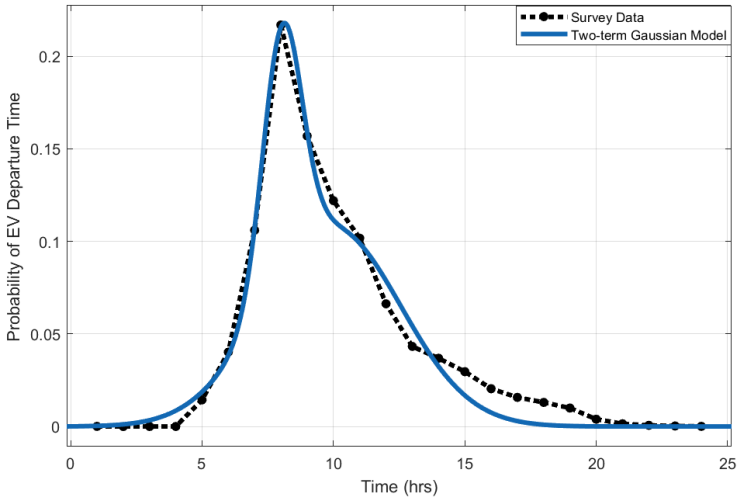
- Uncertainty in modeling EVs: The stochastic nature of EVs is due to the random behavior of each EV owner. Scheduling EV charging depends on three uncertain parameters: time of arrival to the residence level charger having a standard deviation of, $\Delta t_{ar}$, the state of charge of the EV battery on arrival having a standard deviation of, $\Delta P^{req}$, and the time of departure the next day with a full EV battery having a standard deviation of, $\Delta t_{dep}$. To simulate EV availability in residential parking lots, data obtained from the US department of transportation [111] is used to model arrival and departure times of cars to residences. A two-term Gaussian model, represented by (7.6), is fit as illustrated in Figure 6.3 respectively.

$$\mathbf{P}(t) = a_1 e^{-((t-b_1)/c_1)^2} + a_2 e^{-((t-b_2)/c_2)^2}, \forall t \in N_T \tag{6.15}$$

  The probability of departure/arrival time, $t$, where $t$ is between 1 and 24, is represented by $\mathbf{P}(t)$. $a_1$ and $a_2$ represents the scaling factors, $b_1$ and $b_2$ represents the mean, and $c_1$ and $c_2$ represents the standard deviations of the PDF. Table 6.1 demonstrates the properties of the arrival and departure time density functions. To evaluate the goodness of the fit, the Root Mean Squared Error (RMSE) was used. RMSE was determined to be 0.00845 for departure time, and 0.005336 for arrival time demonstrating the function's fit for prediction. Hence, the availability of EV $h$, represented as $a_{h,t}$ (6.6), depends on the arrival and departure times obtained probabilistically from the gaussian PDF. The initial State of Charge (SOC) of each EV is randomized to be normally distributed with a mean of 30% and a standard deviation of 4%. Hence, the required power to charge EV $h$ battery, $P_h^{req}$, can be determined from




(a)




(b)

Figure 6.3: PDF of EV (a) arrival, and (b) departure times

Table 6.1: Arrival and Departure Time PDF Properties

| **Parameters** | $a_1$ | $a_2$ | $b_1$ | $b_2$ | $c_1$ | $c_2$ |
|---|---|---|---|---|---|---|
| Departure | 0.13 | 0.11 | 8.05 | 9.93 | 1.05 | 3.73 |
| Arrival | 0.07 | 0.05 | 18.64 | 17.92 | 3.43 | 6.37 |

the stochastic SOC as it is assumed that the car should be completely charged on departure.

- Uncertainty in modeling HPs: The operation of HPs relies on the ambient temperature, $T_t^e$. In the event of colder weather in winter (or higher temperatures in summer), the heat pump would require more electrical power, $P_{h,t}^{hp}$, to maintain the indoor temperatures, $T_{h,t}^i$, within the desired range, $[T_h^{min}, T_h^{max}]$. However, there is uncertainty associated with the forecasted outdoor temperature which can be quantified in terms of its standard deviation, $\Delta T^e$, which impacts the day-ahead load scheduling. Uncertainty in the ambient temperature, $\Delta T^e$, hence is modelled as a normal density function with a standard deviation of 1℃.

### 6.3.2 Sensitivity Analysis

The robustness of the proposed congestion management scheme is impacted by the uncertainty, $U$, in scheduling the flexible load, $P_{h,t}^f$, identified in the previous subsection. If consumers deviate from their load requirements, the multi-objective Pareto weight, $\alpha$, determined in Section 6.2, might not manage existing network congestion. To ensure the robustness of the proposed multi-objective congestion management scheme, the uncertainty propagation theorem [112] is adopted. Based on [112], the uncertainty in power flowing in a network branch, $\Delta F_t^b$, is a function of uncertainties in EV and HP modeling parameters, i.e. $U = \{\Delta t_{ar}, \Delta t_{dep}, \Delta P^{req}, \text{and } \Delta T^e\}$. Hence, propagation of uncertainty from the input variables to the line loading and quantified as the standard deviation of the line loading, $\Delta F_t^b$, can be determined as follows,

$$\sum_{b \in N_b} \Delta F_t^b = \sum_{i \in N_d} DE_i \sqrt{(\Delta P_{i,t}^{hp})^2 + (\Delta P_{i,t}^{ev})^2} \tag{6.16}$$

where,

$$(\Delta P_{i,t}^{ev})^2 = (\frac{\partial P_{i,t}^{ev}}{\partial t_{ar}} \Delta t_{ar})^2 + (\frac{\partial P_{i,t}^{ev}}{\partial t_{dep}} \Delta t_{dep})^2 + (\frac{\partial P_{i,t}^{ev}}{\partial P^{req}} \Delta P^{req})^2 \tag{6.17}$$

and,

$$(\Delta P_{i,t}^{hp})^2 = (\frac{\partial P_{i,t}^{hp}}{\partial T^e}\Delta T^e)^2 \tag{6.18}$$

where the partial derivatives $\frac{\partial P_{i,t}^{ev}}{\partial t_{ar}}$, $\frac{\partial P_{i,t}^{ev}}{\partial t_{dep}}$, $\frac{\partial P_{i,t}^{ev}}{\partial P^{req}}$, and $\frac{\partial P_{i,t}^{hp}}{\partial T^e}$ represents sensitivity coefficients. Hence, to ensure the robustness of the proposed model the sensitivity of the flexible loads to changes in the uncertainty parameters impacting the line loading is studied. As each aggregator, $i$, is responsible for its own flexible load scheduling, the sensitivity of multi-objective congestion management problem (6.7) variables, represented by $x_t^i$, where,

$$x_t^i = [P_{i,t}^{ev} \quad P_{i,t}^{hp}]^T, i \in N_a, t \in N_T \tag{6.19}$$

to the uncertainty of EV arrival time, departure time, SOC, and ambient temperature is studied. Hence, rewriting (6.7) in standard form for each aggregator, $i$, in the network (hence subscript $i$ has been dropped),

$$\begin{aligned} \min_x \; & x^T\bar{\beta}x + g^T x + m \\ \text{s.t.} \quad & Ax = b, (\lambda) \end{aligned} \tag{6.20}$$

where $\bar{\beta} = (1-\alpha)\beta$, constant $m = \alpha P_t^{nf} 1$, and $g_t = [\alpha 1 + (1-\alpha)(p_t 1)^T]$. $A$ and $b$ are the coefficients of the active constraints related to EV and HP modeling (6.1-6.6) determined after solving (6.7) deterministically. $\lambda$ is the Lagrange multiplier of the active constraints. For each aggregator, $i$ , the associated Lagrangian function, $L(x, \lambda)$, is

$$L(x, \lambda) = x^T\bar{\beta}x + g^T x + m - \lambda(Ax - b) \tag{6.21}$$

Minimizing the Lagrangian function over $x$ results in,

$$x = 0.5\bar{\beta}^{-1}(A^T\lambda - g) \tag{6.22}$$

Using the Lagrangian's function's differentiation over the Lagrangian multipliers, the results obtained are substituted in (6.22). Optimal variable $x^*$ is hence defined as,

$$x^* = \bar{\beta}^{-1}A^T(A\bar{\beta}^{-1}A^T)^{-1}(b + 0.5A\bar{\beta}^{-1}g) - 0.5\bar{\beta}^{-1}g \tag{6.23}$$

The change in the optimal solution, $x^*$, as a result of changes in the uncertain variables, $U$, reflected by changes in coefficient $b$, is,

$$\frac{\partial x}{\partial b} = \bar{\beta}^{-1} A^T (A \bar{\beta}^{-1} A^T)^{-1} \tag{6.24}$$

Hence, to determine the impact on congestion in the distribution network, uncertainty in the power flow, $\Delta F_t$, in the network at the time, $t$, as a result of the inherent uncertainties in EV and HP loading is determined as follows,

$$\begin{aligned} \Delta F_t &= \sum_i DE_i (\Delta P_{i,t}^{ev} + \Delta P_{i,t}^{hp}) \\ &= \sum_i DE_i (\frac{\partial x}{\partial b}) \Delta b \end{aligned} \tag{6.25}$$

where $D$ is the power transfer distribution factor and $E_i$ is the customer to bus mapping matrix for aggregator $i$.

### 6.3.3 Robustness Enhancement of Proposed Scheme through Uncertainty Propagation

As a result of the uncertainty in scheduling consumers load, the deterministic scheme explained in Section 6.2 may not clear congestions in the real-time market using the determined the Pareto weight, $\alpha$. The modeled congestion management scheme identifies four sources of uncertainty, $U = \{\Delta t_{ar}, \Delta t_{dep}, \Delta P^{req}, \text{and } \Delta T^e\}$. Using (6.24-6.25), the sensitivity of the consumers' load, and hence the line loading $F_t$, is determined for changes in each of the uncertain variables independently. Respective rows of vector $b$ corresponding to changes in EV power as a result of changes in arrival time, departure time, and EV charge required results in determining the partial derivatives: $\{\frac{\partial P_{i,t}^{ev}}{\partial t_{ar}}, \frac{\partial P_{i,t}^{ev}}{\partial t_{dep}}, \frac{\partial P_{i,t}^{ev}}{\partial P^{req}}\}$. Similarly, rows of vector $b$ corresponding to changes in HP power as a result of changes in ambient temperature result in $\frac{\partial P_{i,t}^{hp}}{\partial T^e}\}$. Based on (6.16), uncertainty in power flowing in the distribution network, $\Delta F_t^b$, depends on the sensitivity of the EV and HP power, $\zeta^U$, to changes in the uncertainty variables, $U$. The robustness of the proposed congestion management scheme is hence determined as the probability, $\mathbf{P}$, of the overloading of the main feeder in the

distribution network as a result of load scheduling uncertainties, $U$, as follows,

$$\begin{aligned}\mathbf{P}(\sum_{b\in N_b} F_t^b \leq (1-\delta)F_{max}) \\ = \mathbf{P}(\sum_{i\in N_d} DE_i\zeta_i^U \Delta U \leq (1-\delta)F_{max})\end{aligned} \tag{6.26}$$

The resulting distribution of $\sum_{i\in N_d} DE_i\zeta_i^U \Delta U$ is a normal distribution since the uncertain variables are normally distributed as well. Hence, the variance of the total distribution is a linear combination of the variances of the flexible load uncertainties. Hence, to measure the robustness of the proposed scheme, the probability of overloading the network using (6.26) is determined and robustness constraint (6.14) is checked for the result of the Pareto optimal obtained in the deterministic case following Figure 6.2. If the constraint is satisfied, then the result is robust. Else, the robustness of the proposed model needs to be enhanced iteratively by updating the Pareto with a step size, $\gamma$, proportional to the sensitivity of the line loading to the uncertainty in the load schedule. Algorithm 1 illustrates the steps involved to determine the optimal Pareto weight, $\alpha$, taking into consideration the uncertainty of the consumers' load. On executing Algorithm 1, the probability of the resulting optimal solution, $P_{i,t}^*$, not causing congestion in the network due to randomness of EV arrival time or departure time, EV power required, and ambient temperature, should be below $\eta$.

## 6.4 Case Study, Results and Discussion

The IEEE 33 bus system [1], is adopted as a case study in this chapter. The distribution network consists of 32 residential load buses representing both flexible and non-flexible loads. The default loading of the IEEE 33 bus system represents the non-flexible base load profiles of the load buses. The flexible residential loads consist of EVs and HPs [113]. The case study involves a total of 32 aggregators, one aggregator representing consumers of each load bus. The various parameters needed for simulating the operation of the HP and the EV are listed in Table 6.2. The houses were assumed to be single-storey houses of an average height of 8ft and their house areas were randomly chosen between 1500 to 2500 sq. ft. GAMS [86] and MATLAB R2021a were used for executing the optimizations.

Table 6.2: Case study parameters

| **Variable** | **Value** |
|---|---|
| Coefficient of Performance ($C_h$) | 2.2 |
| Residential House Areas | 1500-2500 $ft^2$ |
| Height of the houses | 8 ft |
| House Temperature Range $[T^{min}, T^{max}]$ | 18-24°C |
| EV battery size | 25 kWh |
| Maximum EV charging power ($P^{ev_{max}}$) | 11 kW |
| Power flow limit of main feeder ($F_{max}$) | 7.88 MW |
| Upper voltage limit | 1.05 pu |
| Lower voltage limit | 0.95 pu |

**Algorithm 1** Robust Enhanced Multi-objective Congestion Management Scheme

**Input:** Consumers' comfortable internal temperature range: $T_h^{min}$ and $T_h^{max}$, required EV charging power, $P_h^{ev}$, EV availability for charging, $a_{h,t}$, and PDFs of uncertain parameters, $U = \{\Delta t_{ar}, \Delta t_{dep}, \Delta P^{req}, \text{and } \Delta T^e\}$.
**Output:** Multi-objective function Pareto weight, $\alpha$, and optimal load schedule, $P_{i,t}^*$, for aggregator, $i$.
**Initialize:** Set $\alpha^0 = 0$ for iteration $k = 0$.

1. **while** $(\alpha^{k+1} - \alpha^k > \tau)$ **do**

   (a) Using $\alpha^k$ and mean of the random variables, $U$, solve multi-objective optimization (6.7) for $i \in N_A$ to determine consumers' optimal load, $P_{i,t}^*$.

   (b) Each aggregator forwards their total optimal consumer loads, $P_{i,t}^*, \forall i \in N_A \text{and } \forall t \in N_T$, to the DNO.

   (c) The network operator performs power flow analysis to determine the power flow in each branch in the network, $F_t^b$.

   (d) The DNO checks for congestion and determines the extent of congestion, $C_t^b$, with respect to a branch's maximum limit.

   $$C_t^b = F_t^b - F_{max}^b, \forall b \in N_b$$

   (e) The DNO updates the Pareto weight, $\alpha^k$, such that,

   $$\alpha^{k+1} = \alpha^k + D\theta \min(b, F_t^b - F_{max}^b)$$

   (f) **if**$(\alpha^{k+1} < 0)$ **then**

   $$\alpha^{k+1} = 0$$

2. Using $\alpha^k$, solve (6.24-6.25) to determine the sensitivity, $\zeta^U$, of the line loading to changes in the random variables, $U$.

3. Determine if the robustness constraint (6.14) is satisfied as a result of flexible load uncertainties, $U$.

4. **while** $\mathbf{P}(F_t^b \leq (1-\delta)F_{max}^b) \leq \eta$ **do**

   (a) Set $\alpha^{k+1} = \alpha^k + \gamma\zeta_i^U$, where $\gamma$ is a step size. Since $\alpha^k$ obtained from step 1 clears congestion in the network, $\alpha^{k+1} \geq \alpha^k$ also clears congestion as the weight of flattening the load curve increases.

   (b) Using the updated Pareto weight, $\alpha^{k+1}$, the multi-objective function (6.7) is solved for each aggregator $i \in N_A$ to determine consumers' optimal load, $P_{i,t}^*$.

   (c) Repeat steps 2 and 3.

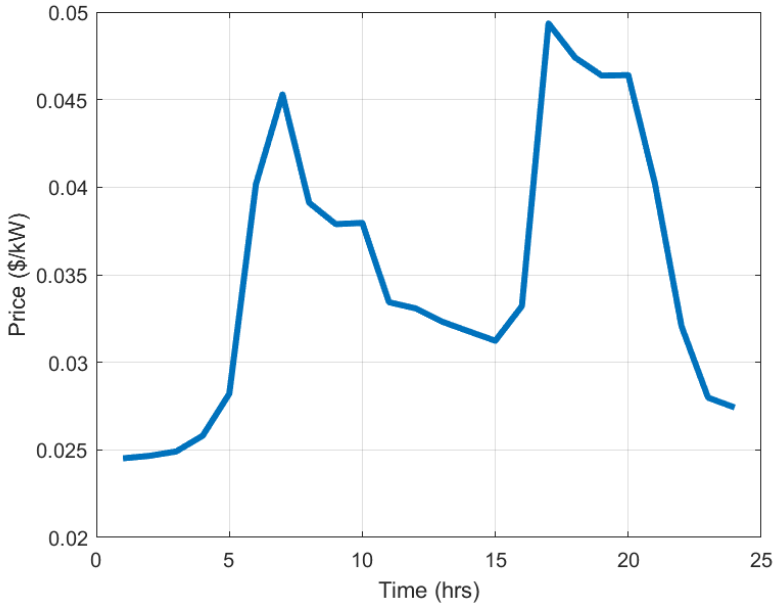



Figure 6.4: Day-ahead electricity price.

### 6.4.1 Deterministic Multi-Objective Flexible Load Scheduling

Using the case study explained above, Figure 6.4 illustrates the forecasted day-ahead price of electricity, $p_t$. To develop the Pareto front, the multi-objective function weight, $\alpha$, is varied in (6.7) from 0 to 1, in increments of 0.01. The resulting Pareto optimal front of the multi-objective optimization is illustrated in Figure 6.5. Neither point on the Pareto front is considered better than the other except in terms of the higher-level objective of a user. An $\alpha$ closer to 0 increases the importance of price-based scheduling resulting in a more economical consumer load schedule. This is illustrated in Figure 6.5 as a decrease in the price objective function at the cost of an increase in the valley filling objective value. Similarly, an $\alpha$ closer to 1 increases the importance of valley-filling-based scheduling resulting in a more flattened load curve.

Solving the normalized multi-objective function (6.7), Figure 6.6 illustrates the effect of varying the multi-objective function weights, $\alpha$, on the power flowing, $F_t$, in the main feeder of the IEEE 33 bus system. An $\alpha$ of 0 represents price-based flexible load scheduling. Hence, as the aggregator schedules the load by minimizing consumption costs, the load is concentrated at times in which the cost of electricity is low leading to congestion at times $t = 20 - 23$. However, as $\alpha$ increases, the dominance of the valley-filling load scheduling is

observed to increase and the curve is flattened. An $\alpha$ of 1 represents valley filling flexible load scheduling. The impact of changing $\alpha$ is seen in the PAR of the load buses. An $\alpha$ of 0 results in a mean PAR of 1.3936 while an $\alpha$ of 1 returns a mean PAR of 1.0011. Hence, the PAR keeps improving as $\alpha$ increases.

Figure 6.7 illustrates the trade-off between electricity price and that of feeder congestion level as the weight, $\alpha$, of the objective function (6.7) varies. The importance of valley filling load scheduling increases as the weight, $\alpha$, increases. This results in a flexible load schedule that is more costly compared to that of lower weights where price-based scheduling is dominant. However, a higher weight indicates lower congestion levels.

### Comparison of Results with Existing Distributed Dynamic Tariff Congestion Management Scheme and Discussion

To evaluate the performance of the proposed multi-objective congestion management scheme, the results obtained on simulating the IEEE 33 bus case study are compared with that of the existing DDT congestion management scheme [26]. Comparison is executed in terms of electricity price paid by consumers and PAR of the power flowing in the main feeder as follows.

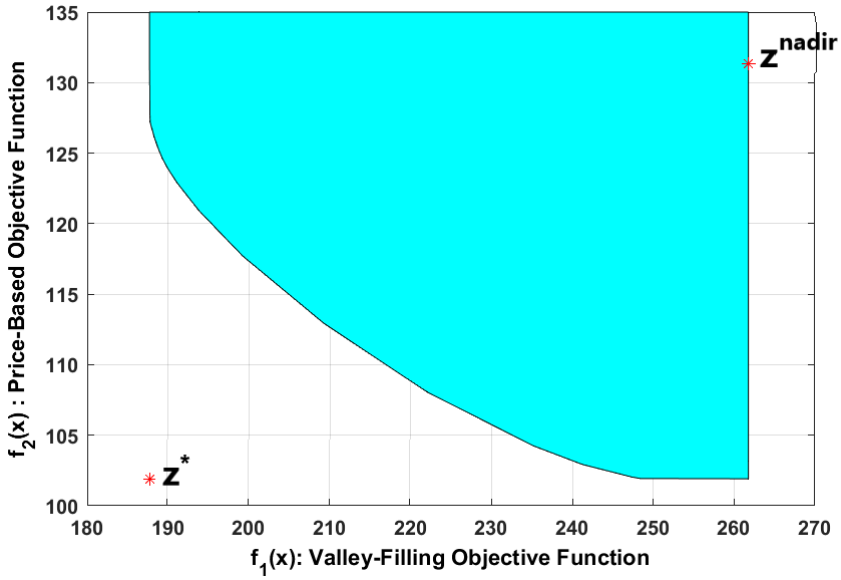



Figure 6.5: Pareto optimal front, ideal and nadir points

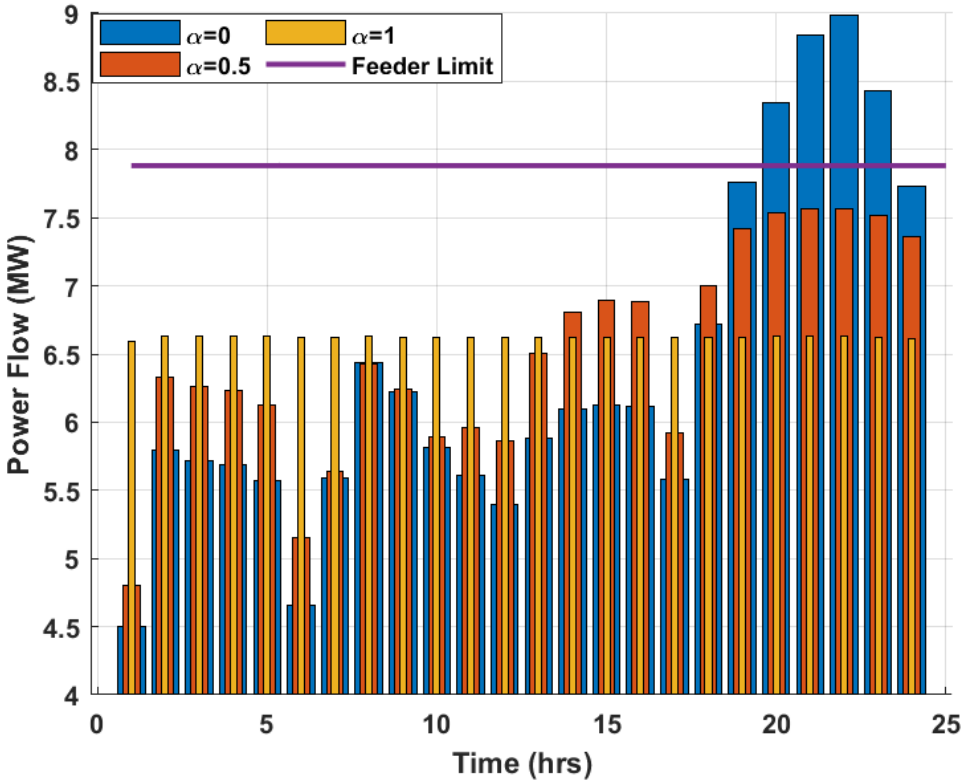



Figure 6.6: Effect of varying multi-objective function weight, $\alpha$, on power flowing in main feeder

- Electricity Price: DDT congestion management results in scheduling the load such that the electricity cost of the consumers is minimized. Hence, as illustrated in Figure 6.8, flexible loads are scheduled mainly in the early and late hours of the night when the price of electricity is the lowest. If the line was not congested, consumers had to pay a total of 4853.8$, based on electricity prices illustrated in Figure 6.4. However, as a result of congestion at $t = 21 - 22$, a congestion tariff of $0.06\$/kW$, and $0.075\$/kW$ was, hence, imposed on the consumers at times, $t = 21$ and 22 respectively to alleviate the congestion. This tariff is eventually paid by the consumers as a total increase in electricity cost by 21.6%. On the other hand, no tariffs are imposed using the proposed multi-objective congestion management scheme. The proposed algorithm aims to improve the welfare of the consumer in terms of minimizing electricity price while maintaining indoor temperatures within consumers preferences and charging their EVs based on their availability. Moreover, the proposed scheme improves the

welfare of the network operator, in terms of flattening the curve and reducing the PAR. Consumers following the proposed multi-objective optimization would end up paying a total of 4964.6, which is 15.9% lower than price-based optimization.

- PAR: As DDT congestion management scheme aims to minimize electricity costs, consumer loads end up being concentrated at times in which the electricity price is low causing congestion. To alleviate congestion, tariffs need to be imposed to clear the peak, as illustrated in Figure 6.8. The PAR of the resulting power flowing in the feeder is observed to be 1.362 which is caused as a result of the peak in demand at $t = 21 - 22$ causing congestion. On the other hand, the proposed multi-objective optimization resulted in a congestion-free network with a PAR of 1.152 which is sufficient enough to have a congestion-free feeder at minimum electricity price.

From the above discussion and comparison, the superiority of the proposed multi-objective flexible load scheduling to manage congestion in the network with minimal impact on electricity prices has been demonstrated.

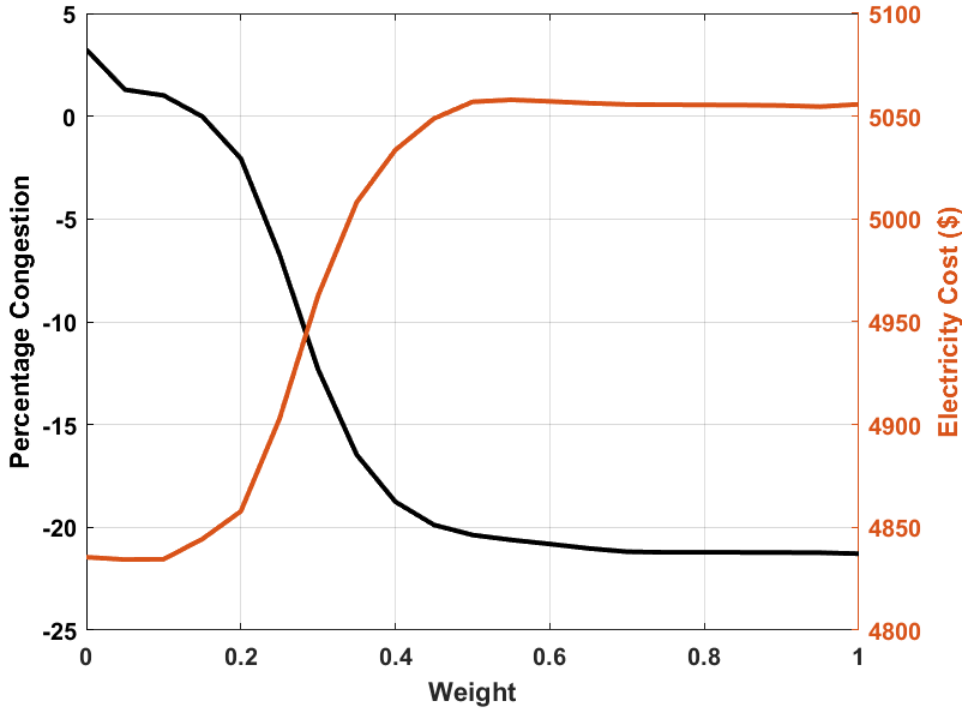



Figure 6.7: Percentage congestion in the network versus electricity cost as a function of Pareto weight

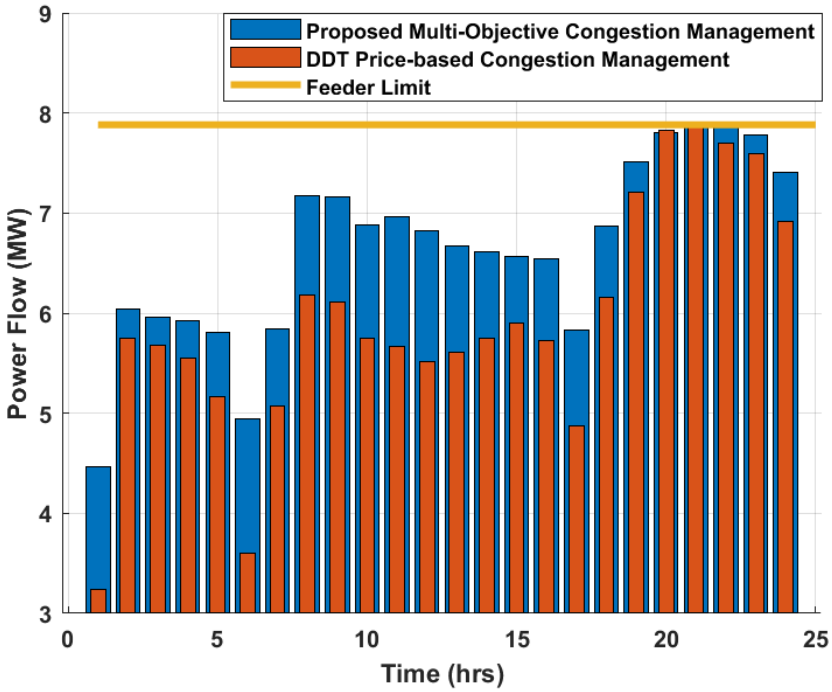



Figure 6.8: Comparison using proposed multi-objective load scheduling versus DDT congestion management scheme

### 6.4.2 Robustness of the Proposed Multi-Objective Congestion Management Scheme

As a result of the uncertainties in the load scheduling design parameters, $U$, as described in Section 6.3, the IEEE 33 bus system is adopted to study the uncertainty of the power flowing in its main feeder to uncertainties in the load, $U$. Four uncertain parameters are considered in the design, where $U = \{\Delta t_{ar}, \Delta t_{dep}, \Delta P^{req}, \text{and } \Delta T_e\}$. Using the results obtained from the deterministic case, the sensitivity, $\zeta_U = \{\frac{\partial F_t}{\partial t_{ar}}, \frac{\partial F_t}{\partial t_{dep}}, \frac{\partial F_t}{\partial P_{req}}, \frac{\partial F_t}{\partial T_e}\}$, of the power flowing in the main feeder to the random design variables was determined by executing (6.24-6.25). For example, as a result of uncertainty in power required by an EV, the sensitivity factor, $\zeta^{Preq} = \frac{\partial F_t}{\partial P_{req}}$, which represents the change in power flowing in the main feeder of the IEEE 33 bus system as a result of 1kWh change in the consumer loads due to more EV charge required, was observed to complement the power flowing in the main feeder. This is illustrated in Figure 6.9. When the main feeder is lightly loaded, the sensitivity is observed to be higher compared to peak times. This results in flattening the

curve and ensuring that no congestion occurs.

Using the sensitivities and the PDFs of the four uncertain parameters, $U$, Algorithm 1 was executed. Using the deterministic model, a Pareto weight, $\alpha = 0.4328$, resolves the congestion in the distribution network as illustrated in Figure 6.10. However, on evaluating the robustness constraint (6.14) of the resulting distribution due to the uncertainties in the load, $U$, given $\delta = 5\%$, change in the line loading, $F_t^b$, in the main feeder was not satisfied, given $\eta = 0.997$. The Pareto had to be, thus, updated to $\alpha = 0.4928$ following Algorithm 1 at which the robustness constraint (6.14) was satisfied. Figure 6.10 illustrates the difference in power flowing in the main feeder as a result of the change in the Pareto weight. The deterministic scheme having a lower Pareto weight of $\alpha = 0.4328$ did not satisfy the robustness constraint (6.14). As observed at times $t = 21 - 22$, power flowing in the main feeder is just below the feeder limits. Any slight increase in consumer demand at those times would cause congestion in the network. Hence, the robust scheme was executed and it resulted in having a larger Pareto which ensures that the power flowing in the main

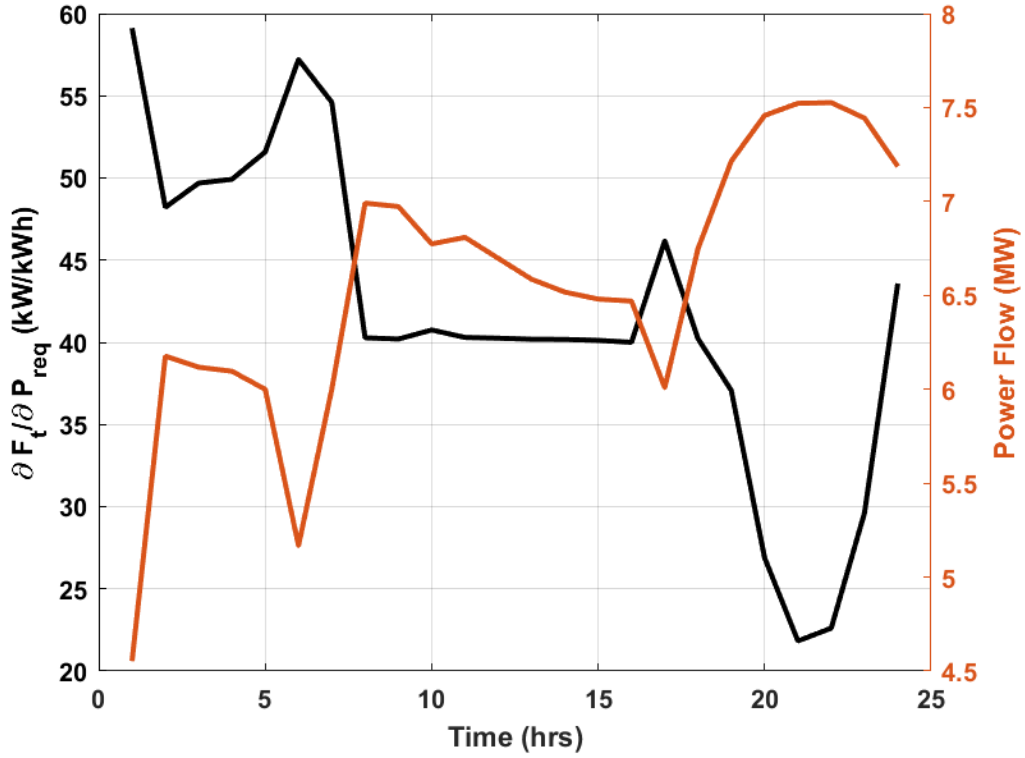



Figure 6.9: Sensitivity of the IEEE 33 bus system main feeder line loading to changes in EV power required

feeder is below its congestion limit, as illustrated in Figure 6.10.

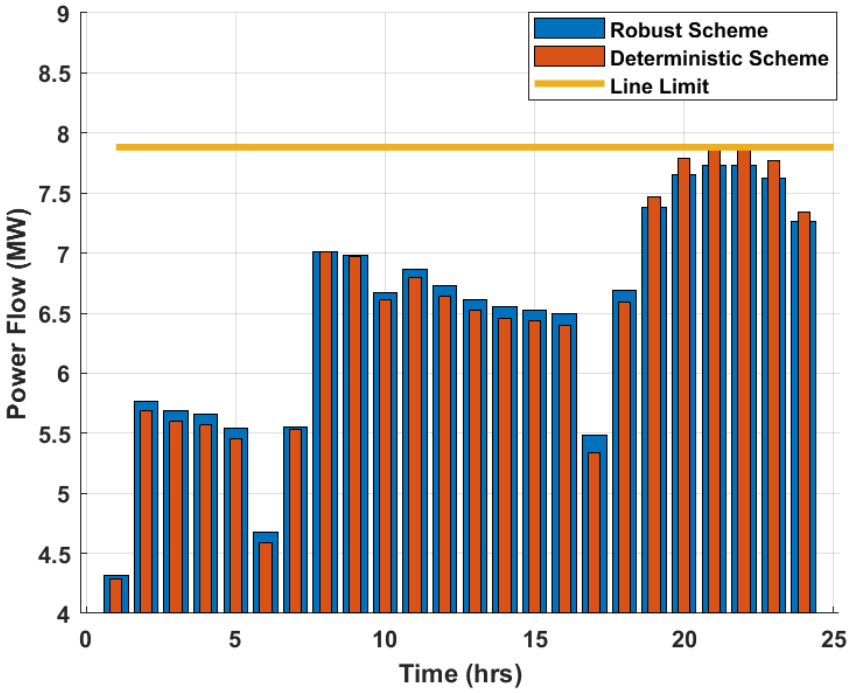



Figure 6.10: Comparison between the robust and deterministic schemes in terms of power flowing in the main feeder

## 6.5 Conclusions

In this chapter, a multi-objective flexible load scheduling algorithm was proposed to manage congestions in the distribution network. The proposed model combines the advantages of price-based and valley-filling demand-side management using multi-objective optimization. An interactive method was then utilized by the DNO to search for the optimal solution that clears congestion in the distribution network. The higher the congestion, the higher is the weight given to the valley-filling portion of the multi-objective problem compared to that of the price-based objective function. This results in determining an optimal Pareto from the resulting Pareto front that is sufficient enough to relieve congestion at the minimum electricity price. Moreover, the stochastic nature of flexible loads

has also been incorporated into the congestion management scheme. A sensitivity analysis was executed to determine the propagation of uncertainty in the proposed model ensuring that the probability of overloading the network is less than a specific level given the uncertainty involved in scheduling the flexible loads. The proposed congestion management scheme was compared with the existing Distributed Dynamic Tariff price-based congestion management scheme to demonstrate the superiority of the technique. The proposed multi-objective model resulted in the most economical solution in the presence or absence of congestion and an improved peak to average ratio compared to that of the price-based method. Therefore, combining the advantages of price-based and valley-filling DSM into one optimization problem resulted in a model that is economical for the consumer and also relieves congestion.

[1]

[1]This work has been published in: Gul M Khan, O., Youssef, A., Salama, M. and El Saadany, E. *Robust Multi-Objective Congestion Management in Distribution Networks.* IEEE Transactions on Smart Grid Power Systems, 2022, doi: 10.1109/TPWRS.2022.3200838.

# Chapter 7

# Congestion Management in Distribution Networks Using Reinforcement Learning

## 7.1 Introduction

In the existing congestion management literature, as discussed in Chapter 2, consumers are the owners of flexible and non-flexible loads and they are represented in the electricity market through the aggregators. Aggregators are load-serving entities responsible for scheduling their consumers' loads. Consumption preferences, such as the charging behavior of Electric Vehicles (EVs) and indoor temperature requirements, have to be communicated, via the neighborhood area network, to aggregators to minimize consumers' costs and to schedule their loads optimally. However, aggregators are capable of analyzing individual customers' data they have been provided legally. Such aggregators referred to as honest-but-curious aggregators, follow the communication protocols but can infer information from consumer acquired data compromising the privacy of consumers [114]. Knowing a consumer's availability for EV charging or their indoor temperature requirement during certain hours of the day can result in the aggregator indirectly knowing consumers' lifestyles or behavior. As the electrical grid is modernized, it is critically important to ensure the collection of consumer data in a manner that improves the grid's efficiency while protecting consumers' privacy. Hence, optimal scheduling of consumers' loads is proposed to be executed at the individual smart meter level combined with efficient additive secret sharing [115] to maintain the privacy of consumers from semi-honest aggregators.

The optimal aggregated load schedules are submitted by the aggregators in the wide area network to the Distribution Network Operator (DNO) as illustrated in Figure 7.1. The DNO, in turn, is responsible for managing any congestion in the network. In the distribution network, most congestion management schemes fall into two categories: those that use locational marginal prices to determine congestion tariffs and/or subsidies needed as a way to alleviate network overload, and those that forecast consumer demand. In [116], distribution locational marginal price (DLMP) was proposed to manage congestion caused by EV. The DNO is responsible for determining the DLMP by solving a constrained social welfare linear optimization problem using the forecasted EV demand. However, the error associated with EV load forecasts is a problem and linear optimization can result in multiple schedules. To ensure the uniqueness of the optimal flexible load schedule, [24] proposed a quadratic optimization for scheduling aggregator loads. The DNO is expected to forecast the demand of consumers' flexible loads. This is, however, not easy in reality. Moreover, the quadratic terms come from forecasting the price sensitivity of the consumers in the network which is also a difficult task. To remove the uncertainty caused by forecasting consumers' requirements, Huang et al. [26] utilized quadratic optimization for the aggregators to determine their consumer's schedules. The aggregators' load demands are then communicated to the distribution network operator, who uses the marginal price of service costs based on voltage and flow limits to set the Distributed Dynamic Tariff (DDT). The determined rate is sent to the aggregators to re-optimize their flexible load schedules using the new prices. In the process of determining the congestion tariff, which alleviates any existing congestion, this process is repeated several times based on the step size chosen. In [117], the problem of forecasting the rate of change of consumer demand to changes in price, referred to as consumer price sensitivity [24], is solved by adopting a quadratic cost model of the power consumed. Although this method relies least on forecasted terms, the process of determining the tariff that manages congestion is iterative requiring multiple back and forth transmission of data using the communication network.

Subsidy-based method [27] and peak time rebate [118] have also been utilized in the literature as incentive-based Demand Side Management (DSM) congestion management methods. In [27], two-level optimization is utilized by the network operator to determine the needed subsidy to alleviate congestion. The first level of optimization involves determining the minimum subsidy that alleviates network congestion. The second level of optimization involves determining the optimal aggregator schedule that minimizes electricity consumption costs for their respective consumers. However, the effort needed to solve the dynamic subsidy problem is more compared to the Dynamic Tariff (DT) method. Sarker et al. [118] utilized time-dependent economic incentives to minimize the cost of electricity on consumers while managing congestion. However, the aggregator was responsible

for determining the sufficient incentive needed by the consumers to shift their demand. For this method to work, aggregators should be aware of the line capacities of their nodes. Hence, the work restricts the network to only one aggregator whose functions are executed by the DNO.

Existing congestion management techniques are defined as model-based methods, requiring an optimization model for aggregator scheduling and for determining congestion tariff by the network operator. The model-based methods, however, require prior knowledge of the exact load models. However, flexible load models are stochastic and are affected by factors such as temperature, location, etc. Obtaining stochastic models for such loads may not be easily available in practice. Moreover, these model-based schemes rely on the accuracy of uncertain parameters, such as consumers' energy price sensitivity. This step is a difficult task considering the heterogeneity of consumers and their behavioral differences [40]. Moreover, the models require back and forth iterations between the network operator and aggregators via the communication network to determine the needed tariff to alleviate network congestions. There is no guarantee that the iterations will complete as consumers' comfort preferences might not be met causing the persistence of peak load and congestion not being managed in the day-ahead market. Due to the above limitations, a method needs to be developed to determine an appropriate congestion tariff that relieves network congestion. As the problem requires decision-making in an uncertain environment, and given the large volume of data available in the smart grid, a data-driven machine learning model is proposed as a congestion management model in the distribution network. Proven the high accuracy of deep learning-based models in other applications in power systems, and their capability to learn patterns unsupervised, they are ideal for determining the required tariffs and/or subsidies to alleviate congestion. Specifically, Deep Deterministic Policy Gradient (DDPG) Reinforcement Learning (RL) is utilized as a model-free technique that does not require explicit probabilistic models of the controllable loads to determine the congestion tariff that would alleviate congestion. Instead, RL trains an agent to take appropriate actions in a dynamic environment to maximize long-term reward [119]. The distribution network operator represents the agent that senses the state of the environment and determines, accordingly, the action needed to manage congestion. The overall aim of the agent is to maximize a numerical reward signal that is calculated as a consequence of actions taken. DDPG determines a deterministic policy for determining the action needed given continuous stochastic environment state.

RL has been utilized in the literature to manage congestion through reconfiguration of the distribution network. [120] utilized a RL assisted multi-objective bacterial foraging optimization algorithm to solve its many-objective distribution network reconfiguration model. The model aims to improve the accommodated of renewable energy resources while

maintaining the stability of network operations. Similarly, [121] developed a data driven batch constrained RL model for dynamic distribution network reconfiguration to improve system's performance. Bahrami et al. [122] proposed a RL algorithm to remotely control flexible loads in the distribution network considering network constraints. A two-stage voltage control model adopting RL was developed in [123] to mitigate voltage violations caused by the increased penetration of EVs in the network. However, to our knowledge, RL has not been adopted to determine congestion tariffs and/or incentives to motivate consumers to shift their loads from peak to off-peak time managing distribution network congestion.

In this chapter, we aim to develop a DDPG RL model [124], having a continuous state and action space, to determine the needed tariffs and/or subsidies to alleviate existing congestions in the distribution network. To the best of our knowledge, this is the first work that applies RL to solve congestion in the distribution network. The contribution of this chapter is achieved through completing the following milestones:

- The congestion management problem is formulated as a Markov Decision Process where the distribution network represents the environment from which the network states are extracted.
- Historical data and interactions with aggregators and Home Energy Management System (HEMS) are utilized to train the DDPG reinforcement learning model. The RL model's objective is to manage congestion, minimize costs, and/or improve the peak-to-average ratio of line loads by using tariffs and subsidies. The trained RL model would be operated by the DNO and adopted in the day-ahead market to determine the congestion tariff and/or subsidy needed to alleviate any congestion in the distribution network.
- A case study is simulated and results are compared with existing DSM-based congestion management techniques.

The overall model proposed for managing congestion in the distribution network is illustrated in Figure 7.1.

The rest of the chapter is organized as follows: in Section 7.2 optimization of consumer load schedule and its aggregation by additive secret sharing is explained. In Section 7.3 reinforcement learning is introduced, followed by developing the proposed system model in terms of the environment, agent, and reward signal. Section 7.4 illustrates a case study adopted for implementing the proposed model. The results obtained and their comparison with an existing DSM-based congestion management model is explained in Section 7.5. Finally, the chapter is concluded in Section 7.6.

## 7.2 Consumer Load Scheduling and Aggregation

Consumers' smart meters' HEMSs are utilized for optimally scheduling their flexible loads. Hence, this scheme does not share consumers' load utilization preferences with their respective aggregators, hence, protecting consumers against honest-but-curious aggregators [125] who collect and analyze consumer information, threatening their privacy. Consumer's loads are aggregated using an aggregator oblivious scheme such that the aggregator is not capable of learning any unintended information about its consumers.

### 7.2.1 Consumer Flexible Load Scheduling

Each aggregator, $a$, in the distribution network, where $a \in N_A$ and $N_A$ is the set of aggregators in the network, is responsible for $N_k$ consumers, as illustrated in Figure 7.2. Given the day-ahead electricity price, $p_t$, and to ensure that the aggregators are consumer load oblivious, each consumer smart meter is assigned to schedule its flexible load. Hence, consumers' preferences in utilizing their flexible loads are maintained private and not shared with any other entity. Quadratic optimization [26] is utilized at the consumer level to schedule the flexible loads using the HEMSs as follows,

$$\min_{P^f_{h,t}} \sum_t {P^f_{h,t}}^T \beta P^f_{h,t} + P^f_{h,t}(p_t + a_t) \tag{7.1}$$

Hence, the objective of each HEMS is to minimize its consumer's total electricity cost. $P^f_{h,t}$ represents the flexible load of consumer $h$, at time $t$, where $h \in N_k$ and $N_k$ represents the set of consumers aggregator $a$ is responsible of. Moreover, $t \in N_t$ where $N_t$ represents the set of time slots considered in the day-ahead market. Moreover, $\beta$ is the price sensitivity coefficient matrix and $a_t$ represents the congestion tariff and/or subsidy. The base loads, $P^{nf}_{h,t}$ are not considered in the objective function as they are assumed to be inflexible. However, they will be considered in the line loading of the distribution network.

The HEMS ensures that the consumer flexible load utilization preferences are met through constraints imposed in solving the quadratic optimization problem (7.1). Initially, the HEMSs schedule their flexible loads using a congestion tariff, $r_t$, equal to zero. This is later updated based on the determined congestion tariff that alleviates any overload in the network. Solving the optimization problem (7.1) results in determining the total load requirement, $P_{h,t}$ for consumer $h$ as follows,

$$P_{h,t} = (P^{nf}_{h,t} + P^f_{h,t}), h \in N_k, t \in N_t \tag{7.2}$$

### 7.2.2 Additive Secret Sharing Consumer Data Aggregation

To communicate with the DNO, and to represent the consumers in the electricity market, network aggregators require knowledge of their consumers' total load. However, trusting the aggregator with such private information is risky. Ensuring the collection of consumer data in a manner that improves the grid's efficiency while protecting consumers' privacy is critical. Shamir's additive secret sharing scheme is proposed to maintain the privacy of consumers from honest-but-curious aggregators [126] [127]. In this scheme $k$ shares, where $k$ represents the number of houses belonging to aggregator $a$ on one bus, are constructed from the load profile of consumer $h$ per time slot, $P_{h,t}$. Although simple to execute, this cryptographic technique provides a secure computation protocol as every share at every time step, $t$, is uniformly distributed at random and an adversary would require all $k$ shares of a consumer load profile to be able to reconstruct it. Each consumer load would then retain one of its shares and distribute the remaining $k-1$ shares to the consumers in the neighborhood area network. The consumers would then submit their share along with their neighborhood shares that it has received to their aggregator. The aggregator would hence receive the total consumer load without knowing the specific consumption details of each consumer.

## 7.3 Reinforcement Learning Congestion Management System Design

The aggregators in the network are responsible for privately aggregating their consumers' load profiles and forwarding their total load, $P^a$, to the DNO, as illustrated by step 5 in Figure 7.1. However, consumers' controllable loads, such as EVs, are stochastic and their utilization depends on uncertain factors such as consumers traveling behavior. To optimally determine the congestion tariff needed to alleviate congestion, complete statistical information of the loads is required. Such information is not readily available in a practical system. Hence, a data-driven machine learning model is proposed to manage congestion problems in distribution networks. More specifically, having the capability to be model-free and adapt to stochastic changes in its environment, RL is utilized as a machine learning technique that determines changes in electricity price to alleviate network congestion.

The proposed RL congestion management model consists of the DNO, the aggregators,

and the consumers, as illustrated in Figure 7.1. Aggregators and consumers represent the environment of the proposed model. As explained earlier in Section 7.2, consumers' smart meters communicate their additive secret shared load profile to the aggregators. Aggregators are then responsible for transmitting their total loads to the DNO. The DNO represents the trained agent in the RL model: observing the environment's state, and deciding on the action in terms of tariff and/or subsidy to alleviate existing congestion in the network. The action, representing the congestion tariff and/or subsidy, is decided in only one step, contrary to existing model-based techniques which require multiple iterations between the network operator and the aggregators. The DNO relies on the smart grid's communication infrastructure to receive aggregators' load schedules and send price signals via the Wide Area Network. The interaction between the RL agent (the DNO) and the environment (the aggregators) in the network, can be depicted in Figure 7.3 and is explained in detail next.

### 7.3.1 Formulation of the Markov Decision Process

The congestion management problem is modeled as a finite Markov Decision Process (MDP). MDP represents the mathematical framework describing the problems' environment in reinforcement learning. The environment of the congestion management problem is represented by the distribution network consumers and aggregators. Aggregators are entities responsible for providing the day-ahead electricity prices to their consumers, as illustrated by step 1 in Figure 7.1. Consumers' HEMS are responsible for scheduling their flexible load using the scheme explained in Section 7.2 and forwarding it to their aggregators, as illustrated by steps 2 to 4 in Figure 7.1 respectively. The consumers in the distribution network are assumed to be represented by $N_a$ aggregators. Aggregators (who innately represent the consumers) forward their shiftable and non-shiftable loads to the DNO, as illustrated by step 5 in Figure 7.1. The MDP is then represented by a quadtuple $< S, A, R, S' >$ wherein each component is described as follows:

- **State Set**, $S = \{s^1, s^2, ..s^K\}$: The network operator utilizes the day-ahead aggregator loads, $P_k^a$, day-ahead electricity prices, $p_k$, and the resulting power flowing in the main feeder after performing AC power flow analysis, $P_k^b$, as the environment states, $s_k$, for the RL agent, as illustrated by step 6 in Figure 7.1. Hence, environment state at step $k$ is represented by: $s_k = \{P_k^a, p_k, P_k^b\}$.
- **Action Set**, $A = \{a^1, a^2, ..a^K\}$: The action set represents the congestion tariff and/or subsidy, in the form of a delta increase and/or decrease in day-ahead electricity price, $p_k$. Action, $a_k$, is hence, a vector with $N_t$ dimension. It is bounded based

on whether the model is imposing a tariff and/or subsidy. For a RL model that adopts a congestion tariff: $0 \leq a_k \leq a^{max}$, where $a^{max}$ is the maximum possible tariff that can be imposed. Similarly, for a RL model that adopts a congestion subsidy: $a^{min} \leq a_k \leq 0$, where $a^{min}$ is the minimum possible tariff that can be imposed. For the third scenario in which a RL is trained with both tariffs and subsidies: $a^{min} \leq a_k \leq a^{max}$.

- **Reward Set**, $R = \{r^1, r^2, ..r^K\}$: The reward at step, $k$, in an episode refers to a mapping of each state-action pair to a number that reflects how desirable a state is given the goal it aimed for. The objective of the proposed model is to alleviate distribution network congestion. Hence, designing a reward function that should be maximized within a finite horizon to train the RL agent to achieve the desired objective is important. To assign a reward, $r_k$, the state, $s_{k+1}$, of the distribution network as a result of the action, $a_k$, imposed is observed, as illustrated in Figure 7.3. In the event of congestion, the reward assigned should capture the state of the environment its action caused. Hence, the reward is modeled to be proportional to the amount of congestion in the network. The water-filling algorithm [36] is utilized to fill existing valleys in the distribution network load profile. The reward function, $r_k$, encourages the model to assign actions that minimize the difference between peak load and its valleys using the water-filling algorithm. Based on the water-filling algorithm, flexible load is scheduled at times in which the non-flexible load, $P_k^{nf}$, is low as follows,

$$P_k^f = (\epsilon - P_k^{nf})^+ \tag{7.3}$$

where $\epsilon$ is referred to as the water level. In the absence of congestion, the reward assigned aims to minimize the consumer electricity bill. This ensures that the action imposed is not excessive of what is required to clear the congestion. Moreover, the reward function should ensure that the voltage constraints of the distribution network are met. Hence, the reward function can be defined as follows,

$$r_k = \begin{cases} -\eta|\big(P_k^f - (max(P_k^{nf}) - P_k^{nf})\big)| + \\ \qquad \beta((V_b - V^{max})^+ + (V^{min} - V_b)^+), \text{if } P_k^b > P^{max} \\ -P_k(p_k + a_k), \qquad \text{otherwise} \end{cases} \tag{7.4}$$

where $\eta$ and $\beta$ are positive scaling factors and $P^{max}$ is the maximum branch capacity. $V_b$ represents the networks' bus voltage, while $V^{min}$ and $V^{max}$ are the distribution network voltage limits. Moreover, $(x)^+ = max(x, 0)$.

- **State Transitions**, $S'$: To manage congestion in the distribution network, the state

of the environment, $s_k$, is updated to $s_{k+1}$ on executing congestion tariff/subsidy action, $a_k$. The optimal action, $a_k$, is decided using the actor network optimal policy, $\mu^*(s)$, based on the current state, $s_k$, of the environment such that the expected reward of the model when starting from state, $s_1$, over horizon $K$ is maximized.

### 7.3.2 Training the DNO RL Agent

After formulating the congestion management problem as a MDP, the optimal policy that maps the congested state of the distribution network environment to an uncongested state through the tariffs and/or subsidy action needs to be determined. The DNO represents the RL agent that executes the RL algorithm. Given the environment state, $S$, the RL actor agent executes an action, $A$, that is modified to encourage exploration of all existing actions using the Ornstein-Uhlenbech process [128] to generate a time-correlated noise, $N$, such that

$$A = \mu(S) + N \tag{7.5}$$

Congestion tariff and/or subsidy, in the form of a delta increase and/or decrease in electricity price, $p_k$, is chosen as executed actions, $A$. However, as the overall aim of the proposed RL agent is to determine appropriate agent actions that would alleviate any congestion in the day-ahead market, discretizing the action would lead to a very large action space. Hence, given the large continuous state and action spaces, the DDPG RL algorithm [124] is adopted as it is a model-free method. Using its actor-critic architecture, a DDPG agent finds the optimal policy to maximize its long-term rewards. Since DDPG agents are model-free, they do not store all possible combinations of environment states and consequent actions, so they can handle a large amount of data. A DDPG actor, $\mu(S|\theta^{\mu})$, where $\theta^{\mu}$ represents the actor's weights, is responsible for determining the policy, $\pi$, that maps the action, $A$, given a state, $S$, such that the long-term reward, $V$, is maximized. On the other hand, a DDPG critic, $Q(S, A|\theta^{Q})$, where $\theta^{Q}$ represents the critic's weights, is responsible for utilizing the action and state to return the corresponding expected long-term reward, $V$. Hence, it evaluates how good an action is given a state and an action. Besides the actor and critic networks, a DDPG agent also uses two target networks: target critic, $Q'(S, A|\theta^{Q'})$, and target actor, $\mu'(S|\theta^{\mu'})$, to add stability to the training. $\theta^{Q'}$ and $\theta^{\mu'}$ represents the weights of the target critic and actor respectively. Hence, reinforcement learning happens using estimated targets, which are in turn updated slowly keeping the estimated targets stable.

**Algorithm 2** DDPG RL congestion management algorithm

**Initialize:**

- Randomly set the congestion management RL models' critic, $Q(S, A|\theta^Q)$, and actor, $\mu(S|\theta^\mu)$, networks with weights, $\theta^Q$ and $\theta^\mu$, respectively.
- Set the target critic, $Q'(S, A|\theta^{Q'})$, and the target actor, $\mu'(S|\theta^{\mu'})$, network with weights, $\theta^{Q'}$ and $\theta^{\mu'}$ respectively as follows:

$$\theta^{Q'} \longleftarrow \theta^Q$$
$$\theta^{\mu'} \longleftarrow \theta^\mu$$

**for** training episode=1 *to* $M$ till convergence **do**

- Simulate distribution network initial state, $s_1$, such that $s_1 = \{P_1^a, p_1, P_1^b\}$.
- **for** $k = 1$ *to* $K$ **do**
  - Given distribution network (environment) state, $S$, select congestion tariff and/or subsidy (action), $a_k = \mu(s_k) + N$.
  - Implement the selected congestion tariff and/or subsidy, $a_k$, and observe the resulting change in the distribution network state, $s'_k$.
  - Determine the effectiveness of the selected tariff, $a_k$, on the distribution network and quantify it using reward, $r_k$.
  - Store the congestion management training model's experience tuple $(s_k, a_k, r_k, s'_k)$ in its experience buffer.
  - Sample a random batch of $L$ tuples from the congestion management training model's experience buffer.
  - Set the expected return, $V$, as observed by the model's target network as follows,
    - **if** ($S'$ represents a congestion free distribution network state) **then** $V = R$
    - **else** $V = R + \gamma Q'(S', \mu(S'|\theta^{\mu'})|\theta^{Q'})$

    where $\gamma$ is the discount factor representing how much the utility operator cares about future rewards.
  - Update the RL model's critic network, $Q(S, A|\theta^Q)$, by minimizing the mean squared error as follows,

$$L = \frac{1}{N}\sum(V - Q(S, A|\theta^Q))^2$$

  - Update the actor network by calculating the mean of the policy gradients of the model's sampled batch.
  - Update the target networks using smoothing factor, $\tau$, as follows:

$$\theta^{Q'} \longleftarrow \tau\theta^Q + (1-\tau)\theta^{Q'}$$

$$\theta^{\mu'} \longleftarrow \tau\theta^\mu + (1-\tau)\theta^{\mu'}$$

To train the reinforcement learning congestion management model, given the environment state, $S$, received from the aggregators and the consumers in the distribution network, the RL agent executes an action, $A$, based on the current actor's policy, $\mu(S|\theta^{\mu})$. The action is in the form of positive tariff or negative subsidy that is to be added to the electricity cost. The action is forwarded to the aggregators and consumers in the network, so that they reschedule their flexible loads based on the price change, $p_k \pm a_k$. The updated aggregated consumer load is submitted to the network operator and the resulting change in the state of the environment, $S'$, is observed by the RL critic. The critic evaluates the goodness of the executed action, $a_k$, on the environment in terms of alleviating network congestion by calculating an approximate $Q(S, A|\theta^{Q})$ that depends on $s_k$, $a_k$, and the corresponding immediate reward, $r_k$. Hence, if $s_{k+1}$ reflects an uncongested network, then the training episode is considered successful and the reward, $r_k$, is high. If however, $s_{k+1}$ reflects a congested system, then the training episode is considered unsuccessful and the reward for the state-action pair is low. This continues for a finite horizon until the episode ends by achieving a congestion-free state or reaching the maximum steps limit. The actor and critic policies are not updated after each transition sample. Instead, the quadruple $(S, A, R, S')$ is stored after each step in its experience buffer. A random mini-batch of experiences is then utilized to update the actor and critic networks. Hence, for training the congestion management RL model, multiple episodes that iterate between the utility operator (representing the agent) and the aggregators are executed. Algorithm 2 represents the training algorithm adopted by the DDPG agent to update its actor and critic models for each episode. The training algorithm is executed until the RL model's reward converges to its maximum. The trained model can then be tested in the day-ahead market. Given the day-ahead load schedule of the aggregators in the network, the DNO can use the trained RL model to determine the needed tariff to alleviate any network congestion using a limited number of iterations.

## 7.4 Case Study

In this section, the distribution network studied for congestion is simulated. The proposed RL congestion model is then adopted to manage existing network overloads, and the performance of the model is evaluated against an existing congestion management scheme.

### 7.4.1 Distribution Network

In order to study the proposed reinforcement learning congestion management model, the IEEE 33 bus system [1] is used, as illustrated in Figure 7.4. The test system is a

12.66kV system having one feeder substation, 32 buses representing both residential and commercial loads. Bus 23 and 24, having the largest baseload, represents commercial buses consisting of EV charging parking lots. All the remaining load buses are assumed to be residential, having both flexible and nonflexible loads. The default loading of the IEEE 33 bus system represents the non-flexible base load profiles of the load buses. EVs and air-source Heat Pump (HP) are used to represent the flexible loads owned by residential consumers. Air-source HPs extract heat from the external air for heating and pump heat outside for residential cooling. The thermal dynamics of HPs [113] are modeled by the following constraints,

$$T^i_{h,t} - T^i_{h,t-1} = \frac{1}{C^i_h}(P^{hp}_{h,t}C_h + R^{is}_h(T^s_{h,t} - T^i_{h,t}) + R^{ie}_h(T^e_t - T^i_{h,t})) \tag{7.6}$$

$$T^s_{h,t} - T^s_{h,t-1} = \frac{1}{C^s_h}(R^{is}_h(T^i_{h,t} - T^s_{h,t}) + R^{se}_h(T^e_t - T^s_{h,t})) \tag{7.7}$$

$$0 \leq P^{hp}_{h,t} \leq P^{hp}_{max} \tag{7.8}$$

$$T^{min}_h \leq T^i_{h,t} \leq T^{max}_h \tag{7.9}$$

where $C^i_h$ and $C^s_h$ represent the internal and surface heat capacity of house, $h$, respectively. $R^{is}$, $R^{ie}$, and $R^{se}$ represent thermal resistance between the interior and surface, interior and external, and surface and exterior respectively. $C_h$ symbolizes the coefficient of performance of the HP. $P^{hp}_{max}$ is the maximum heat output limit. $T^i_{h,t}$ is the internal temperature of house $h$ at time, $t$, and $T^{max}_h$ and $T^{min}_h$ are the maximum and minimum indoor temperature preferences of the consumers. $T^e_t$ is the external temperature and $T^s_{h,t}$ is the surface temperature of house $h$ at time $t$. The coefficient of performance of the simulated HPs is 2.2 and single-story houses are simulated having an average height of 8ft. Residential houses and internal temperature preferences were randomly assigned areas between 1500 to 2500 sq. ft. and temperatures between 18 to 24$^\circ C$ respectively.

Similarly, EV charging in the distribution network is modeled by:

$$P^{req}_h \leq \sum_t P^{ev}_{h,t} \tag{7.10}$$

$$0 \leq P^{ev}_{h,t} \leq a_{h,t}P^{ev_{max}}_h \tag{7.11}$$

where $P_h^{req}$ is the total required battery charge for EV $h$, energy at time $t$, $P_h^{ev_{max}}$ is the maximum charging power, and $a_{h,t}$ is how the availability of EV $h$ at time $t$ for charging. Data obtained from the Toronto parking authority [129] representing arrival and departure times of cars in a commercial area parking lot were used to simulate the availability of EVs in commercial and residential parking lots for charging. A subset of the data collected was used to ensure the availability of the EV for a duration greater than their required charging time. In the absence of an EV from the lot, the EV was assumed to be at home. The initial state of charge (SOC) of each EV is randomized to be distributed uniformly between 10% and 20% and it is assumed that the owners would want the car completely charged on departure. The EV battery sizes are assumed to be 10kWh and their maximum residential charging power is 5kW. The case study involves a total of 32 aggregators, one aggregator representing consumers of each load bus. GAMS [86] and MATLAB R2021a was used for executing the load scheduling optimization and training the DDPG RL congestion management scheme.

### 7.4.2 Comparison Algorithm

To analyze the results obtained, the performance of the proposed congestion management scheme is compared with that of the existing model-based DDT congestion management model [26]. DDT relies on aggregators' day-ahead load data to propose a congestion tariff that could alleviate network congestion. This tariff is communicated to the aggregators to shift their consumers' peak demand to minimize their electricity costs. Hence, multiple iterations between aggregators in the network and the utility operator occur to determine the congestion tariff that alleviates congestion. To compare the results obtained through the proposed RL model and that of the DDT scheme, the total electricity cost as a result of each model is determined as follows,

$$Cost = \sum_{h} \sum_{t} P_{h,t}(p_t + r_t) \tag{7.12}$$

Comparison between the proposed scheme and the existing DDT congestion management model is also done in terms of the Peak to Average Ratio (PAR) of the power flowing in the main feeder, $P_t^f$, of the IEEE 33 bus system as follows,

$$PAR = \frac{\max_{t \in N_T} P_t^f}{\frac{1}{T} \sum_{t \in N_T} P_t^f} \tag{7.13}$$

### 7.4.3 RL Training

To train the proposed RL model that manages congestion in the distribution network, the actor, $\mu(S)$, and the critic networks, $Q(S, A)$, are designed to consist of deep neural networks with two hidden layers. Each hidden layer consists of 24 neurons. The rectified linear unit is used as an activation function and Adam algorithm [130] is adopted for gradient-based optimization to update the network weights. Both actor and critic networks are assigned a learning rate of 0.001. The standard deviation for the Ornstein Uhlenbeck [128] is set to 5% of the action space range. The discount factor, $\gamma$, is set at 0.99, the smoothing factor, $\tau$, is set at 0.01, and the batch size is chosen as 64. The model is trained and tested using 100 days of extreme hot weather (33 days), in which average temperature is greater than 28°, extreme cold weather (33 days), in which average temperature is less than −10°, and the remaining represented non-extreme weather conditions in Michigan, USA, where average temperatures were between 0 and 15°, between 2018 to 2021. The extreme weather days are chosen as they are more prone to causing electrical congestion as consumers increasing their HP demand. 70% of randomly selected days were used for training, 30% were used for testing the model.

The case study is simulated using the reward function 7.4 proposed in Section 7.3. For each case, three different scenarios are considered:

- Case 1 (RL+): The actions, $A$, imposed by the RL agent are in the form of positive congestion tariff, $a_k \leq 0.01\$/kW$. Using tariffs, the consumers are discouraged from consuming electricity at times in which the congestion tariffs cause an increase in electricity price.
- Case 2 (RL-): The actions, $A$, imposed by the RL agent are in the form of negative congestion subsidies, $-0.01\$/kW \leq a_k$. Using subsidies, the consumers are encouraged to consume electricity at times in which the electricity cost is low.
- Case 3 (RL +/-): The actions, $A$, imposed by the RL agent are a combination of positive congestion tariffs and negative subsidies, $a_k$. This scheme changes the electricity price based on consumer demand maximizing the utilization of the feeder.

The reward function (7.4) was used to implement three different scenarios, adopting tariffs and/or subsidies, to alleviate congestion in the network. Each training episode is deemed successful if congestion is cleared within 3 steps else the environment is reset. As illustrated in Figure 7.5, the reward obtained for training the combined tariff and subsidy action space model (RL+/-) is initially low as the RL model decides actions randomly

for collecting the samples needed for the experience buffer. Reward then improves as the training continues until the reward function converges for 100 continuous episodes to its maximum and the average steps needed in a loop is 1.

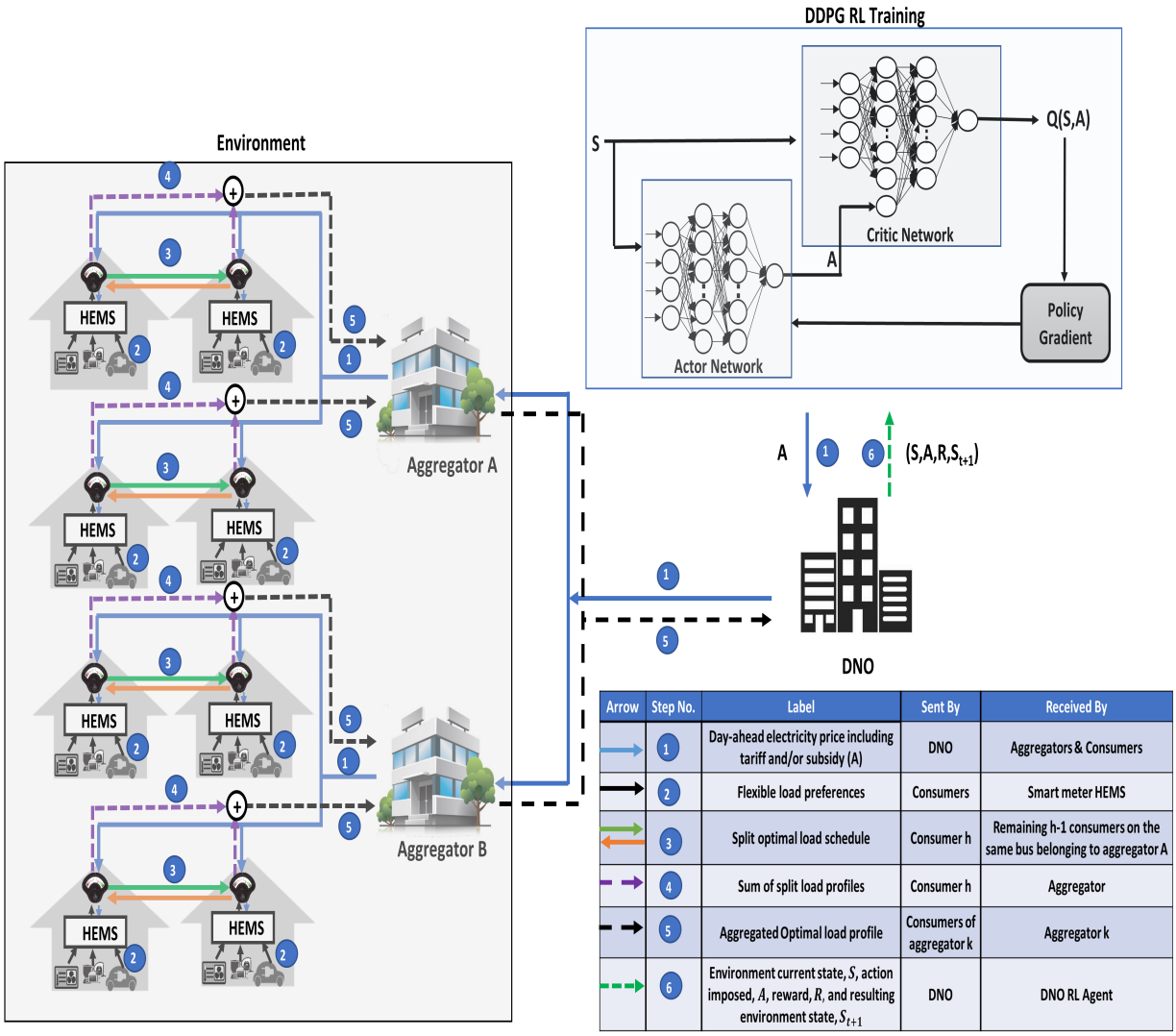
### 7.4.4 Testing Performance

Figure 7.6 illustrates the results obtained for total system electricity cost and PAR for power flowing in the main feeders after testing three different agents trained according to tariff-based action (RL+), subsidy-based action (RL-), or a combination of both (RL+/-). Figure 7.6 also illustrates the results obtained on using the DDT congestion management scheme on the same testing cases. The DDT congestion management scheme aims to minimize electricity costs for the consumer. Hence, the DDT scheme resulted in a lower mean system electricity cost compared to the positive congestion tariff (RL+) case. The RL+ model does not only aim to minimize system costs but also aims to flatten the load curve increasing the utilization of the feeder (7.4). This results in higher electricity costs by 3.7% and lower PAR compared to the DDT scheme. In the subsidy action space, as consumers are paid for not consuming at peak times, the trained RL- model resulted in lower electricity costs. Hence, the reward function encouraged higher subsidies to be imposed to obtain higher rewards compared to having lower subsidies imposed but flattening the load curve. Hence, as illustrated in Figure 7.6(b), the mean PAR of RL- is observed to be worse than that of RL+ by 2.67%. The best results in terms of electricity cost are observed when both congestion tariffs and subsidies are enabled. Combining both action spaces resulted in the reward function being maximum while minimizing electricity costs for the consumer and lowering the PAR of the load curves. Hence, the total mean electricity cost paid by the consumers is lower in the RL+/- case by 6.7% compared to the DDT case scenario. Moreover, the mean PAR has improved by 3.2% indicating an improved utilization of the feeder. Moreover, to reach this result, the DDT congestion management scheme required an average of 7 iterations between the DNO and the aggregators. The RL models, however, returned the result in only one step.

As the combined tariff and subsidy action space model (RL+/-) demonstrated better performance, the reward obtained while training the model, the resulting power flowing in the system's main feeder, and the corresponding electricity cost are analyzed. Figure 7.5 illustrates the reward obtained for training the congestion management model. As observed, when the mean reward of 100 training episodes reaches the maximum the model has converged and training stops. Figure 7.7 illustrates the power flowing in the main feeder for a test case in the absence of a congestion management scheme versus using the proposed model or the DDT scheme. In the absence of congestion management, the main feeder of the IEEE 33 bus system is congested at time $t = 22$ by 0.16kW above its capacity

limit. This happens, as discussed earlier, as a result of low electricity prices encouraging more EV residential charging and HP usage. Although the DDT congestion management scheme only resulted in an increase in tariff only at the congested time, the utilization of the feeder did not improve. On utilizing the trained RL model, a subsidy/tariff is added to the price curve to flatten the load curve, as illustrated in Figure 7.8. Power flowing in the main feeder is observed to be below the congestion limits and has an improved mean PAR of 1.27 compared to that of the DDT scheme (1.32). Hence, although the DDT scheme does alleviate congestion, the feeder's capacity utilization is not improved. Moreover, the total electricity consumption is lower using the proposed RL model. This is again observed to be the case irrespective of the actions imposed being tariff-based and/or subsidy-based proving the superiority of the proposed scheme.

Figure 7.9 illustrates a box plot of the results obtained of the AC power flowing in the IEEE 33 bus system main feeder for the test cases. As observed, the interquartile range of the power flowing in the feeder is the largest for the times in which the electricity price is lower and the line is not congested (times $t = 1$ to 6, 15, 20 and 23 to 24). As a result, the model encourages the consumption of electricity during times when the network is not congested and electricity prices are low. On the other hand, the interquartile range at peak time is the minimum as the model is attempting to alleviate the congestion at that time.




| Arrow | Step No. | Label | Sent By | Received By |
|---|---|---|---|---|
| | 1 | Day-ahead electricity price including tariff and/or subsidy (A) | DNO | Aggregators & Consumers |
| | 2 | Flexible load preferences | Consumers | Smart meter HEMS |
| | 3 | Split optimal load schedule | Consumer h | Remaining h-1 consumers on the same bus belonging to aggregator A |
| | 4 | Sum of split load profiles | Consumer h | Aggregator |
| | 5 | Aggregated Optimal load profile | Consumers of aggregator k | Aggregator k |
| | 6 | Environment current state, $S$, action imposed, $A$, reward, $R$, and resulting environment state, $S_{t+1}$ | DNO | DNO RL Agent |

Figure 7.1: Congestion Management in the Distribution Network using Reinforcement Learning

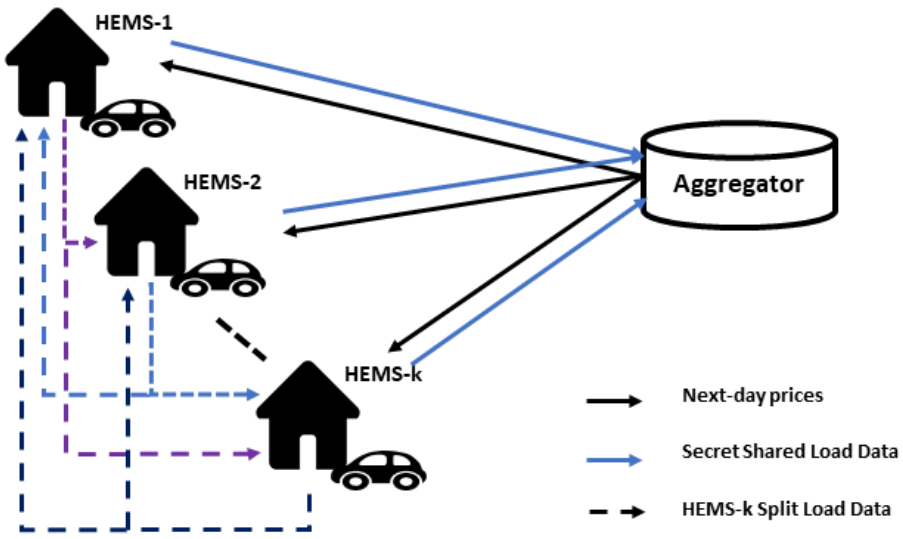



Figure 7.2: Consumer Load Scheduling and Additive Secret Sharing Aggregation

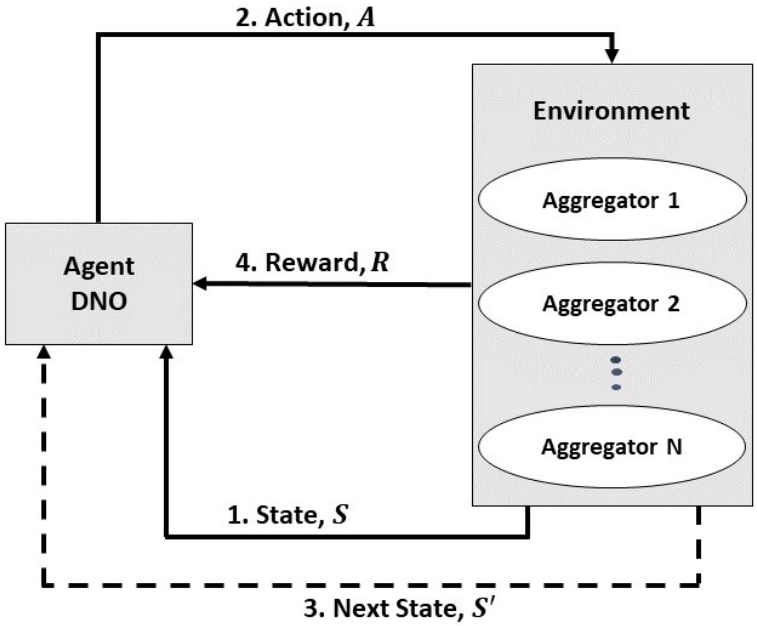



Figure 7.3: Reinforcement Learning Network Model

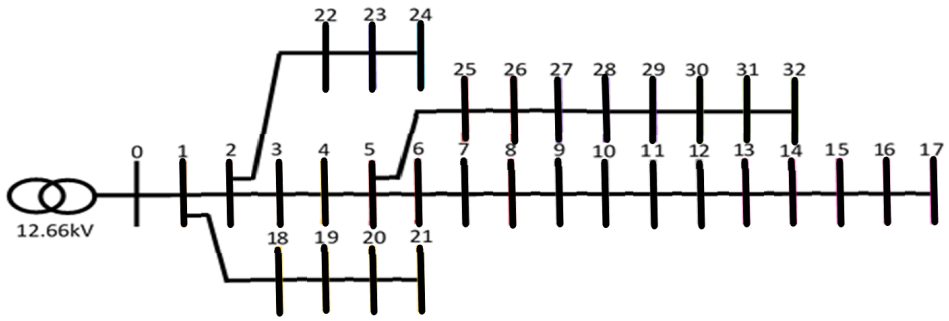



Figure 7.4: IEEE 33 bus system [1]

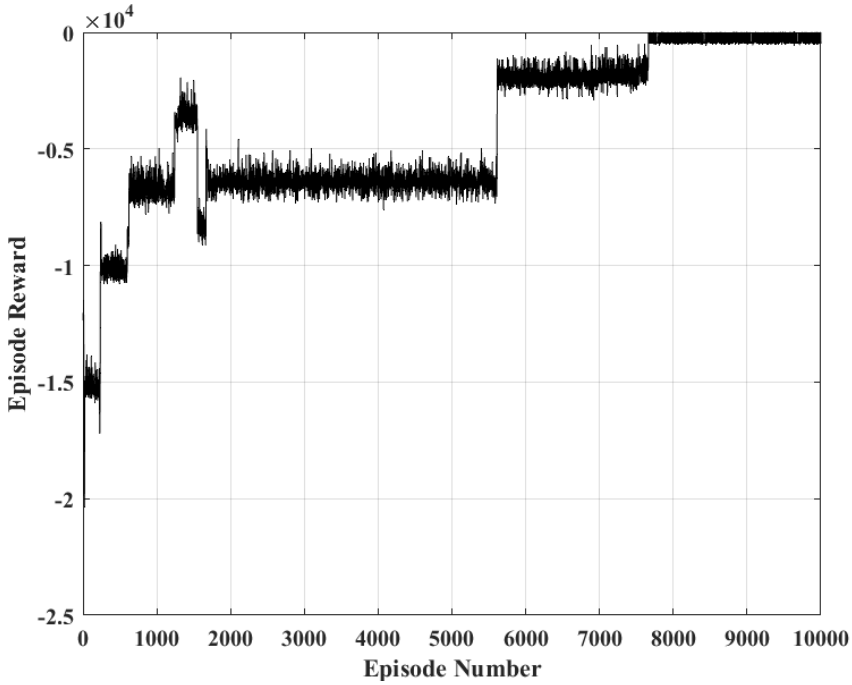
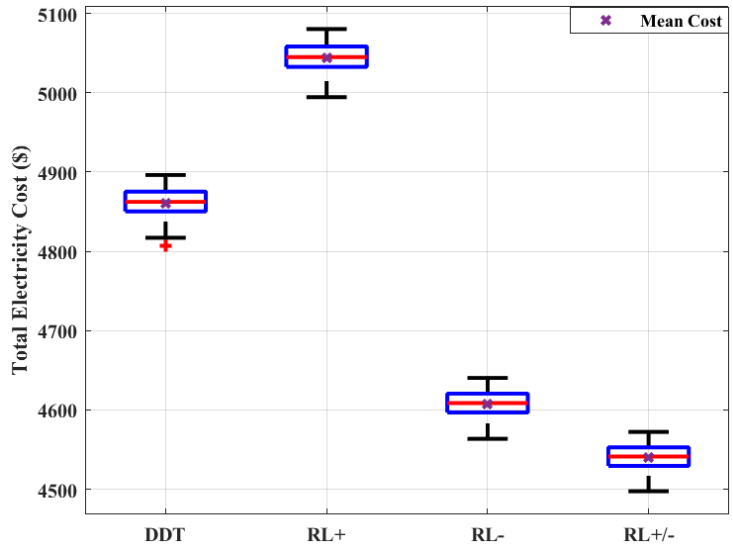
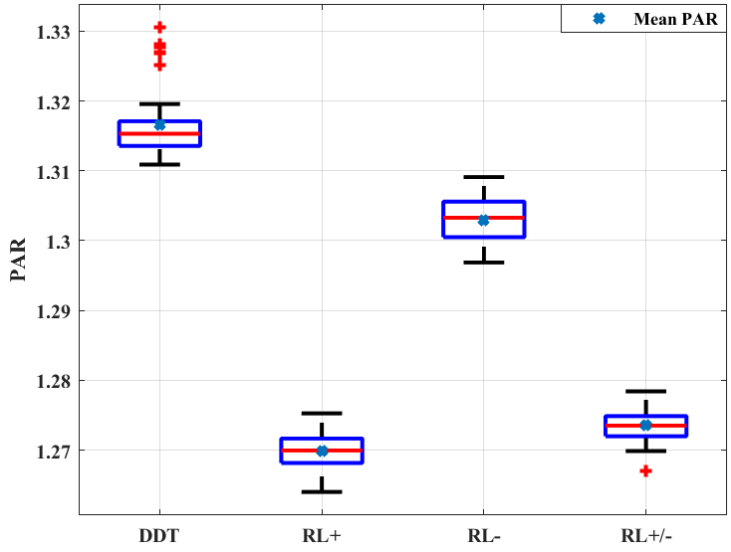



Figure 7.5: Episode Reward on Training RL+/- Agent using the combined tariff and subsidy action space




(a)




(b)

Figure 7.6: Comparison of proposed congestion management scheme with existing DDT scheme in terms of (a) Electricity Cost, and (b) Peak-to-Average Ratio

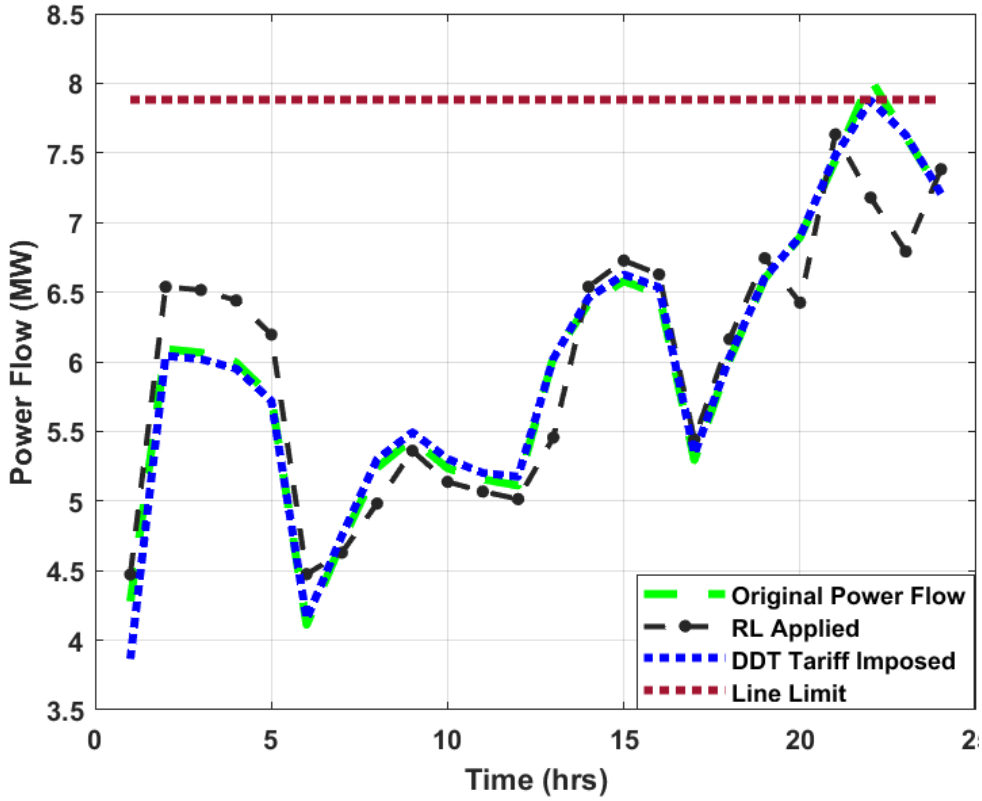



Figure 7.7: Comparison of power flow without any congestion management versus implementing the proposed RL+/- model or the DDT scheme

## 7.5 Conclusions

From the consumers' perspective, minimization of their electricity costs without sacrificing their consumption preferences is important. Utilizing DSM, the smart grid helps in achieving this objective. On the other hand, minimization of PAR of the load curve is a major concern of the utility as when the demand is higher, extra electric plants need to be deployed to generate more energy. Generally, these extra power plants are costly. Hence, minimization of the peak demand results in a reduction in the utility capital cost.

The problem of congestion management in the distribution network requires deciding on an appropriate tariff in an uncertain environment that would resolve the congestion.

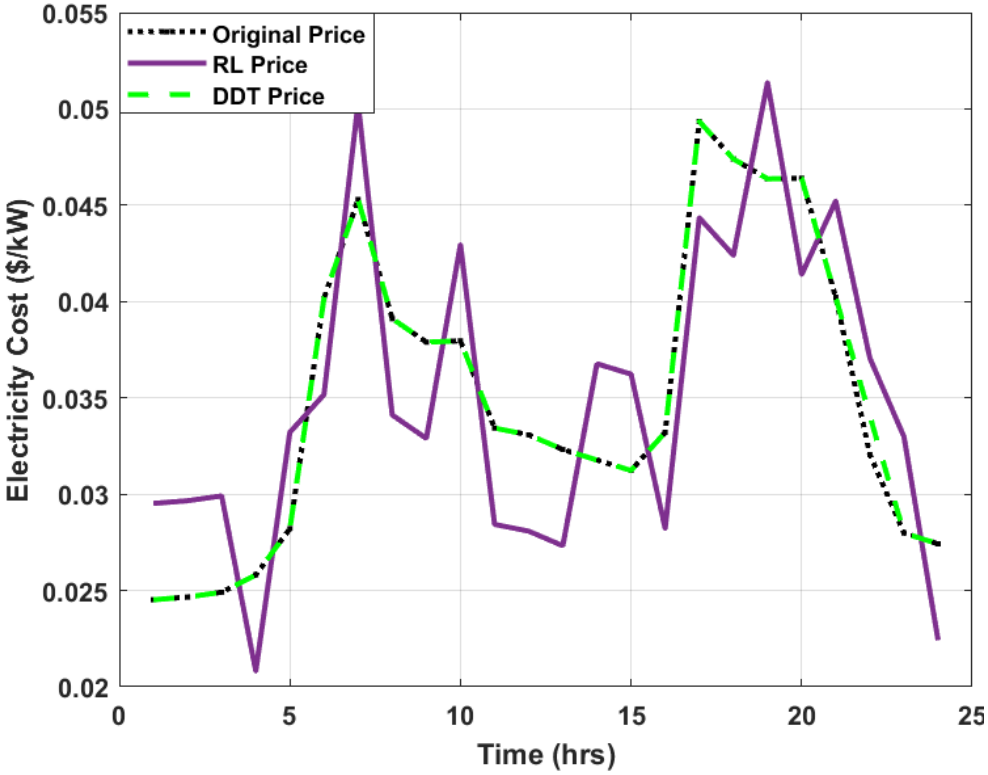



Figure 7.8: Comparison of electricity prices without any congestion management versus implementing the proposed RL+/- model or the DDT scheme

Hence, in this chapter, the DDPG RL is utilized as a model-free technique that does not need require explicit probabilistic models of the flexible loads in the distribution network to determine the required tariff that would alleviate congestion in the distribution network. The RL agent is trained off-policy and utilized by the utility to determine the congestion tariff and/or subsidy in one step. Moreover, as the proposed model aims to improve the PAR of the power flow, the overall electricity cost determined was lower by 6.7% compared to the DDT scheme when using both tariffs and subsidies, and lower by 5.2% when using subsidies only in the adopted IEEE 33 bus system case study. The PAR of the main feeder also was observed to be lower by 2.2%, 0.4%, and 1.14% respectively when using tariffs only, subsidies only, and the combination of both tariffs and subsidies respectively. The utilization of the main feeder's capacity of the IEEE 33 is hence improved using the proposed scheme. Thus, the RL congestion management scheme is not only cost-effective for consumers in terms of electricity, but is also cost-effective for utilities, as the utility

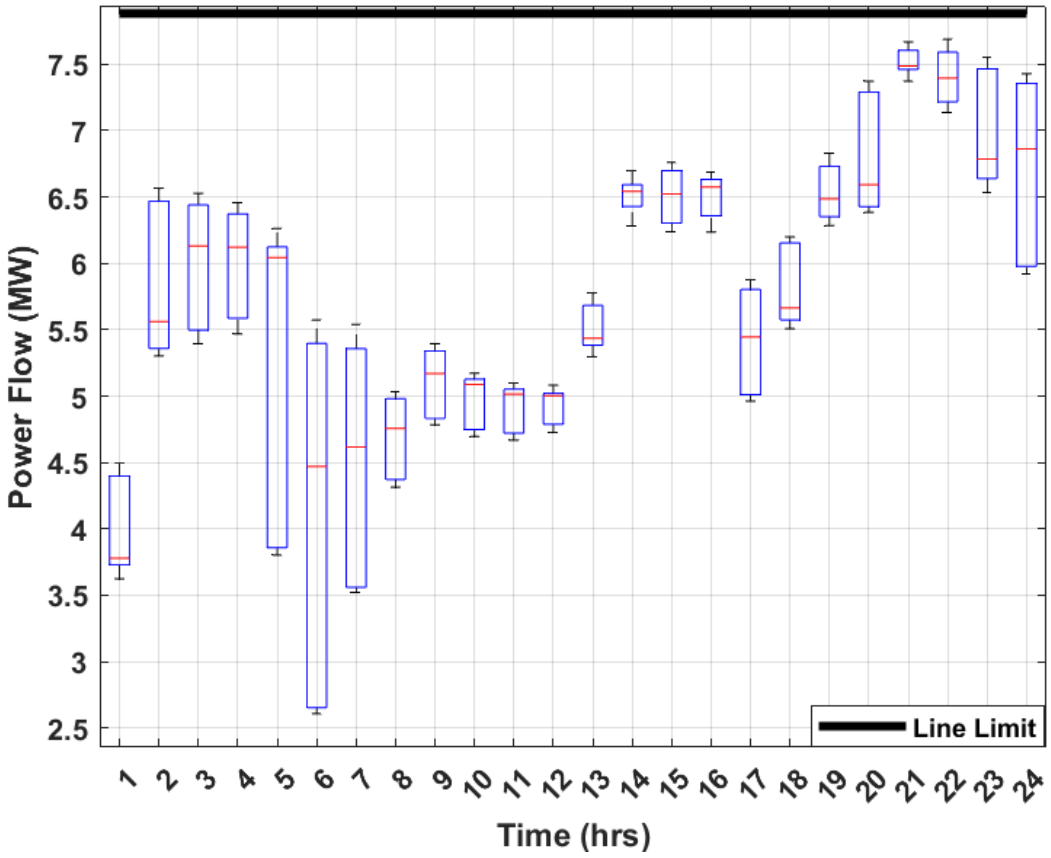



Figure 7.9: Boxplot of the power flowing in the main feeder on testing the trained RL+/- model

capital costs are reduced by alleviating the congestion in the network and flattening the curve.

[1]

[1]This chapter has been published in: Gul M Khan, O., Youssef, A., Salama, M. and El Saadany, E. *Congestion Management in Distribution Networks using Reinforcement Learning.* IEEE Systems Journal, 2022 (Article Submitted on 29th July 2022).

# Chapter 8

# A Cyber-Secure Congestion-Aware Charging Station Assignment for EVs

## 8.1 Introduction

The proliferation of high-demand controllable loads, such as Electric Vehicles (EVs) and Heat Pumps (HPs), is promising for mitigating emission of carbon dioxide in our environments. However, this increased usage of such heavy loads is constantly changing the electricity demand profiles of consumers and creating serious operational challenges for Distribution Network Operators (DNOs) [80]. The high demand of consumers coupled with the uncoordinated operation of heavy flexible loads can cause overloading of the distribution network electricity lines. Network overload can result in impacting voltage stability, reducing power reserve margins, and grid reliability [62]. Hence, resolving distribution grid congestion is considered one of the main duties of the network operator.

As the investment in upgrading the current network infrastructure is costly, researchers have studied how to utilize the flexibility provided by controllable loads in managing congestions in the network. Several studies have proposed methods where consumers forward their flexible load schedules through their aggregators to the utility operator, who modifies the cost of electricity to be proportional to the congestion in the network, motivating consumers to shift their loads from peak to off-peak times. Hence, existing congestion in the day-ahead market is alleviated. Proposed techniques include Distribution Locational Marginal Price (DLMP) [116], Dynamic Tariff (DT) [24], Distributed Dynamic Tariff (DDT) [26], and Dynamic Power Tariff (DPT) [117]. However, all of these techniques

only consider residential level EV charging and schedule consumers loads in the day-ahead market; i.e., they do not consider its impact in real-time.

Researchers have also studied controlling EV charging to manage congestion and guarantee queuing stability, i.e., preventing EV queues from growing indefinitely. Dubey et al. [62], proposed a controlled EV charging schedule in the day-ahead market that aims to improve the voltage quality. The study was restricted to residential charging stations charging within a 12-hour window. No other flexible loads were taken into consideration in the study. In [131], a user-oriented EV assignment algorithm based on the Lyapunov optimization method [132] was proposed to serve a dynamic population of EVs in real-time. In [133], queuing theory combined with Q-learning was adopted for scheduling EVs at Fast Charging Stations (FCSs) to minimize traffic congestion. Similarly, to overcome traffic congestion and reduce EV charging costs, a price incentive-based charging navigation strategy for EVs was proposed in [134]. An event-driven queue model based on discrete event simulation was employed to reflect the charging queue, and manage its related uncertainty. A charging pricing strategy combined with a reservation opportunity cost mechanism encouraged EVs to head to charging stations with lower utilization rates. However, [131], [133], and [134] did not couple the distribution network with the EV assignment problem.

Existing studies had focused either on distribution network congestion or traffic congestion. Studies focusing on both power and transportation congestion are limited. For example, as EVs charging stations couple the transportation and the distribution network, optimal planning of fast charging stations are proposed in [135]- [136]. In [135], a mixed integer linear programming model was developed to determine the location of FCSs such that investment costs are minimized considering the transportation and distribution network constraints. Similarly, in [136], a mixed integer linear problem was modeled minimizing social costs of installation of FCSs are minimized given the transmission network, distribution network, and operation constraints. On the other hand, in [137], the decision-making of a large population of EVs and combustion engines was studied such that their daily travel plan was optimally chosen to minimize charging costs and trip time. The decision-making of EV owners considered traffic congestion as well as power grid congestion. However, queuing time was not considered, and instead was based on the shortest path to the charging station. Xiong et al. [138] developed a simulation platform that models both the transportation and the distribution systems. The model aims to improve the system's stability and efficiency given the various EV charging schemes available, such as controlled charging, price-based charging, or deterministic charging. However, the built framework is not responsible for assigning EVs to charge stations given the state of the transportation and distribution networks. In [139], a peak load management model is proposed to minimize peak loads as a result of EV charging. If an EV owner does not plan on

going on a trip, the batteries are discharged to the grid. This results in decreasing peak load. A charging station selection model is then developed to assign EVs based on minimizing the distance traveled and queuing time. However, the work does not consider the stability of the queuing system. Moreover, it only focuses on the impact of EVs and does not consider the impact of other flexible loads on causing or mitigating grid congestion. In [140], controllable loads in a commercial building and the charging of an EV fleet are jointly scheduled. A decentralized framework was adopted based on an adaptation of the Dantzig-Wolfe decomposition [141]. However, the work does not model EV assignment to charging stations and does not consider the queuing time nor the impact of traffic congestion. Aravinthan et. al [142] proposed a two-step methodology for coordinating the charging of EVs to avoid congestion of the electrical network. In the first stage, day-ahead requests for charging are prioritized and the number of EVs to be charged per hour is optimized. The second stage determines the next hour's maximum number of EVs that can be charged based on network conditions. However, the study focuses on the maximum number of EVs that could be charged and not the charging schedule or assignment of each EV. Moreover, it does not consider traffic congestion nor does it study the impact of other residential loads on network congestion.

It is important to remember that EV assignment cannot be realized without a wireless communication network that enables EVs to send their charging requests and to receive the assignment decision from the controller. However, a wireless communication network will make the power network vulnerable to various cyber-security attacks [81]. The US Department of Transportation specifies gaps in the interdependency environment between the electrical grid and the transportation network due to the lack of cyber security standards [143]. Moreover, the weakness of the EV supply equipment (EVSE) cybersecurity was identified in [144] as its major barrier to EV adoption. In [145], a comprehensive review of the cyber vulnerabilities of the EV charging system was executed and the potential attack vectors and attack surfaces were identified. Similarly, in [146], Ahmed et al. study the exploitation of EV charging technologies to cyber attacks that could compromise the transportation network and the energy management system through data injection. Jeong et al. [147] proposed a novel cyber attack on EVCSs that manipulates EV user data to result in erroneous electricity costs when charging. A mixed integer linear program was developed to study the impact of such an attack on total consumer electricity cost, EV charging schedule, and state of charge of EVs. In [148], a cyber attacker manipulating EVs and their charging to cause frequency instability in the power grid was studied. Moreover, based on [149], charging station infrastructures are open to potential cyber attacks as they are unmanned and located in remote areas occasionally. On the other hand, [150] and [151] demonstrated that an ?? botnet of high-wattage devices provides attackers the ability to

manipulate the demand on the grid resulting in power outages and/or blackouts. Hence, the cyber vulnerabilities of EV assignment models need to be addressed, otherwise it would pose significant threats both to the transportation and electrical networks.

In this chapter, an efficient EV assignment model is proposed to appoint EVs to charge stations minimizing queuing time and managing congestion in the electrical network. The contributions of this chapter can be summarized as follows: (a) Given the day-ahead residential load, a computationally efficient real time algorithm is developed to assign EVs to charging stations such that queuing is stable, while congestion of the distribution network, distance traveled to the charging station, and queuing time are all minimized. Contrary to static vehicle routing in which charging requests and locations are provided to the charging station operator in advance, EV charging requests in this chapter are dynamic, i.e., demands to vary with time [152]. (b) Study the vulnerability of the proposed model to a False Data Injection Attack (FDIA) and propose an intrusion detection technique that adopts existing data in the transportation network.

The rest of the chapter is organized as follows: Section 8.2 describes the system model. In Section 8.3, the research problem is formulated, followed by the methodology proposed to solve it in Section 8.4. In Section 8.5 the cyber vulnerabilities of the proposed framework, and the impact of FDIA on the distribution and transportation network is studied followed by the development of an intrusion detection technique. A numerical study demonstrating the effectiveness of the proposed EV assignment and intrusion detection models are presented in Section 8.6. Finally, the chapter is concluded in Section 8.7.

## 8.2 System Model

We consider a distribution network that serves residential consumers, having both flexible and non-flexible loads, and a transportation network consisting of commercial EV FCSs.

### 8.2.1 Distribution Network

We assume a radial distribution network composed of a set of $N_B$ buses, $\mathcal{B} = \{b_1 \ldots, b_{N_B}\}$, and a set of $N_E$ branches, $\mathcal{E} = \{e_1 \ldots, e_{N_E}\}$. The network is powered up only through bus $b_1$ representing the point of attachment of the network to the main grid. All network buses are constrained with a minimum voltage requirement, $\check{V}$, and all branches are constrained with maximum active power flow limits, $\hat{P}(e)$.

Each bus, $b \in \mathcal{B}$, serves a set of consumers' houses, $\mathcal{H}(b)$. Each house, $h$, has two categories of loads: 1) non-flexible loads, and 2) flexible loads. Non-flexible appliances' demand is non-controllable and hence are non-shiftable, i.e., they do not respond to changes in electricity price. In this chapter, the only flexible loads assumed in house, $h$, are HPs and EVs. A HP follows a simple equivalent thermal parameter (ETP) model [153], where the controlled temperature evolves as

$$\theta(h,t) = \theta_a(t) + P^{HP}(h,t)R^{th}(h) - (\theta_a(t) + P^{HP}(h,t)R^{th}(h) - \theta(h,0))e^{\frac{-t}{R^{th}(h)C^{th}(h)}}, \quad \forall h \in \mathcal{H}(b), \forall t \in \mathcal{T} \tag{8.1}$$

where $\theta(h,t)$ and $\theta_a(t)$ are the internal temperature of the house, $h$, that is to be controlled and ambient temperature at time, $t$, respectively. $R^{th}(h)$ and $C^{th}(h)$ are two fixed parameters, representing the thermal resistance and the thermal capacitance of the house, $h$, respectively. Moreover, $P^{HP}(h,t)$ represents the power consumption of the HP at house, $h$, at time instant, $t$. It should be noted that the system model considers a time horizon of $\mathcal{T} = \{1 \ldots, N_T\}$. To achieve consumer convenience, the controlled indoor temperature, $\theta(h,t)$, should be kept within the band

$$\check{\theta}(h) \leqslant \theta(h,t) \leqslant \hat{\theta}(h) \tag{8.2}$$

where $\check{\theta}(h)$ and $\hat{\theta}(h)$ represent the minimum and maximum temperatures beyond which the operation of the HP becomes inconvenient for the consumer living in house $h$.

As for the residential EV chargers, the amount of energy, $E^{CH}(h,t)$, needed to recharge an EV battery of size, $B^{EV}(h)$, and efficiency, $\eta$, can be deduced from its initial state-of-charge, $SoC(h,0)$. An EV can be charged using the residential level 2 charger based on its availability, $a(h,t)$, as follows

$$E^{CH}(h,t) = \begin{cases} C(h,t)B^{EV}(h) + SoC(h,0)B^{EV}(h), \\ \qquad\qquad\qquad\qquad \text{for } t = 1 \\ C(h,t)B^{EV}(h) + E^{CH}(h,t-1), \text{for } t > 1 \end{cases} \tag{8.3}$$

$$\sum_{t}^{\mathcal{T}} C(h,t) = SoC^{req}(h) \tag{8.4}$$

$$P^{EV}(h,t) = a(h,t)C(h,t)\frac{B^{EV}(h)}{\eta} \tag{8.5}$$

where $P^{EV}(h,t)$ is the EV power needed by EV $h$ at time $t$, and $C(h,t)$ is the amount of charge of EV $h$ at time, $t$, expressed as a percentage. $SoC^{req}(h)$ is the required ?? for the $h^{th}$ EV, determined as $1 - SoC(h,0)$, and $\eta$ is the efficiency of the battery [11].

### 8.2.2 Transportation Network

The transportation network is assumed to consist of a commercial fast charging infrastructure composed of a finite set of $N_c$ charging stations, where $\mathcal{S} = \{s_1, \ldots, s_{N_c}\}$. An EV FCS, $s_i$, is characterized by two parameters: the bus that serves it, $b_i$, and the number of chargers, $Z(s_i)$, in the station. All chargers are assumed to have the same power rating. As a consequence, the time needed to charge an EV's battery is independent of the assigned station. It is assumed that the infrastructure serves EVs within a bounded geographical area. However, the served EV does not need to belong to one of the residential consumers. Hence, we assume that the commercial FCS demand is independent of home EV charging demand. Each EV is equipped with a wireless transceiver which enables two-way communication with a central controller, referred to as a Mobility Service Provider (MSP) [154]. Whenever users need to recharge their EV batteries, a charging request is sent to their MSP which will direct the user toward the appropriate FCS, as illustrated in Figure 8.1. EV owners choice of FCS depends on their need for charging, availability of the charger, convenience in reaching the charging station, and cost of usage. The EV assignment model proposed in this chapter considers all these factors in its formulation. Hence, it is assumed that the EVs follow their MSP's charging station assignment. The system is monitored by the MSP and assignment decisions are made dynamically. The controller does not know (or predict) when and where the charging requests will occur. From the MSP's point of view, the only information known in advance is related to the charging infrastructure, while requests' temporal and spatial arrival follow some general stochastic process. Moreover, the proposed system is modeled such that each charging request must be fulfilled: no request can be denied by the MSP.

## 8.3 Problem formulation

To formulate the congestion management problem mathematically, an objective function, $C(\mathcal{P}^{\mathcal{E}}(e,t))$, should be explicitly defined reflecting the amount of congestion in all distribution network branches at time instant, $t$. Let $\mathcal{P}^{\mathcal{E}} = \{P^{\mathcal{E}}(e,t), e \in \mathcal{E}\}$ denote the

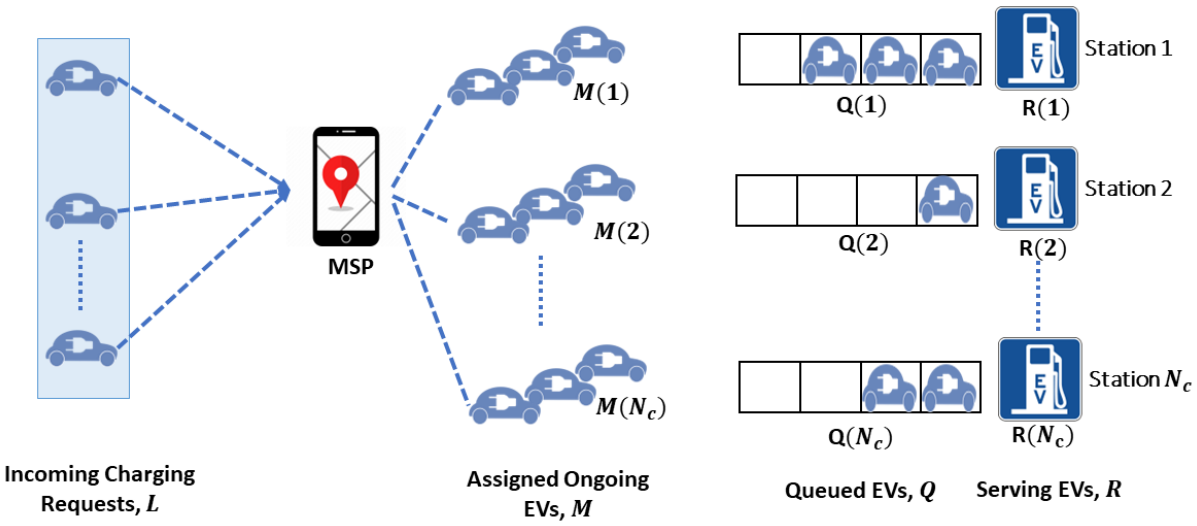



Figure 8.1: Proposed EV queuing model

active power carried in each branch. Hence, the objective function is defined as,

$$C(\mathcal{P}^{\mathcal{E}}(e,t)) \triangleq -\sum_{e\in\mathcal{E}} \log\left[\frac{\hat{P}(e) - P^{\mathcal{E}}(e,t)}{\hat{P}(e)}\right], \forall t \in \mathcal{T} \tag{8.6}$$

Congestion function, $C(\mathcal{P}^{\mathcal{E}}(e,t))$, is observed to be zero in the absence of power flowing in the network branches, $\mathcal{E}$. As the active power flow, $P^{\mathcal{E}}(e,t)$, increases, the cost function, $C(\mathcal{P}^{\mathcal{E}}(e,t))$, increases in a convex fashion and approaches to infinity as the power flow, $P^{\mathcal{E}}(e,t)$, approaches its maximum allowable limit, $\hat{P}(e)$. Utilizing such a congestion function in any optimization algorithm will help in distributing power flows among the network branches.

As congestion is a function of power flowing in the network branches, $\mathcal{E}$, which is a function of consumer demand, power consumption of the flexible residential loads and the FCSs has to be efficiently controlled. Both loads are quite different. Consumption of flexible residential loads can be deferred to non-peak periods, as long as it meets the preferences of the consumers. Flexible residential loads can be scheduled in an offline manner in the day-ahead market based on weather forecasts and EV travel plans. On the contrary, the power consumption of the FCSs is controlled by the amount of EVs directed towards them. Power consumption over a specific time horizon can be shifted from FCS station $s_i$ to station, $s_j$ if EVs are directed from the former to the latter. Therefore,

EVs' assignment decisions are scheduled over space. The assignment of EVs to charging stations should be done within a relatively short period (a few seconds) to ensure EV owner satisfaction. Moreover, in this chapter, charging station loads cannot be scheduled offline as EV charging requests are assumed to be dynamic. Hence, EV charging stations do not have prior knowledge of when their service will be requested. Therefore, EVs' assignments should be decided in real-time and cannot be planned.

The constraints for efficiently controlling the power consumption of residential loads and FCS can be summarized as follows: 1) internal house temperature, $\theta(h,t)$, must remain within the user-specified deadband (8.2), 2) the desired residential EVs' charging requirement, $SoC(req,h)$, must be met during its availability, $a(h,t)$ (8.3-8.5), 3) the active power flow, $P^{\mathcal{E}}(e,t)$, in each network branch should not exceed the branch's maximum limit, $\hat{P}(e)$, 4) bus voltage should not drop beyond the minimum limit, $\check{V}$, 5) the queuing process in each FCS must be stable. While the first four constraints are straightforward and have been considered in modeling the system in Section II, the last one needs further explanation.

Due to the finite number of chargers in each station, $Z(s_i)$, it is quite possible that not every EV can be served immediately and some may have to wait in a "queue" until one of the chargers becomes available. Following up on the work in [131], the proposed queuing model is depicted in Figure 8.1. Different variables of this model are described as follows: $\{R(s,t), s \in \mathcal{S}\}$ represents the number of EVs being served by each charging station, $s$, $\{Q(s,t), s \in \mathcal{S}\}$ represents the number of EVs queued at each station, $s$, waiting for its turn at the FCS, $\{M(s,t), s \in \mathcal{S}\}$ represents the number of EVs travelling towards FCS $s$ after being assigned to it, and $L(t)$ represents the number of EVs waiting to be assigned at time instant, $t$. The combination of $M(s,t)$, $Q(s,t)$, and $R(s,t)$ represent station's $s$ queuing state, $\phi_s(t)$. For a queuing system to be considered stable, queues cannot grow indefinitely [132]. Hence, to ensure stability, the time-average of the expected queues' lengths for all queues must be finite, which in turn implies that their weighted sum is also finite, as follows:

$$\lim_{N_T \to \infty} \frac{1}{N_T} \sum_{t=1}^{N_T} w^l L(t) \\ \left(\sum_{s \in \mathcal{S}} w_s \left(M(s,t) + Q(s,t) + R(s,t)\right)\right) < \infty \tag{8.7}$$

where the weights $\{w^l, w_s\}$ are positive real numbers signifying the impact of EVs waiting to be assigned and EVs already assigned respectively. A popular approach to test or achieve the stability of the proposed queuing system is to use *Lyapunov* function [132].

The key idea is to define a function, $U$, that maps the queuing state $\phi$, where $\phi \in \Phi$, into a non-negative real value, i.e. $U : \phi \rightarrow [0, \infty)$. If function $U$ satisfies the following inequality (Poisson's inequality):

$$\{U(\phi(t+1)) - U(\phi(t))\} \leqslant -|\phi(t)| + \bar{\eta}, \quad \forall \phi(t) \in \Phi, \tag{8.8}$$

where $|.|$ is the $\mathcal{L}^1$-norm and $\bar{\eta}$ is a finite constant, then the stability criterion in (8.7) is achieved and the system is stable. More specifically,

$$\begin{aligned} \lim_{N_T \rightarrow \infty} \frac{1}{N_T} \sum_{t=1}^{N_T} w^l L(t) + \\ \sum_{s \in \mathcal{S}} w_s (M(s,t) + Q(s,t) + R(s,t)) \leqslant \bar{\eta} \end{aligned} \tag{8.9}$$

The inequality in (8.9) implies that the expected queue lengths become bounded if condition (8.8) is satisfied.

The overall congestion management problem is then formulated as the following optimization problem:

$$\min \ \bar{c} \triangleq \sum_{t=1}^{\mathcal{T}} \left\{ - \sum_{e \in \mathcal{E}} \log \left[ \frac{\hat{P}(e) - P^E(e,t)}{\hat{P}(e)} \right] \right\} \tag{8.10a}$$

$$\text{s.t. } (8.1) - (8.5), (8.9) \tag{8.10b}$$

$$V(b,t) \geqslant \check{V}, \quad \forall b \in \mathcal{B}, \forall t \in \mathcal{T} \tag{8.10c}$$

$$P^E(e,t) \leqslant \hat{P}(e), \quad \forall e \in \mathcal{E}, \forall t \in \mathcal{T} \tag{8.10d}$$

$$P^L(b,t) = \sum_{h \in \mathcal{H}(b)} P^{EV}(h,t) + P^{HP}(h,t) + P^{nf}(h,t) \tag{8.10e}$$

$$\begin{aligned} &P^G(b,t) - P^L(b,t) = \\ &V(b,t) \sum_{\forall j \in \mathcal{B}} V(j,t)(G_{b,j} cos(\delta_{bj,t}) + B_{b,j} sin(\delta_{bj,t})) \end{aligned} \tag{8.10f}$$

$$\begin{aligned} &Q^G(b,t) - Q^L(b,t) = \\ &V(b,t) \sum_{\forall j \in \mathcal{B}} V(j,t)(G_{b,j} sin(\delta_{bj,t}) - B_{b,j} cos(\delta_{bj,t})) \end{aligned} \tag{8.10g}$$

where $V(b,t)$ is the voltage of bus $b$ at time instant $t$. Moreover, $\{P^G(b,t),\ Q^G(b,t)\}$ are the generated real and reactive power at bus $b$, $\{P^L(b,t),\ Q^L(b,t)\}$ are the load bus $b$ real and reactive power, $\{G_{b,j}, B_{b,j}\}$ are the conductance and susceptance of the $(b,j)$ element of the admittance matrix, and $\delta_{bj,t}$ is the difference in voltage angles of bus $b$ and $j$. Optimization constraints (8.10b) represents the consumers' flexible loads operation and preferences. Inequality constraints (8.8) and (8.10d) ensures that the bus voltage does not drop beyond its minimum limit and that the power flowing in the feeders does not exceed its thermal limits. Constraint (8.10e) determines the total load in each of the network buses, $N_{\mathcal{B}}$. Constraints (8.10f) and (8.10g) represents the AC power flow equations.

## 8.4 Solution methodology

Solving an optimization problem (8.10) is not an easy task. It involves two types of decisions that need to be taken: residential flexible load should be scheduled in the day-ahead market and EVs need to be assigned to charging stations in real-time. Scheduling residential demand takes place offline and has been studied in the literature [155–157]. Price-based quadratic optimization is adopted to schedule flexible loads over periods when the price of electricity is low [26]. This results in minimizing consumers' electricity costs. Assigning EVs to charge stations, however, is a more challenging task. It is difficult to predict in advance when an EV user will request access to a charging station, the number of charging requests in a specific period and its locations. Furthermore, to make an assignment decision the distance between the assigned station and the EV's location and how much grid congestion will result from the assignment decision (i.e. avoiding transportation network congestion) should also be considered.

Based on the aforementioned discussion, a solution methodology composed of three stages is developed to schedule residential flexible load and assign EVs to charge stations while avoiding grid congestion and minimizing queuing is developed. Initially, an offline day-ahead algorithm is executed to schedule the flexible residential loads. Given the schedule of residential flexible load, the congestion function (8.6), $C(\mathcal{P}^E(t))$, is now a function of real-time EV charging. Hence, the second stage is to approximate the congestion function, $C(\mathcal{P}^E(t))$, offline to become a linear combination of FCS EV serving state, $R(s)$, at each charging station, $s$. The third stage is to run an online algorithm based on Lyapunov optimization for assigning EVs to charge stations. The algorithm will help in ensuring queuing stability. Each of the three stages is discussed in more detail next.

### 8.4.1 Day-ahead Residential Load Scheduling

To schedule consumers' flexible loads, aggregators utilize quadratic optimization [26] [116]. The objective of the optimization is to minimize the electricity cost incurred by a consumer while meeting their comfort requirements as follows:

$$\min_{P^f(h,t)} \sum_{h,t} P^f(h,t)^T \beta P^f(h,t) + P^f(h,t) p_t \\ \text{s.t.}(8.1) - (8.5) \tag{8.11}$$

where $P^f(h,t)$ represents consumer $h$ flexible loads: $P^{EV}(h,t)$ and $P^{HP}(h,t)$ at time $t$. $\beta \in R^{N_T \times N_T}$ represents the price sensitivity coefficient matrix and $p_t$ represents the day-ahead electricity price. The aggregators forward their aggregated loads to the network operator who runs power flow analysis to ensure the absence of congestion in the distribution network lines. In the event of congestion, a tariff [26] is determined proportionally to the congestion of the lines. This tariff increases the electricity price at congestion times and the aggregators shift their consumers' schedules accordingly to non-peak times to minimize their costs.

### 8.4.2 Linear Regression

Using historical data, consumers' average flexible load schedule, $P^f(h)$, can be determined and is no longer an unknown variable. Congestion of the distribution network, $C(\mathcal{P}^E(e,t))$, hence, is now a function of real-time charging station serving states, $R(s,t)$. To determine the relationship between the congestion of the distribution network and the number of EVs being served at FCSs linear regression is utilized [158]. The congestion function, $C(R(s,t))$, is approximated as a linear combination of EV charging station serving states, $R(s,t)$. Historical data is utilized to determine average daily flexible residential loads. The only remaining unknown bus loads are the FCS demand. Hence, $K$ random sets of different FCSs serving states are simulated as a sampling grid and the resultant average congestion, $C(\bar{R}(s))$, is obtained. To model the relationship between congestion in the network and FCSs serving states, multidimensional linear regression is then utilized. The regression coefficients, $w^s$, are determined such that the mean squared error is minimized as follows:

$$\min \sum_{j=1}^{K} \left( C(\bar{R_j}(s)) - \sum_{s \in \mathcal{S}} w^s R_j(s) \right)^2 \tag{8.12}$$

### 8.4.3 Real-time EV Assignment Algorithm

On receiving an EV charging request, the proposed online EV assignment algorithm considers the following factors:

- The tradeoff between delay in assigning an EV to a FCS and queuing at the charging station is represented by weight $w^l$. If $w^l = 0$, then the time spent to assign an EV on receipt of the charging request is infinite, and queuing time at the charging station is minimized. On the other hand, if $w^l$ is set to infinity, then EVs are assigned immediately to charging stations causing an increase in queuing time. Hence, $w^l$ is inversely proportional to assignment delay time. As EV users expect fast response from the MSP on sending an EV charging request, $w^l$ is chosen such that the assignment delay time is only a couple of seconds.

- The length of the queue in terms of EVs ongoing to charging station $s$ represented by $M(s,t)$, EVs queued in that charging station, $Q(s,t)$, and EVs being charged, $R(s,t)$, are weighted by $w_s^m$, $w_s^q$, and $w_s^R$ respectively. The tradeoff parameters are equated to $w^s$ deduced in the linear regression stage as once an EV is assigned to a FCS $s$ then its queuing state is given equal importance.

- The time required for an EV to reach a given station, $d_{js}$, from its EV charging request location, $j$, also influences the EV assignment decision. To calculate $d_{js}$, the average speed of cars in each of the FCS zones and the distance between the EV and each FCS, $x_{js}$, are used. As demonstrated in [131], the expected waiting time from the time an EV charging request is sent to the time the EV charging is completed, $\bar{W}$, is bounded as

$$\bar{W} \leq \frac{1}{\lambda}[\bar{\eta} + w_d \bar{d_{js}} + w^r \zeta_s] \tag{8.13}$$

  where $\bar{d_{js}}$ represents the maximum expected traveling time, and $\zeta_s$ represents the sensitivity of the grid congestion to changes in the load. As weight $w^d$ increases, the waiting time increases but the EV is assigned to a nearer charging station requiring lower traveling time, $d_{js}$. Moreover, the mean traveling time performance $\bar{d}$ is related to the best stabilizable value, $\bar{d}^*$, using:

$$\bar{d} \leqslant \bar{d}^* + \frac{\bar{\eta}}{w^d} \tag{8.14}$$

  Hence, $w^d$ is inversely proportional to travelling time, $\bar{d}$.

- As the EV assignment problem is coupled with the electrical grid, the impact of adding EV charging load to the network has to be incorporated. The sensitivity of the congestion function (8.6) to changes in the load, $\zeta_s$, is obtained after day-ahead residential load scheduling and is scaled using $w^r$, which represents the importance of electrical grid congestion in EV assignment.

Algorithm 3 demonstrates the steps followed from the time an EV charging request is received by the MSP and its assignment to an EV charging station.

## 8.5 Cyber Security of the Proposed Real-time EV Charging Assignment to FDIA

The basic characteristics that define a cyber-secure system are represented by the CIA triad [159] which symbolizes confidentiality, integrity, and availability. Confidentiality ensures restricted access to sensitive information, while integrity confirms the authenticity of such private information. Finally, ensuring the availability of service guarantees authorized users access to the service as and when needed. The success of EV charging, hence, depends on the CIA of the EV assignment system which can threaten the reliability of the electrical grid if security vulnerabilities are not addressed. When needing to recharge, an EV user communicates with its MSP through a wireless mobile application to determine the nearest available charging station, $s$, as illustrated in Figure 8.2. A cyber attacker can compromise the MSP enabling access to an EV drivers' personal and vehicle information, assigning EV drivers to busy charging stations, or affecting the billing and payment of consumed electrical energy. In this chapter, the impact of a FDIA on the MSP on EV assignment is demonstrated and an intrusion detection technique is proposed.

**Algorithm 3** Dynamic assignment algorithm for EVs

**Input:**

- Weight, $w^l \in \mathbb{R}^+$, associated with $L$ number of EVs requesting charging and waiting to be assigned.
- Set of weights, $\{w^s, \forall s \in \mathcal{S}\}$, obtained from linear regression stage for $N_c$ charging stations.
- Weight, $w^d \in \mathbb{R}^+$, associated with EVs' traveling times to the $N_c$ charging stations.
- Maximum number of ongoing EVs, $\left\{\hat{M}(s), \forall s \in \mathcal{S}\right\}$.
- A maximum number of assigned EVs per time step, $\hat{x}$.

1. **for** $t \in \{0, 1, 2, \ldots\}$ **do**
   (a) Read the queuing state variables: $L(t), M(s,t), Q(s,t), R(s,t) \quad \forall s \in \mathcal{S}$.
   (b) Read the locations of $J$ waiting requests, where $J = \min\left(L(t), \hat{x}\right)$.
   (c) Set the time counter, $t_c(m)$, for the $m \in J$ new waiting requests to zero.
   (d) Determine the time needed to travel from charging request location to $N_c$ charging stations, $d_{js}, \forall j \in J$.
   (e) Sort $J$ in descending order based on time since EV charging request was sent, $t_c(j)$.
   (f) **for** $j \in \{1, \ldots, J\}$ **do**
      i. Calculate $g(s) := w^l L(t) - w^s \left[M(s,t) + Q(s,t) + R(s,t)\right] - w^d d_{js} - w^r \zeta_s, \quad \forall s \in \mathcal{S}$
      ii. **if** $\max_s g(s) \leqslant 0$ **then** Request charging request, $j$, to be deferred to the next time step. Update $t_c(J) = t_c(J) + t_s$ where $t_s$ is the time step.
      iii. **else** Assign charging request, $j$, to station $s^* = g(s)$

Utilizing any of these vulnerabilities can have devastating effects given the coupling of the

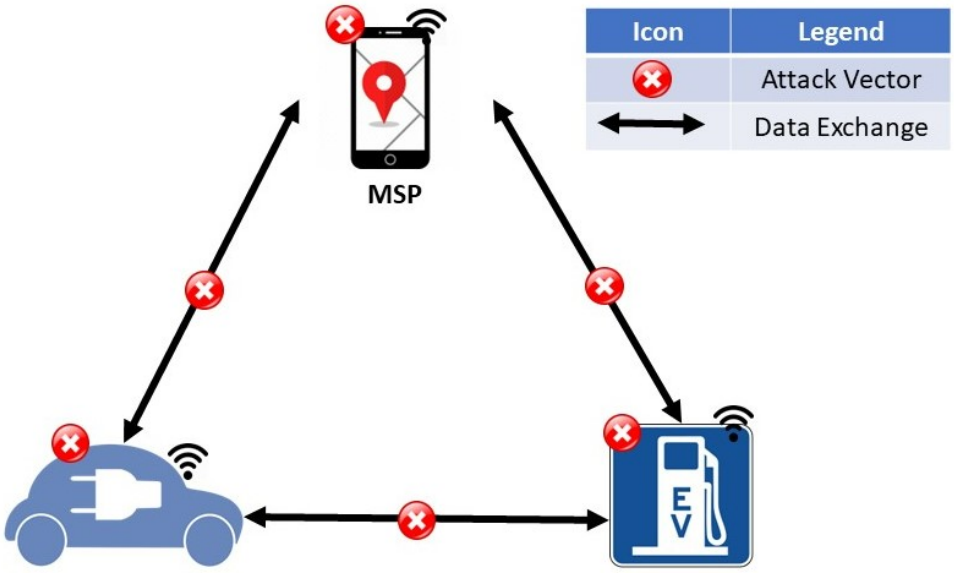



Figure 8.2: Cyber vulnerabilities in the EV charging process.

transportation and the distribution network. In this chapter, the impact of cyber attacking the MSP and implementing a FDIA such that the EVs are incorrectly assigned to cause long queues at the FCSs and user inconvenience is studied.

### 8.5.1 EV Assignment Model under FDIA

As the MSP is the central operator that connects EVs to charging stations, a cyber attacker compromising the EV assignment decision of the MSP can result in directing EVs to incorrect charging stations. This would cause long queues at FCS impacting EV owners' quality of driving. EV owners are inconvenienced as they would need to queue longer to get charged if their EV battery ?? cannot take them to another charging station or would need to travel more distance to reach an alternative charging station.

The cyber attacker utilizes the historical data it has acquired through eavesdropping on the distribution network to determine the most sensitive electrical bus to changes in the load. The attacker injects false information in the MSP to assign EVs to the corresponding charging station, $s_a$, that is located on that bus. This would result in all EVs being redirected to one charging station, resulting in long waiting queues.

### 8.5.2 Cyber Attack Intrusion Detection

The transportation network relies on sensors to determine the volume of traffic in real-time through its on-site sensors that are connected to the local controller unit (LCU). The LCU operates the traffic displays and is wirelessly connected to the Traffic Management Center (TMC) that manages real-time traffic, stores controller data, and modifies traffic display timings [160]. Moreover, smart parking systems based on the Internet of Things are being developed consisting of sensors, communication, and application layer and are implemented [161, 162]. Hence, existing transportation network resources can be utilized to alert the MSP in the event of an FDIA.

As illustrated in Figure 8.3, sensors can be deployed at the entrance and exit of the charging station to determine the number of electric vehicles present in the station. The three most common types of sensors adopted are radar sensors, wireless ultrasonic sensors, and wireless magnetometer sensors. These sensors differ in their installation, the way vehicles are identified, and their performance in extreme weather conditions. The information obtained through the installed sensors at all charging stations is communicated wirelessly with the LCU through various access points. The local controller unit evaluates the received information and in the event that a certain charging station has more than $\Gamma_s$ percent of EVs compared to other charging stations an alert is raised. The alarm is communicated to the network operators who would then investigate the possibility of an attack. The second level of cyber intrusion detection is the installation of CCTV cameras that broadcast the live streaming of the entrance and exit of charging stations. In the event that an MSP operator observes a difference in the number of EVs queued an alert is raised.

## 8.6 Case Study and Results

The IEEE 33 bus system [1], illustrated in Figure 8.4, is adopted as a distribution network case study in this chapter. Each of the 32 load buses is assumed to supply power to 10 houses. The houses were assumed to be single-story houses of an average height of 8ft and their house areas were randomly chosen between 1500 to 2500 sq. ft. The default loading of the IEEE 33 bus system represents the non-flexible base load profiles, $P^{nf}(h)$, of the load buses. Each house, $h$, has a level-2 EV charger of 6 kW and an HP power rating of 5 kW. In addition, determining the hosting capacity of the network, the distribution network is modeled to supply power to $N_c = 4$ commercial FCSs located at load buses $b_2, b_3, b_{18}$, and $b_{33}$. Each station is equipped with 12, 12, 5, and 7 level-3 chargers of 80

kW power rating respectively. The $N_c$ stations are assumed to be located in the corners of a square of 10 km length. The average speed of an EV is assumed to be 50 km/hr and its battery capacity is $B^{EV}(h) = 50$ kWh. The initial charge, $SoC(h, 0)$, of the EVs is assumed to be uniformly distributed across $[0, 50]$ kWh. The arrival of charging requests is assumed to follow a Poisson distribution with parameter $\lambda = 2$ requests/minute. The charging request source locations are randomized to be uniformly distributed in the interval [0,10]. GAMS [86] and MATLAB R2021a were used for simulating the model.

Using randomly generated data, assignment delay weight, $w^l$, is varied between 0 and 1 as illustrated in Figure 8.5 and the delay in the assignment is measured for various $w^d$. As observed, as $w^l$ increases, assignment delay decreases. (8.13) demonstrates that system time (which includes assignment delay time) is proportional to $w^d$. Hence, as $w^d$ increases, assignment delay time increases as illustrated in Figure 8.5. Setting the maximum acceptable assignment delay time to 5 seconds, the shaded area represents the possible choices of trade off parameters $w^l$ and $w^d$. Thus, a $w^d$ larger than 0.1 and a $w^l$ lower than 0.5 does not satisfy the assignment delay constraint. Moreover, as congestion impacts the entire grid, $w^r$ is given equal weight as $w^l$ and is expected to be larger than $w^d$. Figure 8.6 illustrates the impact of varying $w^d$ and $w^l$ on travelling time. As observed, traveling time is inversely proportional to $w^d$. Hence, the least travelling time is given by $w^d = 0.1$, and a $w^l = 0.95$. These weights are used for the remaining analysis of the proposed EV assignment framework.

### 8.6.1 Performance Comparison

The performance of the proposed methodology is compared to the scenario in which the scheduling of flexible loads is not controlled, i.e. absence of demand response (DR). Under the latter, residential owners maintain internal house temperatures at a certain level and charge their EVs at their own convenient time when electricity prices are low. Moreover, real-time EV users are assumed to head towards the nearest charging station (NCS) from their current locations. Hence, the comparison case is referred to as *NCS* when evaluating the results.

### 8.6.2 Results and Performance evaluation

For $\lambda = 2$ charging requests/minute, the power flowing in the main feeder, $P_t^{f_1}$, of the IEEE 33 bus is demonstrated in Figure 8.7. As observed, the Peak-to-Average Ratio (PAR) of $P_t^{f_1}$ of the proposed framework is lower than that when no DR is executed by 3.7%. Hence, the proposed model improves the utilization of the network which is advantageous to the network operator while meeting the user's demand requirements. The impact of the

EV charging model on bus voltage was also studied. The NCS method resulted in voltages at bus 18 exceeding the bus voltage limits set between 0.95 to 1.05pu. This is expected as EVs are not being directed to charging stations at buses that are not heavily loaded. As the demand for EV charging increases at only certain charging stations that have high demand, the impact on voltage is observed. However, on adopting the proposed EV assignment model, the bus voltages remain between 0.95 to 1.05pu. Figure 8.8 illustrates a comparison between the two models in terms of the voltage at the further most bus 18 of the IEEE 33 bus system. Moreover, congestion over $\mathcal{T}$, $\bar{c}$, is determined for $\lambda = 0 - 3$, as illustrated in Figure 8.9. As observed, the superiority of the proposed framework is proven as average congestion is lower than the scenario in which no DR is implemented. In fact, the utilization of the distribution network through the proposed model improves by 37.5% under moderate traffic when the number of charging requests is 1.

As EVs request to be directed to charging stations, the MSP aims to minimize their queue time at the charging station while also minimizing the impact on the grid. As described in Section IV, the MSP takes assignment decisions every 0.1 minutes using different weights. Hence, the MSP may sometimes decide to forward an EV to a charging station that is further to manage the electrical load. The sensitivity of the congestion function (8.6) to changes in the load, $\zeta_s$, is obtained from the DNO by the MSP. Table 8.1 illustrates the impact of changing the electrical load of the buses where the FCSs are located on congestion in the network. As observed, FCSs 1 and 2 are less sensitive compared to FCSs 3 and 4. Hence, the MSP would aim to direct EV traffic more towards FCSs 1 and 2 compared to that of 3 and 4. Hence, Figure 8.10 demonstrates the number of EVs charging at FCSs 1 and 4. As observed, being less sensitive to changes in demand, FCS 1 is serving more EVs compared to no EVs charging at FCS 4. FCS 4 being more sensitive to changes in loads have no EVs directed to it as long as the charging requests can be satisfied by other less sensitive FCSs. When compared to the NCS model that does not take sensitivity of the bus at which the FCS is located to changes in demand into consideration, FCS 4 is more populated than that of FCS 1. Moreover, to ensure that queuing time at the charging stations is not impacted, Figure 8.11 illustrates the results obtained on varying $\lambda$ adopting the proposed framework versus that of the NCS model. As observed, as the rate of charging requests, $\lambda$, increases, queuing time also increases from a mean of 70 minutes to 211 minutes when adopting the proposed framework. However, the amount of time an EV has to wait is lower by 38% for $\lambda = 2$ and by 9% for $\lambda = 3$ when adopting the proposed EV assignment compared to that of the NCS model. This results in more satisfied EV consumers.

### 8.6.3 Impact of False Data Injection Cyber Attack

As discussed in Section V, cyber attacking such important frameworks can impact both the transportation and the distribution networks. A cyber attacker can utilize historical data acquired through eavesdropping on the network to determine the most sensitive electrical bus to changes in the load on congestion in the network. In the simulated case study, this is represented by FCS 4. The attacker injects false information to assign EVs to the corresponding charging station, $s_a$, that is located on that bus. This would result in all EVs being redirected to one charging station, resulting in long waiting queues and dissatisfied consumers, whose trust in EV assignment would be impacted.

Figure 8.12 illustrates the power flowing in the main feeder, $P_t^{f_1}$, of the IEEE 33 bus system in normal conditions and when the MSP is attacked. In the cyber attacked scenario, when EVs are directed to one FCS increasing the waiting time there, the demand on the other three buses is reduced where the remaining FCSs are located. Hence, the power flowing in normal conditions in the main feeder of the network is more significant than that of the cyber attacked case as demonstrated in Figure 8.12. This is disadvantageous financially to the DNO as demand is lower. Moreover, the EV users being misled to the wrong charging stations causes long queue lines and times at FCS 4. Moreover, as illustrated in Figure 8.13, the MSP is not aware of the cyber attack happening. Hence, the MSP believes that the EVs are being redirected as observed by the EVCS1-No Attack and EVCS4-No Attack case in Figure 8.13. In reality as demonstrated in the EVCS1-FDIA and EVCS4-FDIA cases in Figure 8.13, FCS 1 has zero EV charging as vehicles have been redirected to FCS 4 making it fully occupied. The queuing time for charging at the FCSs hence drastically increases as illustrated in Figure 8.14 for various $\lambda$. For example, for $\lambda = 2$, the mean queuing time increased from 4 minutes to 440 minutes. This would cause EV owners who still have a charge in their batteries to redirect themselves to other charging stations, resulting in wastage of their time and convenience. As for EV owners who do not have enough charge to reach another FCS, their inconvenience to wait for such long queue times is at its peak.

Table 8.1: Mean sensitivity, $\zeta_s$, of congestion (8.6) to changes in the load.

| **FCS** | **FCS Bus** | **Mean $\zeta_s$** |
|---|---|---|
| 1 | 2 | 66.32 |
| 2 | 3 | 93 |
| 3 | 18 | 332.54 |
| 4 | 33 | 512.13 |

### 8.6.4 Intrusion Detection

The IEEE 33 bus system was utilized to test the proposed intrusion detection system that utilizes existing resources in the transportation network to detect an attack. As illustrated in Figure 8.15, when the number of EVs queued at FCS4 increases by a fixed threshold, $\Gamma_s = 10$, compared to other CSs, an alarm is raised alerting the TMC that a cyber attack is happening. The cyber attacker, hence, would be detected and further manipulation of the EV assignment model is prevented.

## 8.7 Conclusions

In this chapter, the coupling of the electrical and the transportation network was utilized to minimize distribution network congestion and assign EVs to FCSs accordingly. The EV assignment model utilized Lyapunov optimization to ensure queuing stability and provide limits on congestion. The proposed framework results in the MSP assigning EVs such that queuing and traveling time to FCS is minimized while managing distribution network congestion. The cyber security of the proposed framework was also studied and an intrusion detection model that takes advantage of existing sensors in the transportation network was proposed. The proposed model prevents a cyber attacker aiming to increase EV charging queuing time, causing a loss of demand which results in financial losses for the network operator, and results in dissatisfied consumers.

[1]

[1]This work is in review in: Gul M Khan, O., Elghitani, F., Youssef, A., Salama, M. and El Saadany, E. *A Congestion-Aware Charging Station Assignment for EVs.* IEEE Transactions on Smart Grid , 2022 (Article Submitted on 19th July 2022)

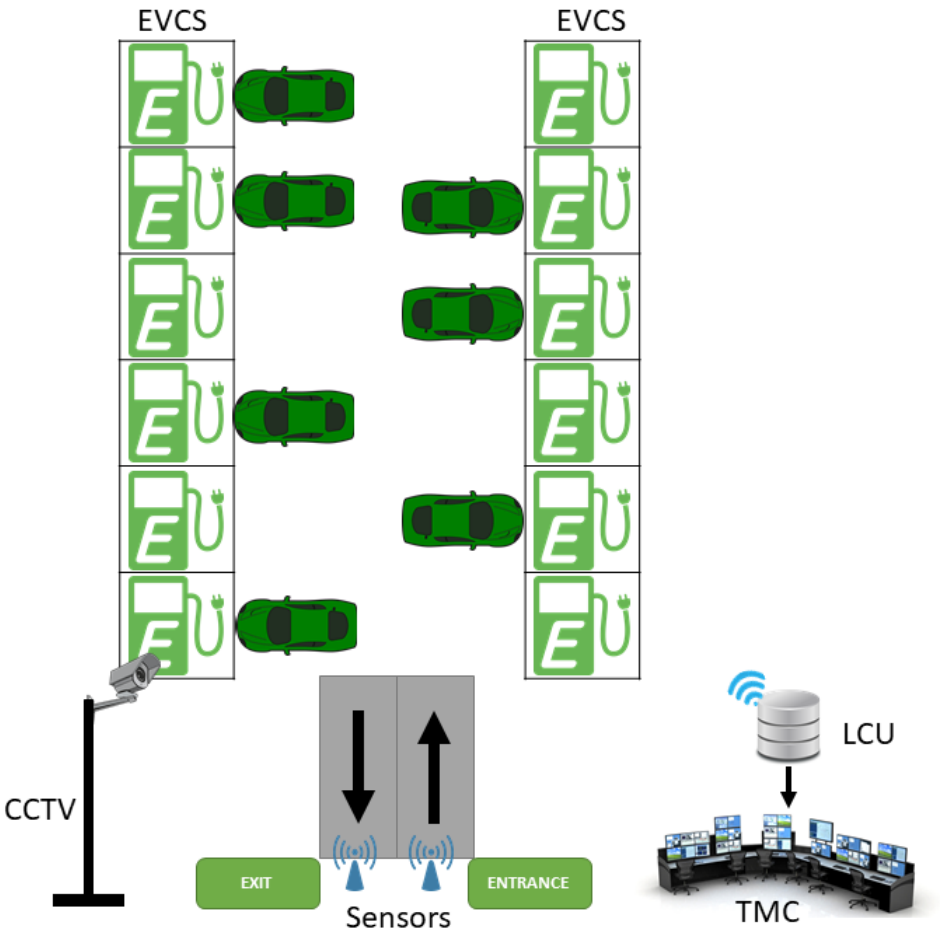



Figure 8.3: Architecture of Proposed Intrusion Detection System

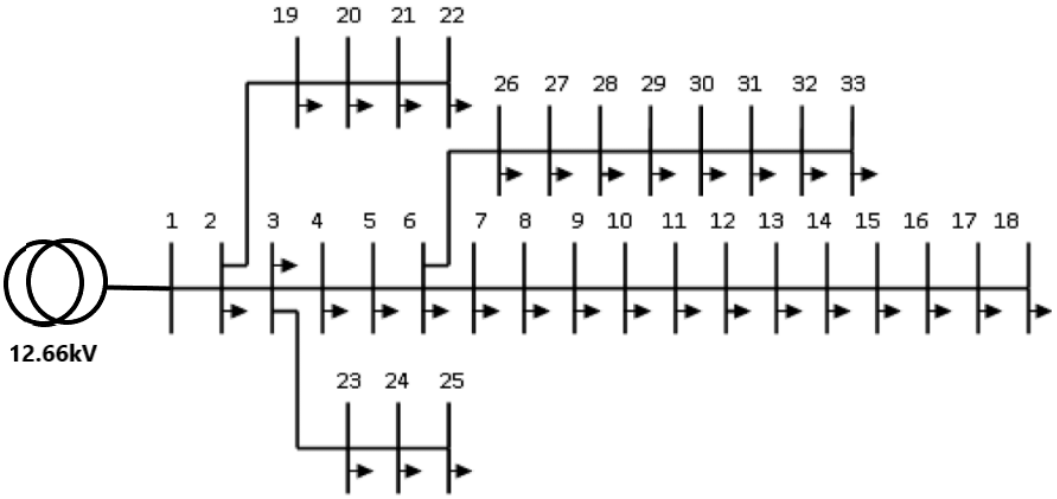



Figure 8.4: IEEE 33-bus system

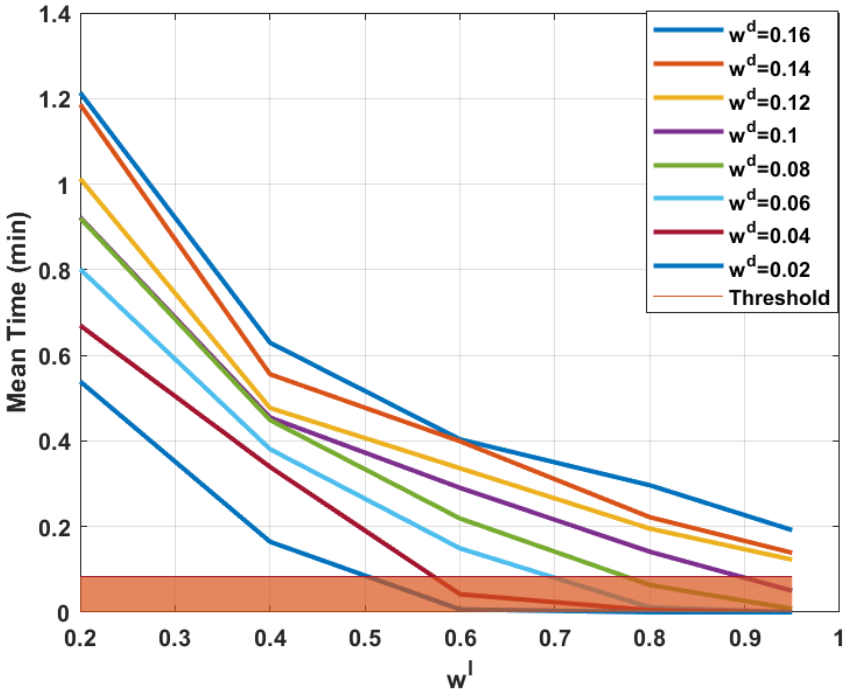



Figure 8.5: Mean assignment delay time

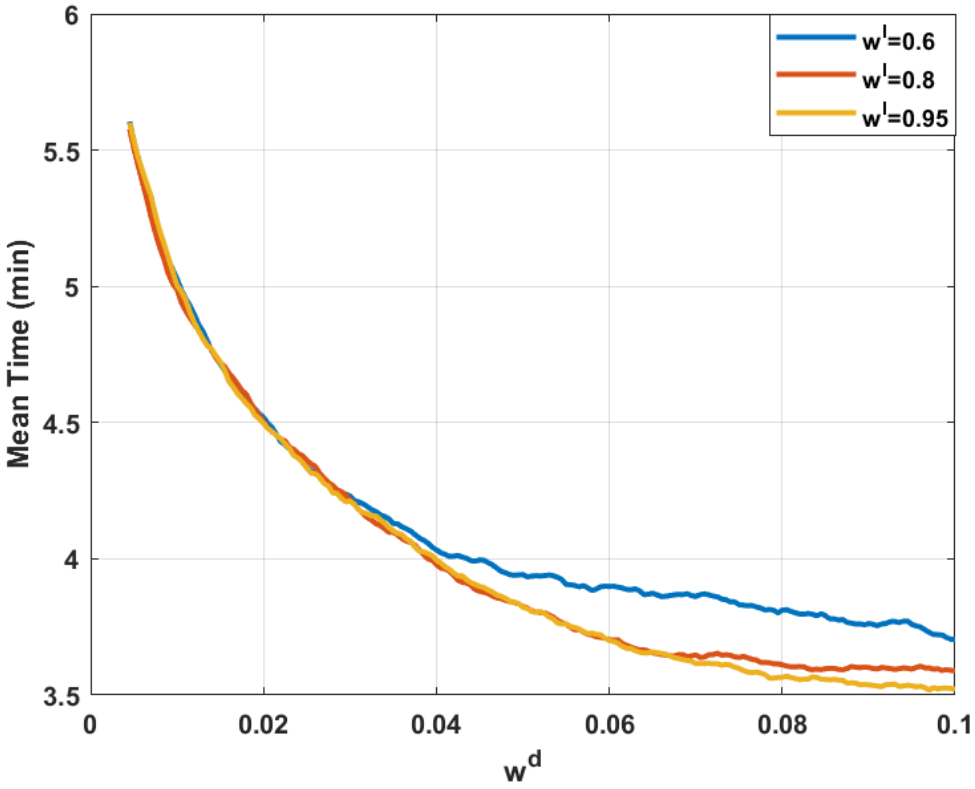



Figure 8.6: Mean travelling time versus trade off parameter $w^d$ for various $w^l$

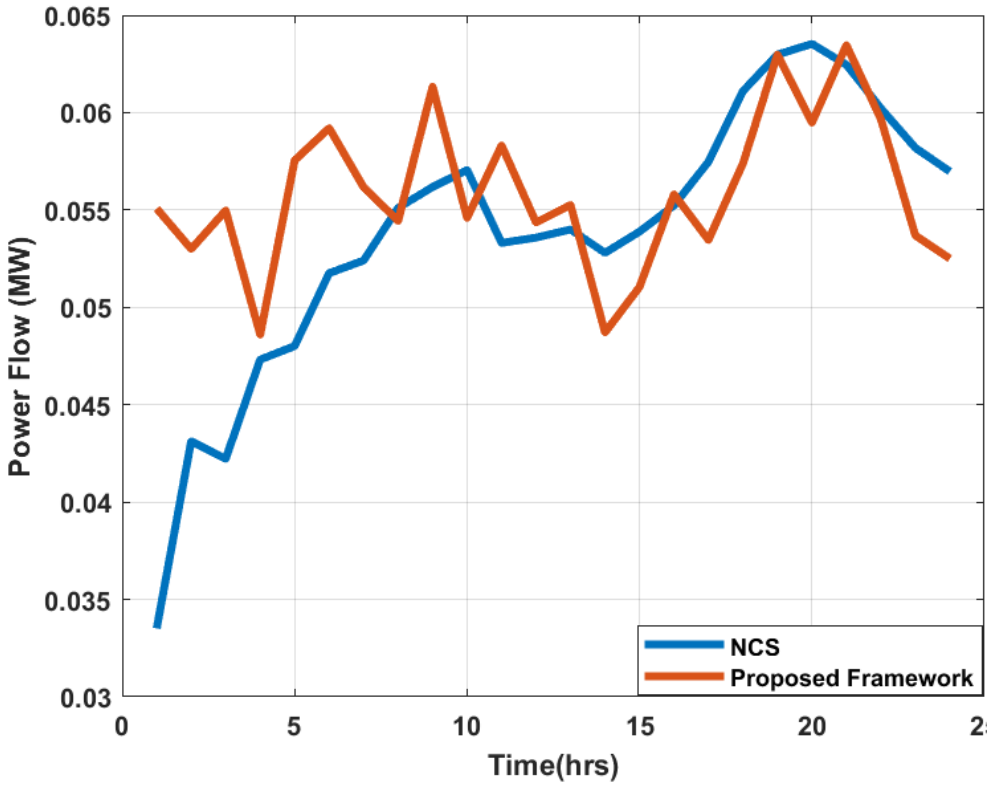



Figure 8.7: Power Flowing in Main Feeder of IEEE 33 bus system of proposed framework versus using nearest charging station assignment policy

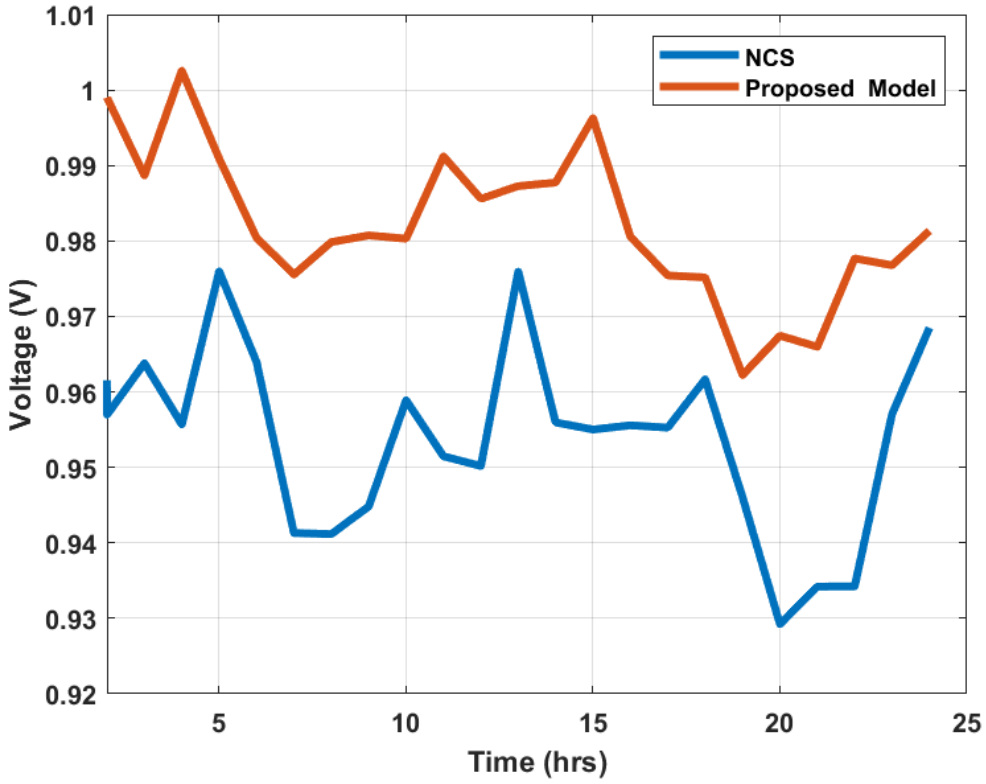



Figure 8.8: IEEE 33 load bus voltages for NCS versus proposed EV charging assignment model.

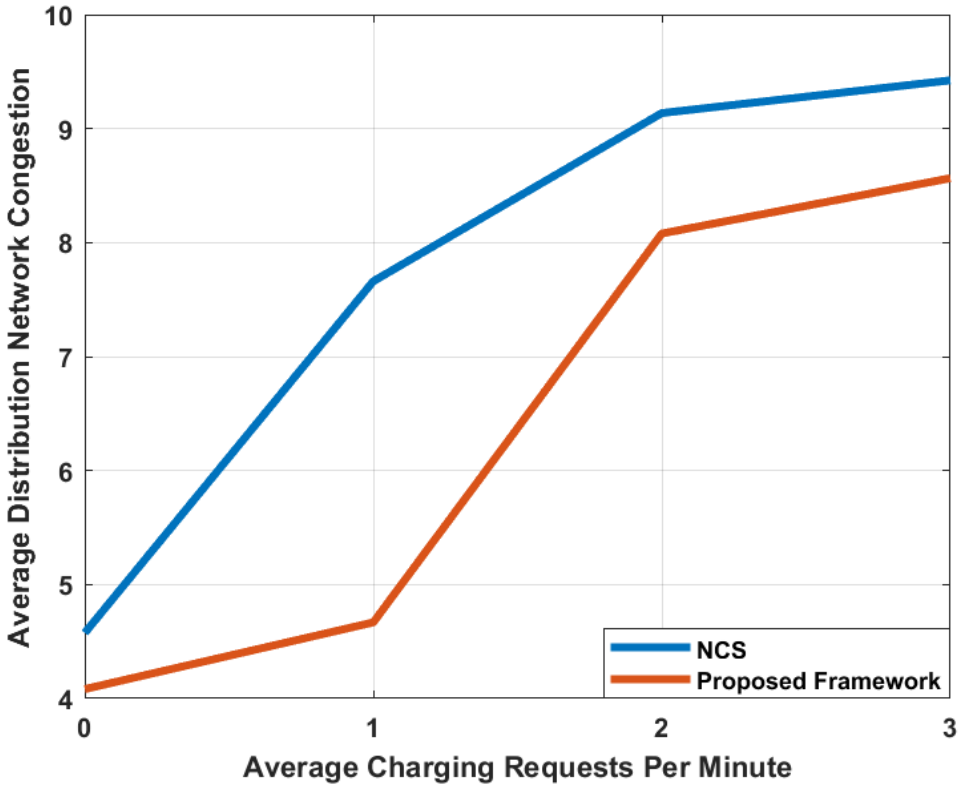
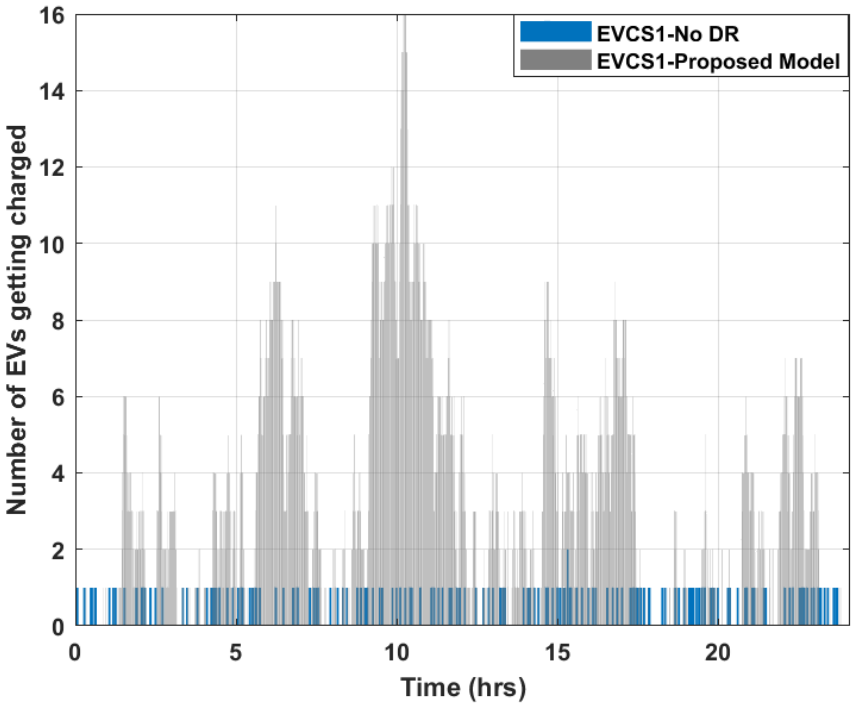
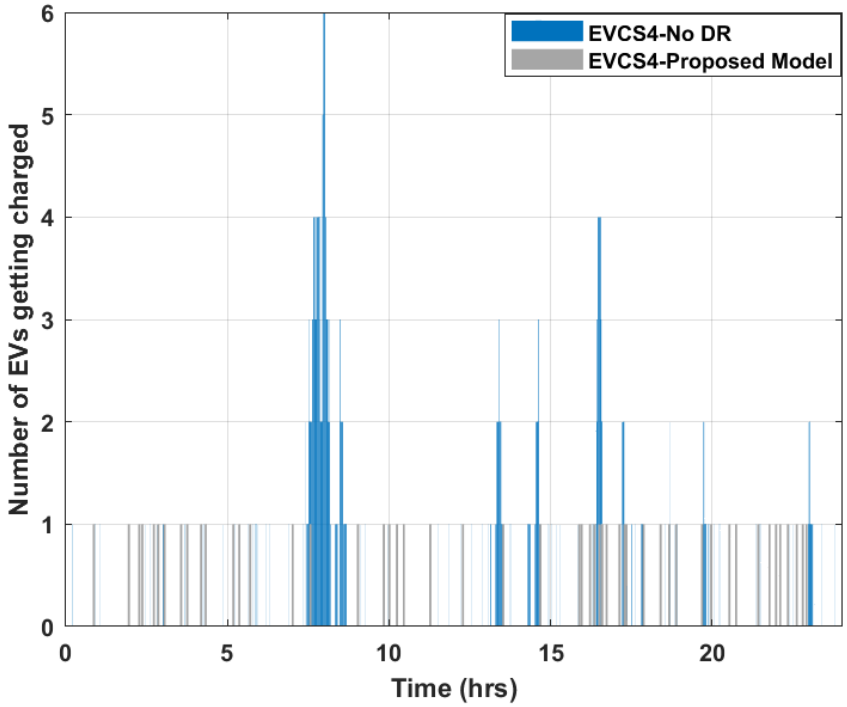



Figure 8.9: Comparison of average congestion, $\bar{c}$




(a)




(b)



Figure 8.10: Number of EVs charging in (a) FCS 1 and (b) FCS 4.

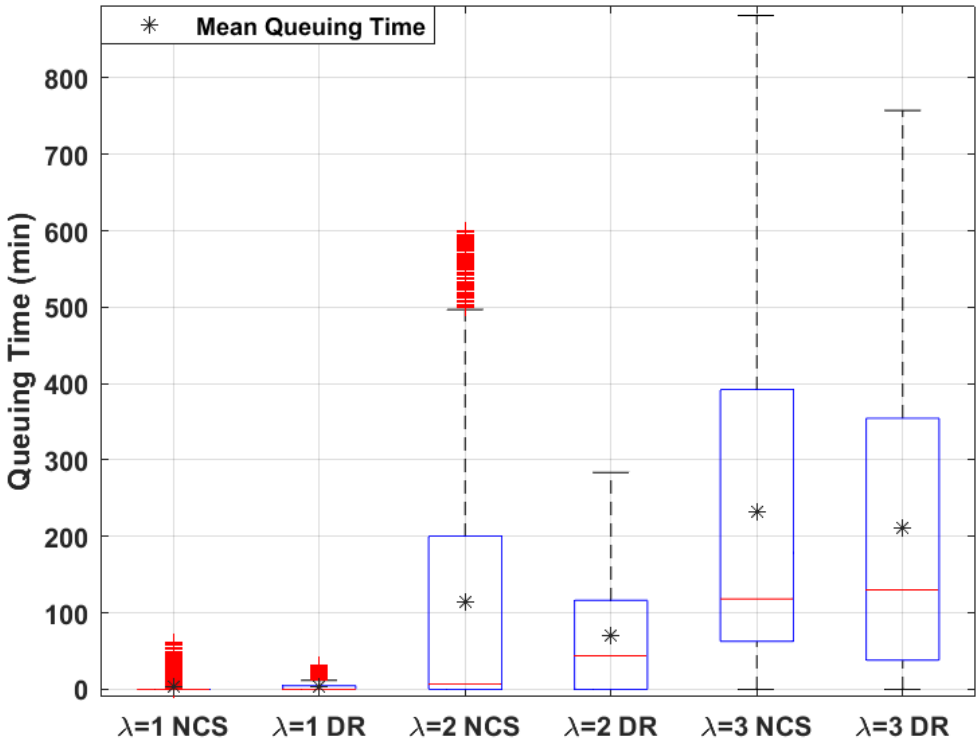



Figure 8.11: Boxplot representation of queuing time in charging station for different rates of charging requests

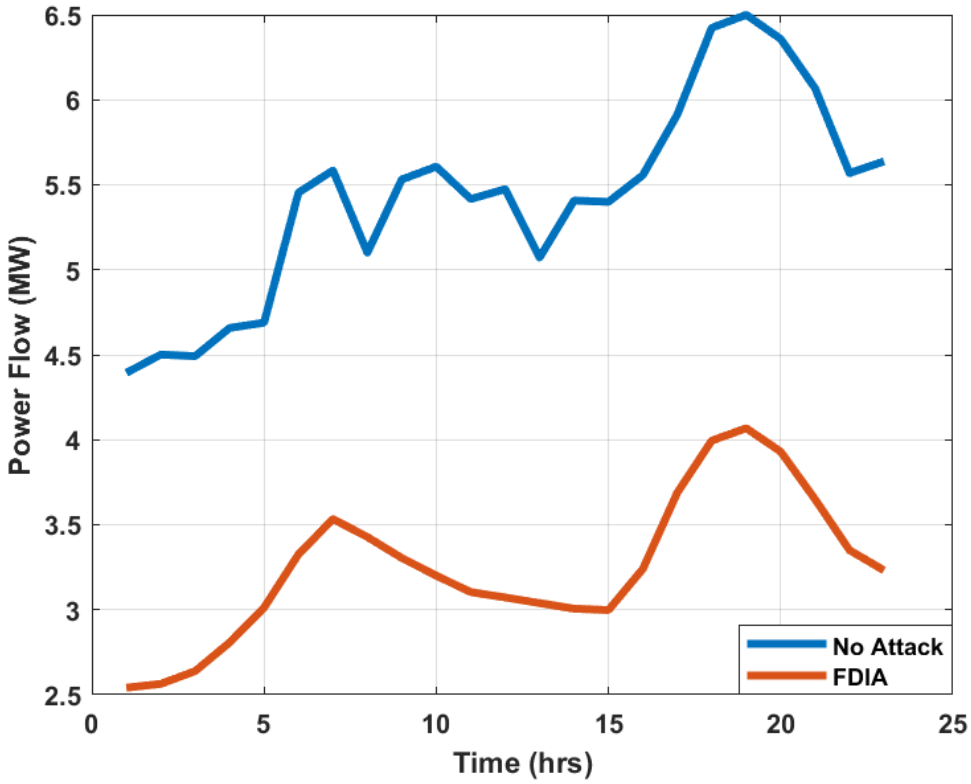
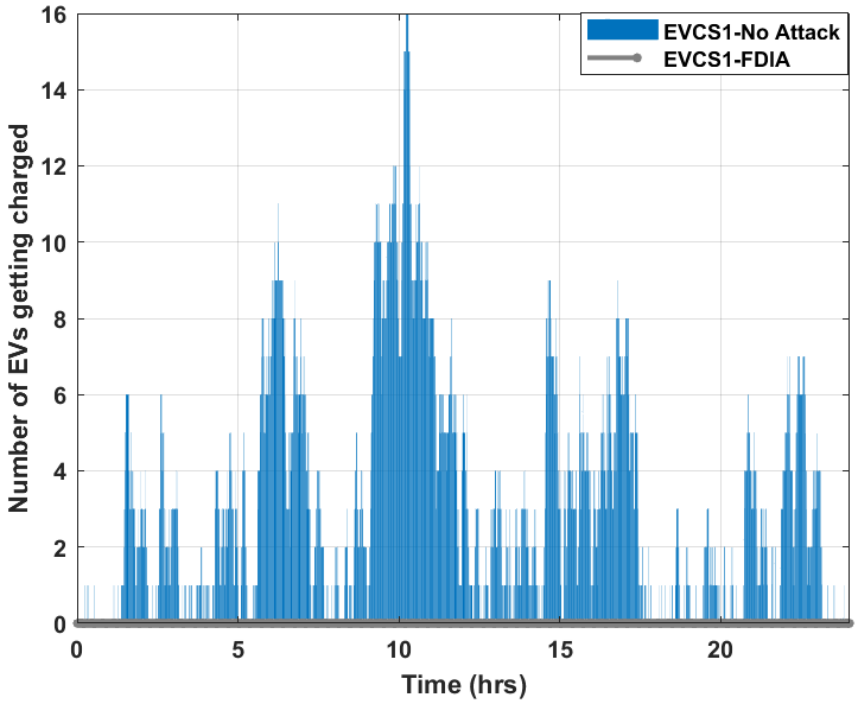
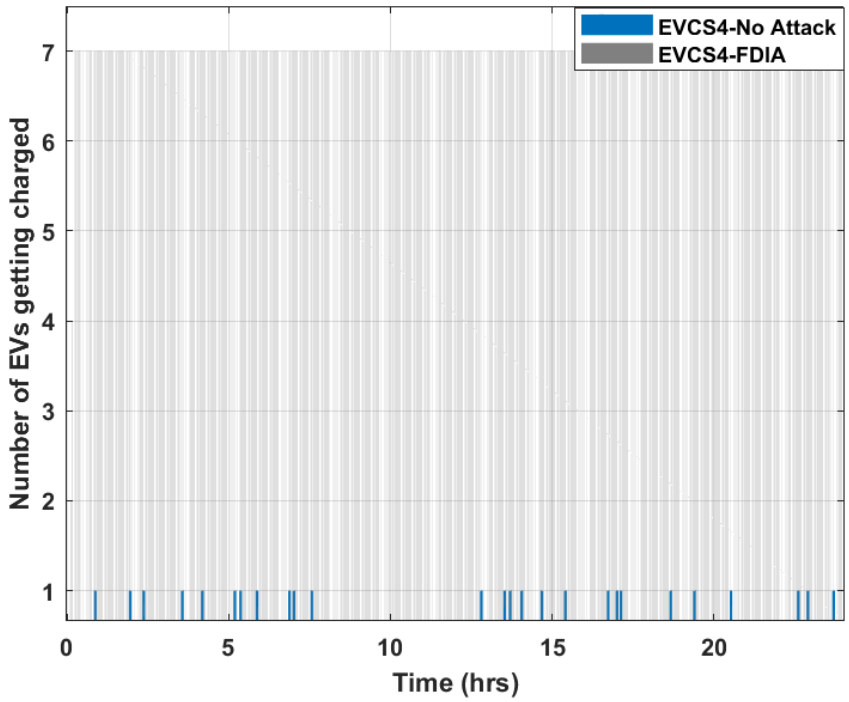



Figure 8.12: Comparison of Power Flowing in Main Feeder of IEEE 33 bus system of proposed framework in the presence and absence of FDIA




(a)




(b)



Figure 8.13: Comparison of number of EVs charging in real time in (a) FCS 1 and (b) FCS 4 for FDIA scenario and not attacked scenario.

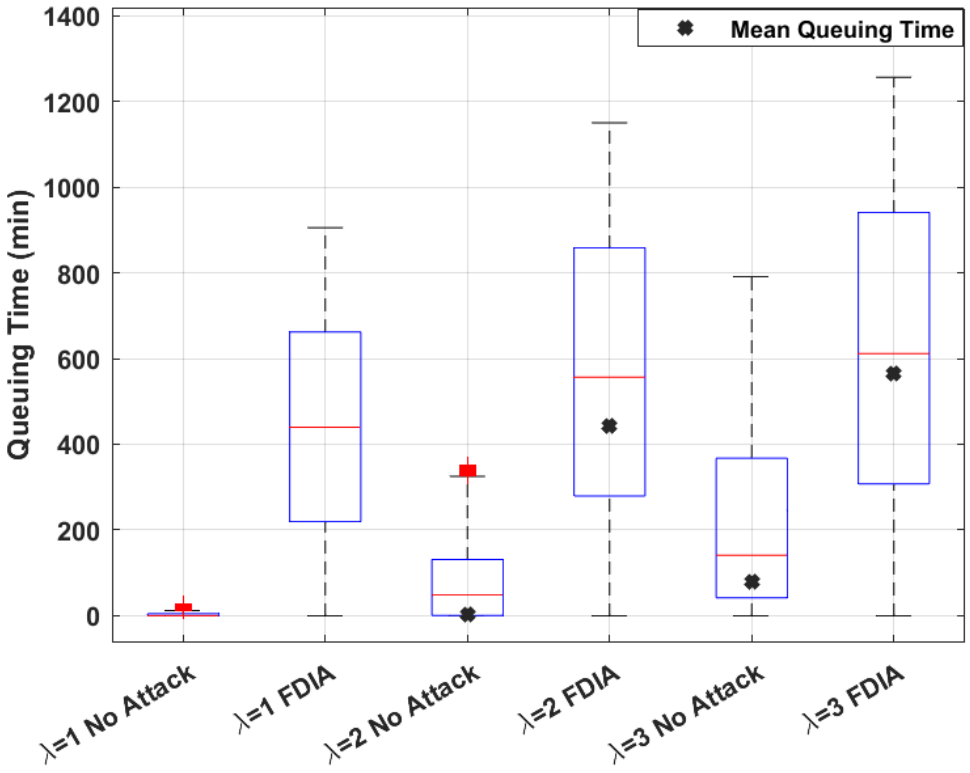



Figure 8.14: Boxplot representation of queuing time in charging station for different rates of charging requests

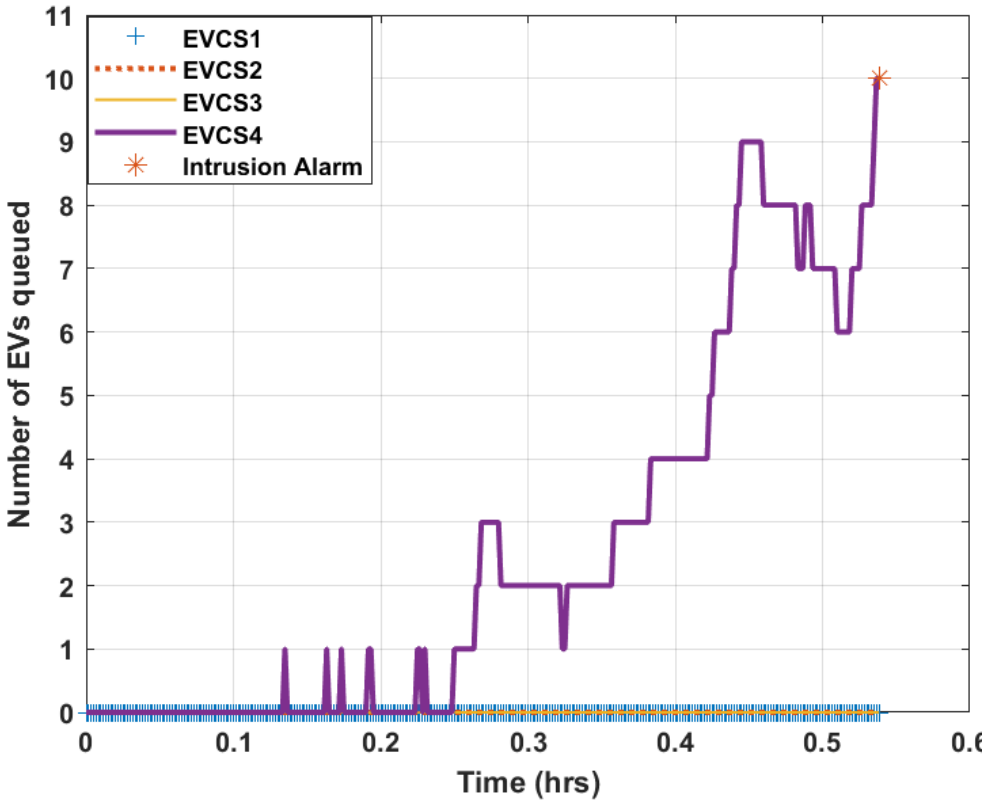



Figure 8.15: Intrusion detector raising an alarm alerting the possibility of FDIA

# Chapter 9

# Contributions and Conclusions

## 9.1 Summary and Conclusions

The evolution of the Traditional Power Grid (TPG) to the digital smart grid creates opportunities for improving the operation of the power system. However, to enjoy the operational benefits associated with the smart grid, the overloading problem of network assets as a result of the uncertainty associated with the penetration of renewable technologies and heavy flexible loads, and the cyber security of the grid are problems that arise in the smart grid. These problems needs to be addressed and their impacts minimized to completely gain the advantages of the smart grid without affecting its operational reliability and efficiency. This was the main objective of this thesis.

Market-based, or indirect, methods for congestion management in distribution networks was specifically investigated as it involves management of existing resources to solve the problem of congestion in the grid. A series of new schemes have been proposed in this thesis addressing the challenges in the existing techniques. The performance of the new methods were validated using case studies and results were compared with existing congestion management schemes. The contents of each chapter in this thesis can be summarized as follows:

- **Chapter 2** went through an elaborate background explaining the concepts of congestion in the distribution network, cyber security and cyber attacks impacting the smart grid. Next, literature review describing existing congestion management techniques in the distribution network, existing cyber attacks and cyber mitigation and/or detection schemes involving customers' smart meters was detailed.

- In **Chapter 3**, the vulnerability of Demand Side Management (DSM)-based congestion management methods to cyber attacks, specifically Load Altering Attack (LAA)s, was studied. An optimization algorithm was developed to determine the aggregators a cyber attacker would stealthily compromise, via minimum alteration of their load profiles, to cause congestion problems. The impact of such attacks on congestion in the distribution network and consumers' electricity bill was then studied to conclude the importance of having secure aggregators that would not be cyber compromised impacting the congestion management schemes.

- **Chapter 4** formulates a mitigation scheme to determine the most critical aggregators in the distribution network. The security of these aggregators was then reinforced to mitigate load altering cyber attacks and securing the network.

- **Chapter 5** focuses on LAAs that could compromise the operation of market-based congestion management methods. A detection technique was proposed using Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN). IEEE 33 bus system was used as a case study to demonstrate the effectiveness of the proposed technique. An accuracy of 97% was obtained proving the capability of using LSTM-RNN to detect a load altering cyber attack compromising aggregators in the network.

- In **Chapter 6**, multi-objective optimization was utilized to schedule flexible loads to alleviate potential congestions in the distribution network. The proposed scheme minimized consumers' electricity cost and decreased the peak to average ratio of the load curve to a required level that alleviates existing congestion. This resulted in a consumer load schedule that was economical and did not require the imposition of congestion tariffs. However, the success of the proposed congestion management scheme relied on the accuracy of the consumer load consumption. Hence, as flexible loads, such as Heat Pump (HP)s are reliant on unreliable weather conditions, uncertainty analysis of consumers' flexible load schedule was executed to ensure the desired robustness of the power flowing in the distribution network to changes in uncertain variables. The results obtained were compared with the existing Distributed Dynamic Tariff (DDT) congestion management scheme demonstrating the advantage of the proposed multi-objective framework in terms of decreasing price and flattening the load curve while alleviating congestion.

- It is very challenging to design a congestion management scheme for the distribution network given the uncertainty of flexible loads consumption and electricity prices. Obtaining stochastic models for such loads may not be easily available in practice.

In **Chapter 7**, a Deep Deterministic Policy Gradient (DDPG) Reinforcement Learning (RL) scheme was proposed to alleviate congestion. DDPG RL is a model free technique that does not require explicit probabilistic models of the controllable loads to determine the change in electricity prices needed, in the form of tariffs and/or subsidies. The DDPG RL technique was compared with the existing model-based congestion management scheme using an IEEE 33 bus system and the results obtained demonstrate the out performance of the proposed technique in terms of electricity cost and peak to average ratio of the load profiles.

- In **Chapter 8**, distribution network congestion is minimized through the proposal of an efficient Electric Vehicle (EV) assignment model that utilizes the coupling of the electrical and the transportation network. The EV assignment model assigns EVs to Fast Charging Stations (FCSs) in real-time such that queuing and traveling time to FCS is minimized while managing distribution network congestion. The vulnerability of the proposed model to a False Data Injection Attack (FDIA) was also studied and an intrusion detection model that takes advantage of existing sensors in the transportation network was proposed.

## 9.2 Direction for Future Work

In the future, the authors believe that the following studies and research directions if investigated can extend and improve the work in this thesis:

- Incorporation of other Renewable Energy Source (RES), such as PVs, and vehicle to grid EVs to study the impact of the bidirectional flow of electricity on congestion in the distribution network in terms of bus voltage as well as thermal limits. The impact of such sources on the proposed congestion management schemes adds to the wholeness of the solution.

- Combine the proposed DSM-based congestion management schemes with direct control methods, such as network reconfiguration, to achieve a more efficient congestion management method.

- Work in this thesis has been mainly focused on the day-ahead market. However, as explained in Chapter 3, there is uncertainty involved in the operation of flexible loads. Hence, a congestion management scheme involving direct control of flexible loads in real-time markets should be investigated.

- Furthermore, combine DSM-based congestion management methods with direct control congestion management methods in the day-ahead market and real-time markets to have a complete congestion management system.
- Study the impact of multiple types of cyber attacks, such as a combination of Denial of Service and False Data Injection attacks, that compromises the availability and integrity of the congestion management scheme. A cyber attack detection scheme that could detect such multi-type cyber attacks needs to be developed.
- Investigate the vulnerability of controlled EV fast charging stations to cyber attacks and study the impact of it being cyber attacked on the grid in terms of congestion in real-time market. Develop a scheme to detect cyber attacks on such EV charging stations.

# Bibliography


[1] M. E. Baran and F. F. Wu. Network reconfiguration in distribution systems for loss reduction and load balancing. *IEEE Transactions on Power Delivery*, 4(2):1401–1407, April 1989.

[2] Robert Wortrich. How does an air source heat pump work in winter?, Dec 2021.

[3] Joe Dammel. What's up with networked geothermal? nbsp;, Aug 2022.

[4] S. Massoud Amin and B.F. Wollenberg. Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine*, 3(5):34–41, 2005.

[5] Salman K. Salman. Evolution of conventional power systems to smart grids. In *2019 54th International Universities Power Engineering Conference (UPEC)*, pages 1–6, 2019.

[6] NY state senate bill s6599. *NY State Senate*, June 2019.

[7] Debra Lew, Jordan Bakke, Aaron Bloom, Patrick Brown, Jay Caspary, Christopher Clack, Nicholas Miller, Antje Orths, Alison Silverstein, John Simonelli, and Robert Zavadil. Transmission planning for 100% clean electricity: Enabling clean, affordable, and reliable electricity. *IEEE Power and Energy Magazine*, 19(6):56–66, 2021.

[8] Too much of a good thing? global trends in the curtailment of solar pv. *Solar Energy*, 208:1068 – 1077, 2020.

[9] Bundesnetzagentur. EEG in numbers. 2018.

[10] T. Vo, A. Haque, P. Nguyen, I. Kamphuis, M. Eijgelaar, and I. Bouwman. A study of congestion management in smart distribution networks based on demand flexibility. In *IEEE Manchester PowerTech*, pages 1–6, 2017.

[11] Fred Lambert. US electric car sales jumped to an impressive record high last quarter, 2022.

[12] Adanna Le Gendre. Central air conditioners and air-source heat pumps, 2022.

[13] Lotte Rasmussen, Chaewon Bang, and Mikael Togeby. Managing congestion in distribution grids - market design consideration. how heat pumps can deliver flexibility though well-designed markets and virtual power plant technology. 2012.

[14] S. Huang, Q. Wu, L. Cheng, Z. Liu, and H. Zhao. Uncertainty management of dynamic tariff method for congestion management in distribution networks. *IEEE Transactions on Power Systems*, 31(6):4340–4347, Nov 2016.

[15] R. A. Verzijlbergh, L. J. De Vries, and Z. Lukszo. Renewable energy sources and responsive demand. do we need congestion management in the distribution grid? *IEEE Transactions on Power Systems*, 29(5):2119–2128, Sep. 2014.

[16] A.N.M.M. Haque, P.H. Nguyen, F.W. Bliek, and J.G. Slootweg. Demand response for real-time congestion management incorporating dynamic thermal overloading cost. *Sustainable Energy, Grids and Networks*, 10:65 – 74, 2017.

[17] A. N. M. M. Haque, P. H. Nguyen, W. L. Kling, and F. W. Bliek. Congestion management in smart distribution network. In *49th Intl. Universities Power Engineering Conference*, pages 1–6, Sep. 2014.

[18] Ben Foster, David Burns, David Kathan, Michael P. Lee, and Samin Peirovi. Assessment of demand response and advanced metering, 2018.

[19] Gaoqi Liang, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318, 2017.

[20] M. M. Pour, A. Anzalchi, and A. Sarwat. A review on cyber security issues and mitigation methods in smart grid systems. In *SoutheastCon 2017*, pages 1–4, March 2017.

[21] C.C. Liu, S. McArthur, and S.J. Lee. *Smart Grid Handbook, 3 Volume Set*.

[22] Tractebel PWC SWECO, Ecofys. Study on the effective integration of distributed energy resources for providing flexibility to the electricity system, 2014.

[23] The authoritative dictionary of ieee standards terms, seventh edition. *IEEE Std 100-2000*, pages 1–1362, Dec 2000.

[24] S. Huang, Q. Wu, L. Cheng, and Z. Liu. Optimal reconfiguration-based dynamic tariff for congestion management and line loss reduction in distribution networks. *IEEE Transactions on Smart Grid*, 7(3):1295–1303, May 2016.

[25] Y. Gu, J. Xie, X. Chen, K. Yu, Z. Chen, and Z. Li. Dynamic tariff method for congestion management in distribution networks. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–6, Nov 2017.

[26] S. Huang, Q. Wu, H. Zhao, and C. Li. Distributed optimization based dynamic tariff for congestion management in distribution networks. *IEEE Transactions on Smart Grid*, 2018.

[27] S. Huang and Q. Wu. Dynamic subsidy method for congestion management in distribution networks. *IEEE Transactions on Smart Grid*, 9(3):2140–2151, May 2018.

[28] Steve Fenrick. *Peak Time Rebate Programs: Reducing Costs While Engaging Customers*. Power System Engineering, Inc. (PSE), 2016.

[29] Shaojun Huang, Qiuwei Wu, Zhaoxi Liu, and Arne Hejde Nielsen. Review of congestion management methods for distribution networks with high penetration of distributed energy resources. In *IEEE PES Innovative Smart Grid Technologies, Europe*, pages 1–6, 2014.

[30] Niamh O'Connell, Qiuwei Wu, Jacob Østergaard, Arne Nielsen, Seung Cha, and Yi Ding. Day-ahead tariffs for the alleviation of distribution grid congestion from electric vehicles. *Electric Power Systems Research*, 92:106–114, 11 2012.

[31] Ruoyang Li, Qiuwei Wu, and Shmuel S. Oren. Distribution locational marginal pricing for optimal electric vehicle charging management. *IEEE Transactions on Power Systems*, 29(1):203–211, 2014.

[32] S. Huang, Q. Wu, S. S. Oren, R. Li, and Z. Liu. Distribution locational marginal pricing through quadratic programming for congestion management in distribution networks. *IEEE Transactions on Power Systems*, 30(4):2170–2178, July 2015.

[33] Haiwang Zhong, Le Xie, and Qing Xia. Coupon incentive-based demand response: Theory and case study. *IEEE Transactions on Power Systems*, 28(2):1266–1276, 2013.

[34] Merwais Shinwari, Amr Youssef, and Walaa Hamouda. A water-filling based scheduling algorithm for the smart grid. *IEEE Transactions on Smart Grid*, 3(2):710–719, 2012.

[35] Niangjun Chen, Chee Wei Tan, and Tony Q. S. Quek. Electric vehicle charging in smart grid: Optimality and valley-filling algorithms. *IEEE Journal of Selected Topics in Signal Processing*, 8(6):1073–1083, 2014.

[36] Zhenpo Wang and Shuo Wang. Grid power peak shaving and valley filling using vehicle-to-grid systems. *IEEE Transactions on Power Delivery*, 28(3):1822–1829, 2013.

[37] Mingxi Liu, Phillippe Phanivong, and Duncan Callaway. Electric vehicle charging control in residential distribution network: A decentralized event-driven realization. In *IEEE Conf. on Decision and Control*, pages 214–219, 2017.

[38] Yuting Mou, Hao Xing, Zhiyun Lin, and Minyue Fu. Decentralized optimal demand-side management for phev charging in a smart grid. *IEEE Transactions on Smart Grid*, 6(2):726–736, 2015.

[39] *Combined Electromagnetism-Like Algorithm with Tabu Search to Scheduling*, page 478–508. IGI Global, 2015.

[40] Yanni Wan, Jiahu Qin, Xinghuo Yu, Tao Yang, and Yu Kang. Price-based residential demand response management in smart grids: A reinforcement learning-based approach. *IEEE/CAA Journal of Automatica Sinica*, 9(1):123–134, 2022.

[41] Yuanzheng Li, Guokai Hao, Yun Liu, Yaowen Yu, Zhixian Ni, and Yong Zhao. Many-objective distribution network reconfiguration via deep reinforcement learning assisted optimization algorithm. *IEEE Transactions on Power Delivery*, 37(3):2230–2244, 2022.

[42] Yuanqi Gao, Wei Wang, Jie Shi, and Nanpeng Yu. Batch-constrained reinforcement learning for dynamic distribution network reconfiguration. *IEEE Transactions on Smart Grid*, 11(6):5357–5369, 2020.

[43] Shahab Bahrami, Yu Christine Chen, and Vincent W. S. Wong. Deep reinforcement learning for direct load control in distribution networks. In *2020 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–5, 2020.

[44] Xianzhuo Sun and Jing Qiu. A customized voltage control strategy for electric vehicles in distribution networks with reinforcement learning method. *IEEE Transactions on Industrial Informatics*, 17(10):6852–6863, 2021.

[45] S. Islam, Z. Baig, and S. Zeadally. Physical layer security for the smart grid: Vulnerabilities, threats and countermeasures. *IEEE Transactions on Industrial Informatics*, 2019.

[46] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57:1344–1371, 04 2013.

[47] Adnan Anwar and Abdun Mahmood. *Cyber Security of Smart Grid Infrastructure*. 01 2014.

[48] Amira Mohammed and Gibin George. Vulnerabilities and strategies of cybersecurity in smart grid - evaluation and review. In *2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE)*, pages 1–6, 2022.

[49] Marilyn Wolf and Dimitrios Serpanos. *False Data Injection Attacks*, pages 73–83. Springer International Publishing, Cham, 2020.

[50] Yingmeng Xiang and Lingfeng Wang. A game-theoretic study of load redistribution attack and defense in power systems. *Electric Power Systems Research*, 151:12 – 25, 2017.

[51] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad. Dynamic load altering attacks against power system stability: Attack models and protection schemes. *IEEE Transactions on Smart Grid*, 9(4):2862–2872, July 2018.

[52] Supriya S. Thakare and Parminder Kaur. Denial-of-service attack detection system. In *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)*, pages 281–285, 2017.

[53] Anibal Sanjab, Walid Saad, Ismail Guvenc, Arif Sarwat, and Saroj Biswas. Smart grid security: Threats, challenges, and solutions. 06 2016.

[54] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng. Cost-effective watermark based detector for replay attacks on cyber-physical systems. In *2017 11th Asian Control Conference (ASCC)*, pages 940–945, Dec 2017.

[55] Jiapeng Zhang and Yingfei Dong. Cyber attacks on remote relays in smart grid. *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9, 2017.

[56] A. Mohsenian-Rad and A. Leon-Garcia. Distributed internet-based load altering attacks against smart power grids. *IEEE Transactions on Smart Grid*, 2(4):667–674, Dec 2011.

[57] Peng Xun, Pei dong Zhu, Sabita Maharjan, and Peng shuai Cui. Successive direct load altering attack in smart grid. *Computers  Security*, 77:79 – 93, 2018.

[58] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li. A denial of service attack in advanced metering infrastructure network. In *2014 IEEE International Conference on Communications (ICC)*, pages 1029–1034, June 2014.

[59] Advanced metering infrastructure and customer systems, 2016.

[60] K. Jhala, B. Natarajan, A. Pahwa, and H. Wu. Stability of transactive energy market-based power distribution system under data integrity attack. *IEEE Transactions on Industrial Informatics*, 15(10):5541–5550, 2019.

[61] H. S. Karimi, K. Jhala, and B. Natarajan. Impact of real-time pricing attack on demand dynamics in smart distribution systems. In *NAPS*, pages 1–6, 2018.

[62] U. Anubunwa, H. Rajmani, R. AbdAlhamed, and P. Pillai. Investigating the impacts of cyber-attacks on pricing data of home energy management systems in DR programs. In *IEEE PESGM*, pages 1–5, 2018.

[63] A. Mohsenian-Rad and A. Leon-Garcia. Distributed internet-based load altering attacks against smart power grids. *IEEE Transactions on Smart Grid*, 2(4):667–674, 2011.

[64] X. Liu and Z. Li. Local load redistribution attacks in power systems with incomplete network information. *IEEE Transactions on Smart Grid*, 5(4):1665–1676, 2014.

[65] Scott Burger, Jose Pablo Chaves-Ávila, Carlos Batlle, and Ignacio J. Pérez-Arriaga. The value of aggregators in electricity systems, 2016.

[66] D. Li, W. Chiu, H. Sun, and H. V. Poor. Multiobjective optimization for demand side management program in smart grid. *IEEE Transactions on Industrial Informatics*, 14(4):1482–1490, April 2018.

[67] R. A. Verzijlbergh, L. J. De Vries, and Z. Lukszo. Renewable energy sources and responsive demand. do we need congestion management in the distribution grid? *IEEE Transactions on Power Systems*, 29(5):2119–2128, Sep. 2014.

[68] O. Sundstrom and C. Binding. Flexible charging optimization for electric vehicles considering distribution grid constraints. *IEEE Transactions on Smart Grid*, 3(1):26–37, March 2012.

[69] Niamh O'Connell, Qiuwei Wu, Jacob Østergaard, Arne Hejde Nielsen, Seung Tae Cha, and Yi Ding. Day-ahead tariffs for the alleviation of distribution grid congestion from electric vehicles. *Electric Power Systems Research*, 92:106 – 114, 2012.

[70] Christine Lai, Nicholas Jacobs, Shamina Hossain-Mckenzie, Cedric Carter, Patricia Cordeiro, Ifeoma Onunkwo, and Jay Johnson. Cyber security primer for der vendors, aggregators, and grid operators, 12 2017.

[71] S. Bi and Y. J. Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Transactions on Smart Grid*, 5(3):1216–1227, 2014.

[72] R. Deng, G. Xiao, and R. Lu. Defending against false data injection attacks on power system state estimation. *IEEE Transactions on Industrial Informatics*, 13(1):198–207, 2017.

[73] X. Liu, Z. Li, and Z. Li. Optimal protection strategy against false data injection attacks in power systems. *IEEE Transactions on Smart Grid*, 8(4):1802–1810, 2017.

[74] A. Sanjab and W. Saad. Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective. *IEEE Transactions on Smart Grid*, 7(4):2038–2049, 2016.

[75] S. Wang, W. Ren, and U. M. Al-Saggaf. Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks. *IEEE Systems Journal*, 11:2640–2651, 2017.

[76] Z. Zhang, R. Deng, D. Yau, P. Cheng, and J. Chen. Analysis of moving target defense against false data injection attacks on power grid. *IEEE Trans. on Information Forensics and Security*, 2020.

[77] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao. On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices. *IEEE Trans. on Industrial Informatics*, 16(2):854–864, 2020.

[78] X. Liu, P. Zhu, Y. Zhang, and K. Chen. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *IEEE Transactions on Smart Grid*, 6:2435–2443, 2015.

[79] P. Jokar, N. Arianpoo, and V. C. M. Leung. Electricity theft detection in ami using customers' consumption patterns. *IEEE Transactions on Smart Grid*, 7(1):216–226, 2016.

[80] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin. Deep learning detection of electricity theft cyber-attacks in renewable distributed generation. *IEEE Trans. on Smart Grid*, 11:3428–3437, 2020.

[81] T. S. Ustun and S. M. S. Hussain. A review of cybersecurity issues in smartgrid communication networks. In *2019 International Conference on Power Electronics, Control and Automation*, pages 1–6, 2019.

[82] J. Zhang, Z. Chu, L. Sankar, and O. Kosut. Can attackers with limited information exploit historical data to mount successful FDI attacks on power systems? *IEEE Trans. on Power Systems*, 33, 2018.

[83] Abdelrahman Ayad, Mohsen Khalaf, and Ehab El-Saadany. Cyber-physical security of state estimation against attacks on wide-area load shedding protection schemes. In *IEEE ISGT Conference*, pages 1–5, February 2019.

[84] K. Khanna, B. Panigrahi, and A. Joshi. Bilevel modelling of false data injection attacks on security constrained optimal power flow. *IET Generation, Transmission Distribution*, 11:3586–3593, 2017.

[85] E. A. Rezai, M. Shaaban, E. F. El-Saadany, and F. Karray. Online intelligent demand management of plug-in electric vehicles in future smart parking lots. *IEEE Systems Journal*, 10:483–494, 2016.

[86] GAMS Development Corporation. General algebraic modeling system (gams) release 24.2.1. Washington, DC, USA, 2013.

[87] D. Das. A fuzzy multiobjective approach for network reconfiguration of distribution systems. *IEEE Trans. on Power Delivery*, 21(1):202–209, 2006.

[88] Overcurrent protection. *National Electrical Code Article 240*, 2017.

[89] S. Huang, Q. Wu, Z. Liu, and A. H. Nielsen. Review of congestion management methods for distribution networks with high penetration of distributed energy resources. In *IEEE PES Innovative Smart Grid Technologies, Europe*, pages 1–6, Oct 2014.

[90] M. Shabanzadeh, M. Eslami, and M. Haghifam. Risk-based medium-term trading strategy for a vpp with first-order stochastic dominance constraints. *IET Generation, Transmission  Distribution*, 11, 2017.

[91] R. A. Jabr. Radial distribution load flow using conic programming. *IEEE Transactions on Power Systems*, 21, 2006.

[92] D. K. Molzahn and I. A. Hiskens. *A Survey of Relaxations and Approximations of the Power Flow Equations*. 2019.

[93] Burak Kocuk, S. Dey, and X. Sun. Strong SOCP relaxations for the optimal power flow problem. *Operations Research*, 64:1177–1196, 2016.

[94] Christodoulos A Floudas. Mixed-Integer Nonlinear Optimization. In *Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications*. Oxford University Press, 11 1995.

[95] Omniyah Gul M. Khan, Ehab F. El-Saadany, Amr Youssef, and Mostafa F. Shaaban. Cyber security of market-based congestion management methods in power distribution systems. *IEEE Transactions on Industrial Informatics*, 17(12):8142–8153, 2021.

[96] R. A. Schmidhuber F. A. Gers and F. A. Cummins. Learning to forget: continual prediction with lstm. *Neural Comput.*, 12:2451–2471, 2000.

[97] Filippo Maria Bianchi, Enrico Maiorino, Michael C. Kampffmeyer, Antonello Rizzi, and Robert Jenssen. *Recurrent Neural Networks for Short-Term Load Forecasting: An Overview and Comparative Analysis*. Springer, 2017.

[98] Perry Lea. *IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security*. Computers, 2020.

[99] Abdelhay A. Sallam and Om P. Malik. *Demand-Side Management and Energy Efficiency*, pages 429–463. 2019.

[100] Shaojun Huang, Qiuwei Wu, Lin Cheng, Zhaoxi Liu, and Haoran Zhao. Uncertainty management of dynamic tariff method for congestion management in distribution networks. *IEEE Transactions on Power Systems*, 31(6):4340–4347, 2016.

[101] Shaojun Huang, Qiuwei Wu, Zhaoxi Liu, and Haoran Zhao. Sensitivity analysis of dynamic tariff method for congestion management in distribution networks. In *2015 IEEE Power Energy Society General Meeting*, pages 1–6, 2015.

[102] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, Berkeley, CA, USA, 2011. USENIX Association.

[103] Ariana Ramos. Aggregators and retailers in electricity markets: Roles and conflicts. *Deliverable 8.5 Energy Storage Deployment Handbook, STORY H2020 Project*, 2020.

[104] Day-ahead market high level design. *Independent Electricity System Operator*, 2019.

[105] International Energy Agency (IEA). Heat pumps, 2021.

[106] Yuttana Kongjeen, Wannawit Junlakan, Krischonme Bhumkittipich, and Mithulananthan Nadarajah. Estimation of the quick charging station for electric vehicles based on location and population density data. *International Journal of Intelligent Engineering and Systems*, 11:233–241, 06 2018.

[107] Ashok D. Belegundu and Tirupathi R. Chandrupatla. *Optimization Concepts and Applications in Engineering*. Cambridge University Press, 2 edition, 2011.

[108] Linjun He, Hisao Ishibuchi, Anupam Trivedi, Handing Wang, Yang Nan, and Dipti Srinivasan. A survey of normalization methods in multiobjective evolutionary algorithms. *IEEE Trans. on Evolutionary Computation*, pages 1–1, 2021.

[109] A new scalarization method for finding the efficient frontier in non-convex multiobjective problems. *Applied Mathematical Modelling*, 39(23):7483–7498, 2015.

[110] Mohamed R. Hamouda, Mohammed E. Nassar, and M. M. A. Salama. A novel energy trading framework using adapted blockchain technology. *IEEE Transactions on Smart Grid*, 12(3):2165–2175, 2021.

[111] Federal Highway Administration. 2017 National Household Travel Survey.

[112] BIPM, IEC, IFCC, ILAC, ISO, IUPAC, IUPAP, and OIML. Evaluation of measurement data: Guide to the expression of uncertainty in measurement, 2008.

[113] W. Liu, Q. Wu, F. Wen, and J. Ostergaard. Day-ahead congestion management in distribution systems through household demand response and distribution congestion prices. *IEEE Transactions on Smart Grid*, 5(6), Nov 2014.

[114] Tassos Dimitriou and Mohamad Awad. Secure and scalable aggregation in the smart grid resilient against malicious entities. *Ad Hoc Networks*, 50, 06 2016.

[115] Lizhi Xiong, Wenhao Zhou, Zhihua Xia, Qi Gu, and Jian Weng. Efficient privacy-preserving computation based on additive secret sharing. *Cryptography and Security*, 2021.

[116] Yujuan Gu, Jun Xie, Xingying Chen, Kun Yu, Zhenyu Chen, and Zuofeng Li. Dynamic tariff method for congestion management in distribution networks. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–6, 2017.

[117] Shaojun Huang, Qiuwei Wu, Mohammad Shahidehpour, and Zhaoxin liu. Dynamic power tariff for congestion management in distribution networks. *IEEE Transactions on Smart Grid*, 10(2):2148–2157, 2019.

[118] M. R. Sarker, M. A. Ortega-Vazquez, and D. S. Kirschen. Optimal coordination and scheduling of demand response via monetary incentives. *IEEE Transactions on Smart Grid*, 6(3):1341–1352, 2015.

[119] ARichard S. Sutton and Andrew G. Barto. *2Reinforcement Learning: An Introduction*. The MIT Press, 2014.

[120] Yuanzheng Li, Guokai Hao, Yun Liu, Yaowen Yu, Zhixian Ni, and Yong Zhao. Many-objective distribution network reconfiguration via deep reinforcement learning assisted optimization algorithm. *IEEE Transactions on Power Delivery*, 37(3):2230–2244, 2022.

[121] Yuanqi Gao, Wei Wang, Jie Shi, and Nanpeng Yu. Batch-constrained reinforcement learning for dynamic distribution network reconfiguration. *IEEE Transactions on Smart Grid*, 11(6):5357–5369, 2020.

[122] Shahab Bahrami, Yu Christine Chen, and Vincent W. S. Wong. Deep reinforcement learning for direct load control in distribution networks. In *2020 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–5, 2020.

[123] Xianzhuo Sun and Jing Qiu. A customized voltage control strategy for electric vehicles in distribution networks with reinforcement learning method. *IEEE Transactions on Industrial Informatics*, 17(10):6852–6863, 2021.

[124] Timothy P. Lillicrap, Jonathan J. Hunt, Alexander Pritzel, Nicolas Heess, Tom Erez, Yuval Tassa, David Silver, and Daan Wierstra. Continuous control with deep reinforcement learning. In Yoshua Bengio and Yann LeCun, editors, *International Conference on Learning Representations*, 2016.

[125] Oded Goldreich. *General Cryptographic Protocols*, volume II, page 615–634. Cambridge University Press, 2009.

[126] Morten Dahl, Valerio Pastro, and Mathieu Poumeyrol. Private data aggregation of a budget. *IACR Cryptology*, 2017.

[127] Qiongxiu Li, Ignacio Cascudo, and Mads Graesbøll Christensen. Privacy-preserving distributed average consensus based on additive secret sharing. In *2019 27th European Signal Processing Conference (EUSIPCO)*, pages 1–5, 2019.

[128] Maria J.P. Peixoto and Akramul Azim. Using time-correlated noise to encourage exploration and improve autonomous agents performance in reinforcement learning. *Procedia Computer Science*, 191:85–92, 2021.

[129] Elham Akhavan Rezai, Mohamed Shaaban, Ehab El-Saadany, and Fakhry Karray. Demand response through interactive incorporation of plug-in electric vehicles. In *2015 IEEE Power Energy Society General Meeting*, pages 1–5, 2015.

[130] Diederik P. Kingma and Jimmy Ba. Adam: A method for stochastic optimization. In *3rd International Conference on Learning Representations (ICLR)*, 2017.

[131] Fadi Elghitani and Ehab F El-Saadany. Efficient assignment of electric vehicles to charging stations. *IEEE Transactions on Smart Grid*, 12(1):761–773, 2020.

[132] Michael J Neely. Stochastic network optimization with application to communication and queueing systems. *Synthesis Lectures on Communication Networks*, 3(1):1–211, 2010.

[133] B. Chen, K. L. Butler-Purry, and D. Kundur. Impact analysis of transient stability due to cyber attack on facts devices. In *NAPS*, pages 1–6, 2013.

[134] Xuecheng Li, Yue Xiang, Lin Lyu, Chenlin Ji, Qian Zhang, Fei Teng, and Youbo Liu. Price incentive-based charging navigation strategy for electric vehicles. *IEEE Transactions on Industry Applications*, 56:5762–5774, 2020.

[135] Hongcai Zhang, Scott J. Moura, Zechun Hu, and Yonghua Song. PEV fast-charging station siting and sizing on coupled transportation and power networks. *IEEE Transactions on Smart Grid*, 9(4):2595–2605, 2018.

[136] Seyed Nasrollah Hashemian, Mohammad Amin Latify, and G. Reza Yousefi. PEV fast-charging station sizing and placement in coupled transportation-distribution networks considering power line conditioning capability. *IEEE Transactions on Smart Grid*, 11(6):4773–4783, 2020.

[137] Mahnoosh Alizadeh, Hoi-To Wai, Mainak Chowdhury, Andrea Goldsmith, Anna Scaglione, and Tara Javidi. Optimal pricing to manage electric vehicles in coupled power and transportation networks. *IEEE Transactions on Control of Network Systems*, 4(4):863–875, 2017.

[138] Jingwei Xiong, Kuilin Zhang, Yi Guo, and Wencong Su. Investigate the impacts of PEV charging facilities on integrated electric distribution system and electrified transportation system. *IEEE Transactions on Transportation Electrification*, 1(2):178–187, 2015.

[139] Dhaou Said and Hussein T. Mouftah. A novel electric vehicles charging/discharging management protocol based on queuing model. *IEEE Transactions on Intelligent Vehicles*, 5(1):100–111, 2020.

[140] Jesus Elmer Contreras-Ocaña, Mushfiqur R. Sarker, and Miguel Ortega-Vazquez. Decentralized coordination of a building manager and an electric vehicle aggregator. *IEEE Trans. on Smart Grid*, 9:2625–2637, 2018.

[141] R.P. Harvey. The decomposition principle for linear programs. *International Journal of Computer Mathematics*, 1:20–35, 1964.

[142] Visvakumar Aravinthan and Ward Jewell. Controlled electric vehicle charging for mitigating impacts on distribution assets. *IEEE Transactions on Smart Grid*, 6(2):999–1009, 2015.

[143] Kevin Harnett, Brendan Harris, Daniel Chin, and Graham Watso. Doe/dhs/dot volpe technical meeting on electric vehicle and charging station cybersecurity report. Technical report, 2018.

[144] Ben Anderson. Securing vehicle charging infrastructure. Technical report, 2021.

[145] Devin Reeh, Francisco Cruz Tapia, Yu-Wei Chung, Behnam Khaki, Chicheng Chu, and Rajit Gadh. Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats. In *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*, pages 1–6, 2019.

[146] S. Ahmed and Fouad. M. Dow. Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems. In *2016 4th International Conference on Control Engineering  Information Technology (CEIT)*, pages 1–5, 2016.

[147] Seong Ile Jeong and DaeHyun Choi. Electric vehicle user data-induced cyber attack on electric vehicle charging station. *IEEE Access*, 10:55856–55867, 2022.

[148] Samrat Acharya, Yury Dvorkin, and Ramesh Karri. Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable? *IEEE Transactions on Smart Grid*, 11(6):5099–5113, 2020.

[149] Christian Hille and Manuel Allhoff. EV charging: Mapping out the cyber security threats and solutions for grids and charging infrastructure. *UtiliNet Europe*, May 2018.

[150] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. In *USENIX Security Symposium*, 2018.

[151] Adrian Dabrowski, Johanna Ullrich, and Edgar R. Weippl. Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well. *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017.

[152] Francesco Bullo, Emilio Frazzoli, Marco Pavone, Ketan Savla, and Stephen L. Smith. Dynamic vehicle routing for robotic systems. *Proceedings of the IEEE*, 99(9):1482–1504, 2011.

[153] Pengwei Du and Ning Lu. Appliance commitment for household load scheduling. *IEEE Transactions on Smart Grid*, 2.

[154] Lucas Terada, Juan López, Nataly Arias, Marcos Rider, Luiz Pereira da Silva, and Eduardo Lacusta Junior. EV charging simulator for public infrastructure considering smart charging and price policies. In *IEEE PES Innovative Smart Grid Technologies Conference*, pages 1–5, 2021.

[155] Jinghuan Ma, He Henry Chen, Lingyang Song, and Yonghui Li. Residential load scheduling in smart grid: A cost efficiency perspective. *IEEE Transactions on Smart Grid*, 7(2):771–784, 2016.

[156] Omar Alrumayh and Kankar Bhattacharya. Flexibility of residential loads for demand response provisions in smart grid. In *IEEE PESGM*, 2020.

[157] Benoit Mattlet and J. Claude Maun. Assessing the benefits for the distribution system of a scheduling of flexible residential loads. In *IEEE ENERGYCON*, pages 1–6, 2016.

[158] D.C. Montgomery, E.A. Peck, and G.G. Vining. *Introduction to Linear Regression Analysis*. Wiley, 2013.

[159] M. Vai, B. Nahill, J. Kramer, M. Geis, D. Utin, D. Whelihan, and R. Khazan. Secure architecture for embedded systems. In *2015 IEEE High Performance Extreme Computing Conference (HPEC)*, pages 1–5, Sep. 2015.

[160] P. Koonce, Lee Rodegerdts, Kevin Lee, Shaun Quayle, Scott Beaird, Cade Braud, Jim Bonneson, Phil Tarnoff, and Tom Urbanik. Traffic signal timing manual. Technical report, 2008.

[161] Yi-Yun Chu and Kai-Hao Liu. Iot in vehicle presence detection of smart parking system. In *2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*, pages 56–59, 2020.

[162] Manickam Ramasamy, Sunil Govinda Solanki, Elango Natarajan, and Tham Mun Keat. Iot based smart parking system for large parking lot. In *2018 IEEE 4th International Symposium in Robotics and Manufacturing Automation (ROMA)*, pages 1–4, 2018.