To the Graduate Council:

I am submitting herewith a dissertation written by Mojtaba Dezvarei entitled "Resiliency of Power Systems in the Cyber Layer: Application to Load Forecasting and Security Assessment." I have examined the final paper copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Electrical Engineering.

_____

Seddik M. Djouadi, Kevin Tomsovic, Major Professor

We have read this dissertation
and recommend its acceptance:

_____

Jinyuan Stella Sun

_____

Hugh Medal

Accepted for the Council:

_____

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

To the Graduate Council:
I am submitting herewith a dissertation written by Mojtaba Dezvarei entitled "Resiliency of Power Systems in the Cyber Layer: Application to Load Forecasting and Security Assessment." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Electrical Engineering.

Seddik M. Djouadi, Kevin Tomsovic, Major Professor

We have read this dissertation
and recommend its acceptance:

Jinyuan Stella Sun

Hugh Medal

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Resiliency of Power Systems in the Cyber Layer: Application to Load Forecasting and Security Assessment

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Mojtaba Dezvarei

August 2023

© by Mojtaba Dezvarei, 2023
All Rights Reserved.

To my love

Acknowledgements

I would like to express my deepest appreciation and gratitude to my academic co-advisors, Dr. Seddik Djouadi and Dr. Kevin Tomsovic, for their time, dedication, and support during my study. I am thankful for the opportunity to teach me how to think creatively and practically during my Ph.D. program. Their warmhearted, trustworthiness, and encouragement will always keep in my mind.

My acknowledgments also go to my committee, Dr. Jinyuan Stella Sun and Dr. Hugh Medal, for their support, guidance, and insightful comments. Undoubtedly their input brought more value to this work. I also would like to thank Dr. Lee D. Han and Dr. Hairong Qi for all the conversations that broadened the horizon of my thoughts. I am also thankful to CURENT for allowing me to learn from professionals collaboratively. In addition, I would like to thank my colleagues and friends for getting along with me either in person or virtually; it is very worth having you all around me.

Last but not least, I would like to express my gratitude to my family for their support, and more importantly, to my love, for her unconditional kindness, love, and support. Indeed without her, this journey would have never started and come to an end.

Wonder is the beginning of wisdom.

–Socrates

Abstract

Integrating sensors, actuators, and communication infrastructure in the electrical grid creates a smart grid, known as a cyber-physical system (CPS), which combines the physical framework with a cyber layer. The cyber layer is crucial as it houses the decision-making responsible for reliable operation. However, the complexity of the physical layers, due partly to the deployment of integrated battery resources (IBRs), and the cyber layer itself, introduces challenges such as reliance on measurement quality and vulnerability to data corruption from cyber threats. These challenges result in uncertainties in the CPS framework, emphasizing the need for accurate and robust responses from the power grid's cyber layer through cyber resiliency. To establish resilient responses, the concept of resiliency and its framework are defined in the context of CPS. Among the functions ensuring the performance and reliability of the power grid, two specific tasks, namely short-term load forecasting (STLF) and security assessment (SA), are examined.

STLF, used for scheduling and assessing power system security, faces challenges with misleading forecasting, particularly anomalies caused by temperature data. To address this, STLF is explored. Similarity measures and a distributed mining of lag correlation approach are utilized to analyze load behavior and detect anomalies. This approach incorporates physical characteristics, making it difficult for malicious actions. The effectiveness of this method is validated using historical load data from the Electric Reliability Council of Texas (ERCOT).

SA evaluates the risk of disruptions in the system operating continuously. Given operational uncertainties and measurement challenges, developing an efficient SA model capable of capturing most scenarios is crucial. Representing the SA task in a graph format enables leveraging connectivity and topological information obtained through centrality measures. A resilient model based on graph neural networks (GNN) is constructed to aggregate data across the grid. The framework's efficacy is demonstrated on the IEEE 118-bus system for voltage stability SA (VSSA) task under various operating points and stress conditions. Comparative analysis, including the evaluation model capacity, highlights the superiority of the proposed method over a neural network approach.

Table of Contents

1 Introduction **1**

1.1 Background . . . 1

1.2 Motivations . . . 3

1.3 Objectives . . . 6

1.4 Previous Works . . . 8

1.5 Summary of Contributions . . . 11

1.6 Dissertation Outline . . . 13

2 Resiliency Concept and Framework **15**

2.1 Background . . . 15

2.2 Towards Resiliency . . . 19

2.2.1 Resiliency Definition . . . 19

2.2.2 Resilience vs. System Characteristics . . . 20

2.2.3 Cybersecurity as Cyber Resilience . . . 22

2.2.4 Resilient Framework . . . 24

2.2.5 Verification of System for Resiliency . . . 27

2.2.6 Resiliency Study Procedure . . . 29

2.2.7 Resilience Metric . . . 31

2.3 Resiliency Loop . . . 36

2.4 Resiliency Response in Power Grid . . . 38

2.4.1 Hardening Power Grid . . . 38

2.4.2 Microgrid Supported Grid . . . 40
2.4.3 Grid Partitioning . . . 40
2.4.4 Cyber Resilience . . . 41
2.5 Discussion on Power Grid Resiliency . . . 42
2.5.1 Definition . . . 42
2.5.2 Structure . . . 42
2.5.3 Metrics . . . 43
2.5.4 Response . . . 43
2.6 Summary . . . 44

3 Cybersecurity in Load Forecasting 45
3.1 Introduction . . . 46
3.1.1 Short-term Load Forecasting Modeling . . . 47
3.1.2 Vulnerability of Independent Variables . . . 49
3.2 Threat Model . . . 50
3.3 Problem Statement . . . 51
3.4 Exploring the Constraints . . . 52
3.5 Similarity Measure . . . 54
3.5.1 Shape-based Approach . . . 54
3.5.2 Feature-based Approach . . . 56
3.5.3 Simulation Framework . . . 62
3.5.4 Results . . . 64
3.6 Lag Relation Analysis . . . 70
3.6.1 Lag Correlation . . . 72
3.6.2 Simulation Framework . . . 73
3.6.3 Results . . . 75
3.7 Summary . . . 78

4 Graph-based Learning for Security Assessment 80
4.1 Introduction . . . 81

4.2 Problem Statement . . . 87
4.3 The Proposed Framework for the SA . . . 91
4.3.1 Feature Generator Engine . . . 91
4.3.2 Learning Model: Graph Neural Network . . . 95
4.4 Simulation Results . . . 101
4.4.1 Data Generation . . . 101
4.4.2 GCN Model Configuration . . . 105
4.4.3 Optimization Set up . . . 106
4.4.4 Performance Evaluation Metric . . . 106
4.4.5 Case Studies Results . . . 107
4.5 Model Capacity Analysis . . . 111
4.5.1 Unseen Data . . . 111
4.5.2 Input Variability . . . 113
4.6 Discussion and Summary . . . 115
4.6.1 Do the topological features boost performance? . . . 115
4.6.2 Training time . . . 116
4.6.3 On a GNN Universal Framework for the SA . . . 116

5 Conclusion and Future Work **118**
5.1 Conclusion . . . 118
5.2 Future Work . . . 120

Bibliography **122**

Appendix **144**
A Graph Theory Preliminaries . . . 144
B Complex Network . . . 147
B.1 Random Graph . . . 148
B.2 Small-World Networks . . . 149
B.3 Scale-Free Networks . . . 149

Vita **152**

List of Tables

3.1 Different L_p distances Fu (2011). 55

3.2 Lookup table of the `dist()` function for $\alpha = 3$. 61

3.3 Similarity measures results. 67

3.4 Percentage variation of SM methods for Intra-day perturbations. . . . 71

3.5 Lag correlation results for historical data. 77

3.6 Lag correlation results for perturbed temperature data based on MLR model. 77

4.1 Confusion matrix. 108

4.2 Base dataset performance evaluation: average value over ten runs. . . 109

4.3 Robustness analysis results. 112

4.4 Variable sensitivity results. 114

B.1 Graph models comparison. 151

List of Figures

1.1 Critical infrastructure sectors. 2
1.2 Examples of power grid dependencies Rinaldi et al. (2001). 4
1.3 FY 2014 incidents reported by ICS-CERT; 245 total incidents. 7
1.4 A CPS illustration of the thesis goal. 7

2.1 The Cyber threat to the electricity sector. Source: Canadian Centre for Cyber Security, Cyber Threat Bulletin. 23
2.2 Resilience performance curve. 25
2.3 Resilience cycle and components. 28
2.4 Disruption category. 30
2.5 Resiliency analysis procedure. 30
2.6 Proposed resilient loop diagram. 39

3.1 Water pipeline flow constraint. 53
3.2 ERCOT weather-based station map with a representation of separated stations. 53
3.3 Distance between two time series. 55
3.4 An example for PPA representation of a time series. 59
3.5 Word presentation in the SAX procedure. 61
3.6 SAX presentation of a time series. 61
3.7 Summer 2020 ERCOT load: West and FarWest stations. 63
3.8 Load vs. temperature curve. 63

3.9 West and FarWest stations load correlation. 63
3.10 MLR models performance: MAE and adjusted R^2. 65
3.11 Variation of SM indices for different SNR cases. 69
3.12 Lagged correlation over time series. 71
3.13 5-minute data: the right figure is historical load data, and the left figure is interpolated temperature from ASOS. 74
3.14 MLR outputs for 5-minute data. 76

4.1 A typical voltage recovery curve. 83
4.2 An illustration of the P-V curve method. 83
4.3 A full security nomogram Morison et al. (2004). 85
4.4 General GNN framework for the security assessment. 90
4.5 Procedure of the proposed GNN-based SA model. 92
4.6 Illustration of various centrality measures Ortiz-Arroyo (2010). 96
4.7 Embedding the feature vector. 96
4.8 General GNN framework for classification problem. 98
4.9 Computational graph of node A: information aggregation from two hops away. 98
4.10 Single line diagram of the IEEE 118-Bus system. 103
4.11 Scaled estimated net load data for 2020 CAISO Duck Curve. 104
4.12 F1-score and loss curve for MLP and GCN models. 108
4.13 Bar graph of results for unseen data. 112
4.14 General state estimation architecture: the dash line blocks are depicted to indicate the procedure for sensitivity analysis of GCN-based SA model. 114

A.1 A simple undirected graph. 146
B.1 Graph models shape and degree distribution: a sample network with 300 nodes. 151

List of Algorithms

1 Procedure 1: Data Generation. 104

Acronym

APIs application programming interfaces

AI artificial intelligence

ANN artificial NN

ASOS automated surface observing systems

ARMA autoregressive–moving-average

BDD bad data detection

BES bulk-electric system

CPD change point detection

CNN convolutional neural network

CISs critical infrastructure sectors

CAIDI customer average interruption duration index

CPS cyber-physical system

DT decision tree

DOE Department of Energy

DL deep learning

DER distributed energy resource

DSA dynamic security assessment

ERCOT Electric Reliability Council of Texas

EMS energy management system

FDI false data injection

FTC fault Tolerant Control

FERC Federal Energy Regulatory Commission

GCN graph convolutional network

GNN graph neural network

HIHP high-impact, high-probability

HILP high-impact, low-probability

IEC International Electronically Commission

IBRs inverter-based resources

LSE least squares error

LQR linear quadratic regulator

LF load forecasting

LSEs load serving entities

LMP locational marginal price

ML machine learning

MAE mean absolute error

MGs microgrids

MLP multi layer perception

MLR multiple linear regression

NN neural Network

NERC North American Reliability Corporation

OPF optimal power flow

PMUs phasor measurement units

PV photovoltaic

PAA piecewise aggregate approximation

PCA principal component analysis

PSSE Power System Simulator for Engineering

RNNs recurrent neural networks

SA security assessment

STLF short-term load forecasting

SE state estimation

SSA static security assessment

SCADA supervisory control and data acquisition

SVM support vector machine

SAX symbolic aggregate approXimation

SAIDI system average interruption duration index

SAIFI system average interruption frequency index

SoS system of systems

VSSA voltage static security assessment

WECC Western Electricity Coordinating Council

Chapter 1

Introduction

1.1 Background

Our society is tightly connected to critical infrastructure sectors (CISs) to carry out multiple functions. The USA Homeland Security has listed sixteen critical infrastructure sectors whose physical or virtual subsystems play a significant role where damage significantly impacts security, economy, national public health, safety, or any combination thereof. Critical infrastructure sectors include energy, chemical, critical manufacturing, food and agriculture, information technology, water, and wastewater. Essential infrastructure sectors are illustrated in Figure 1.1. These systems must maintain acceptable performance during any interruptions caused by fault, attack, and natural disasters Ellinas et al. (2015). Among the CISs, the energy sector, including electricity, oil, and natural gas segments, is a core sector, as other sectors' performance relies on its functionality. The power grid is a *supported infrastructure*, and natural gas, oil, transportation, telecommunications, and water are *supporting infrastructures*. In the traditional structure and under normal operating conditions, the power grid infrastructure requires its generators' natural gas and petroleum fuels. However, utilizing renewable sources, such as wind and photovoltaic (PV) has been changing the use of non-renewable sources for electric



Figure 1.1: Critical infrastructure sectors.
Source: CISA.gov

generation. Therefore, the electric power infrastructure has many considerations to ensure reliable power delivery to other sectors. There are mainly two ways that connect the infrastructures Rinaldi et al. (2001):

- *Dependency*: A linkage or connection between two infrastructures through which the state of one infrastructure influences or is correlated to the state of the other. The relationship is usually unidirectional; infrastructure A depends on B through the link, but B does not depend on A through the same link. Figure 1.2 shows the electrical grid dependencies.

- *Interdependency*: A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. Infrastructure A depends on B through some links, and B likewise depends on A through other links.

In general, infrastructure systems are analyzed in the content of the interdependencies model due to multiple interconnected infrastructures, the so-called system of systems (SoS). Moreover, interdependencies may be divided into four main classes: physical, cyber, geographic, and logical, and each one has distinct characteristics that are not mutually exclusive Rinaldi et al. (2001).

1.2 Motivations

The power grid has been geographically distributed on a large scale to provide electricity for residential, commercial, and industrial customers, and advancement in the sensor, measurement, actuator, and communication technology results in an intelligent grid with many cyber connections acting as a cyber layer. This makes the grid a cyber-physical system (CPS), resulting in more flexibility and functionality at the cost-grown complexity. Besides, the power grid is becoming a leading core in the energy sector due to the demand for zero-carbon emissions for climate change. The vital role of the power grid in the CISs, and its structural complexity call for a

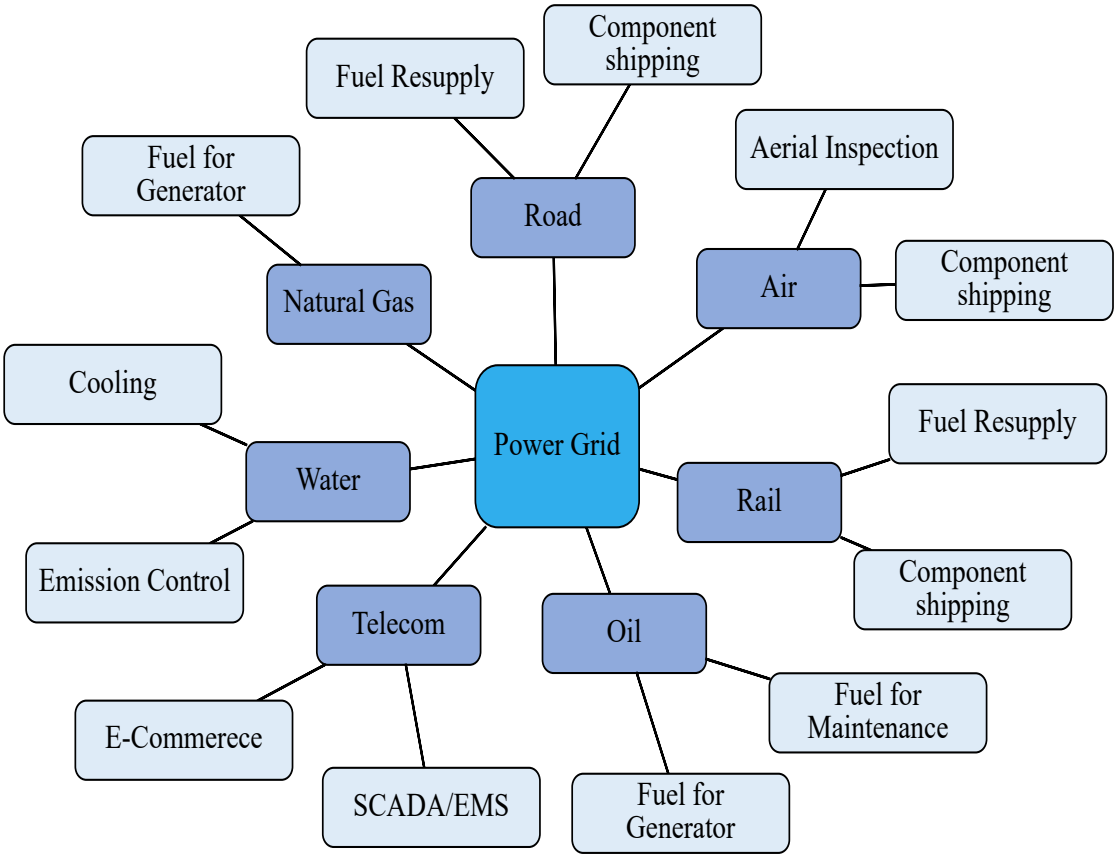


Figure 1.2: Examples of power grid dependencies Rinaldi et al. (2001).

reliable power grid to deliver electricity to all customers. Also, it requires maintaining performance after significant incidents to reduce the debilitating impact on physical or economic security, public health, or safety.

Adding a cyber layer in the power grid has built a valuable framework to carefully monitor and effectively operate the grid due to favorable available data across the grid, such as supervisory control and data acquisition (SCADA) architecture or deployment of phasor measurement units (PMUs). Readily exchanged data provides appropriate decision-making software, such as in the energy management system (EMS). However, it brings new challenges related to cybersecurity, data corruption, and false data injection (FDI), for instance. Therefore, the power grid as a CPS faces threats from both physical and cyber layers. Some examples of incidents are:

- Natural disasters: hurricane Sandy in the USA east coast, 2012.
- Physical attack: damaging two substations by gunfire in North Carolina, in the USA, in December 3, 2022
- Cyber attack: hacking into the power grid control center in Ukraine, 2015.

Therefore, the power grid has to be prepared for incidents that may shut down critical energy infrastructure. This concept can be discussed as a *resilient* power grid: not only to be prepared for uncertainties but also delivers more reliable results to maintain system performance. The question here is that the term resilient still needs to be studied for the power society since many system characteristics only partially address a resilient system.

Data-related threats are currently observed regarding the role of data in the decision-making process and the promising result of data-driven approaches. The rapid rise in cyberattacks has been causing concerns throughout the U.S. economy, and the energy sector is no exception Shea (2018). A survey by the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) 2014 shows that among 245 reported cyber incidents in some critical infrastructure, 32% belong to the

energy sector, indicating its cyber vulnerability. A pie chart diagram showing all the reported sectors' incident share is illustrated in Figure 1.3. Although resiliency mostly centers around high-impact, low-probability (HILP) events, such as natural disasters, the emerging threats due to cyberspace and its underlying backbone make the system vulnerable to a wide range of risks from physical and cyber threats and hazards. In fact, cyberattacks have the potential to cause significant harm by disrupting electricity systems; however, their impact has been relatively confined thus far. For instance, Fischer et al. (2018) provided a list of potential cyberattack scenarios in the electricity system, such as compromised control room SCADA and compromised equipment through the supply chain vulnerabilities.

Considering the standard EMS functions discussed by Giri et al. (2012) and the primal role of decision-making in the electrical system, this thesis first provides a comprehensive review of the notion of resiliency. Subsequently, the thesis will focus on the resiliency of load forecasting (LF) and security enhancement functions.

1.3 Objectives

The importance of the power grid in the CISs, the application of a data-driven model for the decision-making process, and the existence of many threats, particularly cyber-threats, motivate this dissertation to investigate the resiliency of the power grid in the security aspect in two main folds as shown in Figure 1.4:

- *Cyber security*: Providing a defense mechanism against cyber threat in the data decision-making process. One of the imperative decision-making in the EMS is load forecasting. Load forecasting is an essential task that supports utilities to schedule generating sufficient power for balancing supply and demand and can become an attractive target for cyber attacks. As the model relies on input variables, altering them can result in significant forecast errors and lead erroneous decisions resulting in operational damages, market instability, safety,

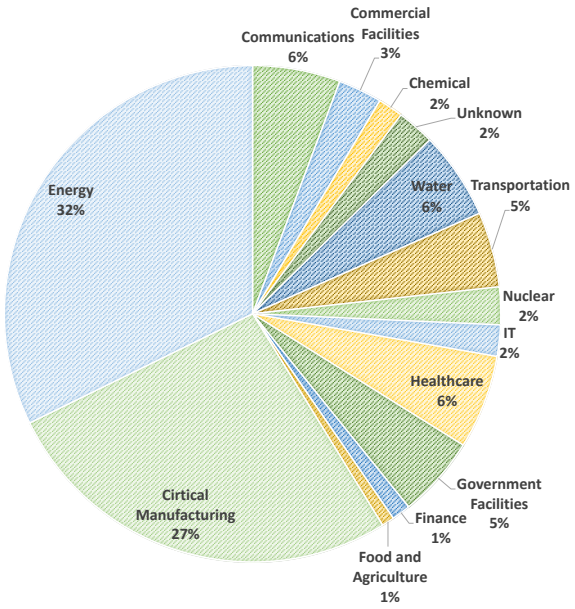


Figure 1.3: FY 2014 incidents reported by ICS-CERT; 245 total incidents.

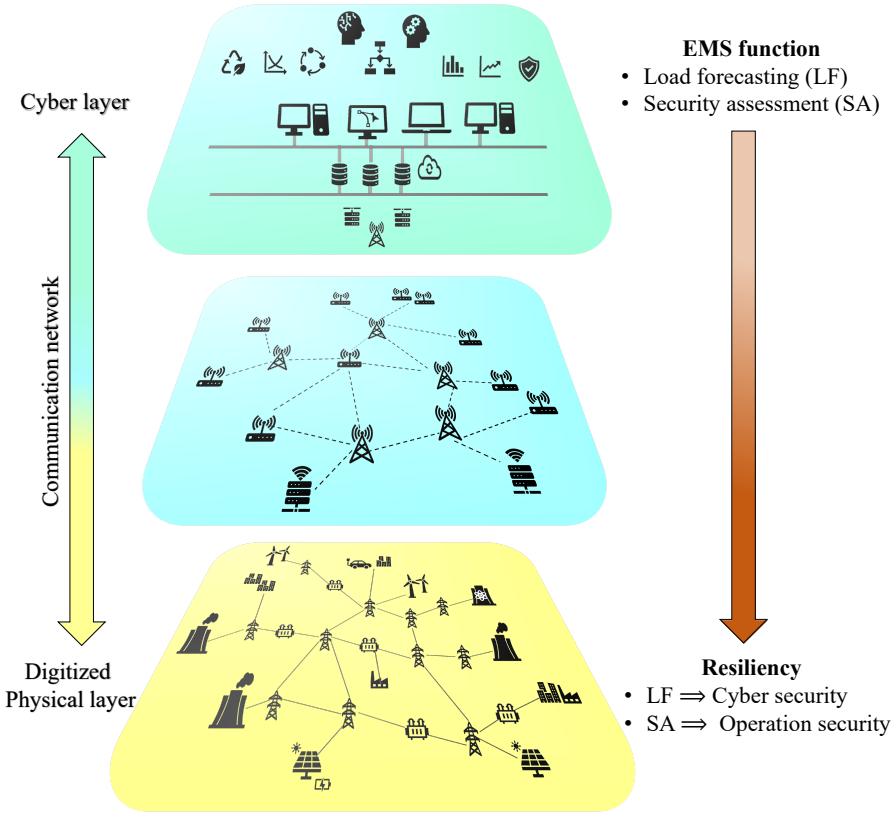


Figure 1.4: A CPS illustration of the thesis goal.

and security violation. Therefore, load forecasting application needs to be cyber-secure to avoid the onset of disastrous consequences.

- *Operational security*: Exploiting a data-driven model to capture more uncertainties due to the power grid's complexity in the form of CPS and CIS. Another vital element in the EMS is the security assessment (SA) function which determines the safe operation in a normal situation and some contingencies scenarios according to the reliability criteria. There are many sources of uncertainty in the power grid operation, such as non-linearity, vast geographical exposure, inverter-based resources (IBRs) deployment, measurement error, and so on. The security classification problem involves a model that captures the operational uncertainties as much as possible to provide more reliable results. Since the SA result will initiate remedial actions, misclassification can bring about instability issues. Hence, the SA model should be cable of supporting uncertainties in the behavior of the grid and input data to offer an accurate and precise assessment of the secure operation of the power grid.

Given the above concerns, this work aims to investigate the resiliency of data-driven decision-making elements of the power grid to guarantee the response to uncertain and alerted input data.

1.4 Previous Works

Before analyzing the resiliency of the power grid decision-maker functions, it necessitates looking at the concept and framework of resiliency through the literature. The resiliency notion was first discussed in Holling (1973) to address equilibrium in ecological systems. Considering the environmental systems' complex behavior that makes it hard to analyze, researchers from other domains started thinking of resiliency and examining its elements, such as in materials science Dessavre et al. (2016), biology Feder et al. (2019), sustainability science Xu et al. (2015), and critical infrastructure

system Rehak et al. (2019). Resiliency as a conceptual term in practice and its vast growing usage in various fields compel researchers to study the concept depending on the subject. Although the power grid is involved with many potential catastrophic incidents interrupting its performance, the analysis of resiliency in the power grid is still new. Although many high-quality works consider resiliency by offering remedial actions after incidents of extreme weather conditions and physical attacks Liu et al. (2016a); Panteli et al. (2016); Nezamoddini et al. (2017), there is a handful of attempts to quantify a resilient framework in the power grid, such as the IEEE PES Task Force: Stanković et al. (2022).

That being said, the resiliency of the power grid functional elements can be further investigated for the cyber layer. The significance of cyber-infrastructure security in conjunction with power application security to prevent, mitigate, and tolerate malfunction is evident Nezamoddini et al. (2017). That is the fundamentals involved with data as a data-driven model in decision-making, such as short-term load forecasting (STLF) and security assessment. Since the performance of these applications is evaluated based on the used model and input data, there can always be room to enhance their capacity, such as, detecting the altered data in the STLF and providing a model capturing uncertain and most information across the system.

The STLF function is to forecast load ranging from the next hour to one week for scheduling purposes, assessing the security of the power system at a future time point, where inaccurate forecasting results in erroneous decisions, such as wrong unit commitment scheduling impacting the cost and reliability of the system Hobbs et al. (1999). The STLF model has become a mature technology due to the massive efforts of utility experts and researchers to derive the most accurate model by using statistical analysis such as regression and autoregressive–moving-average (ARMA) models Chakhchoukh et al. (2010); Hubele and Cheng (1990), and artificial intelligence (AI) approaches such as neural network Bakirtzis et al. (1996), long-term short memory Agrawal et al. (2018). However, vulnerabilities of STLF through false input data need to be analyzed. Data poising Liang et al. (2019), and

integrity attacks Luo et al. (2018) could effectively corrupt various STLF models. In contrast, the task addresses anomaly detection methods, such as descriptive analytic-based methods to protect the forecasting process against cyberattacks on essential data Cui et al. (2019a), and machine learning (ML)-based anomaly detection Yue et al. (2019). Although various methods could effectively capture anomalies in data in the EMS functions, there is yet a scope to fool the result by bypassing the detection schemes, such as in state estimation application Yue et al. (2019). In the STLF application, Chen et al. (2019b) explores the impact of the adversarial attack. The results indicate the possibility of malicious action to over- or under-forecast, leading to a wrong scheduling plan. Hence, it is important to determine a defense mechanism encoded in the STLF, i.e., making it difficult for the attackers to achieve their malicious goal.

The security assessment determines whether a power system can meet specified reliability and security criteria in both transient and steady-state time frames for all credible contingencies Morison et al. (2004). Because of the inherent characteristics of the power grid mentioned above, it is an intricate task to define the secure status of the power grid analytically; therefore, data-driven models are used to assess security transferring to a classification problem resulting in very accurate results. Electrical variables, such as active/reactive line flow, voltage magnitude, phase, bus active/reactive power, etc., are given to the model to classify the operational security of the power grid. It is beneficial to know the topological information grid. Representing the power grid by a graph offers complex system analysis Boccaletti et al. (2006a) via statistical tools to understand the salient properties of the power grid, such as vulnerability analysis Holmgren (2006); Monfared et al. (2014); Hines et al. (2010a), structural modeling Kim et al. (2017), and analysis of blackouts in cascading failure Dobson et al. (2007). Application of the concept of the complex network in the power grid is reviewed in Pagani and Aiello (2013). An introduction to complex networks is given in Appendix B. Although the importance of topological information has been studied, the lack of using topological knowledge in decision-making, such as

the SA, is seen, let alone using a graph as input data. The SA models can be neural Network (NN) Niebur and Germond (1992); Sittithumwat and Tomsovic (2002a), decision tree (DT) Bugaje et al. (2021), support vector machine (SVM) Kalyani and Swarup (2010a), and a deep learning (DL) framework Arteaga et al. (2019a). All these models can only take the grid structure of data, i.e., no consideration of relationships among the variables in a sample, and they are in the form of rows, columns, tables, or image shapes. Therefore, graph input data encapsulating the whole information of the power grid across the buses with branch (edge) connection can be examined to support a SA model. Since the graph data format provides topological information insight, the model based on graph format input can capture more details. It may result in a high-capacity SA model that delivers a resilient framework for data and case study uncertainties.

1.5 Summary of Contributions

Given the above background and objectives, the contributions of this dissertation are summarized as follows:

- *Review of resiliency concept, definition, and framework through various fields of study for the benefit of power system society.* The need for resiliency in the system design and operation is a new trend leading us to more precise definitions. Therefore, an analysis of resiliency geared towards the power system is provided. Through studying resiliency in all sectors, the concept and structure of a resilient system are clarified, such as definition, significant functions, indices, and resiliency response. Moreover, the significance of addressing the resiliency response within the cyber layer of CPS is discussed. Furthermore, we examine potential gaps in the current methods applied to the electrical grid, intending to construct a resilient loop.

- *Exploring the physical-based constraints in the STLF application against a cyberattack, challenging the attacker threat model.* Considering the vital protection of the STLF from cyberattacks, for the first time, the STLF is examined through the lens of physical characteristics to identify constraints. Instead of providing a detection scheme, the physical-based restrictions are proposed to be added to the attacker's problem to enter them into a burdensome task for a successful malicious action. Then, the STLF is formulated as a weather-based process to analyze the relationship between each zone through similarity measures to identify constraints. Different methods, such as shape-based and feature-based, are compared to find an effective way of applying the methods to historical load data. Based on the framework provided, an additional analysis is conducted to explore constraints by examining the correlation between lagged load stations and their corresponding variations.

- *Graph-based learning for the security assessment using electrical and topological information results in a high-capacity model.* Despite the typical use of electrical variables for security classification, topological information obtained by graph centrality measures is proposed to add to the feature database. The system is presented as a graph to extract the topological importance of the power grid after defined scenarios. A graph neural network (GNN) is then proposed for the SA model to benefit from shared information across the power grid, such as features related to the bus with its connected neighbors. Also, a sequential model as a traditional NN model is trained to compare with the proposed model. A voltage static security assessment is considered for the security analysis simulation with a statement about using the proposed approach for dynamic security assessment (DSA) and other variables of interest, such as frequency. Additionally, the performance of the proposed model is verified through robustness and sensitivity analysis.

1.6 Dissertation Outline

This dissertation is organized as follows.

In chapter 2, a review of the resiliency concepts from various fields is presented to provide a clear vision for the power society. As many characteristics can indicate the system's capability defined by standards, an analogy between resiliency and other system features is drawn. Then, the introduced elements in the literature to have a resilient framework are reviewed and discussed. Considering the essential role of data and data-driven models in the operation of CISs, we also delve into the need for cyber resiliency. Acknowledging the vital role of the power grid in the CISs, the proposed resiliency approaches are reviewed, followed by a discussion of the existing gap in the tools and analysis. Furthermore, a control loop scheme is proposed to equip the resiliency in the system analysis.

In chapter 3, a physics-based constraint on the STLF model is explored, as attackers can easily bypass the physics rules. This forces the attackers to satisfy the constraints for successful malicious action, such as stealth. This may challenge their threat capability. In this fashion, first, the STLF is formulated based on a set of stations; that is, the STLF for an area is observed as a set of sub-area defined by weather stations. Then, statistical analysis between the station's time series is studied to derive an index indicating the attack, such as shape-based and feature-based methods in the similarity measure analysis. Furthermore, we conduct a distributed lag correlation analysis among the load stations to create a constraint/monitoring framework that utilizes a short horizon of historical data. This framework aids in detecting potential attacks. Temperature data is chosen to be attacked as it is one of the most influential variables for load forecasting and offers a simple direction for false data injection. The proposed approach is then validated for historical data for the Electric Reliability Council of Texas (ERCOT), ensuring its effectiveness.

In chapter 4, a new SA model based on the GNN model is analyzed to benefit distributed information across the power grid for voltage static security assessment

(VSSA), i.e., classifying the security of operation points after defined contingency in the steady state according to voltage reliability criteria. Also, due to the importance of topological information on the power grid applied in the vulnerability analysis, the centrality measures adapted to electrical distance are computed and appended to electrical variables to have a rich feature database. After generating various operating points, such as different load profiles, stress conditions by the P-V analysis, and contingency scenarios, the effectiveness of the proposed framework is validated for the IEEE 118-bus system. The performance of the model is then compared to the traditional NN model. Furthermore, we evaluate the performance of the GNN model by subjecting it to various new conditions. This analysis aims to assess the model's capacity to handle different scenarios and conduct a comprehensive sensitivity analysis.

In chapter 5, the results of this dissertation are summarized, and then the future work is discussed.

Chapter 2

Resiliency Concept and Framework

This chapter reviews the concept and framework of resiliency to provide suggestions for the power system application. The rapid development of technology, and critical infrastructure systems, which human life strongly depends on, are becoming more demanding, complex, and holistic. Hence, resilient systems against any disruptive events are crucial in order to maintain system performance. The concept and structure of a resilient system are explained by studying resiliency in all sectors. Additionally, the significance of cyber resilience in CPSs is highlighted, along with a discussion on potential gaps in current approaches to establish a resilient control loop. The primary objective of this chapter is to gather insights and information from existing literature to identify the key characteristics of a resilient system and discuss a tailored framework for power systems.

2.1 Background

Our society is tightly connected to critical infrastructure sectors to carry out multiple functions. The USA Homeland Security listed sixteen critical infrastructure sectors whose physical or virtual subsystems play a significant role where destruction significantly impacts security, economy, national public health, safety, or any combination thereof. Critical infrastructures include energy, chemical, critical manufacturing,

food and agriculture, information technology, water, and wastewater. These systems should maintain acceptable performance during any interruptions caused by fault, attack, and natural disasters Ellinas et al. (2015). Thus, designing and examining these systems is indispensable to maintaining functionality, particularly in disruption.

There are many different approaches to preserving and controlling system performance during disruption and avoiding fatal incidents. A fault Tolerant Control (FTC) scheme can be designed to increase availability and reduce the risk of safety hazardous conditions during component failure by fault diagnosis, automatic condition evaluation, and remedial action after fault detection Blanke et al. (2000). FTC has been studied for over twenty years, emphasizing safety issues since high critical systems' loss produces catastrophic consequences for human lives, safety, and financial costs such as nuclear power plants, aircraft, and satellites Yu and Jiang (2015). Robust control theory is another widely used approach to achieve system performance and stability in the presence of undesired external inputs Zhou et al. (1996). Robust control is also utilized in FTC design as a passive approach due to its incorporation of predefined disturbances and uncertainty in the design stage. So the system can continue operating under a given disturbance.

Resiliency is a recent term related to system performance preservation and recovery. For the first time, Holling introduced resiliency to analyze the behavior of ecological systems Holling (1973). Measurements analysis to determine system persistence and its capability to accept changes in the presence of disturbances can be done by preserving the same state variable. Having resiliency is considered in many studies to identify the system's ability to cope with disruptions. Later, the consequences of Hurricane Katrina showed the need for resiliency more than a protection plan. That is a request for robustness, redundancy, resourcefulness, and rapid response capability Meyer et al. (2006). A framework to achieve resiliency is mandatory due to the essential role of critical infrastructure Vugrin et al. (2010). Analysis of resiliency is also an essential part of the critical infrastructure, such as response to natural disaster Quitana et al. (2020), transportation systems to extreme

events Donovan and Work (2017), and food supply chains to unbalance between demand and response Priya Datta et al. (2007); Craighead et al. (2007). In major disasters, demand for healthcare and public health surges need the healthcare system management to integrate resiliency to ensure robustness and preparedness of the health system Keim (2008); Wulff et al. (2015). An example is the COVID-19 pandemic, which emphasizes the extreme need for the health care system and impacts on the material supply chains Hobbs (2020). Moreover, a vital task remains in other critical infrastructures, such as information technology, chemical plants, and crucial manufacturing Riolli and Savicki (2003); Amaral et al. (2015); Shirali et al. (2012); Borchert and Mattoo (2009); Hu et al. (2008).

Among critical infrastructure, the power grid is one of the integral sectors, as other sectors excessively rely on its performance. Complex and high interdependency of the electric power sector with other lifeline networks, such as telecommunication, water, and natural gas, are evident Phillips et al. (2016). Yet resiliency in the power system is still unexplored. However, valuable studies have suggested different ideas to capture resiliency. The necessity of power grid resiliency is utterly apparent. The main reason is that the power grid is becoming more prominent and smarter, where the adaption of resiliency is more challenging for the high impact of low probability events, such as extreme weather events Panteli and Mancarella (2015). Current research plans to deploy resiliency into the power grid due to climate changes, such as experiencing more weather hazard events that can cause significant outages and blackouts Ton and Wang (2015). That is why investigating power system resiliency through forecasting and modeling natural disasters is required Hoffman et al. (2010); Wang et al. (2015). Microgrid structure may be deployed to improve power grid resiliency in the fashion of probabilistic function of fragility, survivability, and recovery Liu et al. (2016b).

Internal effects between sectors, such as gas pipeline scheduling and transposition for reinforcing the power grid, are other approaches to improve system resiliency Shao et al. (2017). The integrated resilience framework is appropriate for the power grid because of its large and complex structure. Integrated resiliency in design is

an optimization problem where its framework consists of preventive response based on power system outage prediction and present emergency response to deal with demand unbalance after a natural disaster Huang et al. (2017). Refinement of the power grid resiliency is also analyzed in the framework of power grid hardening, digitization, and load restoration strategy Bie et al. (2017). Beyond infrastructure resiliency, Panteli et al. (2017) suggests that operational resiliency is the concept of power grid resiliency. Operational resiliency refers to having a strong response to the system for uninterrupted operation, whereas infrastructure resiliency retains the power grid's physical solidity. It is clear that decent structural resiliency establishes an appropriate operational resiliency.

In addition to natural disaster disruption, such as hurricanes, tornados, wildfires, flooding, hail, etc., the power grid is vulnerable to cyber attacks due to communication networks and advanced metering devices. Therefore, a discussion of the definition of cyber-physical resiliency of the power grid is highly required Arghandeh et al. (2016). In the wide-area power grid, studies about control resiliency of cyber attacks, monitoring, and protection are also demanding Sridhar et al. (2012); Ashok et al. (2017).

Regarding previous studies about the resilient power grid, resiliency's general analysis procedure for other sectors follows a similar approach. First, they must consider a resilient concept and an index alongside the disruption type. Then, evaluation of resiliency either qualitatively or quantitatively is required. Finally, a recovery strategy can be selected to meet specified system requirements after a disruption. That is, the resiliency function is a closed-loop diagram starting at the design stage and ending with system restoration. This review presents a most pertinent record of resilient systems, not limited to one system's sector. This direction helps us deliver an insightful argument considering various resilience explanations, skeleton, and indices for evaluation which might be of power system society interest. Furthermore, the gaps in existing strategies will help researchers address resiliency issues with practical insights.

2.2 Towards Resiliency

The resiliency concept and framework are studied in this section.

2.2.1 Resiliency Definition

Before understanding the resiliency concept, it is a good idea to look up the Oxford Dictionary for resiliency's meaning as it says:

Tending to resume the original shape or position after being bent, compressed, or stretched.

This definition specifies resiliency as the ability of the system to maintain its functionality following unpleasant incidents. However, different fields of study, such as critical infrastructure, economics, social, and organization, have modified it as an intelligible meaning related to applications Arghandeh et al. (2016). Besides the general definition of the resilient system in the literature, resiliency's critical elements need to be defined for various systems Francis and Bekera (2014). As the resilient structure is vital for large and critical systems and is strongly associated with its components, it can be considered in the context of complex systems and SoS engineering Uday and Marais (2015); Cuadra et al. (2015). Here, the task is to sketch an overall definition of resiliency to know its framework, not to review the definitions. Therefore, resiliency generally describes a system's capacity to withstand abnormal conditions and recover the performance to the desired level. In fact, a resilient system captures two separate steps:

1. Resist a specific incident after disruptive events, and

2. Restore system performance to an acceptable level rapidly.

To guarantee such above behavior, some system characteristics can be utilized. Thus, it would be beneficial to know them to avoid misusing system characteristics and resiliency features.

2.2.2 Resilience vs. System Characteristics

The main attributes of a system are critical tools of system engineers to analyze system performance and integrity. The emerging need for resiliency forces us to append it to system characteristics and separately evaluate it. For instance, a discussion between sustainability as an essential system characteristic and resiliency determines system abilities during the designing process Fiksel (2003). Also, the study of resiliency concepts probes robustness, hazards, and vulnerability Arghandeh et al. (2016). This part sheds light upon resiliency attributes, emphasizing the power grid compared to the International Electronically Commission (IEC) glossary, dependability section International Electrotechnical Commission et al. (2015). The North American Reliability Corporation (NERC) criteria is also an applicable practice in the industry.

Resilience examines the overall capability of a system and is applicable at the system level rather than the component level. Several other attributes define the characteristics of the entire system, which are examined as follows.

Reliability: The ability of an item to perform as required, without failure, for a given time interval, under given conditions International Electrotechnical Commission et al. (2015). Power grid reliability measures the quality of delivered electrical energy to consumers. Several accepted practices apply to define the reliability of the power grid, including system average interruption frequency index (SAIFI), system average interruption duration index (SAIDI), and customer average interruption duration index (CAIDI). However, they exclude outages following unpredicted disruptions and deficiencies Bie et al. (2017). Resiliency captures system accessibility to meet consumer demand and system security and relies on withstanding sudden disturbances Billinton and Allan (1990). Reliability commonly describes the system's component characteristics and is used to measure the system's performance. Conversely, resiliency defines the system's capability against disruptions that are excluded from reliability consideration.

Availability: It is the ability to be in a state to perform as required. It is also based on other system characteristics, such as reliability, recoverability, etc., International Electrotechnical Commission et al. (2015). Generally, availability is related to the ratio of the system in service and its duration in the power grid. In this context, it means the duration of delivered power to load with respect to a specified duration, for example, a year. In this case, availability guarantees demand. It is evident that availability has a general meaning and powerful characteristic. However, it does not imply a recovery procedure or action conveying resiliency.

Robustness: A robust system can keep system properties within a prescribed area even if the controlled system's properties deviate from the desired operation point International Electrotechnical Commission et al. (2015). Robustness can refer to withstanding everyday events. On the contrary, resiliency requires flexibility, particularly for undetermined incidents. Robustness is likely implied at the design stage, where the system can absorb changes. Undoubtedly, robustness is necessary but not sufficient for a resilient system since it does not include actions to restore the system. This refers to preserving the power grid functionality in the presence of perturbations without any statements about unknown disruptions and recovery procedures.

Recoverability: It is the ability to recover from a failure without corrective maintenance Bakirtzis et al. (1996). Recoverability represents recovering electricity to the network without preserving action after a disruption. In other words, the corrective procedures should apply at the system design level. These procedures include actions as default routine; no additional action is required. Recoverability considers the resiliency restoration step as a passive action.

Dependability: It is the ability to perform as and when required, including availability, reliability, recoverability, maintainability, and maintenance support performance. Other characteristics, such as durability, safety, and security, are also included in this feature. Dependability represents a strong multi-characteristics system, yet it still comprises the cons of each related term discussed previously.

The above explanation shows that there is a strong relationship between resilience and system characteristics that support achieving a resilient system. However, further study is needed to determine the role of each system in a resilient framework. In short, a study about power grid resiliency indicates that robustness and vulnerability analysis is the most common approach to resiliency investigation Cuadra et al. (2015); Bie et al. (2017). That is, robustness refers to withstanding the usual upsetting events, and vulnerability analysis addresses system weakness for various related disruption scenarios.

2.2.3 Cybersecurity as Cyber Resilience

As mentioned earlier, the frequency of cyber incidents is on the rise, particularly in the realm of electrical systems. Real-life examples have illustrated that a successful cyberattack can lead to losing control over devices and processes within electrical systems, leading to physical harm and extensive service disruption. Hence, it is essential for the resilience of electricity systems to include measures that also address the cyber layer. Most of the cybersecurity concerns in the power system stem from IT systems. Figure 2.1 shows potential ways an attacker could compromise industrial control systems for an electrical system. To address these, several comprehensive best practice guides outline cybersecurity measures specifically tailored for implementation in the electricity sector, such as NISTIR 7628 guidelines for smart grid cybersecurity Pillitteri and Brewer (2014).

We do not specifically address digital security concerns that do not directly impact electricity security, such as data privacy and protection. Instead, our focus is on cyber resilience, which refers to the ability of decision-making modules in the cyber layer to exhibit resilient response in the face of cyber incidents that occur outside the central part of the system, such as the control center of a system operator or a large plant operator. This concept is analogous to the system's ability to recover its performance during physical incidents.

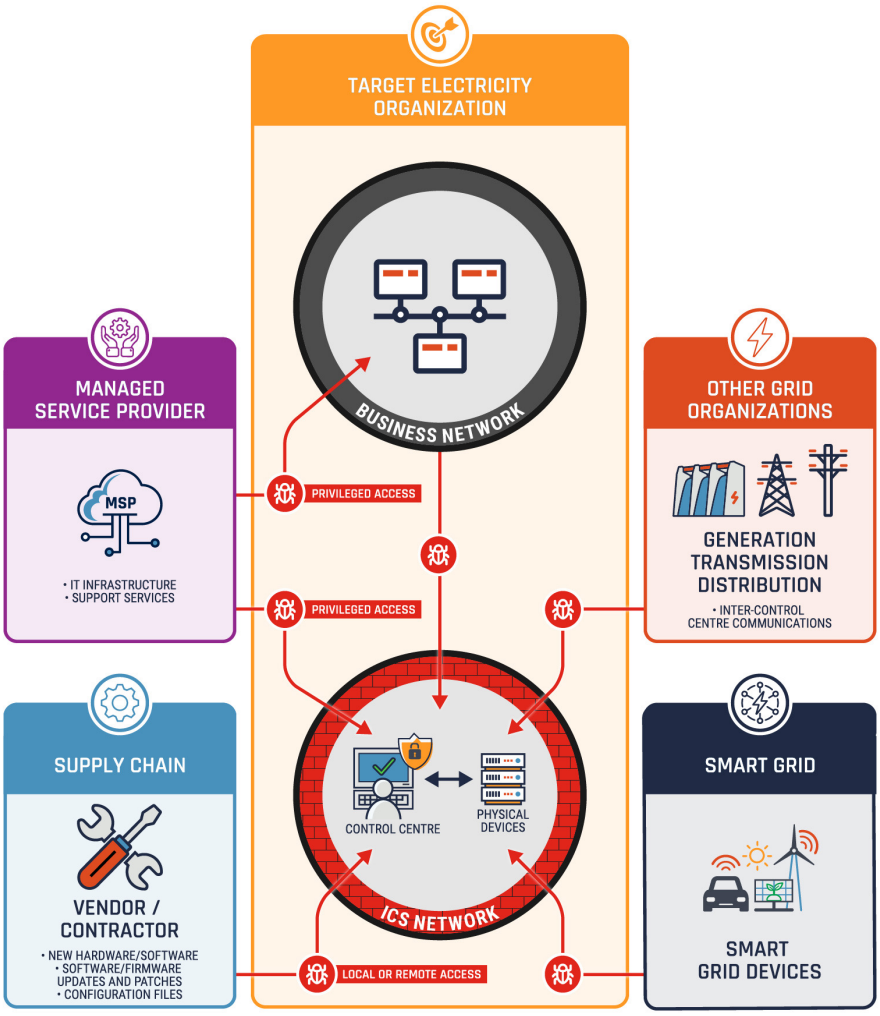


Figure 2.1: The Cyber threat to the electricity sector. Source: Canadian Centre for Cyber Security, Cyber Threat Bulletin.

These cyber incidents can arise from the edges and emerging digital technologies, potentially compromising a significant number of sensor measurements and data. Examples include high-wattage IoT devices like air conditioners, heaters, electric vehicles, and PMUs/SCADA data. While the likelihood of such incidents is subject to debate due to the absence of recorded events, they can be considered as having a low probability. Furthermore, intelligent malicious agents may intensify the impact on system operations through covert actions, leading to high-impact consequences. Hence, cyber resilience/cybersecurity is meant to provide robust decisions that could guarantee the safety and security of the system either by early detection of cyber incidents or by generating an efficient policy/action for a well-ordered recovery.

2.2.4 Resilient Framework

Any sound, resilient policy needs to realize the system's behavior in the presence of disruptions. Regardless of the disruption type, the system's performance deteriorates, and the system must respond in a timely manner Henry and Ramirez-Marquez (2012). Here, an analysis of system performance in the presence of disasters is recommended to provide a measure of resiliency Zobel and Khansa (2014). Moreover, studying the topology of system performance variations helps find a suitable resiliency structure Munoz and Dunbar (2015). Triangle curves and multi-phase resilience trapezoids are typical in examining system resiliency Panteli et al. (2017). Several proposed performance curves in the literature capture the same concept as they point out the advent of reducing performance following a disruption. The only difference is taking various profiles for system response and recovery. The commonly investigated resiliency curve is depicted in Figure 2.2. This figure determines the system performance in three different stages, (1) before disruption, (2) during disruption, and (3) after disruption. First, the system should be designed to withstand the disruption and make appropriate changes with respect to time. Second, the recovery protocol should be determined and exploited to return system performance

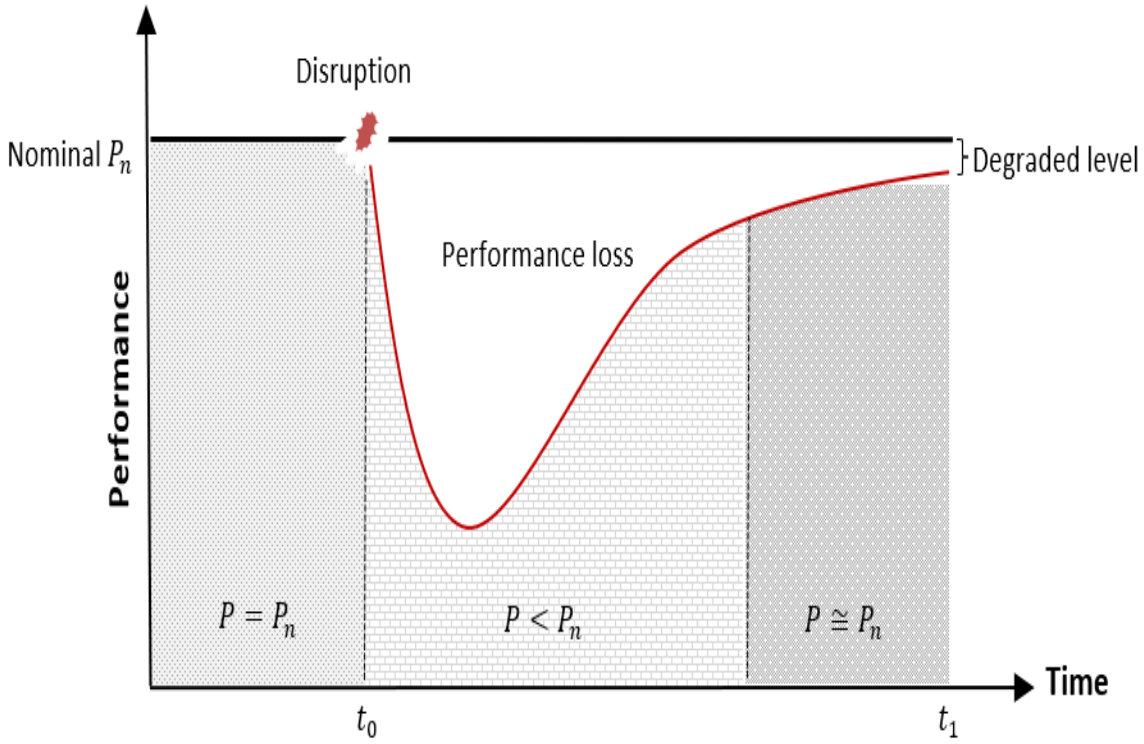


Figure 2.2: Resilience performance curve.

to normal conditions. In this case, appropriate elements must be determined when the system is analyzed. A simple method to determine the composition of resiliency is observing the changes in the performance curve behavior and assigning an action level by considering system response steps in Figure 2.2. Before the disruption, the system must accomplish its task under given disturbances defined at the design stage, implying robustness capability. However, designing a system for low/high probability and low/ high impact disturbances is impractical. Disturbances with high-impact, high-probability (HIHP) are primary external signals to which the system must respond robustly. This approach can be considered a default design routine based on specs. Then, the system should take the necessary steps to start recovering, which should be initiated to restore performance as quickly as possible to the desired conditions.

The analysis of system behavior is the foremost evaluation of resiliency. It is essential to have a framework for critical infrastructure to know how a resilient structure can be configured. As discussed, a resilient framework based on inherent system characteristics supports us in implementing a resilient system. In this case, some features such as robustness, resourcefulness, rapid recovery, and adaptability combine to establish a resilient framework Berkeley et al. (2010). For instance, the resilient structure can break up into components so that each part performs a specific task to achieve resiliency. These components are expected with anticipation and preparedness, linking resistance and absorption, response adaption, and recovery Phillips et al. (2016). This approach helps us properly distribute resources in a networked microgrid to ensure power system resiliency. A further mechanism connects resiliency capacity and absorption, adaption, and restoration capacity as central system features Francis and Bekera (2014). These capacities imply robustness to perturbation, system adjustment vis-à-vis changes, and returning to the desired performance. A generic framework related to the power system is the so-called $4R$'s that expresses *robustness, redundancy, resourcefulness,* and *rapidity* Panteli and Mancarella (2015). Note that redundancy is a practical tool in the system robustness

ability framework. Realizing resiliency as a scheme can be a cycle, including adaption, robustness, and restoration. In this fashion, a resilience cycle is guaranteed when the system withstands and absorbs disruptions. The suggested items that construct the resilience cycle are illustrated in Figure 2.3. This framework will then ensure a resilient system, capturing the two main steps discussed above: withstanding and restoration.

2.2.5 Verification of System for Resiliency

Once the integral parts to build a resilient framework are specified, the system designer should identify some mandatory items aligned with the system's nature. These items should be connected to suitable system disruption types, system attributes, and timely recovery strategies. These items make a clear vision of resiliency realization and implementation. One of the main attempts to address the system properties is vulnerability analysis that inscribes the disruption type. This analysis is an evaluation process to identify potential disrupting events targeting risk assessment.

The power grid is a complex network with many internal and external interactions and is sparsely and densely distributed, and is incredibly vulnerable. Moreover, various disruptive events can happen, i.e., natural disasters, equipment failures, human errors, or deliberate sabotage and attacks Kim and Obah (2007); Yue et al. (2019). In the power system, researchers exploit vulnerability assessment with different points of view, such as topological concerns, computing electrical centrality, cyber risk, natural disaster threats, and power grid interconnections Wang et al. (2010); Bompard et al. (2012); Dai et al. (2014); Cannon (1994). Technically, systems should cope with events with low probabilities and high impacts in this concept. Different infrastructure risks are separated into natural and human threats in North America. A report shows that among 214 emergency events in 2014, the bulk power outages with 87 cases ($\approx 40\%$) were the primary reason due to severe weather conditions Preston et al. (2016). Furthermore, reviewing major historic

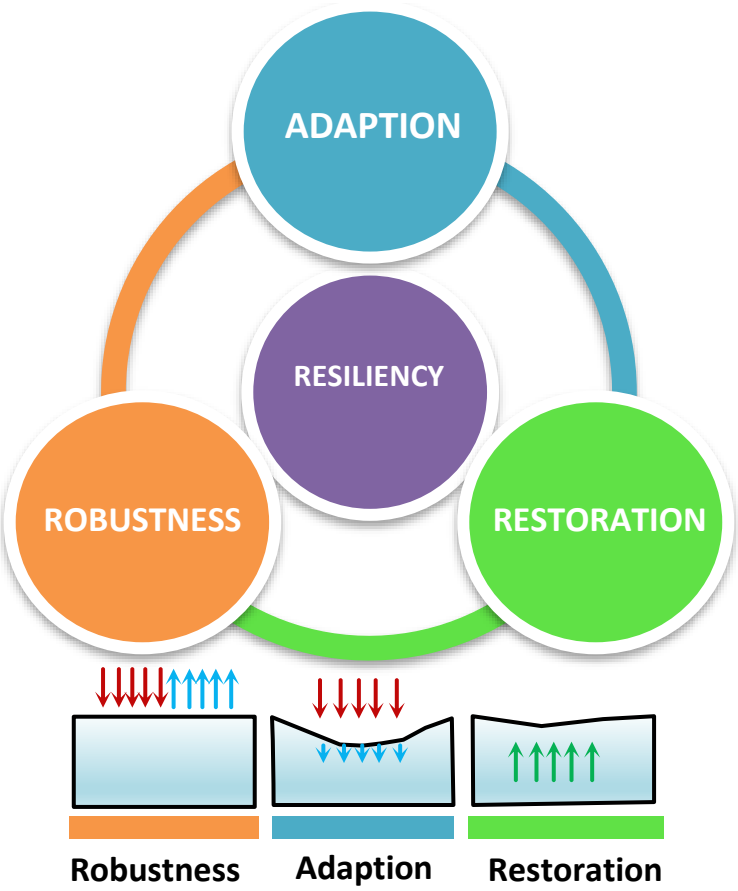


Figure 2.3: Resilience cycle and components.

blackouts from 1965 to 2012, power grid emergency events are categorized into four primary sources: natural, accidental, malicious, and emerging threads with 63% contribution of natural threats Bompard et al. (2013). The first three warning categories are crystal clear. The emerging one refers to threats appearing in evolving power systems, such as distributed energy resource (DER) integration, that causes uncertainty increment or stability decrement. Besides, utilizing a vast number of sensors and the communication network as the cyber layer causes an increase in the frequency of cyber threats in the electrical grid, which Federal Energy Regulatory Commission (FERC) asks for developing new cybersecurity rules for DERs on the bulk electric system, and the U.S. Department of Energy (DOE) will support millions to build "next-generation" cybersecurity research, development, and demonstration projects.

The disruption can be arranged based on the threat's location, internal or external, illustrated in Figure 2.4. These categories help analyze the system and make it easy to provide a solution to resiliency. The internal disruptive events include inherent system uncertainty, component fault, or disturbances where for high probability events, prevention actions are decisive. All natural disasters, physical or cyber-attacks, and disturbances from out of the system are counted as an external category. Thanks to disruption classification, we can distinguish corrective actions for system recovery during the system design stage.

2.2.6 Resiliency Study Procedure

Practicing resiliency needs to analyze the system for two primary purposes. First is determining fundamental expectations from the system when it faces disruption. Second, an analysis of system weaknesses through a vulnerability assessment is required. Thus, the system resiliency definition becomes more apparent and supports engineers in designing appropriate instructions and guidelines to maintain required expectations. An analysis scheme is depicted in Figure 2.5. It can be said that the

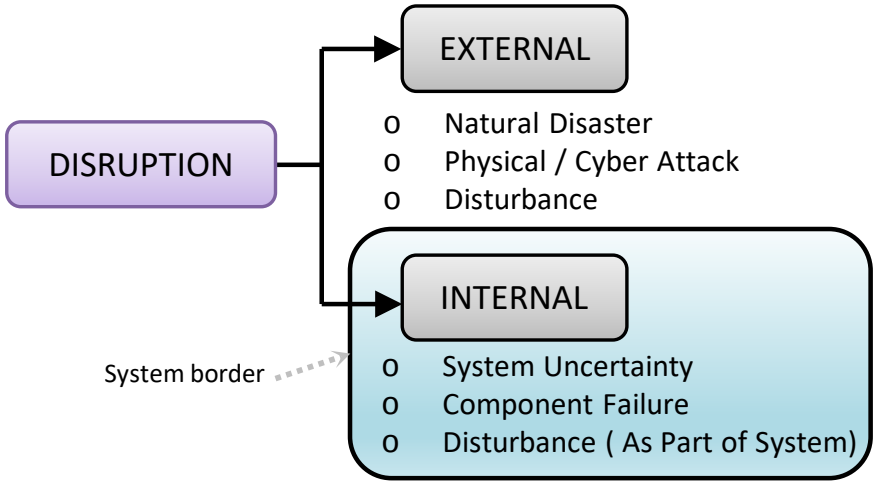


Figure 2.4: Disruption category.

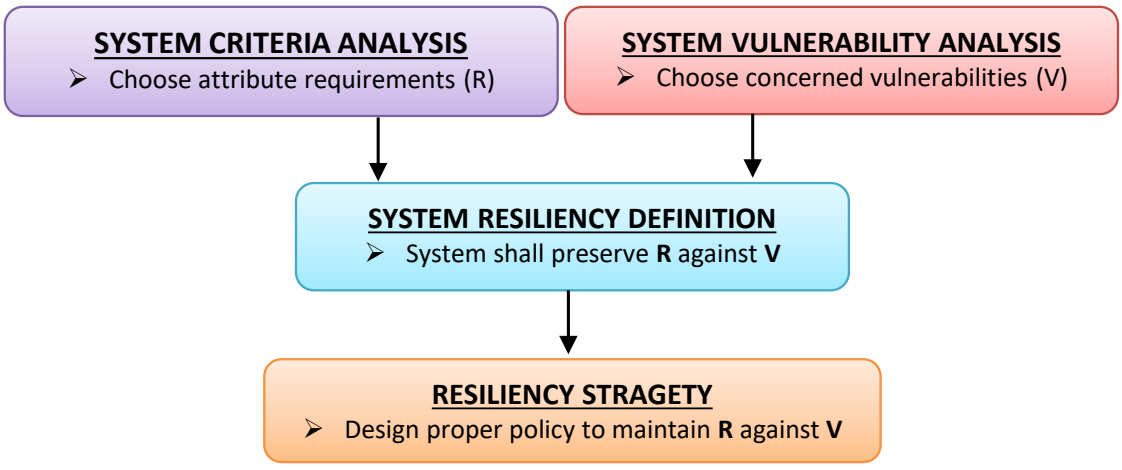


Figure 2.5: Resiliency analysis procedure.

system is resilient enough to meet defined principal requirements for a particular fragility generated by an upsetting event.

2.2.7 Resilience Metric

System performance measurement is validated by its deviation from the desired value. This variation is caused by internal (human error, component failure, etc.) or external (earthquake, hurricane, physical or cyber attacks, etc.) disruption sources, whether intended (intelligent) or unintended. A metric necessitates evaluating system status to demonstrate how far the system is from the normal region. There are three main resilience metric measures Yodo and Wang (2016):

1. Curve methods based on the difference between performance before and after disruption,

2. Ratio of system performance before and after the disruption and

3. A function of system characteristics.

In fact, an index is used to determine the resiliency status. This index assesses the system, provides the resiliency situations, and assists in taking recovery actions based on resilience components. Similar to all assessment procedures, qualitative and quantitative are the prominent methods.

Qualitative Analysis

Qualitative methods evaluate system resiliency with figures and textual data. These tools assess essential system attributes for operation during disruption, called a conceptual framework because it involves system characteristics. The conceptual framework includes a common complex feature to analyze system resiliency Vugrin et al. (2010). This approach considers analyzing a broad spectrum of system characteristics. Its outcome may provide valuable information about system

characteristics and resiliency enhancement and navigate quantitative methods to evaluate system capacities.

Resiliency assessment tasks through qualitative methods can also be carried out based on collected data in a questionnaire or observations Donnellan et al. (2015); Somasundaram and Sivayokan (2013); Bimrose and Hearne (2012). This approach is not common in power grid resiliency. However, a resilience index can be provided by considering the ability of robustness, resourcefulness, and recovery, where it points out a uniform index for critical infrastructure based on data aggregation of quality assurance Fisher et al. (2010).

Quantitative Analysis

On the contrary, the quantitative method explores resiliency metrics by numerical results. The general approach to quantifying resiliency relies on performance measurement. This assessment compares the system's normal and degraded conditions. Understandably, choosing system attributes as performance measures is application-based. Probing the performance curve does formulate quantitative resiliency assessment through different interpretations of system responses to disruption Panteli et al. (2016); Jufri et al. (2019); Amirioun et al. (2019). Data-based methods to characterize performance are obtainable through deterministic and stochastic system modeling approaches.

- Deterministic Modeling

The real-time performance calculation is suggested as a resilience index, such as dynamic analysis, instead of providing a time-independent measure Bie et al. (2017). According to the resiliency performance curve in Figure 2.3, the calculation of performance loss can be derived from finding an equation for the resiliency index. So, it is straightforward to compute the performance loss PL by (2.1) regardless of

any uncertainties Bruneau et al. (2003).

$$PL = \int_{t_0}^{t_1} [P_n(t) - L(t)]dt \tag{2.1}$$

where P_n represents the nominal performance value, $L(t)$ is the time-evolving performance curve following a disruption, t_0 denotes the time of the disruption, and t_1 expresses the time of getting back to nominal or an accepted performance. The less performance decreases, the more resilience is achieved. Another form of resiliency metric in connection with performance is the ratio of the area below the disrupted performance curve to the total area of nominal performance starting from system operation ($t = 0$) Ouyang et al. (2012); Rose (2007), as follows:

$$PL = \frac{\int_0^{t_1} L(t)}{\int_0^{t_1} P_n(t)} dt \tag{2.2}$$

This ratio quantifies the decrement percentage in system response in the presence of disruption. Equations (2.1) and (2.2) address resiliency metrics with respect to nominal and degraded performance with the same resiliency interpretation. The ratio in (2.2) is pertinent to the shape of the performance curve. For instance, Adams et al. (2012) suggests a triangle shape for the performance loss curve following a disruption. In this fashion, (2.1) modifies the percentage performance loss over a time interval of reaching an adequate response. A simple calculation of the triangle is the merit of this assumption. However, the recovery curve shows nonlinear behavior in practical applications. Consequently, it necessitates extra practice to compute the area of the recovery curve Hosseini et al. (2016). Also, finding a deterministic performance function relating resiliency is not clear.

The absorption, adaption, and restoration capacity as system abilities can be considered to check resiliency levels. In this way, systemic impact and total recovery effort caused by disruption can be reduced Vugrin et al. (2011). The systemic impact

is a deviation of the actual and desired performance level following a disruption according to the system's absorptive and adaptive capability. Furthermore, the recovery effort is the number of accessible resources used to recover the system after disruption based on restorative action and procedure. The total recovery effort is a function of consumed recovery time, cost, and allocated resources to rebuild a system with an acceptable performance level. Assuming the performance curve in Figure 2.2, the performance loss has the same concept of systemic impact. However, this performance only depends on recovery time without considering other expended restoration efforts.

- Stochastic Modeling

Data measurement is not possible for all variables. Also, parameter uncertainties and noise affect the parameter values. So, probabilistic modeling plays a key role and can capture random events that cause disrupted performance Anghel et al. (2007). However, stochastic modeling could be complicated to apply. Similar to the deterministic approach, indicating resiliency in probabilistic methods also includes determining performance loss and recovery time. Here, resiliency is defined as the conditional probability of initial performance drop following a disruption r_0 given the restoration time t_1 Chang and Shinozuka (2004). Assume the system desired performance A, in the presence of disruption with magnitude i, the resiliency can be expressed as (2.3):

$$R = P(A|i) = P(r_0 < r^* and\ t_1 < t^*) \tag{2.3}$$

Where r^* is the maximum allowable performance loss, and t^* is the adequate recovery time. This index captures the system's uncertain response, such as the deterministic method, and can be used to generate an alert or notification to initiate a proper recovery action when the thresholds r^*, t^* are exceeded Hosseini et al. (2016).

The resiliency index also includes a function of the reliability factor R and the system's ability to restore to nominal conditions Youn et al. (2011). In this case, the restoration capacity ρ produces a joint probability of system failure rate $(1 - R)$,

mitigation, and recovery effort value κ. This approach introduces stochastic modeling as a resiliency index. Additional terms such as correct event diagnosis λ_D and correct event prognosis λ_P from perturbations need to be introduced as a perfect index by linking to the restoration procedure as follows:

$$\text{Resilience}(\Psi) = R + \rho(R, \lambda_P, \lambda_D, \kappa) \tag{2.4}$$

Where Ψ shows the contribution of reliability and resiliency, where reliability should be considered at the system design level, however, determining ρ as a stochastic function of system characteristics is not effortless; it needs from top to bottom knowledge of the system, such as the SoS analysis method.

Another non-deterministic resiliency framework is examining recovery speed towards normal conditions after incident Yu and Jiang (2015). The main concept here is that rapid recovery indicates high resiliency. This method conveys a stochastic model such that the stochastic process captures system states after any shock by the theory of mean-reversion plus random disruption with Gaussian distribution Zhou et al. (1996). In the sequel, the recovery rate is considered a resiliency metric in (2.5).

$$dX(t) = \lambda(\mu(t) - X(t))dt + \sigma dW(t) \tag{2.5}$$

Where $X(t)$ is a measurable quantity of the system, d denotes the differential operation, λ represents a mean-reversion rate describing the speed of the process returning to its mean value. Also, $\mu(t)$ is the mean or expectation, σ represents volatility, and $W(t)$ is the Brownian motion. In this equation, λ indicates a resiliency measure and plays a key role since it addresses an assumption about the system's tendency to move to the average value over time after a perturbation or a shock. Mean-reversion theory discusses aftershock cases such that the system's performance converges to a long-term average value, particularly in the economy. For instance, in the stock, the market modifies itself based on the index represented by demand and

response. However, mean reversion in the resiliency context should examine proper recovery action to return to the nominal value.

Other resiliency indices also use the stochastic model. For example, the time-related expected value of the annual resiliency AR index is suggested as the ratio of the disrupted system performance curve to the standard one Ouyang et al. (2012). Here, the difference from (2.2) is that the performance curve is a stochastic process, and an average value is needed. Also, the time interval was taken over a year. In general, the various probabilistic outlooks regard the analysis of the power distribution curve of system resiliency against severe weather conditions Fanucchi et al. (2019). This analysis indicates various schemes of resiliency metrics concerning system performance disruptions modeled by a Poisson distribution Ayyub (2014).

2.3 Resiliency Loop

The resiliency index reflects the ability of the system response to react against disruptions. Therefore, a strategy to regain typical conditions is essential. In other words, the system must be designed to restore a normal regime using recovery actions in a short time. According to this challenge, we need to find a mechanism for system restoration procedures.

The restoration mechanism can mimic a feedback loop, detection, and identification scheme. In this case, the feedback signal helps to find the error and improve system characteristics. Also, knowledge of system critical states results in precisely handling disruptions. Following this concept, the system should utilize real-time alerts and notifications when the resiliency index falls from the designed threshold. Studies, such as fault-tolerant systems, have considered this concept, in which fault diagnosis is the basis of the FTC scheme Isermann (2006). Thus, resiliency can benefit from reusing this concept. However, most studies assume the disruption has occurred and discuss the proper resiliency response. Utilizing a resiliency detection scheme is recommended to provide the right recovery action.

There are different ideas proposed in the literature for the system resiliency response. A stochastic mathematical framework to define resiliency strategy may apply if the system takes a state-control random process De Lara (2018). Here, the recovery action is considered without the recovery time. Resiliency can be analyzed in control theory design Vugrin and Camphouse (2011). A linear quadratic regulator (LQR) as an optimal control method can minimize a cost concerning maximum performance restoration based on defining resiliency as a function of the recovery effort and systemic impact. This approach has been tested in a stock management system model with satisfactory results. Nonetheless, defining such a cost function for large-scale systems and minimizing it is challenging, particularly for non-linear systems.

Another mathematical approach to formulate resiliency is the application viability theory and attractor domains Martin et al. (2011). This approach calculates the system trajectories using set value analysis under constraints. Here, optimal control as a resiliency policy management is determined to force the system trajectories to return to operational conditions. This method tackles resiliency by defining a region where the system's evolution from its complement leaves its operational region over a finite time called the viable kernel. Here, the computation burden to identify a viable kernel with a state-space approach is the main drawback Aubin et al. (2011).

An inadequate closed-loop response is apparent, and a systematic resiliency strategy is required (i.e., FTC method and re-configuring scheme). The standard closed-loop control system is responsible for general control purposes, such as stability, reference tracking, disturbances, and noise rejection. However, an individual control loop in connection with resiliency should be added. This loop derives from identifying the system's resiliency status and then initiating the proper response whenever the system resiliency level is below a threshold. The resiliency diagnosis may include (1) internal measuring of system variables related to resiliency, (2) external factors, such as a hurricane where forecasting data is extensive, and (3) a defined index of resiliency as a set point. These three items provide valuable inputs to obtain

resiliency and determine which action should be applied. This scheme lies in control reconfiguration or re-structuring the system to cope with performance degradation, as shown in Figure 2.6. The assumption is made that the communication network is secure and reliable, with no threats compromising the data exchange. As previously mentioned, the focus of cyber security in this thesis lies in developing models that exhibit cyber resilience, such as computation resiliency status and resiliency action blocks in the diagram.

The realization of the diagram may be seen in the physical layer. However, it is also applicable to the cyber layer, wherein the main system is EMS functions that need to exhibit resilience concerning cyber threats, data uncertainty, and distribution. In the next two chapters, we seek to focus on resiliency identification for LF applications, highlighting the adaptive elements in the proposed resilience framework against cyber threats. Moreover, the robust element is addressed for SA applications, targeting the uncertainty of the electrical grid.

2.4 Resiliency Response in Power Grid

Research directions and activities in power systems carry out the following planned actions to support the power grid's resiliency. Each strategy likely considers a part of the resiliency loop shown in Figure 2.6. However, the full resiliency structure implementation is essential to achieve a resilient system.

2.4.1 Hardening Power Grid

Hardening is a pre-disrupt physical activity that makes the system robust to disruption through modifying or improving the power grid structure. For example, hardening electric transmission and distribution actions are about strengthening poles with guy wires or burying power lines underground for wind protection Hoffman et al. (2010).

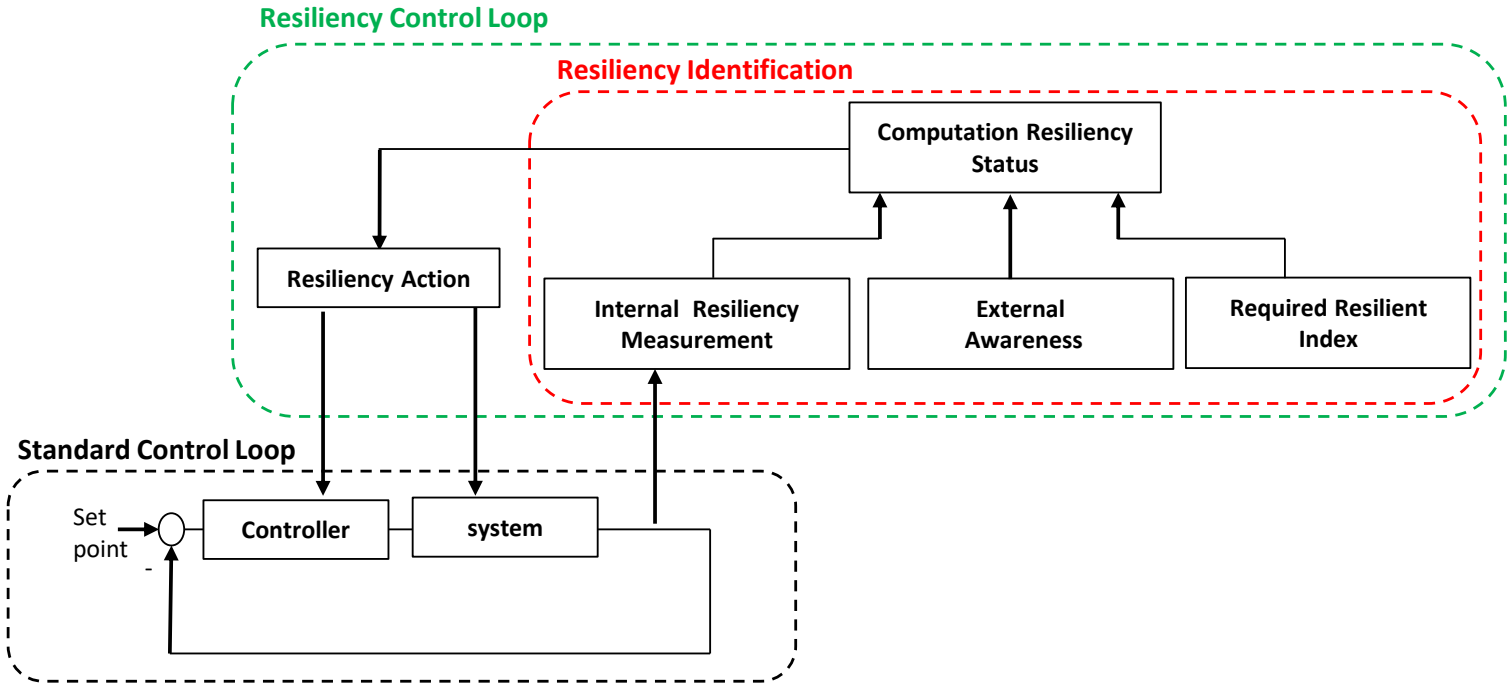


Figure 2.6: Proposed resilient loop diagram.

These organized actions indicate the impact of upgrading the power grid to enhance the system recovery strategy Chen et al. (2017).

2.4.2 Microgrid Supported Grid

In this framework, the grid is utilized by microgrids (MGs) such that its effectiveness preserves power grid performance as a resilient system Li et al. (2017); Chen et al. (2017). MGs can effectively improve resilience transmission and distribution systems due to their operational ability in a controlled, coordinated mode for grid-connected and islanded modes. MG-based strategies for resilience enhancement are presented in Stasinos et al. (2022), including MG-based resilient planning and MG-based operational measures, consisting of preventive MG scheduling and emergency measures and MG-based system restoration. Japan microgrid research and development states that microgrid plays a principal role in overcoming system deficiency following an earthquake or tsunami Marnay et al. (2015). Also, the European megagrid is planning to achieve resiliency based on microgrid structure, including solar and wind resources Strbac et al. (2015).

2.4.3 Grid Partitioning

This approach splits the power grid into subsystems to avoid large disruptive events or blackouts to enhance resiliency in the power system. This is so-called controlled islanding for the prevention of cascading failure in large-scale systems Senroy and Heydt (2006). The potential of controlled islanding is enhancing resiliency by making defensive provisions for severe weather conditions. It configures a closed loop system based on risk assessment to initiate grid splitting Anghel et al. (2007). Since the power system can be analyzed using different objectives, islanding may exploit a resiliency strategy to take care of them. That is, frequency stability and power system restoration are supported over undermining events Teymouri et al. (2017); Tortós and Terzija (2012). However, reconstructing the power grid considering separated

subsystems may include downsides. Once the power grid is islanded, extra efforts for reforming the initial structure are required, where the system may not efficiently preserve the generic system functionality. This shows that controlled islanding may be a conservative approach.

2.4.4 Cyber Resilience

Cyber resilience is a continuous undertaking that requires collaboration between utilities and consulting services to define, as there is no universal solution that fits all scenarios. Since most tools are customized to address specific requirements, developing cyber resilience strategies necessitates joint efforts between utilities and consulting services. For example, Fischer et al. (2018) with the concept of digitalization of the energy allocates cybersecurity to the cyber elements that are necessary for a value chain. The practices in this context primarily focus on safeguarding against information technology-related threats, leveraging guidelines and standards, such as ENISA, NISTIR 7628, NIST SP 800-53, and ISO/IEC 27019. However, there is still a need to incorporate cyber resiliency into the design decision-making module. This entails the development of tools and technologies that empower energy systems to identify and prevent cyberattacks, thereby preventing disruptions autonomously. Additionally, it involves incorporating cybersecurity and resilience features into technologies through a cybersecurity-by-design approach, ensuring that these elements are inherently built into the system from the outset. Examples can be distribution robust optimization for operating transmission systems against cyber-attacks to reduce load shedding and operation costs to benefit end customers generation Zhao et al. (2020), increased cyber situational awareness in the context of a digital twin implementation in the EU electrical power sector Salvi et al. (2022).

2.5 Discussion on Power Grid Resiliency

Many strategies have been introduced in the literature to construct a resilient system with specified resiliency applications. This section presents a discussion and exploration based on reviewed articles to discuss the power grid's resiliency.

2.5.1 Definition

Power society researchers are now familiar with resiliency, such as establishing a special task force for resiliency IEEE PES Task Force: Stanković et al. (2022). Also, recorded events, such as significant blackouts and increasing cyber threats, endorse the need for a resilient system. However, formulating a precise procedure to guarantee resiliency is unclear and challenging in power systems. Different concerns must be addressed as part of resiliency objectives, including small frequency and voltage stability. Hence, future research should attempt to provide a notion for the whole power system resiliency to emphasize requirements or point out the most integral one. Technical committees play a significant role by prioritizing objectives Fisher et al. (2010).

2.5.2 Structure

Several studies and reports define common elements to build a resilience structure, which captures system capabilities, such as adaption, robustness, and restoration. The system should be studied element-wise to determine whether it has the required resiliency components. It means that based on the associated disruptions to the system, vulnerability assessment identifies the system's strengths and weaknesses. Thus, a mitigation action should be defined to reinforce the fragile part of the resiliency components obtained by vulnerability analysis.

2.5.3 Metrics

Various norms define different efficient methods of modeling indices. The modeling stage should consider a quantitative or qualitative approach, system objective, and limitations to define an index. Also, it should be related to system states to capture its behavior, meaning a physical interpretation for tractability. Moreover, since the power grid is considered a complex system Pagani and Aiello (2013), using graph measures is convenient for analyzing the power grid comprehensively. Hence, using graph theory methods for power grid networks is recommended to study resiliency. Graph modeling and centrality measures have already been deployed to analyze the power system vulnerability using topological characteristics; however, the lack of graph theory tools connected with the power system's electrical variable and dynamic is apparent.

2.5.4 Response

A resilient system must be a closed-loop system where recovery action is mandatory. Restoration strategy can be a pre-disruption action, such as system hardening. Also, it may take a conservative approach, such as grid islanding, to stop extensive damage. However, dynamic response or real-time strategy to touch on control problems is worthwhile and operative. For instance, a resilient power system can be transformed into designing a resilient control problem via robust control theory to preserve system performance in the presence of cyber-attacks Zhu and Başar (2011). Therefore, it is vital to have a fully automated, resilient system (for a specified disruption). Such efforts to make a real-time resilient loop, including dynamic remedial action, can be used for future studies.

2.6 Summary

This chapter reviews resilient systems to provide resiliency directions for the power grid. Through studies and reports, the common prevalent resiliency ideas have been discussed. After presenting the concept of resiliency and its definition, some clarifications are provided to identify resiliency from other systems' operational and safety attributes. Additionally, the importance of cybersecurity in decision-making functions, viewed through the lens of cyber resilience, is discussed. A summary of disaster resources, various resilient infrastructure components, and proposed resiliency indices are provided. The review can help for future study, analysis, and deployment of resiliency. Moreover, the absence of real-time resiliency architecture in an all-exclusive manner, such as detection and control, is discussed as the primary obstacle to shaping a resilient power grid. This effort imposes broad and collaborative research and study since the power grid is the core of the critical infrastructure. Due to this fact and having a clear vision of resiliency, the following chapters will offer a resiliency guarantee based on the proposed element of a resilient framework for two data-driven applications in the power grid.

Chapter 3

Cybersecurity in Load Forecasting

One of the main functions of the EMS system is to forecast load profiles to prepare suitable scenarios for the power grid. Short-term load forecasting is an essential task that supports utilities to schedule generating sufficient power for balancing supply and demand and can become an attractive target for cyber attacks. It has been shown that the power system state estimation is vulnerable to false data injection attacks. Similarly, false data injection on input variables can result in large forecast errors. The load forecasting system should have a protective mechanism to mitigate such attacks. One approach is to model physical system constraints that would identify anomalies. This chapter investigates possible constraints associated with a load forecasting application. Looking at regional forecasted loads, we analyze the relationship between each zone through similarity measures used in time series to identify constraints. Additionally, we investigate the lag relationship between load stations using correlation analysis. Comprehensive results for historical ERCOT load data are also presented. Part of the results of this chapter appeared in Dezvarei et al. (2022).

3.1 Introduction

Load forecasting is critical to efficient decision-making in power system operation and planning. Among the load forecasting types, STLF plays a significant role in achieving economic, reliable, and secure operating procedures. The STLF supports a time horizon ranging from one hour to one week. The primary objective of the STLF function is to provide load predictions for the primary generation scheduling functions (unit commitment and hydro scheduling), for assessing the power system's security at any point, and for timely dispatcher information Gross and Galiana (1987).

To predict the electric load, there are critical variables that accurately forecast the load. Many forecasting models with a wide range of methodologies for STLF are suggested in the literature. The models are mainly classified into two groups: statistical techniques, such as multiple linear regression (MLR), ARMA; and AI techniques, such as artificial NN (ANN), fuzzy regression models, SVMs Hong and Fan (2016). All methods are constructed based on input data indicating the independent variables compatible with the forecasting horizon. In STLF, the primary inputs may include weather variables, calendar variables, and the load of the preceding hours Drezga and Rahman (1998); Xie and Hong (2017). In Hong et al. (2011); Wang et al. (2016), the authors consider an additional variable to address locally increasing (or decreasing) load and the fact that electricity demand is affected by the temperatures of the preceding hours, respectively. Therefore, the quantity and quality of input data are significant for an accurate estimation.

Smart grid and renewable energy resources bring opportunities for improved forecasts by providing high-resolution sensing and data acquisition capabilities; however, Kezunovic et al. (2020) discuss big data applications and associated implementation issues in load forecasting. With these new data sources, the input data may face challenges, including measurement device error and cyberattacks (e.g., false data injection) that cause operators to make wrong decisions. The vulnerability analysis for input data in load forecasting is analyzed in Chen et al. (2019c). It is

vital to check the quality of input data to guarantee accuracy. Statistical analysis and information theory Chandola et al. (2009), ML-based method Cui et al. (2019b); Esmalifalak et al. (2014) are some approaches for anomaly detection schemes.

As the attackers also benefit from AI and ML methods, they may deploy sophisticated techniques to bypass the anomaly detection, such as targeting state estimation and electricity market application Liu et al. (2011); Xie and Hong (2017); Zhang and Li (2021). Although the detection scheme imposes difficulty for the attacker, this may be overcome by, for example, reinforcing the threat model Chakraborty et al. (2018). To address the issue, physical-based constraints can provide a more decisive obstacle for the attacker. For example, Li et al. (2021) propose adding inherent constraints in power system state estimation (SE). This idea creates a further constrained problem that needs to be solved by attackers while satisfying the physical systems' inherent constraints. Inspired by this concept, in this chapter, we seek to define a defense mechanism for STLF against adversarial attacks. As load forecasts can be represented as a time series, it offers various tools to identify characteristics. In this regard, data mining approaches and statistical analysis can facilitate us in identifying physical-based constraints. This is the first attempt to define a protective mechanism in STLF associated with these inherent constraints.

3.1.1 Short-term Load Forecasting Modeling

In STLF, the objective is to estimate the load for a short time horizon, typically ranging from the next hour to one week. The main intention of STLF is an hourly prediction of aggregated load. In addition, the STLF may focus on forecasting the daily peak system load, the value of system load at a specific time of day, hourly or half-hourly of system energy, and the daily and weekly system energy Gross and Galiana (1987).

In this regard, the STLF is concerned with scheduling purposes for the most economic commitment of generation sources consistent with reliability requirements

and operational constraints. Furthermore, the load prediction may be used for assessing power system security for the off-line network analysis under which the part of the systems may face stress. The system load is the sum of all the individual demands in all power system nodes. Many factors impact the STLF model of aggregate load. The elements are mainly categorized as follows Gross and Galiana (1987):

- Weather: temperature, humidity, wind speed, ...
- Calendar: time of day, day of week,...
- Social events: Christmas Eve, game day, ...
- Other random factors: Unforeseen events, such as outages,...

Note that utility companies use their developed model, which may differ in independent variables due to the proprieties of the work area. For instance, the reader can see the independent variables of PJM interconnection, a regional transmission organization, LF models as a public report PJM Resource Adequacy Planning Department (2016).

The dependent variable that needs to be estimated is aggregate load, and other variables related to effective factor categories are considered independent variables (explanatory). A practical report indicating independent variables for different load serving entities (LSEs) is found in Carvallo et al. (2016).

The general formulation of STLF is to define a forecasting function f as

$$y_t = f(\bar{X}_t) \tag{3.1}$$

where y_t, and $\bar{X}_t$ are the load and the independent variables at time t.

There are many ways to find f, which are commonly divided into statistical and AI methods. The former is statistical analysis, such as MLR, ARMA, and exponential smoothing models. An AI approach may use an ensemble of machine

learning algorithms for forecasts, such as ANN, fuzzy regression models, SVM, etc. A high-level comparison of load forecasting techniques is presented in Hong and Fan (2016). In this work, the MLR is chosen to apply the proposed methods due to the LF model formulation's simplicity and the variables' role in that. Note that the method which will be proposed is not model-dependent and can be applied to all the LF models. MLR is a broader class of regressions encompassing linear and nonlinear regressions with multiple independent variables $\vec{X}$ and one dependent variable Y. The general linear regression model can be defined as

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \cdots + \beta_n X_n + \epsilon \tag{3.2}$$

where $\beta_0, \beta_1, \ldots$ are the parameters and ϵ is normal random error. Note that second- or higher-ordered terms of independent variables are equivalent to the first-ordered one, and it is a special case of (3.2) Hong et al. (2011).

3.1.2 Vulnerability of Independent Variables

Some independent variables cannot be easily corrupted as their values are widely known. This includes calendar variables (month of the year, day of the week, hour of the day, etc.). Due to the longer time scale, economic factors are not explicitly expressed in STLF models. Weather significantly affects the load pattern, among other variables, because many loads are sensitive to temperatures, such as heating and cooling. The temperature data is the most used feature in many STLF models to capture the load behavior. In this case, the quality of temperature is crucial to STLF accuracy. The temperature used in the STLF model is an estimated value obtained from commercial weather services, external services/application programming interfaces (APIs), or measured from the sensors stations. This also provides a vulnerable area for data disruptions and false attack injections as temperature anomalies can be detected with the help of local load information of power companies Sobhani et al. (2020). Although the detection

scheme can help find the anomaly in temperature, an attacker who also benefits from AI methods would be more challenging. The adversarial attack on temperature data exploited in Chen et al. (2019c) indicates that STLF models are vulnerable to malicious temperature data from online weather services. In addition, an attacker could manipulate load forecasts in arbitrary directions and cause significant and targeted damages to system operations.

3.2 Threat Model

An attacker threat model is a framework that indicates potential adversaries, their capabilities, and the strategies they might use to compromise or disrupt a system's security. In fact, the threat modeling process begins with the development of a data flow diagram, which is then utilized to identify trusted boundaries and identify potential untrusted input Hahn and Govindarasu (2011). This model helps identify and understand the various types of threats that a system may encounter, such as vulnerability analysis.

In the realm of cybersecurity, the attacker threat model considers factors, such as the types of attackers (individuals, groups, insiders, or nation-states), their motives (financial gain, espionage, revenge, etc.), their technical skills and resources, and the methods they might employ to exploit vulnerabilities in the system (e.g., phishing, malware, social engineering). Furthermore, the model defines the specific targets or assets attackers may be interested in compromising, as well as the potential consequences of successful attacks, such as data breaches, service disruptions, financial losses, or damage to the organization's reputation.

In the context of the LF application within the EMS at the control center, our threat model (TM1) assumes that attackers lack access to detailed system models, parameters, or constraints. Instead, they rely on general information available in the public domain and literature to understand the LF application's mechanism and the data collected from outside the system. While insider threats are acknowledged as

a possibility, our threat model primarily focuses on external threats and does not consider any malicious actions from insiders.

In light of this, we specifically investigate the temperature as a targeted variable for attackers, considering that it is collected from outside of the system. To counteract potential attacks, our aim is to establish constraints that can serve as a defense mechanism, enabling the detection of attacker actions within the threat model. Additionally, if attackers manage to gain access to system models named TM2, they must adhere to these constraints to achieve feasible results. The former aspect challenges the attacker's knowledge, while the latter challenges the attacker's capabilities and abilities.

3.3 Problem Statement

The primary objective for the attacker is to remain undetected by system operators while executing an adversarial action. Typically, the attacker's capabilities are limited in order to successfully carry out a malicious action. As a result, the discrepancy between corrupted and actual temperature data will be confined within certain bounds Chen et al. (2019c). Let H represent an attacker targeting a simulated forecasting model that is parameterized by θ. The only constraint in this scenario is to bypass the detection scheme. Introducing physical-based constraints can pose challenges for the attacker. For TM1, the complexity increases for the attacker, as more information is added, further concealing the attacker's knowledge. In the case of TM2, the attacker must first acquire knowledge about the nature of these new constraints and then identify possible attack vectors. In both cases, the problem that the attacker needs to solve can be formulated as the following optimization problem (3.3a) and (3.3b):

$$\min_{\tilde{X}} \quad H_\theta(\tilde{X}) \tag{3.3a}$$

$$s.t. \quad \left\| X - \tilde{X} \right\|_p \leq \epsilon \tag{3.3b}$$

$$g(\tilde{x}) \leq 0 \tag{3.3c}$$

where $\tilde{X}, X$ are the injected and actual temperature data, ϵ is a threshold value, and p shows different norms according to the detection algorithms. Here, we are adding (3.3c) to (3.3) to represent the physical-based constraints. The minimization problem here points out the attacker target as decreasing the load forecast values. The constraint $g(\tilde{x})$ can be imposed either as equality or inequality related to the physical system and topology. The right side of (3.3c) may be defined by an upper bound to deal with various scenarios. The way to find $g(\cdot)$ is discussed in the following sections.

3.4 Exploring the Constraints

Power systems follow some physical and topological constraints. For instance, the output of power metering devices should ideally capture Kirchhoff's laws. For example, the physics law in water pipeline is shown in Figure 3.1 Li et al. (2021), where the flow meters data must follow a linear quality or inequality (3.4) because of the mass flow balance law.

$$F_{meter_1} \geq F_{meter_2} + F_{meter_3} \tag{3.4}$$

This action may present a built-in defense mechanism. Li et al. (2021) studied potential vulnerabilities of ML applied in power systems by proposing constraints that adversarial examples must satisfy the intrinsic constraints of physical systems. In power system SE, the physical constraints have already been encoded in the mathematical model; however, Liu et al. (2011) propose an approach that guarantees passing those constraints in the linear case. The indication of such constraints related to load forecasting applications has not been investigated in the literature. As STLF mainly applies to aggregated loads, the dynamic of loads that follow the physics law is not easily observed. Considering the ERCOT map in Figure 3.2, *to build a set*

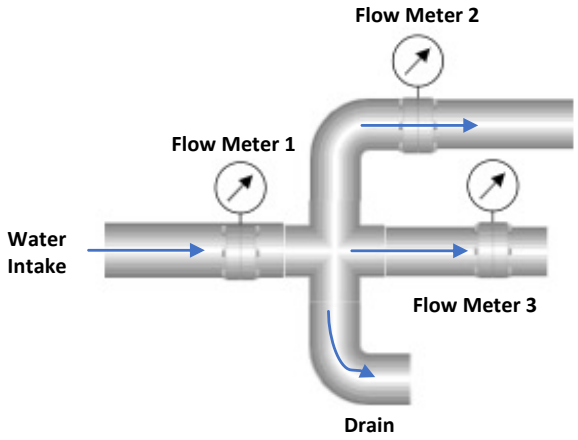


Figure 3.1: Water pipeline flow constraint.

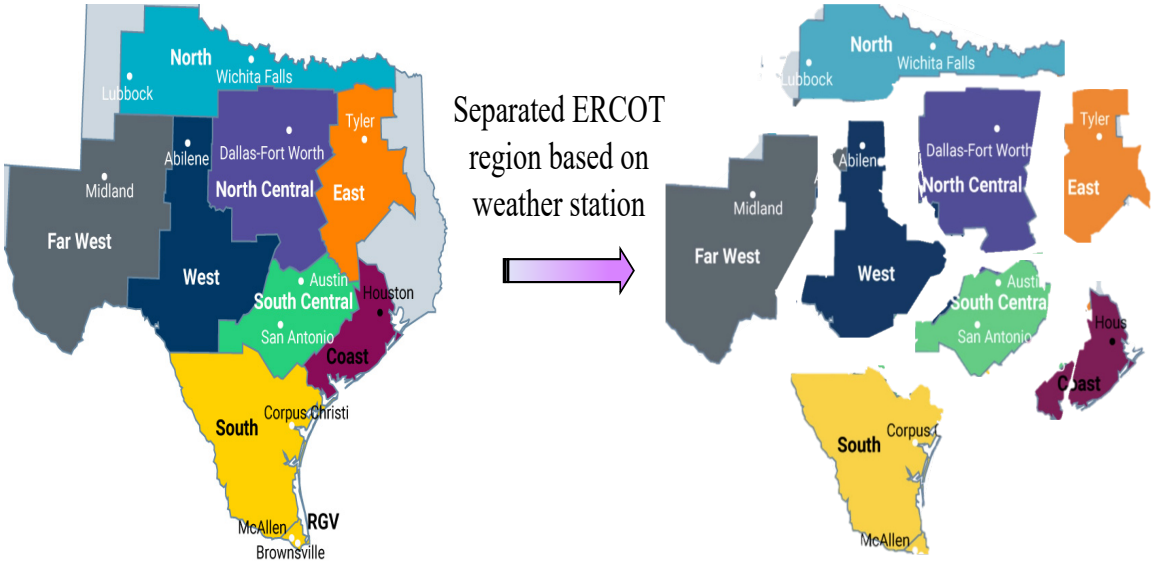


Figure 3.2: ERCOT weather-based station map with a representation of separated stations.

of physical-based constraints, the spatial distribution of various zones is considered. That is, a form of the distributed station is defined for load forecasting. For example, the ERCOT load map can be separated based on eight different weather zones used for whole-area load forecasting. Each zone deploys its weather station to STFL, which may also represent an aggregate. The proposed concept is illustrated for the ERCOT map in Figure 3.2.

3.5 Similarity Measure

Generally speaking, we investigate the relation between the different zones to derive constraints. We are looking for an index representing forecasted variations between zones in this framework. When an attacker intends to inject false data into some weather stations, not all, these indices may identify malicious action. Here, similarity metrics applied in clustering time series are considered to find a relation between zones. In fact, the goal is to explore the physical-based constraints $g(\cdot)$ between zones that these similarity measures may capture.

Definition 1. *The similarity measures $D(X, Y)$ between time series X and Y is a function taking two-time series as inputs and returning the distance d between them Esling and Agon (2012).*

Where $X = \{x_0, x_1, ..., x_{N\text{-}1}\}$ and $Y = \{y_0, y_1, ..., y_{N\text{-}1}\}$. The concept of similarity measure is shown in Figure 3.3. Two common approaches for similarity measure are considered to deploy as shape-based and feature-based methods.

3.5.1 Shape-based Approach

Here, distances are based on directly comparing the raw values and the shape of the series in different manners. That is, distances compare the overall shape of the series. L_p norms are the most widely used distance measures for time series clustering. Table 3.1 shows the definition of the norms. Due to its simplicity, Euclidean distance

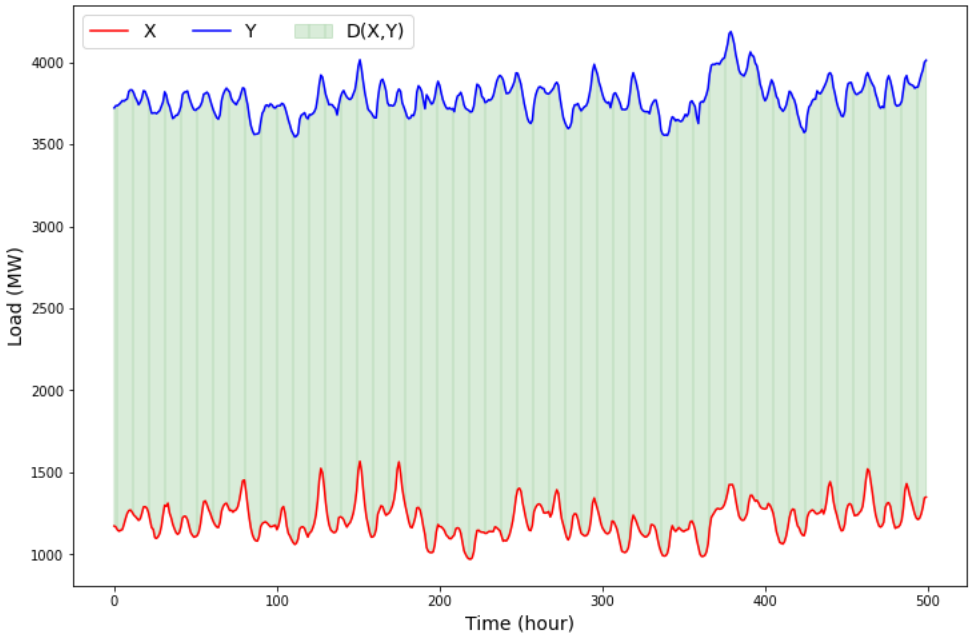


Figure 3.3: Distance between two time series.
Shaded area denotes the distance measure between time series X and Y

Table 3.1: Different L_p distances Fu (2011).

Distance	p	Formula
Manhattan	$p = 1$	$\sum_{i=0}^{N-1} \lvert x_i - y_i \rvert$
Minkowski	$1 < p < \inf$	$\sqrt[p]{\sum_{i=0}^{N-1} (x_i - y_i)^p}$
Euclidean	$p = 2$	$\sqrt{\sum_{i=0}^{N-1} (x_i - y_i)^2}$
Infinite norm	$p = \inf$	$\max_{i=0,\ldots,N-1} \lvert x_i - y_i \rvert$

N denotes the length of the time series.

is a general practice in shape-based methods. Euclidean distance is invariant when dealing with changes in the order that time features are presented. Then d_{EUC} is as

$$d_{EUC}(X,Y) = \sqrt{\sum_{i=0}^{N-1} (x_i - y_i)^2} \tag{3.5}$$

3.5.2 Feature-based Approach

The feature-based method focuses on extracting a set of features from the data presented in time series and calculating the similarity between the features instead of using the raw values of the series. Some of the most used distances based on time series features are as follows.

Correlation-based Distance

One index is to use the Pearson's correlation factor for two time series. The time series are similar if they are highly correlated, even though the observed values may be far apart in terms of the Euclidean distance. Based on Pearson's correlation, Golay et al. (1998) suggest two correlation-based distances for time series X and Y as follows

$$d_{COR\cdot 1}(X,Y) = \sqrt{2\left(1 - COR\left(X,Y\right)\right)} \tag{3.6}$$

$$d_{COR.2}(X,Y) = \sqrt{\left(\frac{1 - \mathrm{COR}\left(X,Y\right)}{1 + \mathrm{COR}\left(X,Y\right)}\right)^{\beta}} \tag{3.7}$$

where $\beta > 0$ is a distance decreasing parameter, and COR is the correlation between X and Y defined as

$$COR(X,Y) = \frac{\sum_{i=0}^{N-1}\left(x_i - \bar{x}\right)\left(y_i - \bar{y}\right)}{\sqrt{\left(x_i - \bar{x}\right)^2}\sqrt{\left(y_i - \bar{y}\right)^2}} \tag{3.8}$$

where $\bar{x}$ and $\bar{y}$ are the mean values of X and Y. It can be observed that a strong positive correlation results in small-scale correlation-based distances, which implies high similarity.

Autocorrelation-based Distance

The other feature-based method is based on estimated autocorrelation functions. The autocorrelation function is the normalized autocovariance function indicating the estimated autocorrelation vectors of two times series as $\hat{\rho}_{X_T}$ and $\hat{\rho}_{Y_T}$, the autocorrelation-based distances between X and Y is defined as follows Galeano and Peña (2001)

$$d_{ACF}\left(X,Y\right)=\sqrt{\left(\hat{\rho}_{X_T}-\hat{\rho}_{Y_T}\right)^{\top}\Omega\left(\hat{\rho}_{X_T}-\hat{\rho}_{Y_T}\right)} \tag{3.9}$$

where Ω represents a weight matrix, and T is the sample size.

Periodogram-based Distance

This method computes the distance between periodograms of two time series in the frequency domain. A periodogram is an estimate of the spectral density of a signal. For a stationary time series process with finite length, the periodogram at the Fourier frequency $\omega_j = (2\pi j)/N$ for $j = 1, 2, \ldots, [N/2]$ (where $[N/2]$ is the largest integer less or equal to $n/2$) is defined as

$$\boldsymbol{P}_x(\omega)=\frac{1}{N}|\sum_{t=1}^{N}x_t e^{-it\omega_j}|^2 \tag{3.10}$$

The scaled periodogram distance can be defined as Caiado et al. (2006)

$$d_{\mathrm{P}}(X,Y)=\sqrt{\sum_{j=1}^{[N/2]}\left[\boldsymbol{P}_x\left(w_j\right)-\boldsymbol{P}_y\left(w_j\right)\right]^2} \tag{3.11}$$

The normalized version gives more weight to the shape of the curve, while the non-normalized contributes to the scale. Measures based on the autocorrelations and measures based on the periodogram are related. However, this application could provide different beneficial estimation results.

Symbolic Representation

The transformation of time series into sequences of discretized symbols can be efficiently processed to extract information about the underlying processes. The symbolic aggregate approXimation (SAX) method proposed in Lin et al. (2003) allows us to investigate the dissimilarity based on the symbolic representation of time series to find the true dissimilarity between the original time series. It lets time series of arbitrary length N be reduced to a string of arbitrary length W ($W < N$, typically $W << N$). The SAX method follows these steps Lin et al. (2003):

- Normalizing each time series to have zero mean and standard deviation of one to avoid misleading comparison.

- Converting to piecewise aggregate approximation (PAA):
  A time series T of length N can be defined in a W-dimensional space by a vector $\overline{T} = \overline{t_1}, \overline{t_2}, \ldots, \overline{t_W}$. The i^{th} element of $\overline{T}$ is calculated by the following equation:

$$\overline{t_i} = \frac{W}{N} \sum_{j=\frac{N}{W}(i-1)+1}^{\frac{N}{W}i} t_j \tag{3.12}$$

  Generally speaking, data is divided into W equal-sized sections, and the mean value of the data falling within a section is computed, and a vector of these means is assigned as a reduced representation. The PPA representation for time series X (Figure 3.3) is computed for three different window sizes and illustrated in Figure 3.4. The larger the window size, the more reduction in data size, and vice versa.

- Discrete representation of obtained PPA. Given the normalization with a highly Gaussian distribution, we can apply a discretization method to generate symbols with equiprobability. In this step, a "breakpoints" list $\mathcal{B} = \beta_1, \beta_2, \ldots, \beta_{\alpha-1}$ needs to be defined to produce α equal-sized areas of area under Gaussian curve $\mathcal{N}(0,1)$ from β_i to $\beta_{i+1} = 1/\alpha$. Once the breakpoints are followed

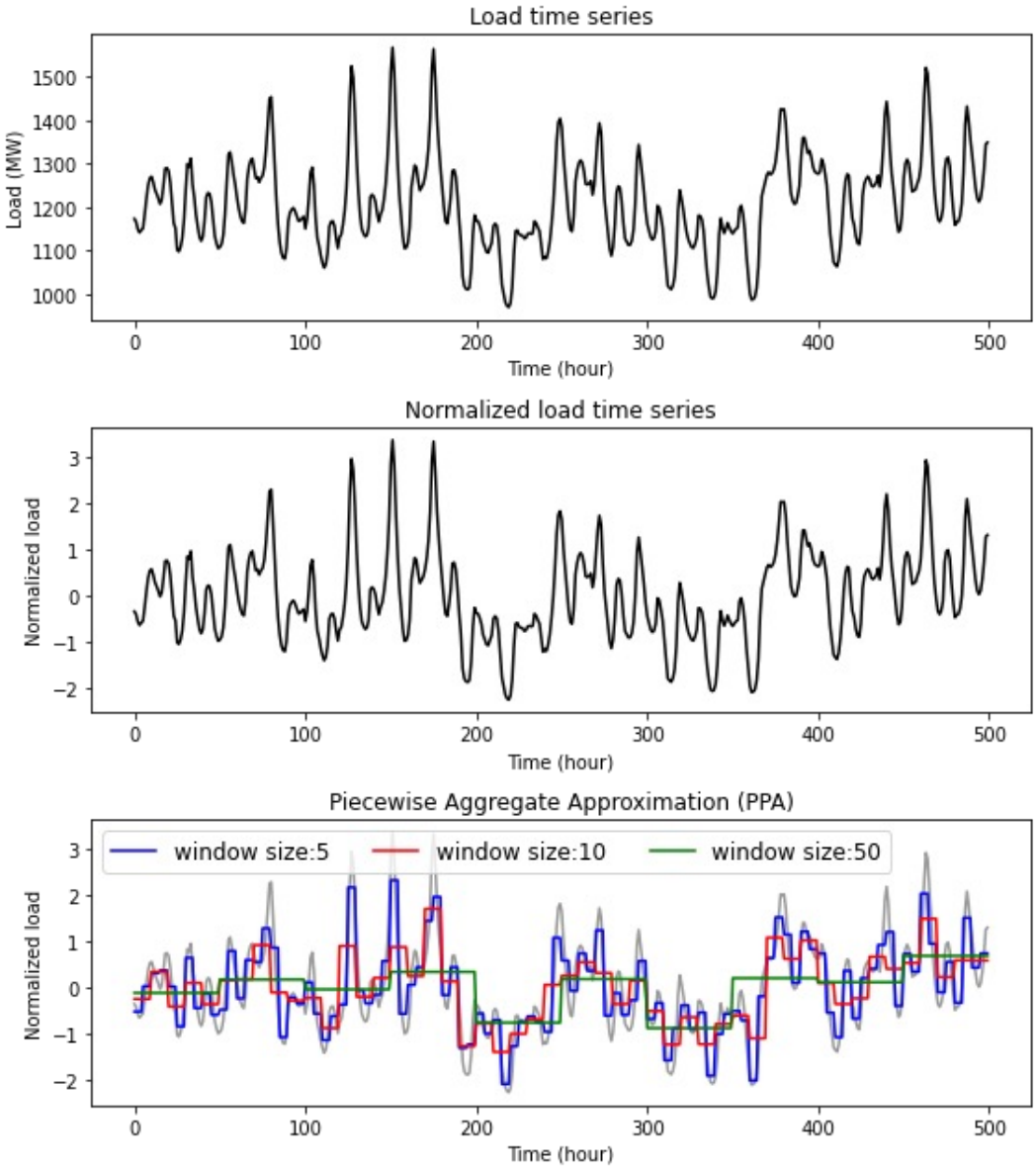


Figure 3.4: An example for PPA representation of a time series.

by discretization, all PPA coefficients are mapped to a symbol based on breakpoints.

- The concatenation of symbols provides a list of the symbol as a word. The number of symbols is defined by α value. For instance, for $N = 500$, $W = 100$ and $\alpha = 3$, we can assign three letters, such as a,b,c for each equal-sized area of Gaussian curve as shown in Figure 3.5. Here word as output is $\underbrace{abaca\ldots cbc}_{\text{W=100}}$. The SAX presentation for our example is illustrated in Figure 3.6 for $\alpha = 2, 4, 16$, where α impacts discretizing levels, i.e., the number of letters in the word output.

- Computing distance of SAX representation of time series as Lin et al. (2003):

$$\text{MINDIST}(\hat{X}, \hat{Y}) \equiv \sqrt{\frac{N}{W}} \sqrt{\sum_{i=1}^{W} (dist(\hat{x}_i, \hat{y}_i))^2} \tag{3.13}$$

where $\hat{X}, \hat{Y}$ are the SAX representation of time series X, Y, the `dist()` function computes distance between each symbol (letter) $\hat{x}, \hat{y}$ using a lookup table illustrated in Table 3.2. The lookup table is only generated once for a specific α, and cell (i, j) value can be calculated as:

$$\text{cell(i,j)} = \begin{cases} 0, & \text{if } |(i,j)| \leq 1 \\ \beta_{max(i,j)-1} - \beta_{min(i,j)}, & \text{if otherwise} \end{cases} \tag{3.14}$$

Where β is a breakpoint, and i and j are lookup table indexes.

More details about the procedure can be found in Lin et al. (2003).

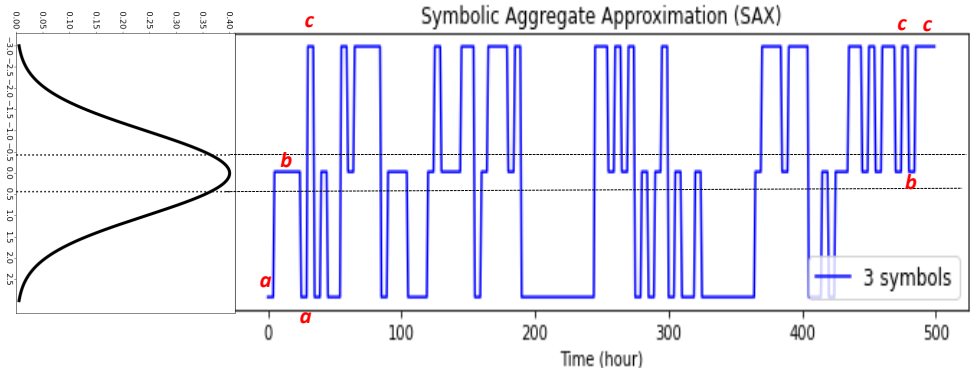


Figure 3.5: Word presentation in the SAX procedure.

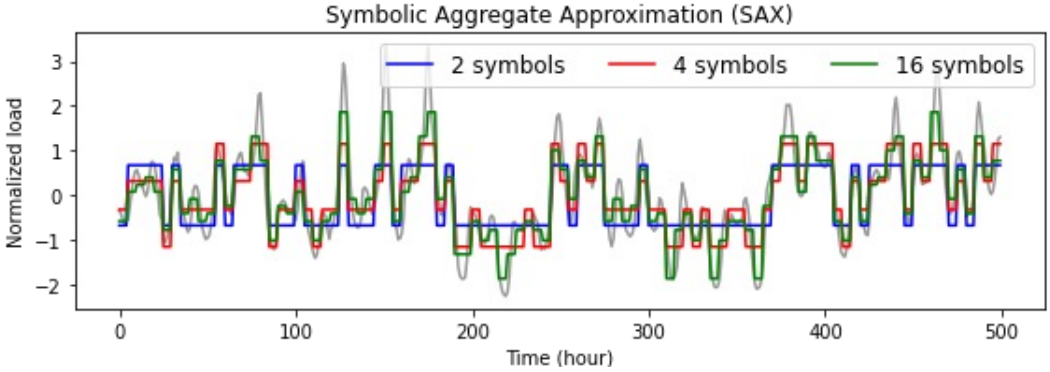


Figure 3.6: SAX presentation of a time series.

Table 3.2: Lookup table of the `dist()` function for $\alpha = 3$.

	a	b	c
a	0	0	0.67
b	0	0	0
c	0.67	0	0

3.5.3 Simulation Framework

Dataset

The ERCOT area can be categorized based on eight weather stations, as shown in Figure 3.2. The data is a historical hourly load for the summer of 2020 and is accessible from the ERCOT website. The dataset includes both the overall consumed load and individual area load. Two `West` and `FarWest` areas are selected to apply the methods, and their load profile is illustrated in Figure 3.7. The ERCOT website does not provide any information about temperature data, so temperature data is collected from automated surface observing systems (ASOS) corresponding to the `West` and `FarWest` weather stations. The pre-processing of the dataset includes handling missing values by past valid data and removing wrong observations (repeated data points), particularly for the temperature data. Figure 3.8 shows the recorded load and temperature. That implies that high temperature causes increased use of demand-side devices such as turning air conditioners on.

Correlation Analysis

To explore possible relations between the loads in the `West` and `FarWest` of the ERCOT, first, the correlation analysis between load data is calculated, and results are shown in Figure 3.9. Although the two zones are geographically separated, these loads correlate strongly. The reason could be the similarity of weather patterns in each zone that demonstrates hidden physical associations.

STLF Modeling

Two MLR models are applied for STLF modeling since the impact of temperature data as an independent variable may be seen explicitly in the formulation. Note that other techniques, either statistical or AI methods, are applicable in this case. Two models, including the interaction effect of independent variables, are assumed Hong

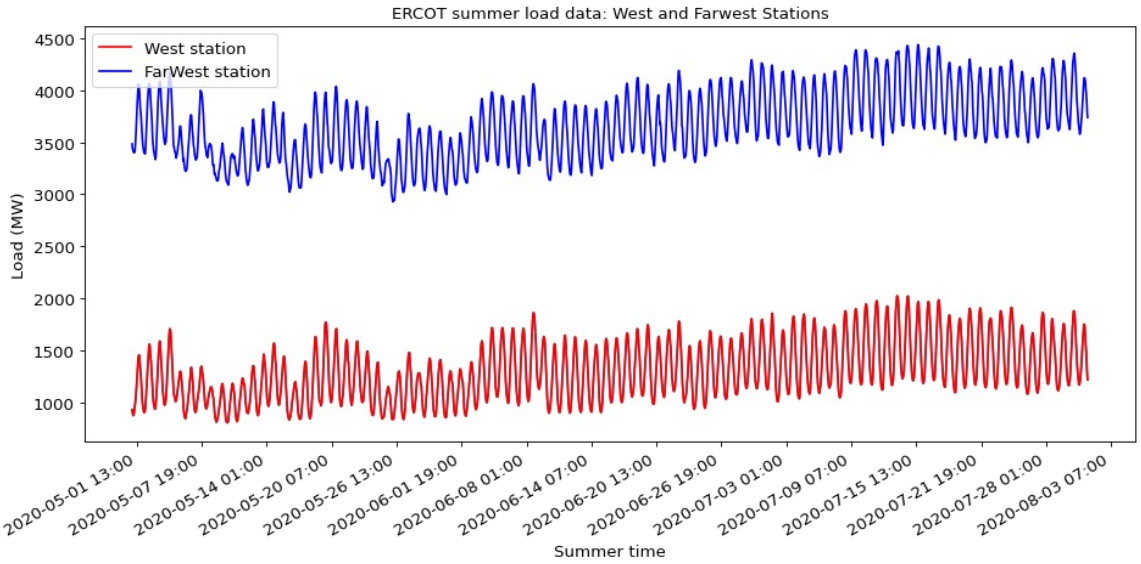


Figure 3.7: Summer 2020 ERCOT load: West and FarWest stations.

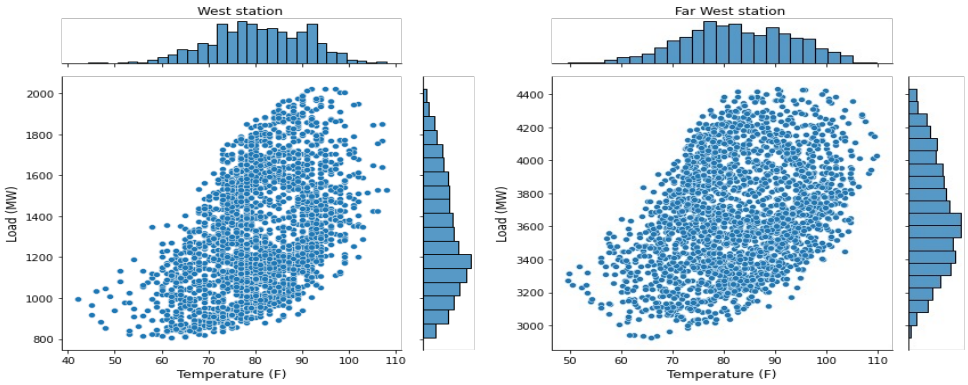


Figure 3.8: Load vs. temperature curve.

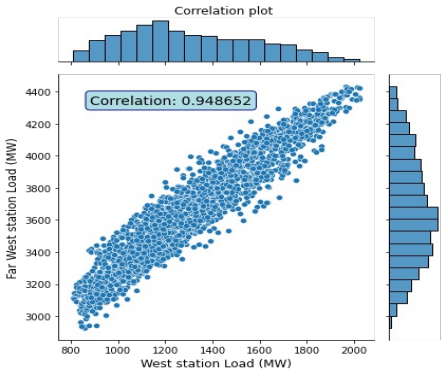


Figure 3.9: West and FarWest stations load correlation.

et al. (2011)

$$f_1 = \beta_0 + \beta_1 T + \beta_1 H + \beta_2 D + \beta_3 LL_{1w} + \beta_4 LL_{2w} \tag{3.15}$$

$$f_2 = \beta_0 + \beta_1 DH + \beta_2 MT + \beta_3 MT^2 + \beta_4 MT^3 + \beta_5 HT + \beta_5 HT^2 + \beta_6 HT^3 \tag{3.16}$$

Where f_1, and f_2 are the forecasted load models. The model parameters $\vec{\beta}$ are obtained based on the least squares error (LSE) method. The variables D, M, and H denote the day of the week, excluding the weekend, month of the year, and hour of the day, respectively. T is the temperature value, and LL_{1w} and LL_{2w} express one and two-week lagged load data, respectively.

Performance Metrics

For this regression task, mean absolute error (MAE) as a measure of errors between observations and predictions, and adjusted R-squared R^2_{adj} indicating corrected goodness-of-fit are chosen for the performance analysis and defined as

$$MAE = \frac{\sum_i^n |\hat{y}_i - y_i|}{n} \tag{3.17}$$

$$R^2 = 1 - \frac{\sum_i^n (\hat{y}_i - \bar{y}_i)^2}{\sum_i^n (y_i - \bar{y}_i)^2} \rightarrow R^2_{adj} = 1 - \frac{(1 - R^2)(n-1)}{(n-p-1)} \tag{3.18}$$

Where n is the total number of samples, $\hat{y}$ is the model output, $\bar{y}$ denotes the average of observations, y denotes real observations, and p indicates the number of independent variables.

3.5.4 Results

Both models consist of continuous variables and categorical variables. The categorical variables need to be coded into a series of variables to be used in the regression modeling. So, variables D, M, and H are encoded as a constant factor in the R programming language. The data set is randomly divided into 70% and 30% for the train and test sets, respectively. Figure 3.10 shows the model's results. The outcomes

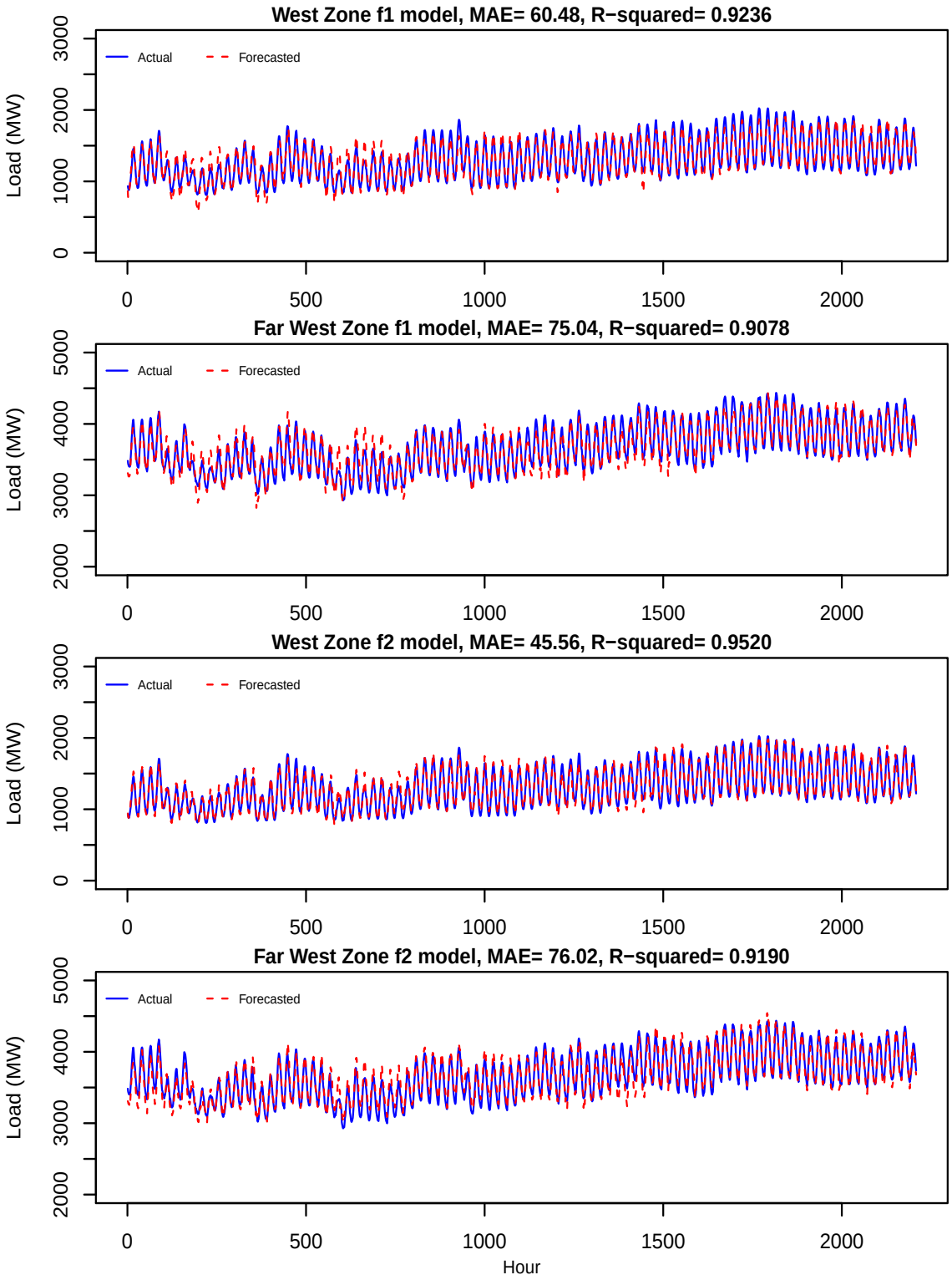


Figure 3.10: MLR models performance: MAE and adjusted R^2.

indicate that either f_1 or f_2 model could efficiently represent the load for both zones.

Once the STLF model is acceptably defined, Gaussian noise with zero mean and unit variance is injected into `West` zone temperature data to only mimic malicious action. Then, the similarity measure methods for the predicted load are applied to see the variation in the measures.

Table 3.3 indicates the variation of similarity measure indices in the presence of the attack. Note that comparing the results between indices is misleading since each measure carries a different scale. The similarity measures change when there is false injection data. Thus, this may be a suitable candidate for constraints in STLF. Among the methods, the variation in d_{SAX} is the largest. The reason can be that the distance measure defined in the symbolic approach creates a lower bound than the distance measures defined in the original time series. Also, the time series is transferred to symbolic representation, and then the variation in data caused by false data injection is more subtle in the SAX framework. The changes in measures are not constant values and will vary under different scenarios, such as other Gaussian signals. Finding an explicit formula or the upper bound capturing different scenarios is essential. In this case, to inject data with a destructive impact on the STLF, attackers must build an attack vector to bypass the measures satisfying the STLF similarity measures.

Various Attack Scenarios

In this section, we assess the proposed methods for various types of attacks. In the literature, intelligent attacks are often called adversarial examples, where the system's output is intentionally altered according to the attacker's objectives. In fact, the adversarial attack is a malicious attempt to perturb a data point to another point such that a sample belongs to a certain target adversarial class Goodfellow et al. (2014). This case is primarily applicable to classification tasks. The following scenarios are considered to resemble malicious action:

Table 3.3: Similarity measures results.

Method		No False Injection		False Injection	
	No Model	f_1	f_2	f_1	f_2
d_{ECU}	110644.5	110587.1	110675.4	110652.9	110602.3
d_{COR1}	0.3204611	0.3183464	0.2687631	0.326226	0.2826415
d_{ACF}	1.247954	1.146977	1.015968	1.149789	1.040784
d_p	0.1336534	0.1309215	0.1109201	0.1273667	0.1091463
d_{SAX}	2.004495	1.735943	1.417392	2.454994	1.002247

- Gaussian perturbations

In the case of a regression task, where the output consists of forecasted data, the aforementioned examples may not be applicable as there is no ground truth for an attacker to manipulate the output. Hence, most attackers are designed based on the nature of the task itself, and a systemic way to generate such scenarios is rarely found. For example, in STLF, attackers may attempt to reduce or increase the peak load value to disrupt scheduling and planning. One approach to achieve this in our framework could be by manipulating temperature variables, which can significantly impact energy consumption patterns. By considering the `West` station, we analyze the indices for various Gaussian noises with $variance = 2, 5, 10$. This leads to different signal-to-noise ratios (SNR) defined as the ratio of signal power to noise power

$$SNR_{dB} = 10log_{10}\left(\frac{P_{signal}}{P_{noise}}\right) \tag{3.19}$$

The results for both f_1 and f_2 are displayed in Figure 3.11. The y-axis represents the percentage of measurement changes when no false data is injected into temperature, while the x-axis represents different SNR cases in dB. Among the measures, d_{SAX} exhibits superior performance, demonstrating greater variability than other indices. This implies that as the noise increases, there are more pronounced changes in the symbolic distance, making it a suitable candidate for anomaly detection.

- Intra-day perturbation

In a different scenario, we can manipulate temperature data during specific time periods, such as peak and/or off-peak hours. This approach involves imitating patterns that could have negative consequences during those particular times, intending to deceive the model. In this case, we focus on the temperature dataset and select samples to manipulate based on two factors: (A) the percentage that is added to the sample values, and (B) the samples that are closer to the maximum values of temperature, specifically related to quartiles, such as the B^{th} percentile. The B^{th}

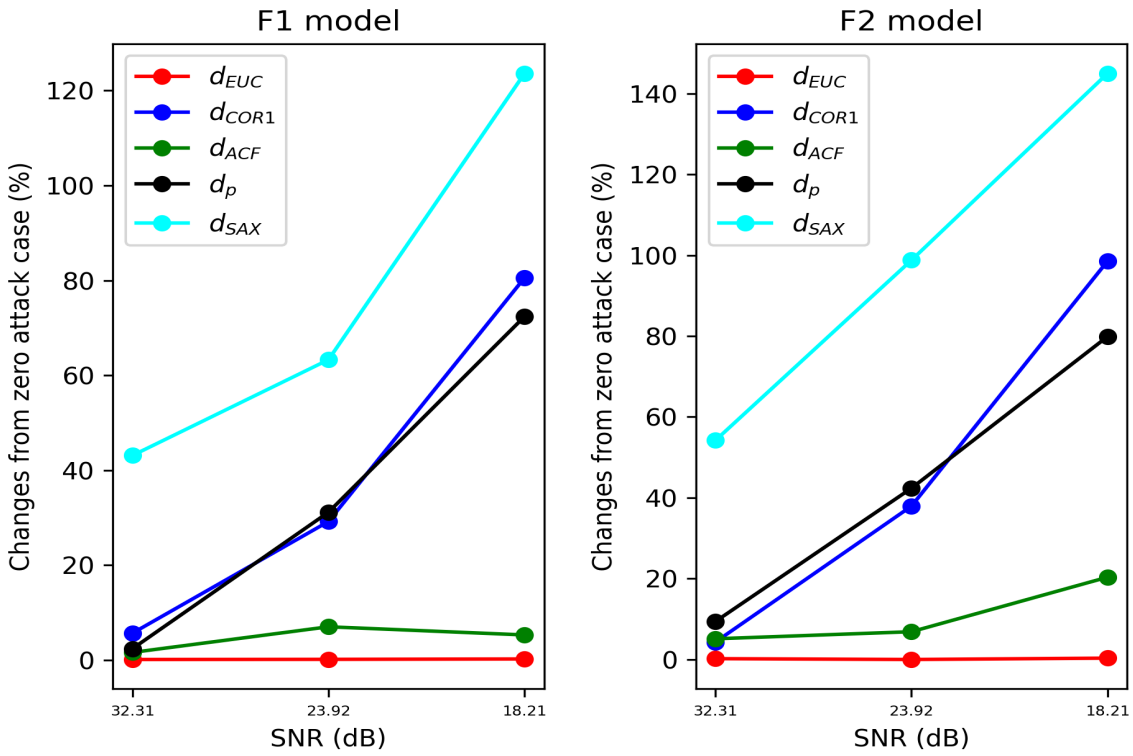


Figure 3.11: Variation of SM indices for different SNR cases.

percentile represents the value that separates the lowest B% of the data from the remaining (100-B)% of data values. This process is reminiscent of increased load forecasting, as it aims to simulate additional hot hours in the data. In this manner, the model could be influenced to predict outcomes that align with the manipulator's objectives, leading to potential misinterpretations or false conclusions.

Regarding the `West` station, Table3.4 presents the case results with varying the two factors mentioned earlier. It is evident that the percentage variation for d_{SAX} is significantly large, reaffirming the efficiency of SAX methods. However, the values are nearly identical across the different cases. This suggests that the SAX distance is insensitive to variations in the intra-day scenario, as the sample data for perturbation is chosen from a specific quartile of data that may be closely clustered together due to the pattern of consecutive hot days, not evenly distributed throughout the time series. Furthermore, d_p also exhibits substantial variation compared to the previous scenario, demonstrating similar results to SAX. By intentionally selecting samples to manipulate at different percentages by B, the metrics based on the frequency domain can effectively capture the anomaly. This is because the distribution of different frequencies present in the time series (frequency content) has been altered in this case. Notably, f_2 is more sensitive than f_1 as the former model incorporates a greater temperature impact on the model's performance.

3.6 Lag Relation Analysis

Referring to the framework proposed in Section 3.4, we can establish a mining approach for dynamic correlations. In experimental research, such as climate change, analyzing lagged correlations among sensors from various locations enables scientists to determine the origins of events over time Chan (1992), or monitoring the performance of large-scale systems, such as data centers, involves mining lagged correlations to gain insights into the shared resources Kutare et al. (2010). The idea of lagged correlation in time series is depicted in Figure 3.12, where time series 1 is

Table 3.4: Percentage variation of SM methods for Intra-day perturbations.

Methods	Case							
	A: 5%, B: 95%		A: 10%, B:95%		A: 10%, B: 90%		A: 10%, B: 15%	
	f_1	f_2	f_1	f_2	f_1	f_2	f_1	f_2
d_{ECU}	0.09	0.07	0.29	0.24	0.52	0.47	0.83	0.77
d_{COR1}	1.08	1.74	1.17	1.24	2.91	4.46	6.06	9.06
d_{ACF}	5.71	5.73	11.38	10.56	14.08	12.34	15.92	12.46
d_p	11.22	12.24	22.86	22.80	28.53	28.46	31.92	31.19
d_{SAX}	18.35	29.29	18.35	29.29	18.35	29.29	0.00	29.29

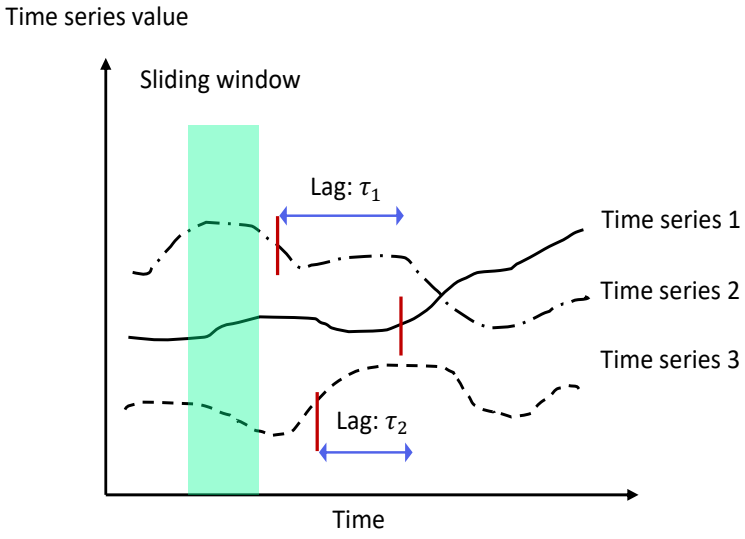


Figure 3.12: Lagged correlation over time series.

correlated to time series 2 and 3 with the lag number τ_1 and τ_1, respectively. The focus here is on Pearson correlation as a popular technique to detect dependency to establish lag relationships for exploring correlations among time series data of load stations. In our STLF application, the objective is to identify the load stations with the highest lag-based correlations. This analysis enables us to determine the most correlated stations based on lag data and subsequently identify the lag duration that aids in detecting anomalies.

3.6.1 Lag Correlation

For a time series i, the sliding window of length h ending at timestamp t is denoted by $s_i^t = (s_{i,t\text{-}h+1}, \ldots, s_{i,t})$ and $s_i^t \in \mathbb{R}^h$ (t is the latest time index). Pearson correlation between sliding windows s_i^{t1} and s_j^{t2} from time series i and j is defined as Guo (2017)

$$\text{rel}\left(\boldsymbol{s}_i^{t_1}, \boldsymbol{s}_j^{t_2}\right) = \frac{\left(\boldsymbol{s}_i^{t_1} - \mu\left(\boldsymbol{s}_i^{t_1}\right) \cdot \mathbf{1}\right) \cdot \left(\boldsymbol{s}_j^{t_2} - \mu\left(\boldsymbol{s}_j^{t_2}\right) \cdot \mathbf{1}\right)}{(h-1)\sigma\left(\boldsymbol{s}_i^{t_1}\right)\sigma\left(\boldsymbol{s}_j^{t_2}\right)} \tag{3.20}$$

Where $\mathbf{1}$ is an all-one vector of dimension h, $\sigma(s_i)$ and $\mu(s_i)$ are the sample standard deviation and mean of the elements in $\boldsymbol{s}_i$, respectively. When $t_1 = t_2$, the correlation between sliding windows of time series i and j is measured as (3.20), representing the synchronized correlation. However, when $t_1 \neq t_2$ it reflects the lagged correlation, which is formally defined as follows:

Definition 2 (τ-lead-lag corrleation)**.** *For a pair of time series i and j ($1 \leq i, j \leq n$), given time instant t and lag τ, the τ-lead-lag relation $\rho_{i,j}(t,\tau)$ between time series i and j is defined as $\rho_{i,j}(t,\tau) = rel(s_i^t, s_j^{t+\tau})(s_i^t, s_j^{t+\tau} \in \mathbb{R}^h)$ Guo (2017).*

Time series i is the leader, and j is the follower. $\rho_{i,j}(t,\tau)$ measures to what extent time series i leads to a correlated variation in time series j with time lag τ.

In practical scenarios, users prioritize recent data to facilitate timely decision-making. Consequently, they must specify the maximum lag when establishing lag relationships. This maximum lag value signifies the historical time frame within

which one should analyze data to identify leading indicators for the current time series. Moreover, it can be interpreted as the duration in advance that users seek to predict future trends based on the detected lead-lag relationships Chan (1992). In our analysis, we will apply this framework to weather-based load stations to address cybersecurity tasks. Specifically, the lag value for a particular station will be utilized to monitor correlated stations and detect anomalies in the STLF process.

3.6.2 Simulation Framework

It is recommended to utilize data with short time stamps for efficient extraction of lag correlation analysis. This enables us to use it as a monitoring scheme, facilitating near-real-time decision-making. Moreover, operation decisions typically run every 10-15 minutes in the EMS to check the system performance and do some actions by operators. This also is an applicable time horizon for reliability concerns and the electricity market.

Dataset

Instead of utilizing one-hour data in Section 3.5.3, we will employ 5-minute data to establish a quick monitoring scheme. This data can be obtained from ERCOT's historical load data from a few days ago. The dataset consists of 5-minute historical load information for all eight stations, spanning from 2022-09-17 00:05 to 2022-09-20 17:15, consisting of 1071 samples. To facilitate practical analysis between the historical data and the output model for attack scenarios, we require temperature data for each station, which should align with the timestamps of the load data.

ASOS provides hourly temperature data, so we apply linear interpolation as a method to estimate values for the 5-minute data points. This interpolation technique creates a straight line between adjacent hourly data points and determines the corresponding values for the 20 data points along that line, each representing a 5-minute interval. Figure 3.13 shows the load and interpolated temperature. The flat

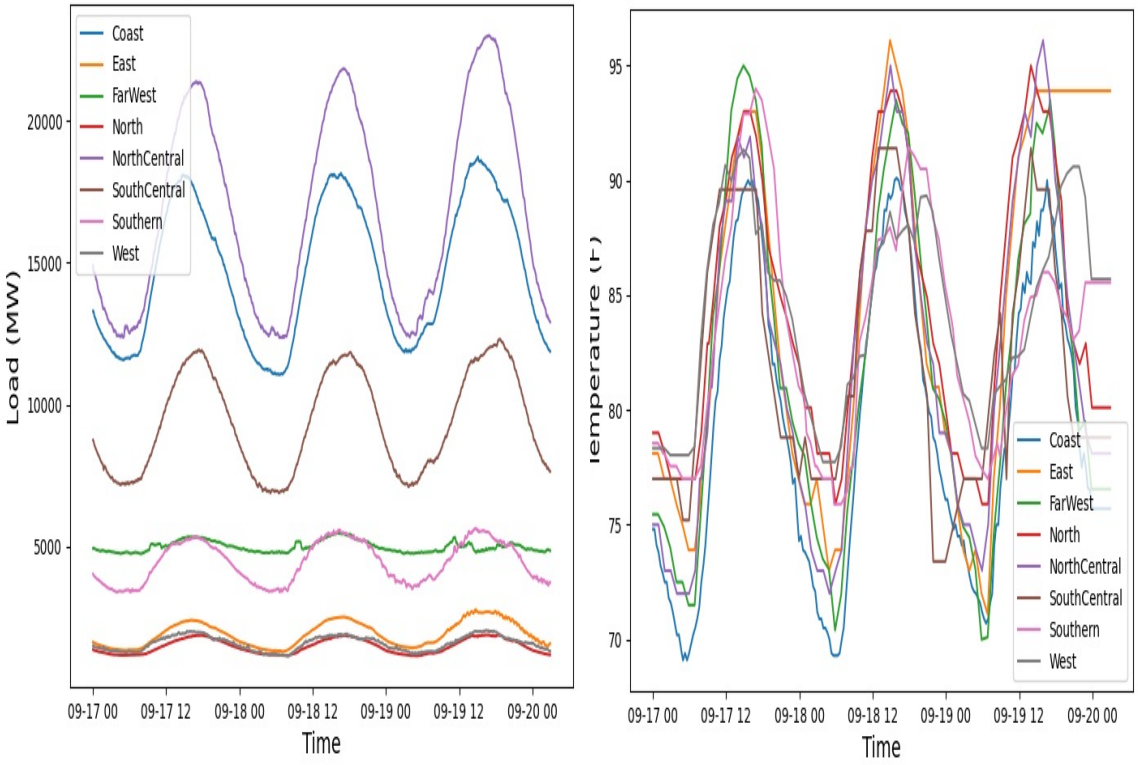


Figure 3.13: 5-minute data: the right figure is historical load data, and the left figure is interpolated temperature from ASOS.

line at the end of each temperature data is due to a lack of record data points at the range that are not recorded in the ASOS, and we substitute the last available value for those points leading to a straight line.

3.6.3 Results

In practice, the forecasted load data is generated by a forecasting model. Here we consider an MLR model, specifically, the model used before as f_1, which is computed for this dataset. The model outputs are illustrated in Figure 3.14, which effectively represents a set of observed data. The goodness of fit of the model is evaluated using the MAE. This framework allows us to simulate anomalies in temperature data that impact the forecasted load.

We first deploy the lag correlation framework for the recorded data. We consider a sliding window size of $h = 10$ and the number of lag steps as ± 24, corresponding to a search of approximately 2 hours for each sample. The lag correlation results for each station are shown in Table 3.5. In the table, each station is paired with another station that exhibits the most correlated relationship based on a specific lag step. Positive lag steps indicate future data points, which can be used for offline study and analysis. However, for online monitoring purposes, these positive lag steps are not applicable as they pertain to future data that is not yet available.

To resemble malicious action, Gaussian noise with zero mean and unit variance is randomly injected into 50% of the temperate data sample. Now, the model outputs the forecasted load for perturbed temperature, which is used for lag correlation analysis with the historical data. The results are shown in Table 3.6, along with the percentage of correlation changes compared to Table 3.5. All paired stations remain fixed except for `NorthCentral`, which has changed to `SouthCentral`. Also, most of the lag step values have changed to new values, indicating a shift in the correlated lag steps. This implies that the load data is not highly correlated with the lag step in Table 3.6, and there is a shifting pattern.

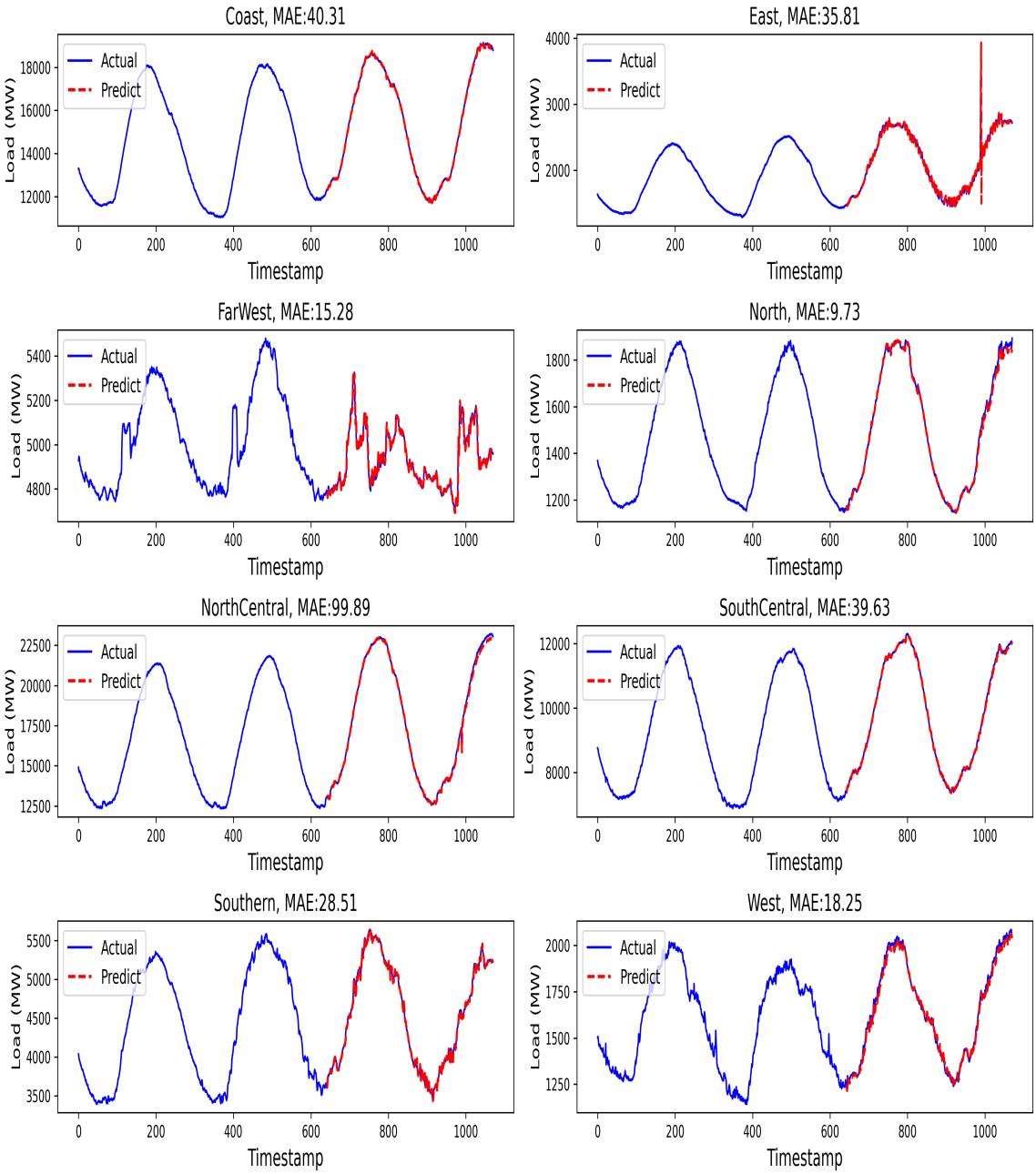


Figure 3.14: MLR outputs for 5-minute data.

Table 3.5: Lag correlation results for historical data.

Station	Correlated to	Correlation	Lag step
Coast	NorthCentral	0.989553	-6
East	NorthCentral	0.983166	-3
Farwest	South	0.76471	1
North	NorthCentral	0.992442	4
NorthCentral	North	0.992442	-4
SouthernCentral	NorthCentral	0.992014	4
South	NorthCentral	0.979007	-6
West	Coast	0.97659	6

Table 3.6: Lag correlation results for perturbed temperature data based on MLR model.

Station	Correlated to	Correlation	Change (%)	Lag step
Coast	NorthCentral	0.989568	0.001516	-6
East	NorthCentral	0.981342	0.185523	**-4**
Farwest	South	0.766965	0.294883	**-2**
North	NorthCentral	0.993323	0.088771	4
NorthCentral	**SouthCentral**	0.991639	0.080912	**-5**
SouthernCentral	NorthCentral	0.992528	0.051814	4
South	NorthCentral	0.980518	0.15434	**-7**
West	Coast	0.976842	0.025804	**5**

As we resemble malicious actions through temperature manipulation, these changes can be considered anomaly causes. By tracking the lag step values and/or paired stations, one can detect variations among the load stations and quickly identify anomalies. These observations lead us to consider the existence of an anomaly in a distributed fashion, where a malicious actor would need to operate on the paired stations simultaneously to avoid detection, especially if they have knowledge of the lag correlation analysis and the station pairing used in an LF model.

3.7 Summary

STLF plays an essential role in power system operation. Collecting temperature, as a critical input from online services, increases the possibility of malicious action. This chapter examines some physical constraints to address the deficiency of detection schemes. A new formulation of STLF based on different spatial coordination is proposed for imposing these constraints. First, similarity measure techniques are applied as constraints in the proposed approach. Simulation results indicate that the applied measures can encode constraints when temperature data is corrupted and be used as an anomaly detection. The simulation results suggest that the applied measures effectively encode constraints when temperature data is corrupted. The distance defined in symbolic space captures variations representing strict constraints according to the proposed STLF topology, outperforming various malicious scenarios. Furthermore, the distance obtained from the frequency domain can serve as a candidate for anomaly detection indices when malicious actions alter the frequency content of the data. Since the measures employed in the analysis may vary depending on the specific scenario, further research can be conducted to define explicit equations describing the constraints or establish upper bounds. Additionally, a lag correlation analysis is performed between load stations to determine the most correlated load stations and lag steps. By monitoring the lag step values and paired stations at a short time horizon, such as using 5-minute data, we can utilize this analysis to detect

anomalies in attacks involving temperature perturbations. This provides a valuable tool for identifying and responding to anomalous behavior.

Chapter 4

Graph-based Learning for Security Assessment

In the power system, security assessment plays a pivotal role in determining the safe operation in a normal situation and some contingencies scenarios. Electrical variables as input variables of the model are mainly considered to indicate the power system operation as secure or insecure, according to the reliability criteria for contingency scenarios. In this approach, the features are in grid format data, where the relation between features and any knowledge of network topology is absent. Moreover, the traditional and common models, such as ANN, are not applicable if the input variables are in the graph format structure. Therefore, we examine the security analysis in the GNN framework such that the GNN model incorporates the network connection and node neighbors' influence for the assessment. Here, the input features are separated graphs representing different network conditions in electrical and structural status. In this study, topological characteristics, as defined by network centrality measures, are incorporated into the feature vector to represent the structural properties of the network. The proposed model is then simulated using the IEEE 118-Bus system to assess the voltage static security. Following this simulation, the model's capacity is validated to ensure its effectiveness and performance.

4.1 Introduction

Security itself means being free from risk and threat. In this context, the power system can not be considered secure since it always anticipates the occurrence of disruption. Also, the possibility of an incident is increasing since the power system is increasingly integrating IBRs, such as wind turbines and solar panels Negnevitsky (2019). So, security in the power system measures the risk or danger of disruption of the continuously operating system. In practice, that is the ability of the system to withstand sudden disturbances with minimum disruption to its performance.

From an operational point of view, the power system is secured if important electrical variables are kept within an acceptable level, such as bus voltage magnitudes and angles, frequency, and power flows in response to disturbances (*contingencies*), such as an electrical short circuit, change of transmission system configurations due to faults or sudden load increase. The SA is an analysis performed to determine whether and to what extent a power system is safe from serious interference in its operation. The SA is carried outs to meet the operation requirement in two manifests Sittithumwat and Tomsovic (2002b):

1. Surviving the ensuing transient and moving into an acceptable steady-state condition.

2. In the new steady-state condition, all components operate within the established limit.

Followed by this time framework, static security assessment (SSA) evaluates the steady-state response, and DSA analyzes the transient response. We are interested in the SSA as utility companies mainly consider it for planning and operation purposes. The acceptable level of variables such as transient voltage magnitude dip and steady-state violation or frequency excursion is determined by reliability criteria provided by, for instance, the Western Electricity Coordinating Council (WECC) or the NERC standards. For instance, WECC criterion TPL-001-WECC-CRT-3.1 transmission

system planning performance provides steady-state voltage ranges at all applicable bulk-electric system (BES) buses following various probable contingencies. A typical voltage recovery curve is depicted in Figure 4.1, indicating the limit range for the voltage post-contingency. The SSA is about the power flow solution at the post-contingency that must comply with the above standard and criteria.

The SA can also target the frequency-related or voltage violation for both dynamic and static analyses. The former is becoming more challenging in power system operation and planning, especially with the increasing penetration level of IBRs, which bring about insufficient inertial and primary frequency responses Morovati and Pulgar-Painemal (2021); Morovati et al. (2021). The authors in Steinkohl et al. (2019) consider the frequency security analysis to provide an appropriate frequency control scheme when power systems utilize the wind energy or frequency security index. This determines the frequency security based on all aspects of the frequency profile presented to specify the relative distance from the security margin Arias et al. (2015). The significance of voltage violation is apparent as several large blackouts are due to the inadequate reactive power supply. For this purpose, the SA may perform to either estimate the distance to the nose point of P-V and/or V-Q curves as a margin Taylor (1994), or classify multiple operating conditions for voltage stability assessment Vanfretti and Arava (2020).

A typical P-V curve is shown in Figure 4.2. The graph is generated by conducting a power-flow simulation for two scenarios: the normal condition (case 1) and an N-1 contingency scenario (case 2). In both cases, the voltage of a specific bus is monitored while making incremental adjustments to the power. This iterative process continues until a power-flow divergence is observed. Every point on the graph signifies a stable operating state, demonstrating that the system has maintained a consistent level of operation. These points indicate that the real-power dispatch of the generation and voltage support equipment has been configured to meet the reliability criteria outlined by NERC/WECC for each operating point displayed on the graph, including the indicated operating limit. As voltage stability is a local phenomenon and is not

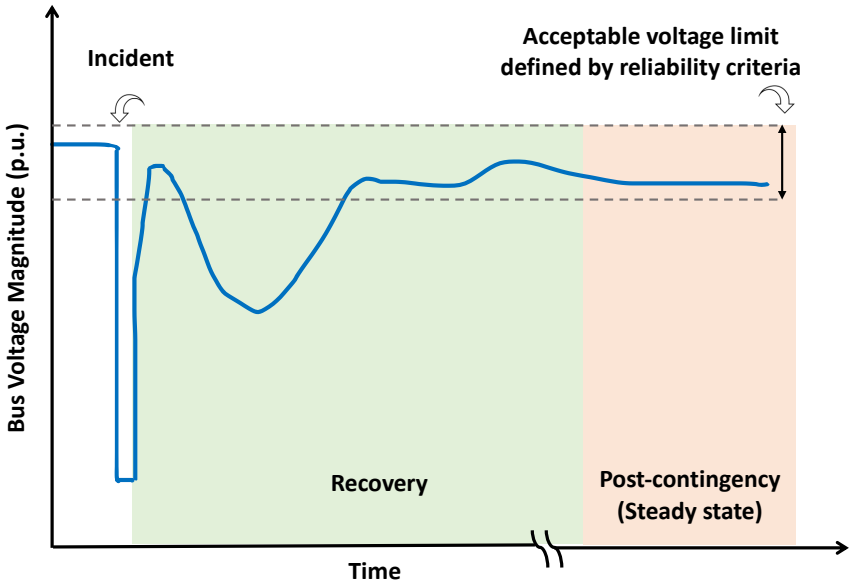


Figure 4.1: A typical voltage recovery curve.

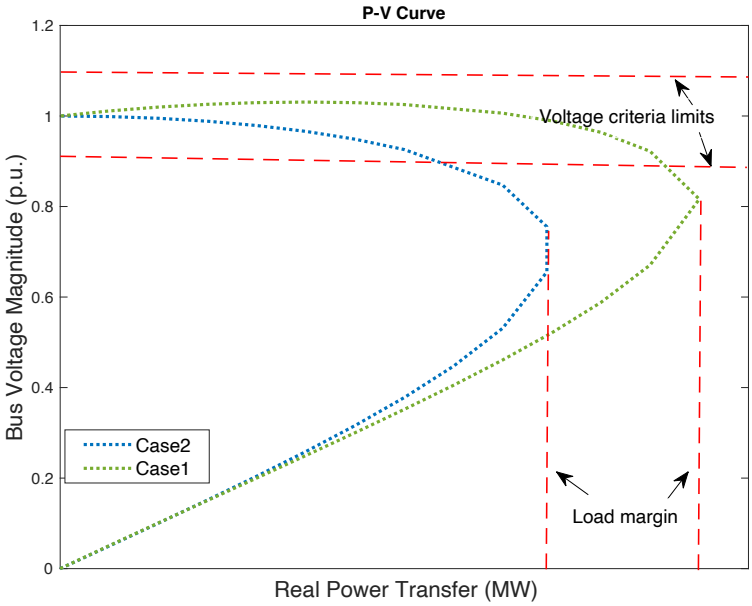


Figure 4.2: An illustration of the P-V curve method.

detectable by voltage itself, the P-V curve estimates the load margin to avoid voltage collapse.

The SA is also categorized for security classification or security margin estimation purposes. Classification determines whether the power system is secure or insecure concerning the threshold. In contrast, the distance (margin) to the insecure condition, the violation threshold, is computed in the security margin. For instance, an online voltage security assessment practice to prevent a large-scale blackout and an estimation loading margin regarding transient frequency criteria capture classification and estimation tasks, respectively Sittithumwat and Tomsovic (2005); Negnevitsky et al. (2015). This chapter focuses on classifying static voltage in the SA, followed by contingency scenarios.

Besides the traditional methods for the SA, such as lookup tables and nomograms, in which the operator decision was essential. A full nomogram defined by boundaries set with respect to limits representing various security criteria is shown in Figure 4.3. The automated SA mechanism uses a model to determine the security status regarding the value of system variables and the measurement of so-called features. Thanks to sensor data availability and/or parameter estimation, AI methods are extensively used in the SA literature. The applications of NN can be used to evaluate the system security by screening the credible contingencies with loading condition and the probable contingencies as the input Sunitha et al. (2013), and to estimate loadability margin concerning frequency deviation with preventive control Sittithumwat and Tomsovic (2002b). A real-time SA to increase awareness about plausible future insecurity is applied using the decision tree form the collection of PMUs data Mukherjee and De (2021). An attempt to classify whether the power system can tolerate an (N-1) fault during different conditions is analyzed via SVM with the principal component analysis (PCA) for dimensional reduction of feature space Andersson (2005). In addition to NN, the promising results of deep learning frameworks for image and speech recognition caused an emerging usage of DL for SA purposes to capture immense amounts of data and deliver valuable information.

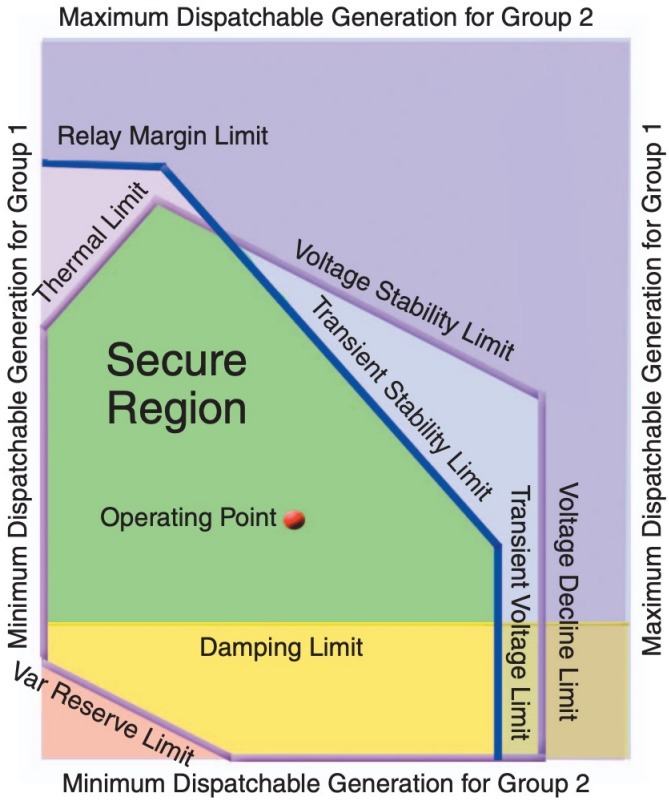


Figure 4.3: A full security nomogram Morison et al. (2004).

As a typical network model, convolutional neural network (CNN) can be exploited for power system transient stability assessment, instability mode prediction, and small-signal stability Shi et al. (2020); Arteaga et al. (2019b). Although ML/AI methods have demonstrated successful applications in various fields, such as image classification, many companies remain hesitant to adopt ML/AI approaches. Instead, the industry predominantly relies on solving the power flow using fast algorithms and resources.

All the above models are associated with grid structure data for input features, meaning that a fixed size of grid data, and it is assumed that instances are independent, is fed to the models. For example, even if a graph represents a grid data format, such as an image, it has a banded structure in its adjacency matrix since all nodes are formed in a grid. This is no longer valid for graph data as the number of neighbors to each node is variable, and differences in size and shape within the graph dataset can not be handled using resizing or crop operation in images. As a unique non-Euclidean data structure and the need for permutation invariant for machine learning models due to graph isomorphism, the GNN model is introduced. Graph analysis focuses on node classification, link prediction, and clustering tasks. Indeed, GNN models are DL-based methods performing on the graph domain.

Due to the promising results of GNN in social science, natural science, protein-protein interaction networks, and knowledge graphs, broad usage of GNN models can be noticed in the literature Wu et al. (2020). However, the application of GNN in power systems is little compared to other domains, and usage of the GNN models in power systems is discussed in Liao et al. (2021). For example, the GNN model using a power flow solution exploited for predicting the electricity market prices addresses scalability and adaptivity challenges of existing end-to-end optimal power flow (OPF) learning results Liu et al. (2021). In security concerns, Huang et al. (2020) provides a scheme combining GNN and recurrent neural networks for stability classification and critical generator identification in transient assessment. A graph convolutional network (GCN) framework can be applied for fault location

identification in a distribution network, indicating GCN model robustness to limited bus measurements and outperforming other machine learning models Chen et al. (2019a). Due to the lack of a GNN model for the SSA, this chapter seeks to form a GNN framework for voltage SSA.

Regardless of which model is used for the SA task, electrical variables such as active/reactive power line flow, bus voltage angle, magnitudes, and active and reactive power of each bus load are mainly considered for input features. This feature space needs the topological knowledge of the power system, as one may represent the power grid as a graph where buses and lines are illustrated as nodes and edges, respectively. The extensive scalability of the power system motivates researchers to model it as a graph to study the system vulnerability in the topological context using centrality measures. These measures may indicate the most salient part against random failures and directed attacks Wang et al. (2010); Hines et al. (2010b).

In this context, the power system characteristics coming from topological information may assist in analyzing the impact of network structure changes to enhance the model performance and ensure robustness for the SA. The centrality measures can be easily computed using the network topology processor's information implemented in EMS. To the best of our knowledge, there is no work in the literature to examine electrical and topological-related variables in the SA framework. Therefore, this chapter proposes a new method for voltage SSA based on the GNN model that combines electrical variables obtained by power flow solution and topological parameters defined by grid centrality measures

4.2 Problem Statement

In this section, the static voltage security analysis is discussed to determine the security status of the power system. Many sources make power systems vulnerable, such as natural calamities, complement failure, fault, internal or external intrusion, human error, etc. In this case, the power system should be able to continue servicing

in case of an unpredicted contingency. If any vulnerable sources interrupt services, such as an outage or blackout occurrence due to cascading failure, the system is insecure (vulnerable). In static security assessment, regardless of transient behavior, the post-contingency time framework is considered when the system reaches a new steady-state operating point. The system is statically secure if the new operating points meet the defined system limitation and reliability criteria. In this fashion, a fast and reliable solution is necessary to assess the security of numerous operating strategies to reduce the risk of catastrophic incidents. This task is involved due to vast sources of vulnerabilities, the large scale of the power system with nonlinear behavior, different operating and operational strategies, changes in topologies, and the computation burden. Therefore, a classification model is a practical approach to dealing with difficulties. Classifiers' merits are that they can be developed offline, current and future operating states can be quickly assessed, and classifying a new steady state power system condition into a secure or insecure class is trivial and does not need protracted computations of an analytical solution.

In the SSA framework, the security variables could be bus voltages or line flows indicating the thermal limits. Here, we consider bus voltage as a security variable; however, the proposed scheme can be applied to other variables and categories, such as dynamic assessment. In the SSA, following a contingency, each bus voltage value is analyzed at post-contingency in which the transient response has died down. As a result, the steady state of voltage (power flow solution) should not violate the range defined by operating limits. It is worth noting there is no updated guideline for the voltage violation range at the steady-state analysis when the IBRs utilize the power grid. However, its impact on the transient response of voltage trajectory for reliability criteria is discussed in Guideline (2018).

In this regard, the problem statement is straightforward: *following a contingency scenario, we seek to define a model that classifies the post-contingency condition of the power system (steady state) based on bus voltages according to a reliability criteria.*

Therefore, the SA model is to classify secure and insecure conditions and notifies the operators to steer the system away from the insecure state in adequate time.

To address the defined problem, a GNN framework for the SA is proposed. As the power grid may be analyzed in the graph representation, the problem here is formulated as a *graph-level classification*, and a graph including its information is assessed for security purposes. An overall framework of the proposed GNN model for SSA is shown in Figure 4.4. As seen, the GNN model is trained for a graph dataset, and the security of a graph input regarding all bus voltages is seen as the model output. The result of secure and insecure status encapsulates the overall condition of the graph according to violation of any bus voltage magnitude. The framework is not limited to voltage SSA and can quickly be adopted for other analyses of dynamic SA tasks. The details of the GNN-based model are described in the following section.

Graph input may also contain hidden information in its structural property, and shared local node information may enhance the model performance. Traditional and most applied models work with grid format input features to label the input dataset as secure/insecure for binary classification (or multi-class SSA Kalyani and Swarup (2010b)), where input features are independent, and there is no information between each feature. For the benefit of edge connectivity of the power grid and the use of the local node information from neighbors, the GNN framework is developed to boost model performance. In this framework, the status of the power grid at steady state condition after contingency is considered as one sample instead of independent variables, such as nodal voltage and line flow. For instance, the number of variables for one input of the non-GNN model could be the number of chosen features multiplied by the number of buses. In contrast, the GNN model only takes one graph as input, and all information is embedded in nodes or edges.

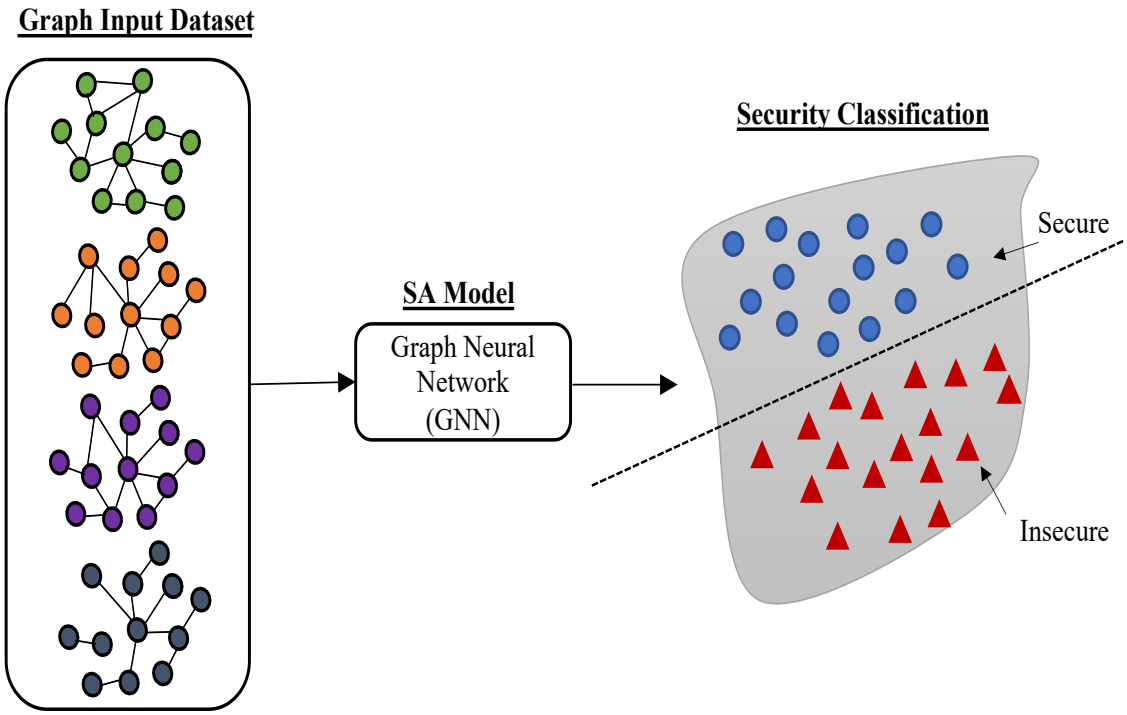


Figure 4.4: General GNN framework for the security assessment.

4.3 The Proposed Framework for the SA

Two following main modules can explain the proposed procedure for the SA model as presented in Figure 4.5.

- *Feature Generator Engine* to create input features,
- *GNN learning model* for the SA task.

4.3.1 Feature Generator Engine

Electrical Variables

Electrical features are selected based on engineering knowledge associated with the SA problem and statistical correlation coefficients to ensure variables fluctuate with each other and eliminate redundancy. The typical electrical variables include line active and reactive power, voltage magnitude, and angle. Considering the voltage SSA problem, the following are chosen as electrical features in the input dataset:

- The voltage magnitude of each bus, V_{mag}
- The active and reactive power of each bus, P, Q

As the power grid provides numerous measurements as an extensive dataset, the SA may involve the curse of dimensionality. Techniques, such as PCA and fisher discrimination, can be applied to identify the most significant and valuable subset of features for accurate classification Andersson (2005); Niazi et al. (2004); Jensen et al. (2001). Only three leading electrical variables are considered in the procedure, so dimensional reduction is no longer needed.

Topological Variables

Power grids have grown organically over the years in a random way to achieve economic benefits and safety, leading to a widely distributed grid with many

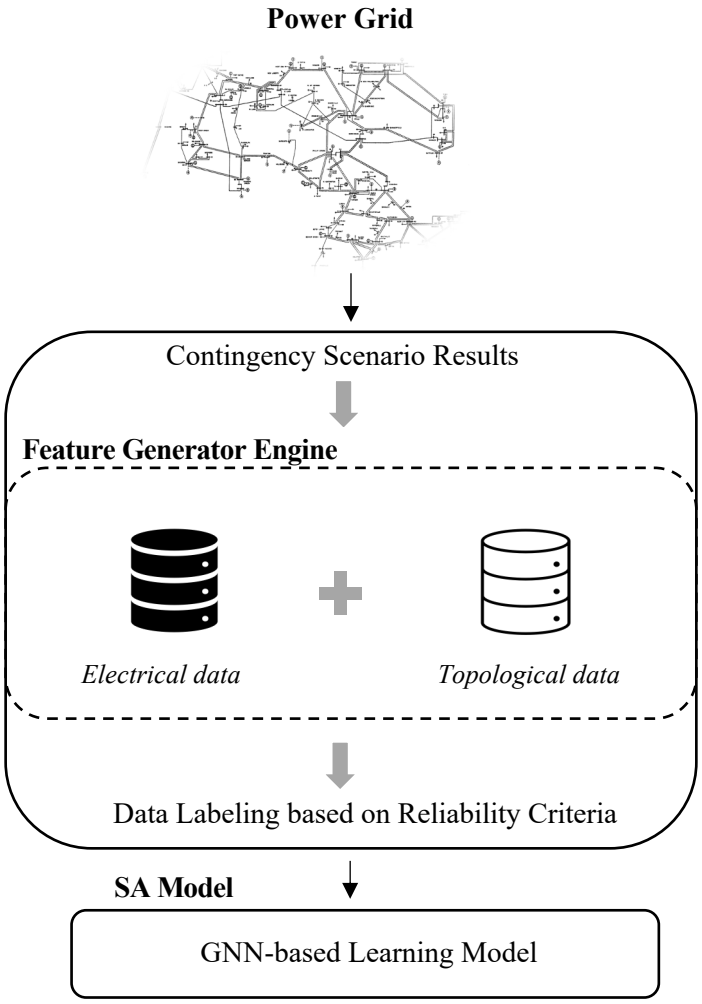


Figure 4.5: Procedure of the proposed GNN-based SA model.

connections between generation units and substations. Therefore, the complexity of the links and being a large-scale system lead researchers to study power grids in the context of graph representation using statistical tools for vulnerability studies Chu and Iu (2017). Table 5 in Pagani and Aiello (2013) reviews various resilience analysis and improvement studies in graph context. This motivates us to investigate the structural properties of the power grid and append topological features into the feature space.

In addition to knowing the number of nodes and edges in a graph, it is worth learning the network's characteristics to indicate the critical part of a network. The metrics so-called *graph centrality* generally measure a unit's prominence; in different substantive settings, i.e., identify the most critical nodes in a graph given its topology with the various definitions of importance. Preliminaries of graph theory are briefly stated in Appendix A. Many centrality measures have been proposed over the years Latora et al. (2017a); in this section, for a graph with V as a number of nodes and E as a number of edges, the most applicable measures in the power grid are discussed as follows to select a new feature for each bus defined in Newman (2018):

- *Degree centrality* (C_d) is a local measure and the simplest centrality measure. It implies that the nodes with a higher degree $deg(v)$, i.e., connected edges, are more solid, and the normalized degree centrality is defined as

$$C_d(v) = \frac{deg(v)}{n-1}$$

- *Clustering Coefficient* (C_c) is a measure of the degree to which nodes in a graph tend to cluster together. For each node i, it is the number of edges between neighbors of a node, divided by the total number of possible edges between those neighbors $C_{c_i} = 2e_i/k_i(k_i - 1)$ where k_i, e_i are the number of neighbors and connected edges between them, respectively.

- *Betweenness centrality* (C_b) consists both of a node and an edge. The most widely used node betweenness reflects a node's influence over the flow of information between other nodes, especially in cases where information flows over a network primarily following the shortest available path. The node betweenness centrality is defined as

$$C_b(v) = \frac{\sum_{s \neq v \neq t \in V} \sigma_{st}(v)/\sigma_{st}}{(n-1)(n-2)/2}$$

  where σ_{st} is the number of shortest paths from s to t and $\sigma_{st}(v)$ is the total number from the mentioned paths that pass through vertex v.

- *Closeness centrality* (C_k) is a way of detecting nodes that can spread information very efficiently through a graph. That is, a node is vital if it has a short distance from many other nodes and is defined as

$$C_k(v) = \frac{\sum_{t \in V \setminus v} d_G(v,t)}{n-1}$$

  where $d_G(v,t)$ is the shortest path length between vertices v and t. This measures how far away a node is from the rest of the network instead of its closeness. Therefore, some researchers define closeness to be reciprocal.

The general concept of the shortest path in a graph is not an appropriate metric for the power grid. The shortest path (geodesic path) between two nodes in a graph is a path with the minimum number of edges (or minimum sum of edge weights for a weighted graph). This definition should be modified to cope with power grid characteristics since the electrical flow finds a path with minimum impedance value. So, the *electrical distance* d_Z defined by Wang et al. (2010) is considered for computing the shortest

path distance based on line impedance as:

$$d_Z(v,t) = \| \sum_{(i,j)\in E\cap\ path(v,t)} Z_{pr}(i,j) \|$$

where $\|.\|$ gives magnitude value, and $Z_{pr}(i,j)$ is the line impedance of the link (i,j).

The literature on centrality measures is quite extensive, and applying only centrality measures to find a set of key players will likely fail. For instance, different essential nodes within a network obtained by various measures are illustrated in Figure 4.6, and indicates that in a specific application, the domain must be determined before a centrality measure could be used correctly Ortiz-Arroyo (2010).

The measures obtain the influential nodes over the graph from a distinct viewpoint. Therefore, the topological measures may aim to fill the possible gap between measures. Hence, beyond the electrical variables, the above measures indicating the topological importance of nodes are added into the features for voltage SSA as two different databases shown in Figure 4.5. In other words, electrical and topological are embedded in each node as the feature vector

$$[V^i_{mag}, P^i, Q^i, C^i_d, C^i_c, C^i_b, C^i_k], \quad \forall i \in Bus\ set$$

The representation of the feature vector is illustrated in Figure 4.7, in which the graph input data with node embedding futures is deployed for the learning task.

4.3.2 Learning Model: Graph Neural Network

Graph neural network framework is chosen as a learning model for voltage SSA. GNN is a type of deep neural network suitable for analyzing graph-structured data. In addition to the deficiency of CNNs and recurrent neural networks (RNNs) with graph-structured data (well-defined only for grid-structured data and only over sequences, respectively, such as images and texts), these models suffer from the variation of size and shape of input, which typically is excepted a fixed size of the information.

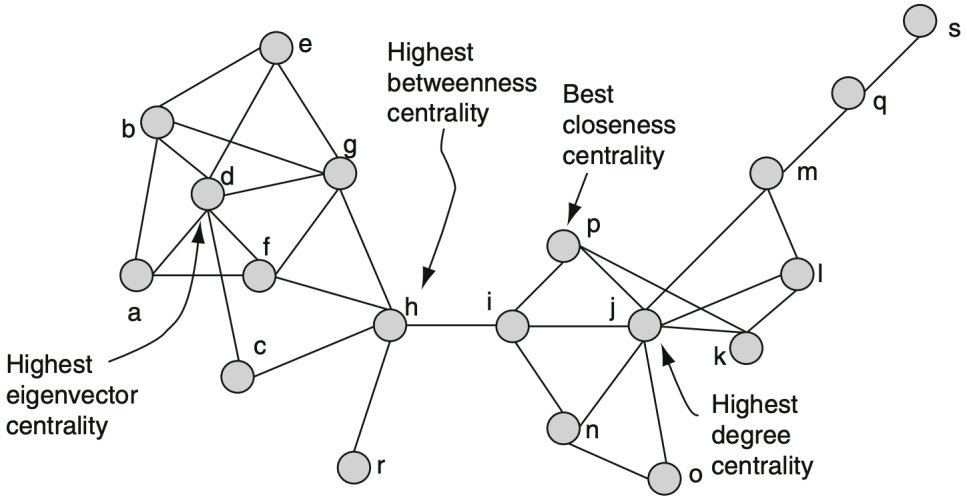


Figure 4.6: Illustration of various centrality measures Ortiz-Arroyo (2010).

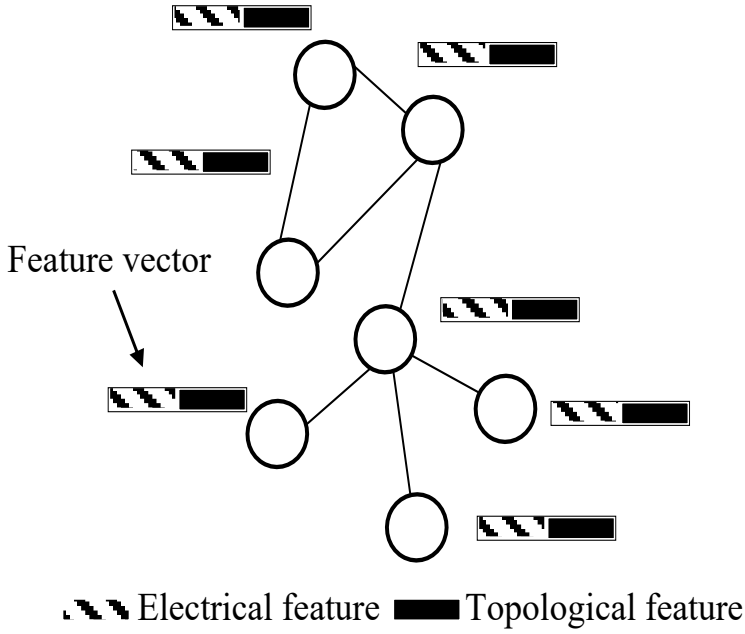


Figure 4.7: Embedding the feature vector.

Moreover, the CNN model is sensitive to input permutations, such as rotating an input picture. To address these challenges, GNN models are proposed to work with graph-structured data as they can handle the changes in shape and size of inputs and are permutation invariant. The overall framework of the GNN model for graph-level classification is shown in Figure 4.8.

The main idea here is to generate representations of nodes that include the information on the graph's structure and any feature information it might have Hamilton (2020). The procedure of GNN is encapsulated in *neural message passing* in which the feature vector of the node is exchanged between nodes and updated using neural networks. There are two main components in GNNs:

- *Aggregate operator* $\mathcal{G}$: permutation invariant function to its neighbors to generate the aggregated node feature.
- *Update operator* $\mathcal{F}$: combining the message from the previous aggregated node feature to generate updated node embedding.

$\mathcal{G}$ and $\mathcal{F}$ can be any arbitrary differentiable functions (i.e., neural networks), where $\mathcal{G}$ has to be a permutation invariant operator.

The general procedure of aggregation and updates for a sample graph is shown in Figure 4.9. The node neighbors form a computational graph to aggregate and update information, such as from node A's local graph neighbors (i.e., B, C, and D). The messages from these neighbors are also based on information aggregated from their neighbors, and so on. This visualization shows a two-layer version of a message-passing model since the data is aggregated from two hops. Notice that each node has its computation graph in which the GNN forms a tree structure by unfolding the neighborhood around the target node. The NN modules act as both $\mathcal{G}$ and $\mathcal{F}$, meaning that the input, the aggregated information from node neighbors, passes through to a neural network to generate updated node embedding features.

Mathematically, for a graph G, a hidden embedding vector of a node h_u^k corresponding to each node $u \in V$ is updated according to the aggregated information

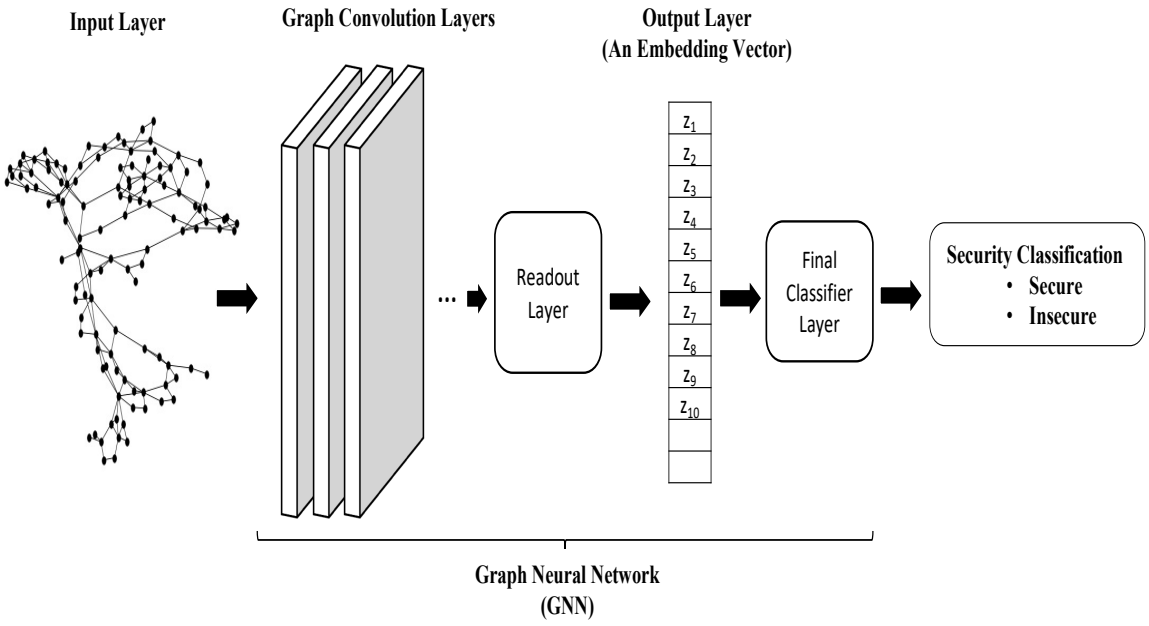


Figure 4.8: General GNN framework for classification problem.

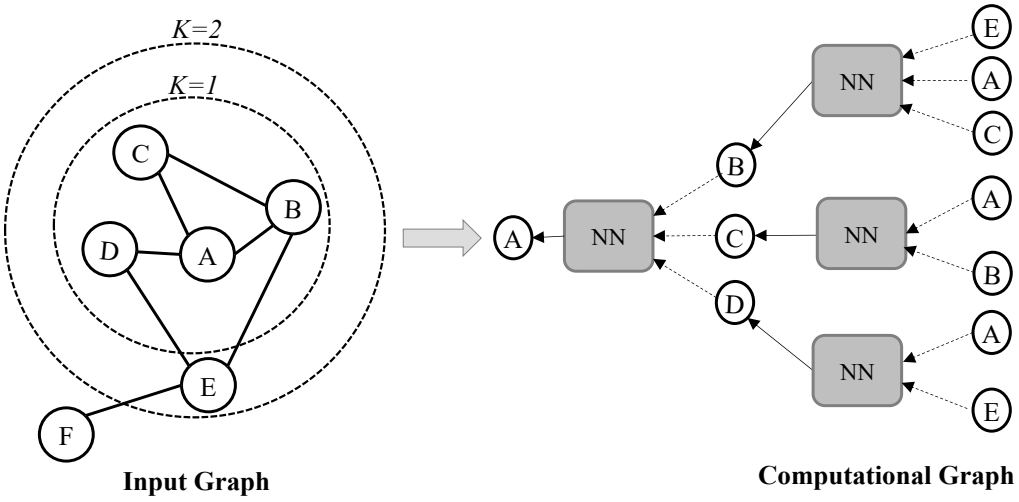


Figure 4.9: Computational graph of node A: information aggregation from two hops away.

from u's graph neighborhood $\mathcal{N}(u)$ Hamilton (2020)

$$h_u^{(k+1)} = \mathcal{F}^{(k+1)}\left(h_u^{(k)}, \mathcal{G}^k(\{h_v^{(k)}, \forall v \in \mathcal{N}(u)\})\right) \tag{4.1}$$

where k as iteration (or layer) indicates the number of hops that every node embedding contains information from its k-hop neighborhood. After k iterations, the embedding h_u of node u may encode the topological and feature-based information in the k hop neighborhood. After running K iterations of the GNN message passing, the output of the final layer can be used to define the embeddings for each node, i.e., $\mathbf{z}_u = \mathbf{h}_u(K), \forall u \in V$.

Depending on the choice of aggregate and update function, many GNN models are reviewed in Zhou et al. (2020). For example, the basic GNN framework is similar to a multi layer perception (MLP) as it has linear operations followed by a single element-wise non-linearity. This chapter considers the graph convolutional network model developed by Kipf and Welling (2016) as the SA model. The general idea of GCN is to apply a convolution operator similar to CNN but over a graph.

Graph Convolutional Network

The GCN is based on spectral methods, in which the representation of a graph lies in the spectral domain, utilizing the Laplacian eigenvectors. The propagation rule is inspired by a first-order approximation of localized spectral filters on graphs. Given a $N \times M$ feature matrix X (N: number of nodes, M: number of features) as input matrix, the GCN procedure is as Kipf and Welling (2016):

- Construct a self-connection by adding the identity matrix I_N to the adjacency matrix A

$$\tilde{A} = A + I_N \tag{4.2}$$

- Use the symmetric normalization of the Laplacian to define the convolutional filters

$$L_{norm} = D^{-\frac{1}{2}} L D^{-\frac{1}{2}} \tag{4.3}$$

- Applying a normalization trick to solve exploding/vanishing gradient problems as

$$I_N + D^{-\frac{1}{2}} A D^{-\frac{1}{2}} \rightarrow \tilde{D}^{-\frac{1}{2}} \tilde{A} \tilde{D}^{-\frac{1}{2}} \tag{4.4}$$

  where $\tilde{D}_{ii} = \sum_j \tilde{A}_{ij}$ acting as a row-wise summation of the adjacency matrix with self-connection producing the degree of each node.

Considering H as the updated feature matrix and W the layer-specific trainable weight matrix, the update rule and the layer-wise propagation rule is

$$H^{(l+1)} = \sigma\left(\tilde{D}^{-\frac{1}{2}} \tilde{A} \tilde{D}^{-\frac{1}{2}} H^{(l)} W^{(l)}\right) \tag{4.5}$$

where σ is an activation function, such as the $ReLU(\cdot) = max(0, \cdot)$, $W^{(0)} \in \mathbb{R}^{M \times d}$ with d the number of hidden units, and $H^{(0)} = X$. After K layers, the GCN produces a node-level output $H^K = Z$ (an $N \times d$ feature matrix). Note that for GCN with multiple hidden layers, the dimensions of the weight matrices will change accordingly. In the last layer, node embedding H^K can pass to a readout layer to present one vector for the final classifier R with learnable parameters to perform graph-level predictions as

$$z_G = R\left(Readout(H^{(K)})\right) \tag{4.6}$$

The whole procedure lies on the symmetric-normalized aggregation as well as the self-loop update approach for each node as

$$h_u^{(l+1)} = \sigma\left(W^l \sum_{v \in \mathcal{N}(u) \cap \{u\}} \frac{h_u^l}{\sqrt{|\mathcal{N}(u)||\mathcal{N}(v)|}}\right) \tag{4.7}$$

where $|\cdot|$ indicates the size of the node's neighborhoods to train the weight matrix W.

Considering the voltage SSA as supervised graph-level classification, the *softmax* function (4.8) is applied to determine the predicted probability that the graph belongs to the class G_i.

$$softmax(z_{G_i}) = \left(\frac{e^{z_{G_i}^T}}{\sum_{i=1}^{n} e^{z_{G_i}^T}} \right) \tag{4.8}$$

where z_{G_i} is graph-level embedding over a set of labeled training graphs $T = \{G_1, \ldots, G_n\}$.

Therefore, the GCN model is applied for voltage SSA in a graph-structured data. The task here is graph-level security classification. Each input is a power grid graph at post-contingency conditions, in which each node has topological and electrical features. The node features are aggregated and updated with their k-neighbors information during the learning procedure. Then, the last layer classifies the final representations of each graph obtained by the readout layer as secure/insecure. This procedure is repeated to train the weight matrix w.r.t minimizing a loss function. The actual label as secure/insecure is defined according to the reliability criteria of bus voltages in steady-state.

4.4 Simulation Results

We use MATLAB and Power System Simulator for Engineering (PSSE) commercial software to generate different cases for simulation purposes. The GCN learning model is implemented using PyTorch Geometric Fey and Lenssen (2019).

4.4.1 Data Generation

The IEEE 118-Bus system is considered for the simulation. This system represents a simple approximation of the American Electric Power system (in the U.S. Midwest)

as of December 1962 that contains 19 generators, 35 synchronous condensers, 177 lines, 9 transformers, and 91 loads as shown in Figure 4.10. The primary practice of generating data in power system applications is running different contingency scenarios. Due to the highly interconnected nature of modern power systems and various energy market scenarios, operating conditions and even the topology of a power system change frequently. Capturing all changes in the power system while generating data is an intricate task since the source of variation needs to be clarified, and the power grid operates at various points. An approach mentioned in Procedure 1 is employed for data generation to provide a rich dataset. Two sources of variations are assumed in the data generation loop as follows:

- *Load variation during day*: the actual net load varies during the day because of the time of day. Here, it is assumed that the 118-bus system follows the same feature as the estimated net load for 2020 from the CAISO "Duck Curve" Wang (2017). Then, the actual load is scaled by the same factor as the Duck curve for different times of the day, as shown in Figure 4.11. Each scale factor is applied for randomly chosen 70% of load buses mimicking changes in load profile.

- *Stress conditions*: in this case, the P-V analysis is involved using a series of load flow solutions for the incremental power transfers (MW) between *source* (delivers transfer power) and *sink* (absorbs transfer power) areas at a constant power factor. As shown in Figure 4.10, generators at buses 65, 66, and 69 and load at buses 20, 21, 22, 23, and 115 are considered source and sink areas, respectively. This case results in various operating conditions before the voltages pass the threshold or the load flow does not solve. The P-V solution parameters applied in the PSSE setting are 0.5 MW as power mismatch tolerance and 1000 MW as maximum incremental transfer with an initial transfer of 10 MW by 10 MW transfer increment tolerance.

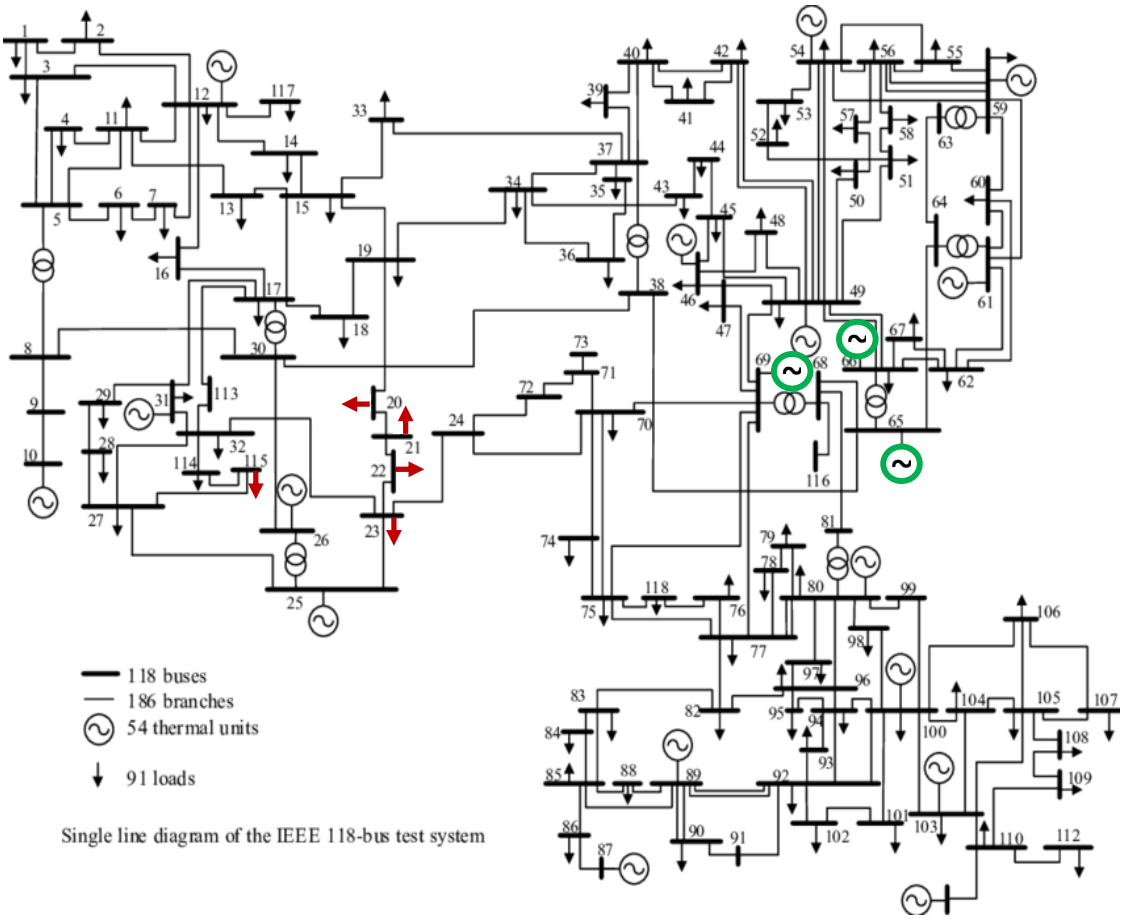


Figure 4.10: Single line diagram of the IEEE 118-Bus system.
The source area in the P-V analysis is indicated by green circles, representing generators located at buses 65, 66, and 69. The sink area is illustrated by red arrows, representing loads at buses 20, 21, 22, 23, and 115.

Procedure 1: Data Generation.

```
/* capturing load variation.                                          */
for each operating point do
    for scenario in the contingency list do
        /* capturing stress conditions.                               */
        while power transfer < maximum incremental transfer;
         do
            solve power flow;
            if (solution not found and voltage violation) then
                break, go to the next scenario;
            else
                increase power transfer;
            end
        end
    end
end
```

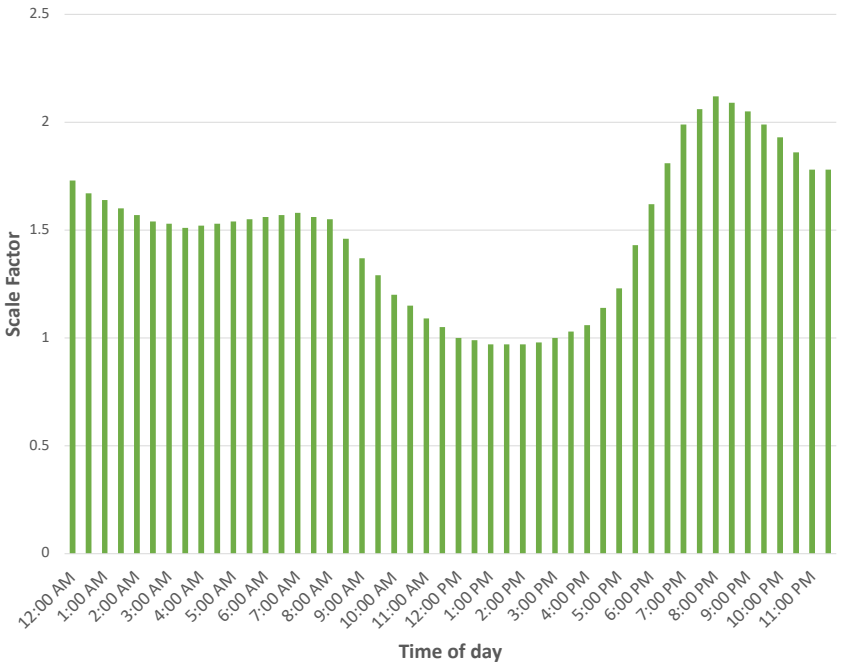


Figure 4.11: Scaled estimated net load data for 2020 CAISO Duck Curve.

Voltage operation threshold is assumed 0.90-1.10 p.u. of the steady-state of nominal voltage (post contingency), which single contingency (category P1) of TPL-001-WECC-CRT-3.2 defines. The value outside of the range violates the reliability criteria and needs the operators' action.

As a result, 21379 cases were generated, out of which 19668 cases were secure, and the remaining 1711 cases were insecure. The result shows an imbalanced dataset which is rational as the power grid should be secure for most single contingencies (N-1). Each sample indicates a power grid in post-contingency conditions as a graph. The electrical feature obtained by the power flow solution and topological feature computed by centrality measures is then embedded in each node feature vector. The dataset is randomly split into a 60:20:20 ratio for training, validation, and test sets. The batch size indicating the number of training samples utilized in one training iteration is 128.

4.4.2 GCN Model Configuration

The GCN architecture for voltage SSA as a graph-level classification task is as follows:

- *Convolutional layer*: embedding each node by performing six layers of GCN with $\mathrm{ReLU}(x) = \max(x, 0)$ as the activation function for each layer, all with a hidden-dimension size of 32.
- *Readout layer*: aggregating node embeddings into a unified graph embedding by averaging the node embeddings
- *Final classifier*: a linear classifier with a softmax function to transfer the embedding size of hidden dimension to the number of classes.

This architecture results in 10,946 trainable parameters.

4.4.3 Optimization Set up

Considering binary cross-entropy as the loss function (4.9), the model parameters are trained using the adaptive moment estimation (Adam) optimizer with an initial learning rate of 10^{-3} and decay the learning rate based on training results to a minimum of 10^{-5} for regularization for 200 epochs.

$$\mathcal{L} = -(y \log(\hat{y}) + (1 - y) \log(1 - \hat{y})) \tag{4.9}$$

where y is the true label and $\hat{y}$ denotes the predicted label by (4.8).

4.4.4 Performance Evaluation Metric

For classification problems, evaluation metrics are used to compare the expected class label to the predicted class label. Since the power system should be operational safe for $(N - 1)$ contingency, most of the dataset is secure, leading to an imbalanced dataset. A commonly used performance metric in binary classification tasks, particularly when the classes are imbalanced, is F1-score. It combines precision and recalls into a single metric to measure the model's accuracy. Geometric mean, G-mean, is another performance metric used in binary classification tasks when dealing with imbalanced datasets. It is particularly useful when the performance of a model needs to be evaluated based on both sensitivity (true positive rate) and specificity (true negative rate) Manning et al. (2010).

F1-score and G-mean are defined as:

$$\text{F1-score} = 2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$$
$$\text{G-mean} = \sqrt{\text{recall} \times \text{specificity}}$$

By considering all four possible outcomes of a classification problem, TP: True Positive, FN: False Negative FP: False Positive, TN: True Negative, a confusion

matrix shown in Table 4.1, enables us to understand the following:

$$\text{Precision} = \frac{TP}{TP + FP}, \quad \text{Recall} = \frac{TP}{TP + FN}, \quad \text{Specificity} = \frac{TN}{TN + FP}$$

4.4.5 Case Studies Results

Single-line contingency $(N - 1)$ scenarios are run as a base case to generate samples according to the procedure in Section 4.4.1. The same dataset but in grid-structure data is applied to an MLP model to investigate the application of GCN. For a fair comparison, the MLP model is configured to have a similar number of trainable parameters (10,699) to the GCN model. The MLP model consists of 4 fully connected layers (dense). Other settings, such as the activation function, the number of hidden channels, and optimization parameters are the same.

Training performance metrics and loss are depicted in Figure 4.12 with electrical and topological input features. As shown, for the same number epoch, not only does GCN provide a better classification result, but its loss value shows convergence to a smaller value than the MLP model. Considering the performance metrics mentioned in Section 4.4.4, Table 4.2 indicates both GCN and MLP model's performance. For investigation of features type's impact on voltage SSA, the models have been trained separately for four different groups of input features:

- Electrical variables: bus voltage magnitude, bus active and reactive power;
- Topological variables: bus degree centrality, bus clustering coefficient, bus betweenness centrality, and bus closeness centrality;
- Voltage magnitude plus topological variable;
- Both electrical and topological variables.

Table 4.1: Confusion matrix.

	Predicted Positive	Predicted Negative
Actual Positive	TP	FN (Type II error)
Actual Negative	FP (Type I error)	TN

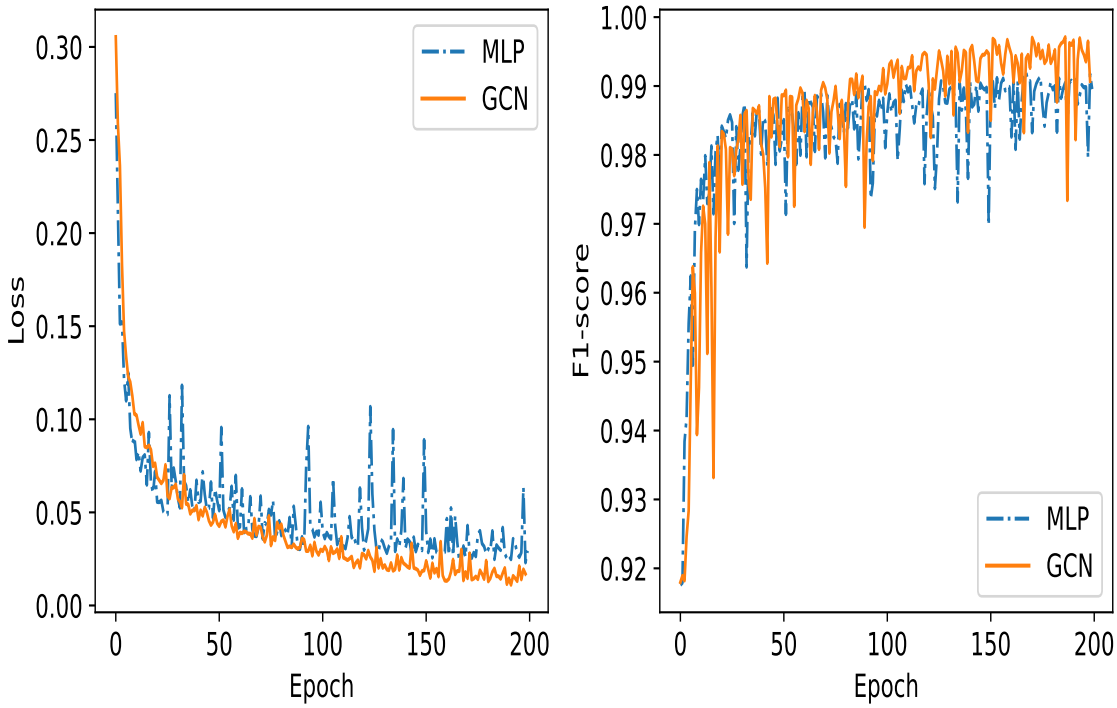


Figure 4.12: F1-score and loss curve for MLP and GCN models.

Table 4.2: Base dataset performance evaluation: average value over ten runs.

Variable type	Model	F1-score			G-mean		
		Training set	Validation set	Test set	Training set	Validation set	Test set
Electrical (E)	GCN	99.25	99.08	99.09	97.61	97.04	97.08
	MLP	99.06	99.16	99.08	97.02	96.30	96.89
Topological (T)	GCN	92.43	91.95	91.57	91.30	91.00	91.23
	MLP	92.26	92.29	91.08	90.30	89.05	90.63
Voltage and Topological (V.T)	GCN	99.36	98.86	99.29	98.12	97.22	97.53
	MLP	99.04	98.32	99.09	97.40	97.02	97.03
Electrical and Topological (E.T)	GCN	99.40	98.74	99.50	97.82	96.54	97.58
	MLP	98.87	98.6	99.14	97.20	96.26	96.29

The results show that the GCN model outperforms the MLP model as it provides higher evaluation scores. Still considering only topological variables deliver acceptable performance, and adding the voltage magnitude variable increases the test performance by 8.43% (F1-score) and 6.90% (G-mean). This is the expected result, as the voltage variable plays a key role in voltage security assessment.

Moreover, one may state that there is only a bit of improvement in metrics either the GCN model is deployed or topological variables are added. The point here is that improving the performance of an accurate model is challenging since the model may face overfitting. The capacity of the proposed model is analyzed later on.

Furthermore, in power system security assessment, the consequences of misclassification may result in a blackout or increased operation cost. Considering the result of both variables mentioned in Table 4.2, the GCN model could do the task by providing correct classification by 106 samples (more TP and less FN rate) obtained from the F1-score. Regarding practical application, each sample's correct classification is substantial and can be identified via a *penalty matrix* McCalley et al. (2010). NERC's guidelines approved a matrix comprising violation risk factors and violation severity levels, establishing base penalty amounts since the protection and remedial action are activated based on classification output. Therefore, slightly enhancing the performance of the SA model not only lowers the risk of the consequences of a wrong decision but also avoids paying penalizing fines.

The other finding refers to the importance of topological variables. Once voltage magnitude is added to topological variables, F1-score and G-mean metrics increase compared to only electrical variables; this indicates topological variables have meaningful intake in the voltage security analysis. The physics behind this observation needs to be clarified. However, incorporating the importance of buses across the grids reveals the impact of topological changes. Combining all electrical and topological variables in the feature set provides the highest value of evaluation metrics. In all cases, the GCN model outperforms the MLP because the GCN model captures and updates node information from its neighbors, leading to more

informative node features. Indeed, the performance of voltage SSA is enhanced by the usage of information sharing and embedding between buses.

4.5 Model Capacity Analysis

To analyze the ability of the built models to adapt appropriately to new, previously unseen samples, so-called *generalization of model*, the following scenarios are simulated to observe model capacity.

4.5.1 Unseen Data

In this case, different datasets are generated to evaluate the efficiency of models for unseen samples. For case 1, a new operating point scaled by "Duck Curve" is generated randomly. Then single-line contingencies followed by the increment of power transfer in the system are applied, such as Procedure 1. 1795 samples are generated in this case. Case 2 is constructed based on double-line contingency (N-1-1) from the normal operating point. In this fashion, 15923 double-line scenarios, including base case, are generated without running stress conditions. Only 500 cases out of all double-line cases are randomly chosen for power transfer for the sake of data generation speed. This results in 5108 samples. Now, both new datasets are evaluated for the trained models to see the effectiveness of the SA for unseen datasets.

Table 4.3 shows models' analysis results and performance as the bar graph is shown in Figure 4.13 for visual observation. As seen, the F1-score drops in both models; however, in both new datasets and for all variable types, the GCN drops less than the MLP model, indicating more model capacity to classify the unseen data. The model's performance varies depending on the variable type. That is, a relation between feature space and new cases is noticed. Since the operating point is associated with the electrical variables, the trained models based on those are more sensitive than double-line contingency cases that address the topological changes. It

Table 4.3: Robustness analysis results.

Variable type	model	F1-score	
		Case 1	Case 2
Electrical	GCN	96.19	97.97
	MLP	91.09	97.11
Topological	GCN	90.34	83.25
	MLP	89.69	82.97
Voltage and Topological	GCN	91.22	98.50
	MLP	93.22	94.50
Electrical and Topological	GCN	94.42	95.46
	MLP	89.69	92.17

Case 1: New operating point, Case 2: Random double-line contingency.

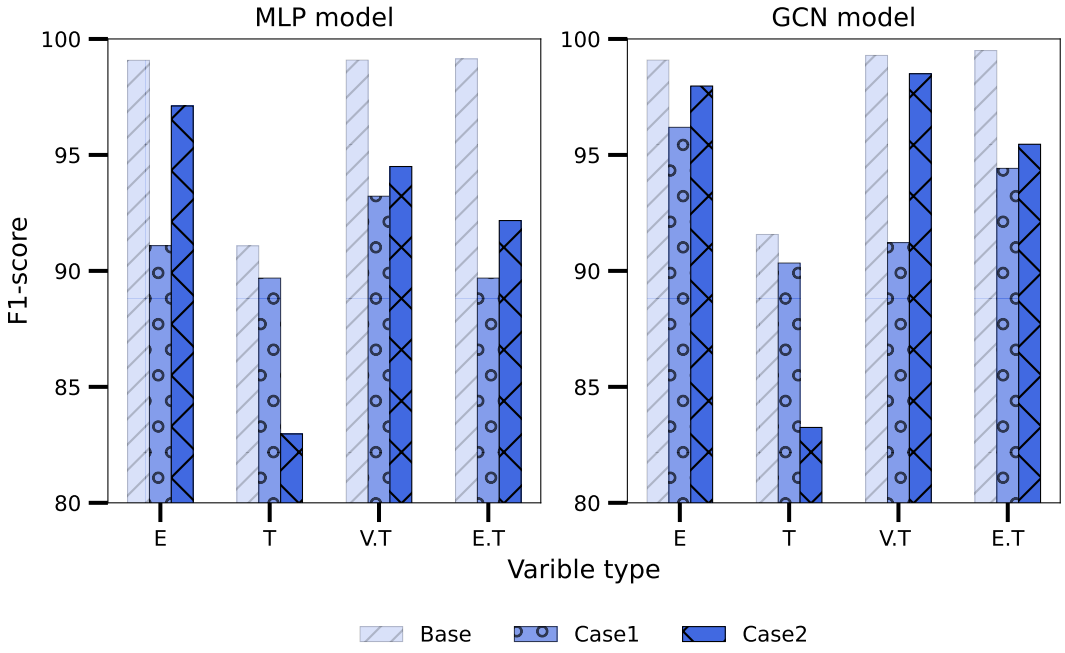


Figure 4.13: Bar graph of results for unseen data.

is also observed that trained models based on topological variables are resilient for new operating points and sensitive to double-line contingency datasets. Thanks to the combination of both variable types in features, the models perform accurately for both new cases. That is, the model can capture the variation of new datasets from changes in operating point or grid topology. Furthermore, the GCN outperforms the MLP, signifying the functionality of GCN due to feature embedding aggregation and updating operation.

4.5.2 Input Variability

Beyond the impact of the unseen dataset, the model can be analyzed when input variables are changed to see how it may impact output classification. Here, the sensitivity analysis examines the change in the target output when one of the input features is perturbed. Regarding the state estimation architecture, variables in the SA are estimated from the measurement and status of, specifically, electrical variables. Topological variables might need to be more informed by the estimation of topology processors due to reported inaccurate data coming from SCADA or the limitation of source measurement. Despite this, it is unlikely to have changes in the electrical variables. Variation of voltage magnitude is considered for sensitivity analysis as electrical variables are mainly studied for perturbation analysis due to the device measurement error or being prone to false data injection.

Considering a general state estimation architecture shown in Figure 4.14 from Abur and Exposito (2004) related to the SA, a perturbation block is only added to mimic the voltage variation due to SE error. In practice, the disturbances are mainly added to measurements, and here the block only represents voltage variations (SE error) to do sensitivity analysis. We randomly choose 10% of buses to inject 5% nominal voltage magnitude as a new test set. The models' performance for this scenario is mentioned in Table 4.4, in which the superiority of the GCN model compared to the MLP model is once more seen as the performance of the GCN

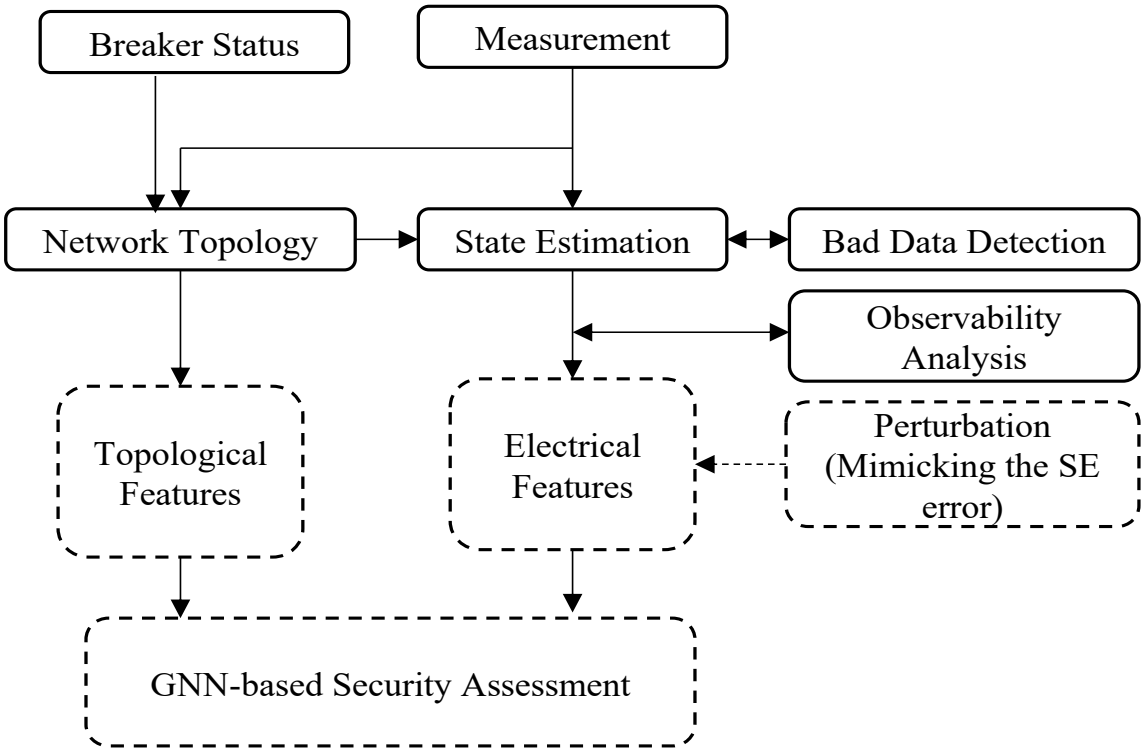


Figure 4.14: General state estimation architecture: the dash line blocks are depicted to indicate the procedure for sensitivity analysis of GCN-based SA model.

Table 4.4: Variable sensitivity results.

Variable type	model	F1-score
Electrical	GCN	97.90
	MLP	94.01
Voltage and topological	GCN	98.77
	MLP	95.66
Electrical and topological	GCN	98.86
	MLP	95.87

classifier is less degraded. One may ask that the SE bad data detection (BDD) scheme can capture this variation and label it as an anomaly before it goes through monitoring and operation. As in real practice, there is no specified threshold for BBD, and it also varies depending on operational considerations; the proposed scenario can be applied without practical issues. Although classification performance reduces, using the GCN model with both electrical and topological information results in less sensitivity for voltage magnitude variation. That is clear that this scenario does not apply to models with only topological variables.

4.6 Discussion and Summary

This chapter introduced the GCN model for voltage SSA by considering the topological variables obtained from the topology of the power grid after contingency scenarios. The following can be discussed in this framework:

4.6.1 Do the topological features boost performance?

As the results show, the topological variables could enhance the model performance for security assessment and increase the model's capacity, through model capacity analysis, particularly for the GCN model. Furthermore, the type of centrality measures is also indispensable. Although the topological variables capture the power grid's structure properties, all graph centrality measures do not enhance performance. During the simulation, *harmonic centrality*, which measures the average distance of a node to the other nodes in the network, was also computed. Adding this measure interestingly lowered the best model performance in Table 4.2 by 8.9%. The reason could be that the topological feature voltage SSA may depend on nodes-related measures mentioned in Section 4.3.1. Therefore, the measures referring directly to distances can be misleading for the voltage SSA.

4.6.2 Training time

The GNN-based model involves feature aggregation and updates from nodes' neighbors, so the training procedure takes longer than the MLP model. For instance, for both feature types in Table 4.2, the training time for the GCN and the MLP is 1971 and 63 seconds, respectively. Although the GCN model took much more time for the training (about 32 times the MLP), it resulted in better performance than the MLP for various scenarios. Moreover, the proposed voltage SSA is applied for an offline SA scheme in which training time is not a concern.

4.6.3 On a GNN Universal Framework for the SA

There is no limitation of the proposed GNN-based SA model for voltage SSA to apply for any other security assessments, such as frequency and dynamic security assessment Mukherjee and De (2021); Wang (2017). The framework is universal such that only the procedure of data generation and reliability criteria must be adapted. For example, in voltage DSA, the dynamic simulation needs to be run, and then bus voltage trajectories must be monitored to apply appropriate reliability criteria.

In conclusion, a GCN model as a GNN-based framework is introduced for voltage SSA. Despite the traditional input features, such as grid format data, a graph format structure is proposed for security analysis of the power grid. A graph then represents the status of a power grid in which each node (bus) consists of features where the GCN model acts on aggregated and updated bus features from its neighbors to deliver a well-informed design for the SA. In addition to electrical variables, topologically related variables obtained from graph centrality measures indicating a structural property of the power grid are appended to the feature space. A dataset capturing possible variations, such as daily changes in load profile and grid stress condition for voltage stability, is generated for model validation purposes. Simulation results show the outperformance of the GCN model compared to the traditional neural network. The impact of the new feature vector is observed in model performance.

Moreover, the proposed framework is studied for unseen data and variations to examine the model's generalization. The outcomes once more confirm the superiority of the GCN model. As the GCN model makes a decision using the neighbor information of each bus where the SA is reformulated in the graph context, it provides more capacity for security classification due to the information distributed over the network. Although this chapter focuses on voltage security in the steady state, the developed scheme can adapt to any security assessment, such as dynamic, considering other stability problems, such as frequency.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

This dissertation investigates the resiliency of data-driven modules in the electrical grid. The power system as the cyber-physical system is a prime sector among critical infrastructure, so resiliency is particularly important. The advancements in device manufacturing, such as sensors, actuators, and communication networks, offer more flexibility for the decision-making process. That is, the cyber layer is more critical than ever. This work aims at resiliency analysis of two main EMS data-driven modules, load forecasting and security assessment, to deliver resilient approaches regarding cyber security and operation security, respectively.

In chapter 2, the notion and characteristics of a resilient system are presented through the literature review from various fields of sciences to benefit power systems. Given two primary tasks of a resilient system as incident withstanding capability and recovery action, robustness, adaption, and restoration are outlined as the significant elements guaranteed a resilient framework of the study. Some leading indices measuring a system's resiliency are discussed similarly to other system performance metrics. Then, from a control point of view, a high-level feedback loop ensures the framework is effective. Considering the importance of power systems, some

of the suggested methods addressing the resilient behavior of the power grid are reviewed. Furthermore, an element-wise discussion of the power grid regarding resilient framework, plus possible gaps and future direction, are presented.

In chapter 3, the resiliency of short-term load forecasting for cyber threats is investigated. Since temperature is a substantial variable for the STLF and is measured from external models, the risk of a cyberattack is high. Therefore, approaches to derive physics-based constraints are carried out to hinder the attacker and make malicious action more involved. First, the STLF of an area is seen as the sum of weather-based stations. The relation of each load time series is studied by employing similarity measures for a physics-based constraint. Resembling a malicious effect on temperature data, applying various measures on the ERCOT historical load significantly reveals changes in the indices for the SAX method. The proposed framework demonstrating the hidden physical interaction among the weather-based stations can be used for anomaly notification or needs to be satisfied by the attacker for a successful malicious result. Moreover, a lag correlation scheme is developed for a short time horizon of data, enabling a distributed analysis of load stations to identify the most correlated stations with corresponding lag step values. This framework allows one to detect anomalies by monitoring changes in the lag step and paired station based on correlation.

In chapter 4, the security assessment task is analyzed to deliver a framework that captures more uncertainties of power systems operating points and measurement. As the vulnerability of the power grid can be studied in the framework of a complex network, first topological importance of the power grid is examined as a new feature set, then appending it to the electrical variables. As the information of the electrical grid is interconnected, a graph neural network model for the SA is explored to benefit the distributed knowledge across the grid. The proposed model is then better informed. The framework is verified for a voltage static security assessment task of the IEEE 118-Bus system. The security classification results using the graph-based learning model perform better than the traditional dense neural network for different

case studies. The proposed SA model can comparably deliver a resilient response in this framework.

5.2 Future Work

Building upon the foundation of the research conducted in this dissertation, several potential areas for future research can be identified. These areas include:

1. Due to the growing complexity of CPSs, particularly in the case of the electrical grid, the traditional separation between physical and cyber layers is no longer applicable. As a result, it becomes necessary to reevaluate the concept of resiliency and its framework. One potential avenue for exploration is the development of a comprehensive scheme encompassing both physical and cyber incidents. Recognizing that threats can manifest in either domain makes it evident that addressing these risks requires a multi-layered approach.

2. The suggestion of a weather-based framework serves as an inspiration to explore the adaptation of a distributed scheme for cyber security, specifically at a non-aggregated level, such as the customer level. This approach would involve considering individual customers and their associated security needs. Furthermore, it is essential to delve into the analysis of the time complexity of this scheme and explore methods for reducing the search space, ultimately aiming to enhance its efficiency and effectiveness.

3. The locational marginal price (LMP) is a pricing mechanism in electricity markets that provides pricing signals at the nodal level. As LMP represents the economic dispatch solution, it reflects the operation and constraints of the electrical grid infrastructure. As a result, LMP can be utilized as a signal to incorporate load behavior analysis and calculate system-level measures for station price and price-load interactions for security purposes. By considering LMP in load behavior models, a more comprehensive understanding of market

dynamics and price-load relationships can be obtained to detect anomalies. To detect such anomalies, it is proposed to employ a change point detection (CPD) method, which identifies time steps when load, temperature, and LMP time series transition into a new abnormal mode.

4. The GNN model can undergo additional analysis for dynamic security assessment, such as focusing on voltage and frequency stability. Furthermore, the model can be adapted to incorporate edge information, such as transmission line parameters and flow, to better understand the impact of link information for security assessment.

Bibliography

Abur, A. and Exposito, A. G. (2004). *Power system state estimation: theory and implementation*. CRC press. 113

Adams, T. M., Bekkem, K. R., and Toledo-Durán, E. J. (2012). Freight resilience measures. *Journal of Transportation Engineering*, 138(11):1403–1409. 33

Agrawal, R. K., Muchahary, F., and Tripathi, M. M. (2018). Long term load forecasting with hourly predictions based on long-short-term-memory networks. In *2018 IEEE Texas Power and Energy Conference (TPEC)*, pages 1–6. IEEE. 9

Amaral, A., Fernandes, G., and Varajão, J. (2015). Identifying useful actions to improve team resilience in information systems projects. *Procedia Computer Science*, 64:1182–1189. 17

Amirioun, M., Aminifar, F., Lesani, H., and Shahidehpour, M. (2019). Metrics and quantitative framework for assessing microgrid resilience against windstorms. *International Journal of Electrical Power & Energy Systems*, 104:716–723. 32

Andersson, C. (2005). *Power system security assessment: application of learning algorithms*. Department of Industrial Electrical Engineering and Automation, Lunds University. 84, 91

Anghel, M., Werley, K. A., and Motter, A. E. (2007). Stochastic model for power grid dynamics. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 113–113. IEEE. 34, 40

Arghandeh, R., Von Meier, A., Mehrmanesh, L., and Mili, L. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, 58:1060–1069. 18, 19, 20

Arias, A., Martínez, L. H., Hincapie, R. A., Granada, M., et al. (2015). An ieee xplore database literature review regarding the interaction between electric vehicles and power grids. *2015 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM)*, pages 673–678. 82

Arteaga, J.-M. H., Hancharou, F., Thams, F., and Chatzivasileiadis, S. (2019a). Deep learning for power system security assessment. In *2019 IEEE Milan PowerTech*, pages 1–6. IEEE. 11

Arteaga, J.-M. H., Hancharou, F., Thams, F., and Chatzivasileiadis, S. (2019b). Deep learning for power system security assessment. In *2019 IEEE Milan PowerTech*, pages 1–6. IEEE. 86

Ashok, A., Govindarasu, M., and Wang, J. (2017). Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the IEEE*, 105(7):1389–1407. 18

Aubin, J.-P., Bayen, A. M., and Saint-Pierre, P. (2011). *Viability theory: new directions*. Springer Science & Business Media. 37

Ayyub, B. M. (2014). Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making. *Risk analysis*, 34(2):340–355. 36

Bakirtzis, A., Petridis, V., Kiartzis, S., Alexiadis, M., and Maissis, A. (1996). A neural network short term load forecasting model for the greek power system. *IEEE Transactions on power systems*, 11(2):858–863. 9, 21

Barabási, A.-L. (2009). Scale-free networks: a decade and beyond. *science*, 325(5939):412–413. 148

Berkeley, A., Wallace, M., and Coo, C. (2010). A framework for establishing critical infrastructure resilience goals. *Final Report and Recommendations by the Council, National Infrastructure Advisory Council*. 26

Bie, Z., Lin, Y., Li, G., and Li, F. (2017). Battling the extreme: A study on the power system resilience. *Proceedings of the IEEE*, 105(7):1253–1266. 18, 20, 22, 32

Billinton, R. and Allan, R. N. (1990). Basic power system reliability concepts. *Reliability Engineering & System Safety*, 27(3):365–384. 20

Bimrose, J. and Hearne, L. (2012). Resilience and career adaptability: Qualitative studies of adult career counseling. *Journal of Vocational Behavior*, 81(3):338–344. 32

Blanke, M., Frei, W. C., Kraus, F., Patton, J. R., and Staroswiecki, M. (2000). What is fault-tolerant control? *IFAC Proceedings Volumes*, 33(11):41–52. 16

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwang, D.-U. (2006a). Complex networks: Structure and dynamics. *Physics reports*, 424(4-5):175–308. 10

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwang, D.-U. (2006b). Complex networks: Structure and dynamics. *Physics reports*, 424(4-5):175–308. 149

Bompard, E., Huang, T., Wu, Y., and Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power & Energy Systems*, 50:50–64. 29

Bompard, E., Pons, E., and Wu, D. (2012). Extended topological metrics for the analysis of power grid vulnerability. *IEEE Systems Journal*, 6(3):481–487. 27

Borchert, I. and Mattoo, A. (2009). *The crisis-resilience of services trade*. The World Bank. 17

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., and Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake spectra*, 19(4):733–752. 33

Bugaje, A.-A. B., Cremer, J. L., Sun, M., and Strbac, G. (2021). Selecting decision trees for power system security assessment. *Energy and AI*, 6:100110. 11

Caiado, J., Crato, N., and Peña, D. (2006). A periodogram-based metric for time series classification. *Computational Statistics & Data Analysis*, 50(10):2668–2684. 57

Cannon, T. (1994). Vulnerability analysis and the explanation of 'natural'disasters. *Disasters, development and environment*, 1:13–30. 27

Carvallo, J. P., Larsen, P. H., Sanstad, A. H., and Goldman, C. A. (2016). Load forecasting in electric utility integrated resource planning. 48

Chakhchoukh, Y., Panciatici, P., and Mili, L. (2010). Electric load forecasting based on statistical robust methods. *IEEE Transactions on Power Systems*, 26(3):982–991. 9

Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., and Mukhopadhyay, D. (2018). Adversarial attacks and defences: A survey. *arXiv preprint arXiv:1810.00069*. 47

Chan, K. (1992). A further analysis of the lead–lag relationship between the cash market and stock index futures market. *The Review of Financial Studies*, 5(1):123–152. 70, 73

Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):1–58. 47

Chang, S. E. and Shinozuka, M. (2004). Measuring improvements in the disaster resilience of communities. *Earthquake spectra*, 20(3):739–755. 34

Chen, C., Wang, J., and Ton, D. (2017). Modernizing distribution system restoration to achieve grid resiliency against extreme weather events: an integrated solution. *Proceedings of the IEEE*, 105(7):1267–1288. 40

Chen, K., Hu, J., Zhang, Y., Yu, Z., and He, J. (2019a). Fault location in power distribution systems via deep graph convolutional networks. *IEEE Journal on Selected Areas in Communications*, 38(1):119–131. 87

Chen, Y., Tan, Y., and Zhang, B. (2019b). Exploiting vulnerabilities of load forecasting through adversarial attacks. In *Proceedings of the Tenth ACM International Conference on Future Energy Systems*, pages 1–11. 10

Chen, Y., Tan, Y., and Zhang, B. (2019c). Exploiting vulnerabilities of load forecasting through adversarial attacks. In *Proceedings of the Tenth ACM International Conference on Future Energy Systems*, pages 1–11. 46, 50, 51

Chu, C.-C. and Iu, H. H.-C. (2017). Complex networks theory for modern smart grid applications: A survey. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 7(2):177–191. 93

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., and Handfield, R. B. (2007). The severity of supply chain disruptions: design characteristics and mitigation capabilities. *Decision Sciences*, 38(1):131–156. 17

Cuadra, L., Salcedo-Sanz, S., Del Ser, J., Jiménez-Fernández, S., and Geem, Z. W. (2015). A critical review of robustness in power grids using complex networks concepts. *Energies*, 8(9):9211–9265. 19, 22

Cui, M., Wang, J., and Yue, M. (2019a). Machine learning-based anomaly detection for load forecasting under cyberattacks. *IEEE Transactions on Smart Grid*, 10(5):5724–5734. 10

Cui, M., Wang, J., and Yue, M. (2019b). Machine learning-based anomaly detection for load forecasting under cyberattacks. *IEEE Transactions on Smart Grid*, 10(5):5724–5734. 47

Dai, Y., Chen, G., Dong, Z., Xue, Y., Hill, D. J., and Zhao, Y. (2014). An improved framework for power grid vulnerability analysis considering critical system features. *Physica A: Statistical Mechanics and its Applications*, 395:405–415. 27

De Lara, M. (2018). A mathematical framework for resilience: dynamics, uncertainties, strategies, and recovery regimes. *Environmental Modeling & Assessment*, 23(6):703–712. 37

Dessavre, D. G., Ramirez-Marquez, J. E., and Barker, K. (2016). Multidimensional approach to complex system resilience analysis. *Reliability Engineering & System Safety*, 149:34–43. 8

Dezvarei, M., Tomsovic, K., Sun, J. S., and Djouadi, S. M. (2022). Exploring physical-based constraints in short-term load forecasting: A defense mechanism against cyberattack. In *2022 IEEE Power & Energy Society General Meeting (PESGM)*, pages 1–5. IEEE. 45

Dobson, I., Carreras, B. A., Lynch, V. E., and Newman, D. E. (2007). Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 17(2):026103. 10

Donnellan, W. J., Bennett, K. M., and Soulsby, L. K. (2015). What are the factors that facilitate or hinder resilience in older spousal dementia carers? a qualitative study. *Aging & mental health*, 19(10):932–939. 32

Donovan, B. and Work, D. B. (2017). Empirically quantifying city-scale transportation system resilience to extreme events. *Transportation Research Part C: Emerging Technologies*, 79:333–346. 17

Drezga, I. and Rahman, S. (1998). Input variable selection for ann-based short-term load forecasting. *IEEE Transactions on Power Systems*, 13(4):1238–1244. 46

Ellinas, G., Panayiotou, C., Kyriakides, E., and Polycarpou, M. (2015). Critical infrastructure systems: Basic principles of monitoring, control, and security. In *Intelligent monitoring, control, and security of critical infrastructure systems*, pages 1–30. Springer. 1, 16

Esling, P. and Agon, C. (2012). Time-series data mining. *ACM Computing Surveys (CSUR)*, 45(1):1–34. 54

Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., and Han, Z. (2014). Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal*, 11(3):1644–1652. 47

Fanucchi, R. Z., Bessani, M., Camillo, M. H., Soares, A. d. S., London Jr, J. B., Desuó, L., and Maciel, C. D. (2019). Stochastic indexes for power distribution systems resilience analysis. *IET Generation, Transmission & Distribution*, 13(12):2507–2516. 36

Feder, A., Fred-Torres, S., Southwick, S. M., and Charney, D. S. (2019). The biology of human resilience: opportunities for enhancing resilience across the life span. *Biological psychiatry*, 86(6):443–453. 8

Fey, M. and Lenssen, J. E. (2019). Fast graph representation learning with pytorch geometric. *arXiv preprint arXiv:1903.02428*. 101

Fiksel, J. (2003). Designing resilient, sustainable systems. *Environmental science & technology*, 37(23):5330–5339. 20

Fischer, L., Uslar, M., Morrill, D., Döring, M., and Haesen, E. (2018). Study on the evaluation of risks of cyber-incidents and on costs of preventing cyber-incidents in the energy sector. *European Commission: Berlin, Germany*. 6, 41

Fisher, R., Bassett, G., Buehring, W., Collins, M., Dickinson, D., Eaton, L., Haffenden, R., Hussar, N., Klett, M., Lawlor, M., et al. (2010). Constructing a resilience index for the enhanced critical infrastructure protection program. Technical report, Argonne National Lab.(ANL), Argonne, IL (United States). Decision and 32, 42

Francis, R. and Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, 121:90–103. 19, 26

Fu, T.-c. (2011). A review on time series data mining. *Engineering Applications of Artificial Intelligence*, 24(1):164–181. xii, 55

Galeano, P. and Peña, D. (2001). Multivariate analysis in vector time series. 57

Giri, J., Parashar, M., Trehern, J., and Madani, V. (2012). The situation room: Control center analytics for enhanced situational awareness. *IEEE Power and Energy Magazine*, 10(5):24–39. 6

Golay, X., Kollias, S., Stoll, G., Meier, D., Valavanis, A., and Boesiger, P. (1998). A new correlation-based fuzzy logic clustering algorithm for fmri. *Magnetic resonance in medicine*, 40(2):249–260. 56

Goodfellow, I. J., Shlens, J., and Szegedy, C. (2014). Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*. 66

Gross, G. and Galiana, F. D. (1987). Short-term load forecasting. *Proceedings of the IEEE*, 75(12):1558–1573. 46, 47, 48

Guideline, N. R. (2018). Bps-connected inverter-based resource performance. *North American Electric Reliability Corporation (NERC): Atlanta, GA, USA*. 88

Guo, T. (2017). *Distributed Time Series Analytics*. PhD thesis. 72

Hahn, A. and Govindarasu, M. (2011). Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid*, 2(4):835–843. 50

Hamilton, W. L. (2020). Graph representation learning. *Synthesis Lectures on Artifical Intelligence and Machine Learning*, 14(3):1–159. 97, 99

Henry, D. and Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety*, 99:114–122. 24

Hines, P., Cotilla-Sanchez, E., and Blumsack, S. (2010a). Do topological models provide good information about electricity infrastructure vulnerability? *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 20(3):033122. 10

Hines, P., Cotilla-Sanchez, E., and Blumsack, S. (2010b). Do topological models provide good information about electricity infrastructure vulnerability? *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 20(3):033122. 87

Hobbs, B. F., Jitprapaikulsarn, S., Konda, S., Chankong, V., Loparo, K. A., and Maratukulam, D. J. (1999). Analysis of the value for unit commitment of improved load forecasts. *IEEE Transactions on Power Systems*, 14(4):1342–1348. 9

Hobbs, J. E. (2020). Food supply chains during the covid-19 pandemic. *Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie*, 68(2):171–176. 17

Hoffman, P., Bryan, W., Farber-DeAnda, M., Cleaver, M., Lewandowski, C., and Young, K. (2010). Hardening and resiliency: Us energy industry response to recent hurricane seasons. *Office of Electricity Delivery and Energy Reliability, US Department of Energy, OE/ISER Final Report*. 17, 38

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual review of ecology and systematics*, pages 1–23. 8, 16

Holmgren, Å. J. (2006). Using graph models to analyze the vulnerability of electric power networks. *Risk analysis*, 26(4):955–969. 10

Hong, T. and Fan, S. (2016). Probabilistic electric load forecasting: A tutorial review. *International Journal of Forecasting*, 32(3):914–938. 46, 49

Hong, T., Wang, P., and Willis, H. L. (2011). A naïve multiple linear regression benchmark for short term load forecasting. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–6. IEEE. 46, 49, 62

Hosseini, S., Barker, K., and Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145:47–61. 33, 34

Hu, Y., Li, J., and Holloway, L. E. (2008). Towards modeling of resilience dynamics in manufacturing enterprises: Literature review and problem formulation. In *2008 IEEE International Conference on Automation Science and Engineering*, pages 279–284. IEEE. 17

Huang, G., Wang, J., Chen, C., Qi, J., and Guo, C. (2017). Integration of preventive and emergency responses for power grid resilience enhancement. *IEEE Transactions on Power Systems*, 32(6):4451–4463. 18

Huang, J., Guan, L., Su, Y., Yao, H., Guo, M., and Zhong, Z. (2020). Recurrent graph convolutional network-based multi-task transient stability assessment framework in power system. *IEEE Access*, 8:93283–93296. 86

Hubele, N. and Cheng, C.-S. (1990). Identification of seasonal short-term load forecasting models using statistical decision functions. *IEEE Transactions on Power Systems*, 5(1):40–45. 9

IEEE PES Task Force: Stanković, A., Tomsovic, K., De Caro, F., Braun, M., Chow, J., Äukalevski, N., Dobson, I., Eto., J., Fink, B., Hachmann, C., Hill, D., Ji, C.,

Kavicky, J., Levi, V., Liu, C.-C., Mili, L., Moreno, R., Panteli, M., Petit, F., Sansavini, G., Singh, C., Srivastava, A., Strunz, K., Sun, H., Xu, Y., and Zhao, S. (2022). Methods for analysis and quantification of power system resilience. *IEEE Transactions on Power Systems*, pages 1–14. 9, 42

Isermann, R. (2006). *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media. 36

Jensen, C. A., El-Sharkawi, M. A., and Marks, R. J. (2001). Power system security assessment using neural networks: feature selection using fisher discrimination. *IEEE Transactions on power systems*, 16(4):757–763. 91

Jufri, F. H., Widiputra, V., and Jung, J. (2019). State-of-the-art review on power grid resilience to extreme weather events: Definitions, frameworks, quantitative assessment methodologies, and enhancement strategies. *Applied Energy*, 239:1049–1065. 32

Kalyani, S. and Swarup, K. S. (2010a). Classification and assessment of power system security using multiclass svm. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 41(5):753–758. 11

Kalyani, S. and Swarup, K. S. (2010b). Classification and assessment of power system security using multiclass svm. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 41(5):753–758. 89

Keim, M. E. (2008). Building human resilience: the role of public health preparedness and response as an adaptation to climate change. *American journal of preventive medicine*, 35(5):508–516. 17

Kezunovic, M., Pinson, P., Obradovic, Z., Grijalva, S., Hong, T., and Bessa, R. (2020). Big data analytics for future electricity grids. *Electric Power Systems Research*, 189:106788. 46

Kim, C. J. and Obah, O. B. (2007). Vulnerability assessment of power grid using graph topological indices. *International Journal of Emerging Electric Power Systems*, 8(6). 27

Kim, D. H., Eisenberg, D. A., Chun, Y. H., and Park, J. (2017). Network topology and resilience analysis of south korean power grid. *Physica A: Statistical Mechanics and its Applications*, 465:13–24. 10

Kipf, T. N. and Welling, M. (2016). Semi-supervised classification with graph convolutional networks. *arXiv preprint arXiv:1609.02907*. 99

Kutare, M., Eisenhauer, G., Wang, C., Schwan, K., Talwar, V., and Wolf, M. (2010). Monalytics: online monitoring and analytics for managing large scale data centers. In *Proceedings of the 7th international conference on Autonomic computing*, pages 141–150. 70

Latora, V., Nicosia, V., and Russo, G. (2017a). *Complex networks: principles, methods and applications*. Cambridge University Press. 93

Latora, V., Nicosia, V., and Russo, G. (2017b). *Complex networks: principles, methods and applications*. Cambridge University Press. 148

Li, J., Yang, Y., Sun, J. S., Tomsovic, K., and Qi, H. (2021). Conaml: Constrained adversarial machine learning for cyber-physical systems. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pages 52–66. 47, 52

Li, Z., Shahidehpour, M., Aminifar, F., Alabdulwahab, A., and Al-Turki, Y. (2017). Networked microgrids for enhancing the power system resilience. *Proceedings of the IEEE*, 105(7):1289–1310. 40

Liang, Y., He, D., and Chen, D. (2019). Poisoning attack on load forecasting. In *2019 IEEE innovative smart grid technologies-Asia (ISGT Asia)*, pages 1230–1235. IEEE. 9

Liao, W., Bak-Jensen, B., Pillai, J. R., Wang, Y., and Wang, Y. (2021). A review of graph neural networks and their applications in power systems. *Journal of Modern Power Systems and Clean Energy*. 86

Lin, J., Keogh, E., Lonardi, S., and Chiu, B. (2003). A symbolic representation of time series, with implications for streaming algorithms. In *Proceedings of the 8th ACM SIGMOD workshop on Research issues in data mining and knowledge discovery*, pages 2–11. 58, 60

Liu, S., Wu, C., and Zhu, H. (2021). Graph neural networks for learning real-time prices in electricity market. *arXiv preprint arXiv:2106.10529*. 86

Liu, X., Shahidehpour, M., Li, Z., Liu, X., Cao, Y., and Bie, Z. (2016a). Microgrids for enhancing the power grid resilience in extreme conditions. *IEEE Transactions on Smart Grid*, 8(2):589–597. 9

Liu, X., Shahidehpour, M., Li, Z., Liu, X., Cao, Y., and Bie, Z. (2016b). Microgrids for enhancing the power grid resilience in extreme conditions. *IEEE Transactions on Smart Grid*, 8(2):589–597. 17

Liu, Y., Ning, P., and Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):1–33. 47, 52

Luo, J., Hong, T., and Fang, S.-C. (2018). Benchmarking robustness of load forecasting models under data integrity attacks. *International Journal of Forecasting*, 34(1):89–104. 10

Manning, C., Raghavan, P., and Schütze, H. (2010). Introduction to information retrieval. *Natural Language Engineering*, 16(1):100–103. 106

Marnay, C., Aki, H., Hirose, K., Kwasinski, A., Ogura, S., and Shinji, T. (2015). Japan's pivot to resilience: How two microgrids fared after the 2011 earthquake. *IEEE Power and Energy Magazine*, 13(3):44–57. 40

Martin, S., Deffuant, G., and Calabrese, J. M. (2011). Defining resilience mathematically: from attractors to viability. In *Viability and resilience of complex systems*, pages 15–36. Springer. 37

McCalley, J., Oluwaseyi, O., Krishnan, V., Dai, R., Singh, C., and Jiang, K. (2010). System protection schemes: limitations, risks, and management. *Final Report to the Power Systems Engineering Research Center (PSERC)*. 110

Meyer, R. J., Daniels, R., Kettl, D., and Kunreuther, H. (2006). Why we under-prepare for hazards. *On risk and disaster: Lessons from Hurricane Katrina*, 153:174. 16

Monfared, M. A. S., Jalili, M., and Alipour, Z. (2014). Topology and vulnerability of the iranian power grid. *Physica A: Statistical Mechanics and its Applications*, 406:24–33. 10

Morison, K., Wang, L., and Kundur, P. (2004). Power system security assessment. *IEEE power and energy magazine*, 2(5):30–39. xiv, 10, 85

Morovati, S. and Pulgar-Painemal, H. (2021). Control coordination between dfig-based wind turbines and synchronous generators for optimal primary frequency response. In *2020 52nd North American Power Symposium (NAPS)*, pages 1–6. IEEE. 82

Morovati, S., Zhang, Y., Djouadi, S. M., Tomsovic, K., Wintenberg, A., and Olama, M. (2021). Robust output feedback control design for inertia emulation by wind turbine generators. *IEEE Transactions on Power Systems*. 82

Mukherjee, R. and De, A. (2021). Real-time dynamic security analysis of power systems using strategic pmu measurements and decision tree classification. *Electrical Engineering*, 103(2):813–824. 84, 116

Munoz, A. and Dunbar, M. (2015). On the quantification of operational supply chain resilience. *International journal of production research*, 53(22):6736–6751. 24

Negnevitsky, M. (2019). High renewable energy penetration and power system security: new challenges and opportunities. In *10th International Scientific Symposium on Electrical Power Engineering, ELEKTROENERGETIKA 2019*, pages 16–25. 81

Negnevitsky, M., Tomin, N., Kurbatsky, V., Panasetsky, D., Zhukov, A., and Rehtanz, C. (2015). A random forest-based approach for voltage security monitoring in a power system. In *2015 IEEE Eindhoven PowerTech*, pages 1–6. IEEE. 84

Newman, M. (2018). *Networks*. Oxford university press. 93

Nezamoddini, N., Mousavian, S., and Erol-Kantarci, M. (2017). A risk optimization model for enhanced power grid resilience against physical attacks. *Electric Power Systems Research*, 143:329–338. 9

Niazi, K., Arora, C., and Surana, S. (2004). Power system security evaluation using ann: feature selection using divergence. *Electric Power Systems Research*, 69(2-3):161–167. 91

Niebur, D. and Germond, A. J. (1992). Power system static security assessment using the kohonen neural network classifier. *IEEE Transactions on Power Systems*, 7(2):865–872. 11

Ortiz-Arroyo, D. (2010). Discovering sets of key players in social networks. In *Computational social network analysis*, pages 27–47. Springer. xiv, 95, 96

Ouyang, M., Dueñas-Osorio, L., and Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural safety*, 36:23–31. 33, 36

Pagani, G. A. and Aiello, M. (2013). The power grid as a complex network: a survey. *Physica A: Statistical Mechanics and its Applications*, 392(11):2688–2700. 10, 43, 93

Panteli, M. and Mancarella, P. (2015). The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine*, 13(3):58–66. 17, 26

Panteli, M., Mancarella, P., Trakas, D. N., Kyriakides, E., and Hatziargyriou, N. D. (2017). Metrics and quantification of operational and infrastructure resilience in power systems. *IEEE Transactions on Power Systems*, 32(6):4732–4742. 18, 24

Panteli, M., Trakas, D. N., Mancarella, P., and Hatziargyriou, N. D. (2016). Boosting the power grid resilience to extreme weather events using defensive islanding. *IEEE Transactions on Smart Grid*, 7(6):2913–2922. 9, 32

Phillips, J., Finster, M., Pillon, J., Petit, F., and Trail, J. (2016). State energy resilience framework. Technical report, Argonne National Lab.(ANL), Argonne, IL (United States). 17, 26

Pillitteri, Y. V. and Brewer, L. T. (2014). Nistir 7628 revision 1 guidelines for smart grid cybersecurity. In *Proc. Smart Grid Interoperability Panel (SGIP)*, page 668. 22

Preston, B. L., Backhaus, S. N., Ewers, M., Phillips, J., Silva-Monroy, C., Dagle, J., and King, J. (2016). Resilience of the us electricity system: a multi-hazard perspective. *DOE report, August*. 27

Priya Datta, P., Christopher, M., and Allen, P. (2007). Agent-based modelling of complex production/distribution systems to improve resilience. *International Journal of Logistics Research and Applications*, 10(3):187–203. 17

Quitana, G., Molinos-Senante, M., and Chamorro, A. (2020). Resilience of critical infrastructure to natural hazards: A review focused on drinking water systems. *International Journal of Disaster Risk Reduction*, page 101575. 16

Rehak, D., Senovsky, P., Hromada, M., and Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International journal of critical infrastructure protection*, 25:125–138. 9

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, 21(6):11–25. xiii, 3, 4

Riolli, L. and Savicki, V. (2003). Information system organizational resilience. *Omega*, 31(3):227–233. 17

Rose, A. (2007). Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environmental Hazards*, 7(4):383–398. 33

Salvi, A., Spagnoletti, P., and Noori, N. S. (2022). Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, 112:102507. 41

Senroy, N. and Heydt, G. T. (2006). A conceptual framework for the controlled islanding of interconnected power systems. *IEEE transactions on power systems*, 21(2):1005–1006. 40

Shao, C., Shahidehpour, M., Wang, X., Wang, X., and Wang, B. (2017). Integrated planning of electricity and natural gas transportation systems for enhancing the power grid resilience. *IEEE Transactions on Power Systems*, 32(6):4418–4429. 17

Shea, D. (2018). Hardening the grid: how states are working to establish a resilient and reliable electric system. In *National Conference of State Legislatures (NCSL) website*. 5

Shi, Z., Yao, W., Zeng, L., Wen, J., Fang, J., Ai, X., and Wen, J. (2020). Convolutional neural network-based power system transient stability assessment and instability mode prediction. *Applied Energy*, 263:114586. 86

Shirali, G., Motamedzade, M., Mohammadfam, I., Ebrahimipour, V., and Moghimbeigi, A. (2012). Challenges in building resilience engineering (re) and adaptive capacity: A field study in a chemical plant. *Process safety and environmental protection*, 90(2):83–90. 17

Sittithumwat, A. and Tomsovic, K. (2002a). Dynamic security margin estimation using artificial neural networks. In *IEEE Power Engineering Society Summer Meeting,*, volume 3, pages 1322–1327. IEEE. 11

Sittithumwat, A. and Tomsovic, K. (2002b). Dynamic security margin estimation using artificial neural networks. In *IEEE Power Engineering Society Summer Meeting,*, volume 3, pages 1322–1327. IEEE. 81, 84

Sittithumwat, A. and Tomsovic, K. (2005). Dynamic security margin estimation with preventive control using artificial neural networks. *International Energy Journal*, 6. 84

Sobhani, M., Hong, T., and Martin, C. (2020). Temperature anomaly detection for electric load forecasting. *International Journal of Forecasting*, 36(2):324–333. 49

Somasundaram, D. and Sivayokan, S. (2013). Rebuilding community resilience in a post-war context: developing insight and recommendations-a qualitative study in northern sri lanka. *International journal of mental health systems*, 7(1):3. 32

Sridhar, S., Hahn, A., and Govindarasu, M. (2012). Cyber attack-resilient control for smart grid. In *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pages 1–3. 18

Stasinos, E.-I. E., Trakas, D. N., and Hatziargyriou, N. D. (2022). Microgrids for power system resilience enhancement. *iEnergy*, 1(2):158–169. 40

Steinkohl, J., Wang, X., Davari, P., and Blaabjerg, F. (2019). A frequency security analysis of wind integrated power systems with frequency controls. In *18th Wind Integration Workshop*. Energynautics. 82

Strbac, G., Hatziargyriou, N., Lopes, J. P., Moreira, C., Dimeas, A., and Papadaskalopoulos, D. (2015). Microgrids: Enhancing the resilience of the european megagrid. *IEEE Power and Energy Magazine*, 13(3):35–43. 40

Sunitha, R., Kumar, R. S., and Mathew, A. T. (2013). Online static security assessment module using artificial neural networks. *IEEE transactions on power systems*, 28(4):4328–4335. 84

Taylor, C. W. (1994). *Power System Voltage Stability*. McGraw-Hill. 82

International Electrotechnical Commission et al. (2015). International electrotechnical vocabulary—part 192: Dependability. *International standard IEC*, pages 60050–192. 20, 21

PJM Resource Adequacy Planning Department (2016). Load forecasting model whitepaper. Technical report, PJM Interconnection. https://www.pjm.com/~/media/library/reports-notices/load-forecast/2016-load-forecast-whitepaper.ashx/. 48

Teymouri, F., Amraee, T., Saberi, H., and Capitanescu, F. (2017). Toward controlled islanding for enhancing power grid resilience considering frequency stability constraints. *IEEE Transactions on Smart Grid*, 10(2):1735–1746. 40

Ton, D. T. and Wang, W. P. (2015). A more resilient grid: The us department of energy joins with stakeholders in an r&d plan. *IEEE Power and Energy Magazine*, 13(3):26–34. 17

Tortós, J. Q. and Terzija, V. (2012). Controlled islanding strategy considering power system restoration constraints. In *2012 IEEE Power and Energy Society General Meeting*, pages 1–8. IEEE. 40

Uday, P. and Marais, K. (2015). Designing resilient systems-of-systems: A survey of metrics, methods, and challenges. *Systems Engineering*, 18(5):491–510. 19

Vanfretti, L. and Arava, V. N. (2020). Decision tree-based classification of multiple operating conditions for power system voltage stability assessment. *International Journal of Electrical Power & Energy Systems*, 123:106251. 82

Vugrin, E. D. and Camphouse, R. C. (2011). Infrastructure resilience assessment through control design. *International journal of critical infrastructures*, 7(3):243–260. 37

Vugrin, E. D., Warren, D. E., and Ehlen, M. A. (2011). A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Process Safety Progress*, 30(3):280–290. 33

Vugrin, E. D., Warren, D. E., Ehlen, M. A., and Camphouse, R. C. (2010). A framework for assessing the resilience of infrastructure and economic systems. In *Sustainable and resilient critical infrastructure systems*, pages 77–116. Springer. 16, 31

Wang, P., Liu, B., and Hong, T. (2016). Electric load forecasting with recency effect: A big data approach. *International Journal of Forecasting*, 32(3):585–597. 46

Wang, Q. (2017). *Online Dynamic Security Assessment Using Phasor Measurement Unit and Forecasted Load*. PhD thesis, Arizona State University. 102, 116

Wang, Y., Chen, C., Wang, J., and Baldick, R. (2015). Research on resilience of power systems under natural disasters—a review. *IEEE Transactions on Power Systems*, 31(2):1604–1613. 17

Wang, Z., Scaglione, A., and Thomas, R. J. (2010). Electrical centrality measures for electric power grid vulnerability analysis. In *49th IEEE Conference on Decision and Control (CDC)*, pages 5792–5797. 27

Wang, Z., Scaglione, A., and Thomas, R. J. (2010). Electrical centrality measures for electric power grid vulnerability analysis. In *49th IEEE conference on decision and control (CDC)*, pages 5792–5797. IEEE. 87, 94

Watts, D. J. and Strogatz, S. H. (1998). Collective dynamics of 'small-world'networks. *nature*, 393(6684):440–442. 148

Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., and Philip, S. Y. (2020). A comprehensive survey on graph neural networks. *IEEE transactions on neural networks and learning systems*, 32(1):4–24. 86

Wulff, K., Donato, D., and Lurie, N. (2015). What is health resilience and how can we build it? *Annual Review of Public Health*, 36:361–374. 17

Xie, J. and Hong, T. (2017). Variable selection methods for probabilistic load forecasting: Empirical evidence from seven states of the united states. *IEEE Transactions on Smart Grid*, 9(6):6039–6046. 46, 47

Xu, L., Marinova, D., and Guo, X. (2015). Resilience thinking: a renewed system approach for sustainability science. *Sustainability Science*, 10(1):123–138. 8

Yodo, N. and Wang, P. (2016). Engineering resilience quantification and system design implications: A literature survey. *Journal of Mechanical Design*, 138(11). 31

Youn, B. D., Hu, C., and Wang, P. (2011). Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design*, 133(10). 34

Yu, X. and Jiang, J. (2015). A survey of fault-tolerant controllers based on safety-related issues. *Annual Reviews in Control*, 39:46–57. 16, 35

Yue, M., Hong, T., and Wang, J. (2019). Descriptive analytics-based anomaly detection for cybersecure load forecasting. *IEEE Transactions on Smart Grid*, 10(6):5964–5974. 10, 27

Zhang, Q. and Li, F. (2021). Cyber-vulnerability analysis for real-time power market operation. *IEEE Transactions on Smart Grid*. 47

Zhao, P., Gu, C., Ding, Y., Liu, H., Bian, Y., and Li, S. (2020). Cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks. *IEEE Transactions on Power Delivery*, 36(4):2253–2263. 41

Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C., and Sun, M. (2020). Graph neural networks: A review of methods and applications. *AI Open*, 1:57–81. 99

Zhou, K., Doyle, J. C., Glover, K., et al. (1996). *Robust and optimal control*, volume 40. Prentice hall New Jersey. 16, 35

Zhu, Q. and Başar, T. (2011). Robust and resilient control design for cyber-physical systems with an application to power systems. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pages 4066–4071. IEEE. 43

Zobel, C. W. and Khansa, L. (2014). Characterizing multi-event disaster resilience. *Computers & Operations Research*, 42:83–94. 24

ToC

Appendix

A Graph Theory Preliminaries

A graph G is defined as $G = (V, E)$, where set V is the set of vertices (nodes), and E is the set of edges. Here, V and E are always finite. An edge x, y is said to join the vertices x and y and is denoted by xy. If $xy \in E(G)$, then x and y are adjacent or neighboring, and the vertices x and y are incidents with the edge xy.

A *directed graph* is a connected one where all the edges are directed from one vertex to another. A directed graph is sometimes called a *digraph*. In contrast, a graph with bidirectional edges is called an *undirected graph*. A *clique* is a subset of vertices of an undirected graph such that every two distinct vertices in the clique are adjacent.

The *Adjacency matrix* of the graph $G = (V, E)$ is an $n \times n$ matrix $A = (a_{ij})$, where n is the number of vertices in G, $V = \{v_1, \ldots, v_n\}$ and a_{ij} = number of edges between v_i and v_j. When $a_{ij} = 0$, (v_i, v_j) is not an edge in G. The matrix A of an undirected graph is symmetric, i.e., $A^T = A$. In the case of a directed graph, the same definition remains while the matrix A is no more symmetric and depends on the direction of the edge.

The *Incidence matrix* I of an undirected graph has a row for each vertex and a column for each edge of the graph. The element $I_{i,j}$ of I is one if the i^{th} vertex is a vertex of the j^{th} edge and 0 otherwise. In directed graph, the element $I_{i,j}$ is -1 if the

i^{th} vertex is an initial vertex of the j^{th} edge, 1 if the i^{th} vertex is a terminal vertex, and 0 otherwise.

The *Laplacian matrix* or Kirchhoff matrix of a graph carries the same information as the adjacency matrix but has different valuable and vital properties, many relating to its spectrum. The Laplacian matrix is defined as $L = D - A$, where D is a diagonal matrix indicating the degree matrix.

A toy example is depicted in Figure A.1, where the clique are $C_1 = \{1, 2, 3\}$, $C_2 = \{2, 3, 4\}$ and the property matrices are as follows.

$$D = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$I = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, L = \begin{bmatrix} 2 & -1 & -1 & 0 & 0 \\ -1 & 4 & -1 & -1 & 0 \\ -1 & -1 & 4 & -1 & 0 \\ 0 & -1 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 1 \end{bmatrix}$$

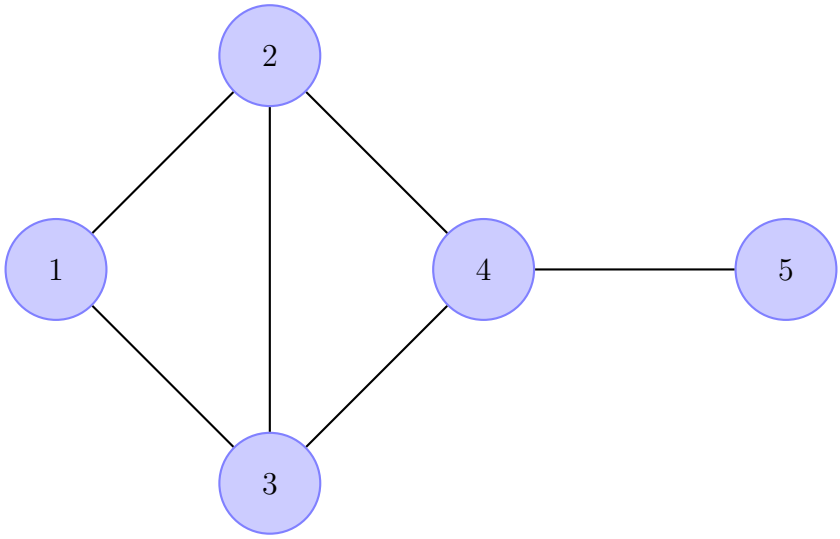


Figure A.1: A simple undirected graph.

B Complex Network

A collection of entities combined for a particular purpose is called a network. Many networks, such as the Internet, power grids, aviation networks, citation networks, food webs, economic networks, metabolic networks, neural networks, etc., surround us. A network can be a tangible object in Euclidean space, such as a power Grid, Internet, highway, or neural network. One can define entities in an abstract space, such as a circle of acquaintances and individual collaboration. Technology development makes the systems large and involves lots of communication. A *complex network* can thus be defined as an extensive collection of interconnected nodes. The main reason to call complex networks is that they are generally so huge that it is impossible to understand or predict their overall behavior by looking into the behavior of individual nodes or links.

To study the behavior of complex networks, researchers seek to discover the properties that support them to analyze complex network behavior using graph theory. Since the complex network is modeled as a set of vertices and edges, almost all efforts were about defining new concepts and measures to characterize the topology of real networks by the main characteristics. Note that modeling the complex network as a graph is a strong assumption since the dynamic units and their connections are considered a set of vertices and edges. The connections that usually depend on time, space, and many other details are translated to the existence of an edge. However, in many cases of practical interest, such an approximation provides a simple but informative representation of the entire system. The topology of a complex network follows some features in reality. Thanks to the available database, the three initial observations in the real network are:

- *The small-world property*: This property was first realized by Milgram in the 1960s in a series of social psychology experiments to approximate the number of steps in a chain of acquaintances. The experimental result showed that the number of links needed to reach the target person had an average value of just

six. This property was also seen in another experiment about successful e-mail exchange and is found in other real networks such as biological and technological ones Latora et al. (2017b). It indicates that most nodes in the graph are not neighbors of one another, but most nodes can be reached from every other node by a small number of hops or steps, meaning a small distance. In social science, it is related to *six degrees of separation* idea.

- *Clustering*: The real network is cliques form, indicating circles of vertices in which every vertex knows every other. This captures the node tendency to cluster and is calculated as the clustering coefficient by Watts and Strogatz Watts and Strogatz (1998).

- *Scale-free degree distributions*: In some networks, it is seen that all nodes in a network do not have the same number of edges. The edge of the node is indicated as a distribution function $P(k)$, which gives the probability that a randomly selected node has exactly k edges. If the $P(k)$ of a network has the power-law tail, i.e., $P(k) \sim k^{-\lambda}$, it is called scale-free degree distribution. This implies the existence of a small group of nodes with many connected edges, such as the World-Wide Web or metabolic networks Barabási (2009).

Considering the above characteristics, mainly three models are used to model a real network.

B.1 Random Graph

A random graph is a general term for probability distributions over graphs. Given an arbitrary node distribution, generating a random graph named *generalized random graph* is possible. The systematic study of random graphs was introduced by Erdös and Rènyi and indicated as $G_{N,K}^{ER}$. The *ER* random graph instruction is that regarding N disconnected nodes, start connecting couples of randomly selected nodes, prohibiting multiple connections, until the number of edges equals K. An alternative

version would be connecting N nodes with probability p or $(1-p)$ and denoted as $G_{N,p}$. This model is the ensemble of all such graphs in which a graph having m edges appears with probability $p^m(1-p)^{(M-m)}$ where $M = 1/2n(n-1)$ is the maximum possible number of edges. ER random graphs are the most studied among graph models. However, they can not provide a solid model presenting real complex network characteristics, and their structural properties vary with p.

B.2 Small-World Networks

This model was introduced by Watts and Strogatz (WS) and denoted as $G^{WS}_{N,K}$ to capture both the small-world property and high clustering coefficient. The construction method is about re-rewiring the graph given a probability p. That makes a ring with N nodes, in which each node is symmetrically connected to its $2m$ nearest neighbors for a total of $K = mN$ edges. Then, for every node, each link connected to a clockwise neighbor is rewired to a randomly chosen node with a probability p and preserved with a probability $(1-p)$. Here, the network's properties are a function of rewiring probability p and the network size N. Nevertheless, the WS graph illustrates some features of a real complex network. The construction procedure is highly nonlinear on the average shortest path length Boccaletti et al. (2006b), and not only affects the nearest neighbors' structure but also opens new shortest paths to the next-nearest neighbors.

B.3 Scale-Free Networks

In this type, the node degree distribution of the graph follows a power-law distribution. *Static scale-free networks* is obtained as a special case of generalized random graphs with a given degree distribution. If the model includes a growth and aging process, it is called an evolving scale-free network introduced by Barabási−Albert (BA) and denoted as $G^{BA}_{N,K}$. This model was inspired by the World Wide Web, consisting of two main properties to encapsulate evolution in the complex network

growth and preferential attachment. The modeling instruction is to start with m_0 isolated nodes; at each time step $t = 1, 2, 3, ..., N-m_0$, a new node j with $m \leq m_0$ links is added to the network. The probability that a link will connect j to an existing node i is linearly proportional to the actual degree of i: $\prod_{j \to i} = \frac{k_i}{\sum_l k_l}$. The more node degree at node i, the more chance to absorb a new edge.

The Overall comparison between the network modeling approaches is stated in Table B.1, and the graphical difference can be seen in Figure B.1 for a synthetic graph with 300 nodes. Looking at both the graph model and its degree distribution, one may conclude that the scale-free networks have nodes with high degree (Hub) due to node degree power-law distribution, making them robust against random failure and attack. However, having a hub drives the graph vulnerable to intentional failures or attacks. The clustering and small-world property are seen in the small-world model as expected due to its modeling procedure. While the ER random graph benefits from a vigorous mathematical theory to show many properties, such as phase transition (changing in the structure and having giant components), it does not perfectly mimic reality. It is no longer used in the model of real complex networks.

Table B.1: Graph models comparison.

Network	P(k)	<L>	C	Homogeneity
ER random	Possion	Relatively Large	Small	Homogeneity
WS small-world	Possion	Small	Large	Homogeneity
BA Scale Free	Power-law	Large	Relatively Small	Heterogeneity

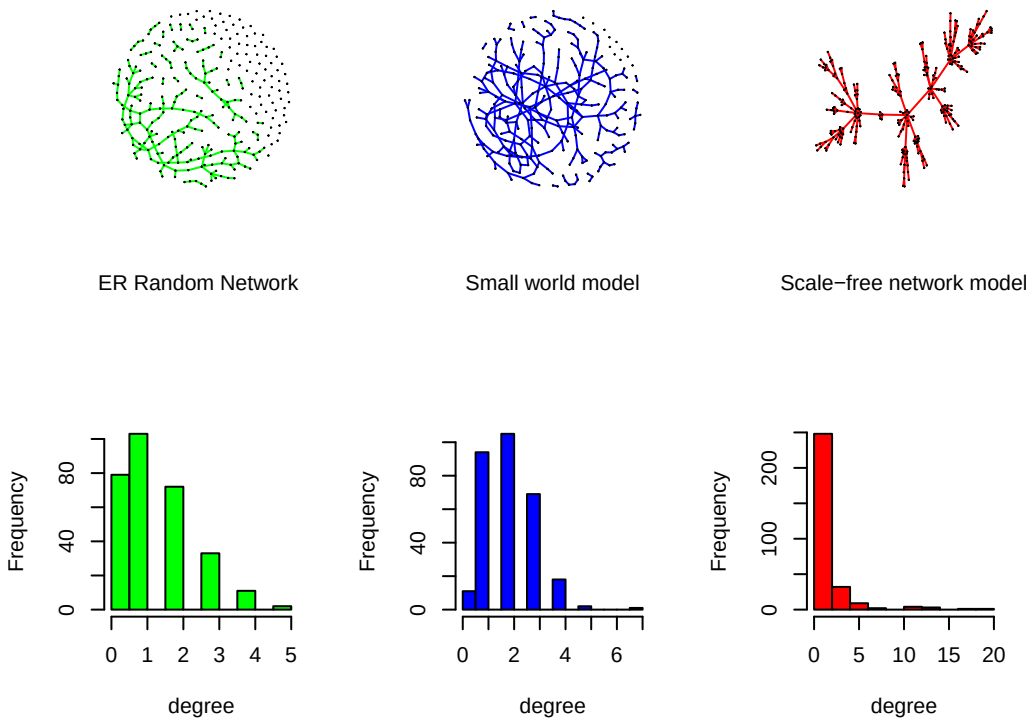


Figure B.1: Graph models shape and degree distribution: a sample network with 300 nodes.

Vita

Mojtaba Dezvarei obtained a B.S. degree in Electrical Engineering, specializing in control systems, from Imam Khomeini International University, Iran, in 2011. He furthered his education with an M.S. degree in Electrical Engineering, focusing on control systems, from the University of Tennessee, Knoxville, TN, USA, in 2022. Currently, Mojtaba is pursuing a Ph.D. in Electrical Engineering at the University of Tennessee, Knoxville, TN, USA, while serving as a research assistant in the Department of Electrical Engineering and Computer Science. He also holds seven years of practical experience as an electrical, control and automation engineer.

Mojtaba's research interests revolve around resiliency and security analysis of the electrical grid. He also specializes in control system theory and design, data-driven models, and the application of data science to address challenges in cyber-physical systems, with a particular focus on smart grids.