Florida International University

FIU Digital Commons

FIU Electronic Theses and Dissertations University Graduate School

10-29-2018

Game-Theoretic and Machine-Learning Techniques for Cyber-Physical Security and Resilience in Smart Grid

Longfei Wei
lwei004@fiu.edu

Follow this and additional works at: https://digitalcommons.fiu.edu/etd

Part of the Information Security Commons, Numerical Analysis and Scientific Computing Commons, Power and Energy Commons, Systems and Communications Commons, and the Theory and Algorithms Commons

Recommended Citation
Wei, Longfei, "Game-Theoretic and Machine-Learning Techniques for Cyber-Physical Security and Resilience in Smart Grid" (2018). *FIU Electronic Theses and Dissertations*. 3850.
https://digitalcommons.fiu.edu/etd/3850

This work is brought to you for free and open access by the University Graduate School at FIU Digital Commons. It has been accepted for inclusion in FIU Electronic Theses and Dissertations by an authorized administrator of FIU Digital Commons. For more information, please contact dcc@fiu.edu.

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

GAME-THEORETIC AND MACHINE-LEARNING TECHNIQUES FOR CYBER-PHYSICAL SECURITY AND RESILIENCE IN SMART GRID

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

by

Longfei Wei

2018

To: Dean John L. Volakis
College of Engineering and Computing

This dissertation, written by Longfei Wei, and entitled Game-Theoretic and Machine-Learning Techniques for Cyber-Physical Security and Resilience in Smart Grid, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Malek Adjouadi

Armando Barreto

Jean Andrian

Walid Saad

Arif I. Sarwat, Major Professor

Date of Defense: October 29, 2018

The dissertation of Longfei Wei is approved.

Dean John L. Volakis
College of Engineering and Computing

Andrés G. Gil
Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2018

© Copyright 2018 by Longfei Wei

All rights reserved.

DEDICATION

To my parents, for their love, endless support, and encouragement.

ACKNOWLEDGMENTS

This dissertation would not have been completed without the support of my advisor, committee, colleagues, friends, and family.

First of all, my sincere appreciation goes to my major professor, Dr. Arif I. Sarwat, who offered me the opportunity to be in the great family of the Energy, Power and Sustainability (EPS) Group. His motivating personality and endless encouragement improved my abilities in the early stages of research. In addition, he gave me great freedom to explore and learn to do independent research, and helped me grow as a researcher over the last five years.

I would also like to show my gratitude to my committee members, Dr. Malek Adjouadi, Dr. Armando Barreto, Dr. Jean Andrian, and Dr. Walid Saad, for their support, insightful comments, and constructive suggestions. One of the first classes I took at FIU was Image Processing, taught by Dr. Adjouadi. He was a great teacher, and everything I learned in the class laid a solid foundation for the rest of my pursuit. I also came to interact with Dr. Barreto initially through the class of Neural Network, which directly influenced my dissertation regarding machine learning parts. Dr. Andrian was the teacher of my Random Signal Principles class. He continued to offer valuable research suggestions afterwards, which were to the great benefit of my dissertation writing. I started my PhD on a collaborative project with Dr. Saad, and he provided me a deep insight of game theory. He has always been a great inspiration for me since then.

I am grateful to all the members of the EPS Group for creating a wonderfully collaborative work environment. In particular, thanks to Dr. Amirhasan Moghadasi and Dr. Arash Anzalchi for their help and many interesting and insightful conversations. I would also like to thank the staffs of the Electrical and Computer Engineering Department for their great commitment to student services.

A very special gratitude goes out to the National Science Foundation (NSF) for providing partial research funding. I also acknowledge the doctoral DYF fellowship from FIU graduate school during the fall semester of 2018. All this would be impossible without their generous support.

Finally, last but by no means least, I want to dedicate the dissertation to my father, Bin Wei, and my mother, Xichun Zheng, for their love and for fostering all my academic endeavors.

ABSTRACT OF THE DISSERTATION

GAME-THEORETIC AND MACHINE-LEARNING TECHNIQUES FOR CYBER-PHYSICAL SECURITY AND RESILIENCE IN SMART GRID

by

Longfei Wei

Florida International University, 2018

Miami, Florida

Professor Arif I. Sarwat, Major Professor

The smart grid is the next-generation electrical infrastructure utilizing Information and Communication Technologies (ICTs), whose architecture is evolving from a utility-centric structure to a distributed Cyber-Physical System (CPS) integrated with a large-scale of renewable energy resources. However, meeting reliability objectives in the smart grid becomes increasingly challenging owing to the high penetration of renewable resources and changing weather conditions. Moreover, the cyber-physical attack targeted at the smart grid has become a major threat because millions of electronic devices interconnected via communication networks expose unprecedented vulnerabilities, thereby increasing the potential attack surface. This dissertation is aimed at developing novel game-theoretic and machine-learning techniques for addressing the reliability and security issues residing at multiple layers of the smart grid, including power distribution system reliability forecasting, risk assessment of cyber-physical attacks targeted at the grid, and cyber attack detection in the Advanced Metering Infrastructure (AMI) and renewable resources.

This dissertation first comprehensively investigates the combined effect of various weather parameters on the reliability performance of the smart grid, and proposes a multilayer perceptron (MLP)-based framework to forecast the daily number of power interruptions in the distribution system using time series of common weather data. Compared with traditional statistical models, the proposed framework can reduce the Mean Squared

Error (MSE) by 8.77% and 61.37% for sustained and momentary power interruption forecasting, respectively. Regarding evaluating the risk of cyber-physical attacks faced by the smart grid, a stochastic budget allocation game is proposed to analyze the strategic interactions between a malicious attacker and the grid defender. A reinforcement learning algorithm is developed to enable the two players to reach a Nash equilibrium, and the risk of the cyber-physical attack can be assessed based on the game equilibrium. Simulation results on the IEEE 9-bus and 118-bus systems have shown that the attacker and the defender should take different strategies corresponding to the resources owned.

Furthermore, this dissertation develops a multimodal data-driven framework for the cyber attack detection in the power distribution system integrated with renewable resources. This approach introduces the spare feature learning into an ensemble classifier for improving the detection efficiency, and implements the spatiotemporal correlation analysis for differentiating the attacked renewable energy measurements from fault scenarios. Numerical results based on the IEEE 34-bus system show that the proposed framework achieves the most accurate detection of cyber attacks reported in the literature. To address the electricity theft in the AMI, a Distributed Intelligent Framework for Electricity Theft Detection (DIFETD) is proposed, which is equipped with Benford's analysis for initial diagnostics on large smart meter data. A Stackelberg game between utility and multiple electricity thieves is then formulated to model the electricity theft actions. Finally, a Likelihood Ratio Test (LRT) is utilized to detect potentially fraudulent meters, where, for each smart meter, the successful detection rate is achieved more than 95% and the false alarm is controlled beyond 10%, when the electricity is stolen in 50%.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

LIST OF ABBREVIATIONS

AGC	Automatic Generation Control
AMI	Advanced Metering Infrastructure
CME	Customer Momentary Experience
CPS	Cyber-Physical System
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DOE	Department of Energy
DoS	Denial of Service
ELM	Extreme Learning Machine
EMS	Energy Management System
FDI	False Data Injection
HILF	High Impact, Low Frequency
ICT	Information and Communication Technology
IoT	Internet of Things
JAL	Joint Action Learners
kNN	k-Nearest Neighbours
LBNL	Lawrence Berkeley National Laboratory
LRT	Likelihood Ratio Test
MAIFI	Momentary Average Interruption Frequency Index
MDP	Markov Decision Process
MI	Mutual Information
MLP	Multilayer Perceptron
MPE	Markov Perfect Equilibrium
NCDC	National Climatic Data Center
NERC	North American Electric Reliability Corporation

NIST	National Institute of Standards & Technology
PCA	principal Component Analysis
PG&E	Pacific Gas & Electric
RL	Reinforcement Learning
RMSE	Root Mean Squared Error
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCADA	Supervisory Control And Data Acquisition
SOM	Self Organizing Map
SSE	Sum of Squares Due to Error
SVM	Support Vector Machine
UFLS	Underfrequency Load Shedding
V2G	Vehicle to Grid
WLS	Weighted Least Square

CHAPTER 1

Introduction

The electric grid is one of the nation's most critical technological infrastructures, whose reliability and resilience are essential for the continuous grid operation and control, and also critical for the other interdependent infrastructures, such as communication networks, water supply systems, and transportation networks [1]. The critical and networked nature of the electric grid renders it susceptible to system disturbances from natural and man-made hazards, including, for instance, hurricanes, wildfires, ice storms, earthquakes, and malicious cyber and physical attacks [2]. These disturbances may not only lead to the failure of one electrical element, but also may cascades to other networks and cause the failure of other independent elements, resulting in a catastrophic widespread failure.

The major goal of this dissertation is to propose new mathematical methods and analytical tools for addressing the reliability and resilience aspects of the electric grid. A summary of the research background, literature review, and novel contributions of this dissertation will be included in the following sections of this chapter, which are organized as follows. Section 1.1 presents the power interruption problems caused by the various weather conditions, and describes the cyber-physical security issues introduced by the integration of the Information and Communication Technologies (ICTs). Section 1.2 reviews the current application of game-theoretic tools and machine-learning techniques for modeling and analyzing the reliability and resilience problems faced by the electric grid. In Section 1.3, the main contributions of this dissertation are summarized from the research areas, including system reliability forecasting, risk assessment of cyber-physical attacks targeted at the electric grid, and cyber attack detection in the Advanced Metering Infrastructure (AMI) and renewable energy resources. Finally, Section 1.4 outlines the general organization of this dissertation.

1.1 Research Background and Motivation

The smart grid is the next generation electrical infrastructure utilizing ICTs, which incorporates an advanced communication network into the traditional electric grid of generation, transmission and distribution components that enables the bidirectional communication between the electric utility and its customers [3]. A conceptual model proposed by the National Institute of Standards & Technology (NIST) of the United States in [4] defines seven important domains for the smart grid including bulk generation, transmission, distribution, customers, service provider, operations and markets, as shown in Figure 1.1. The ICTs facilitate the smart grid with effective operation, monitoring and control, enable predictive maintenance and self-healing responses to system disturbances, automate maintenance and operation, and encourage expanded deployment of renewable energy resources. However, the high penetration of renewable resources, a growing in electricity demands, and adverse weather conditions make meeting the reliability objectives in the smart grid increasingly challenging. According to the Lawrence Berkeley National Laboratory's (LBNL) report in 2016 [5, 6], the annual cost for power interruptions to the electricity customers of the United States is estimated to be $110 billion, which has increased more than 30% since 2004.

The power interruptions in the smart grid can be caused by a wide range of factors, such as adverse weather conditions, equipment failures, animals, trees, wildfires, and human errors [7, 8]. However, adverse weather conditions are usually the most important causes of the power interruptions in the current electric grid [9–13]. According to the reliability data collected by the United States Department of Energy (DOE) [14] from 1992 to 2011, adverse weather conditions contributed more than 64% of the total number of power interruptions. Extreme weather events have become more frequent and costly in recent decades. Especially, over the past three decades, the number of recorded extreme

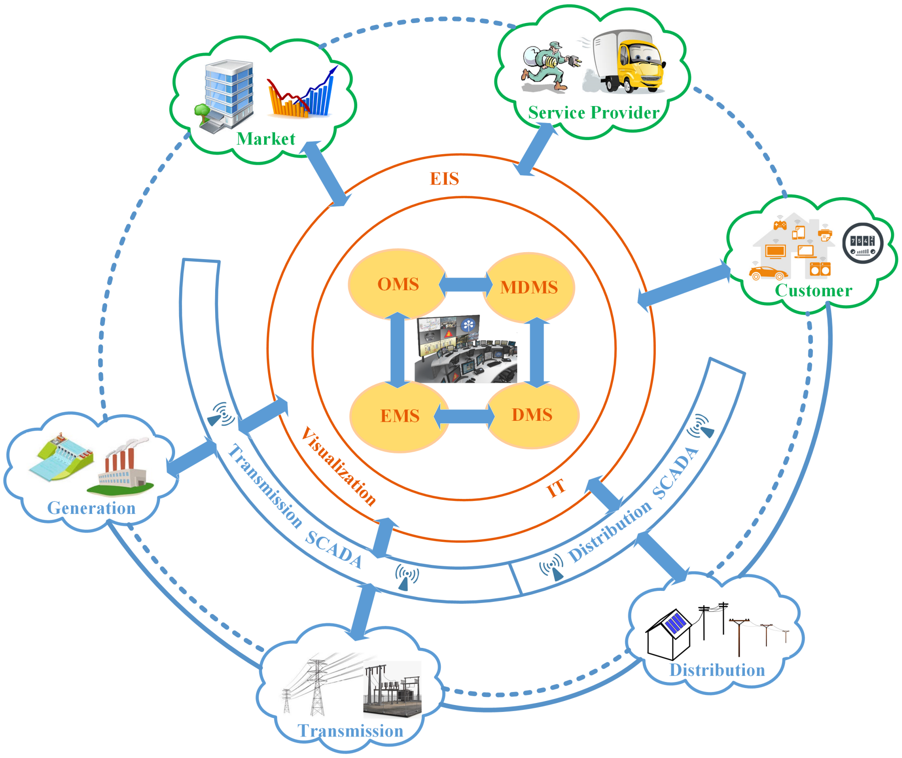


Figure 1.1: The smart grid conceptual model proposed by the United States NIST.

weather events in the world has increased from around 200 a year to over 400 per year [15]. The extreme weather events, such as hurricanes, wind storm, lightning, ice storm, and high/low temperatures, often can cause large-scale power interruptions. For example, hurricane Irma caused about 65% of the Florida state containing 6.5 million homes and businesses to lose power in 2017 [16]. Despite the potential for frequently changing weather conditions, the aging electric grid infrastructure has also resulted in an increasing number of intermittent power interruptions and an observed decrease in system reliability performance.

Furthermore, the large-scale, interconnected nature of smart grid renders the system susceptible to a range of cyber and physical attacks owing to a dramatic increase in its attack surface. This has raised serious concerns about security, as summarized in Table 1.1. It is important to note that attacks on one realm, say physical, have definite impacts on

Table 1.1: Physical and Cyber Attacks Targeted at the Smart Grid

Attack Vector	Year	Target	Impact
Stuxnet (CP)	2010	PLCs	Damage to nuclear SCADA
Flame (C)	2012	Microsoft Windows	Cyber espionage
Shamoon (C)	2012	Microsoft Windows	Cyber espionage
Red October (C)	2012	Computer Networks	Cyber espionage
Snipers (PC)	2013	Power Substation	Power outages in the substation
BlackEnergy3 (CP)	2015	Information Systems	Power outages of 225,000 customers
Mirai Botnet (C)	2016	Computer Networks	Disruption of Internet services
WannaCry (C)	2017	Microsoft Windows	200,000+ computers affected

the other (cyber), and vice versa. Accordingly, each attack vector (malware, worm or some form of physical assault) is labeled as **PC** to signify an attack on the *Physical* realm causing *Cyber* implications; **CP** to signify an attack on the *Cyber* realm causing *Physical* implications; and **C** to signify an attack on the *Cyber* realm alone. Additionally, the importance of human behavior in the proliferation and strength of attacks is irrefutable. Physical attacks may disrupt the power plants, transmission lines, and substations of the power grid. For instance, the Metcalf Sniper Attack on California's Pacific Gas & Electric (PG&E) in April 2013 by unidentified gunmen led not only to power outages, but also underscored the vulnerability of the grid [17]. Moreover, the emergence of cyber-attacks may seek accessibility to the Supervisory Control And Data Acquisition (SCADA) or AMI, thereby gaining remote access and/or control, and effectively compromising important electronic resources. The Stuxnet worm [18] was first discovered in 2010, which infected numerous industrial control systems and was responsible for causing substantial damage to power systems. The fear of such acts has peaked after the success of a coordinated cyber-attack, which used the infamous BlackEnergy3 malware to target networks serving several Ukirainian cities, eventually affecting 225,000 customers [19]. Such a malicious attack on critical Cyber-Physical System (CPS) infrastructure such as the smart grid can have a debilitating impact on every person's life and on national security.

1.2 Literature Review: Game-Theoretic and Machine-Learning Approaches

In order to design a resilient and secure smart grid against changing weather conditions and cyber-physical attacks, it will have to build on the solid mathematical methods and analytics tools. Game theory provides a mathematical framework for analyzing and implementing security solutions, and machine learning introduces an analytical approach to transform the high-dimensional data produced by the smart grid into meaningful representations, such as system operation patterns, fault detection, and control commands. Especially, game-theoretic methods and machine-learning techniques have been applied at multiple layers of the smart grid for addressing the reliability and security issues.

Smart Grid Reliability Analysis Based on Weather Conditions

For evaluating the effect of various weather conditions on the smart grid reliability performance, a wealth of researchers have investigated the effect of extreme weather conditions, such as floods, hurricanes, and ice storms, on the electric grid reliability performance [20–26] in the last decades. In [20], a three-state weather model was formulated for the predictive reliability assessment of the electric distribution systems, where the system failure rate was analyzed based on extreme weather conditions. The potential effects of extreme weather conditions and climate changes on power system components' operation and reliability were reviewed in [21], and the mitigation framework was outlined for boosting the resilience of electrical networks. In [22], a mathematical framework was presented to assess the risk of extreme weather cases on the power systems, in which the performances of system protection devices were evaluated under extreme events. Additionally, a risk-based defensive islanding algorithm was proposed in [23] for boosting the power grid resilience to extreme weather events. However, all of these works only consider extreme weather conditions. Although severe weather events can cause a large number of power interruptions, it is not common to consider these events under normal operation conditions. The major of electric customers' interruptions happen under normal weather conditions.

Recently, *statistical analysis techniques* were introduced in [27, 28] to analyze the relationship between the number of power interruptions on electric distribution networks and common weather parameters, such as temperature, wind, air pressure, and lightning. The number of power interruptions was predicted based on the total sum of the statistical model of each weather parameter. However, the power interruptions related with common weather conditions are essentially the result of combined action of many factors. The power interruption prediction only based on statistical models might be compromising due to the various effects of different weather parameters.

Smart Grid Protection Against Cyber-Physical Attacks

A series of research [29–34] based on *game-theoretic methods* has been proposed for defending the smart grid from various types of cyber and physical attacks. Especially, a zero-sum static game model was proposed in [29] to compute optimal defense strategies that seek to protect physical infrastructures of the power grid against physical attacks. In order to protect the communication network of the power grid, a game equilibrium obtained from a zero-sum static game model between an intentional attacker and a fusion-based defender was introduced and studied in [30]. In [31], a zero-sum game-theoretic framework was formulated to investigate the interactive decision-making process between a sensor node and an attacker who can launch denial-of-service (DoS) attacks. For defending against false data injection (FDI) attacks on power grid state estimation, in [32], the least-budget defense strategy in the game equilibrium was proposed to render power grids immune to FDI attacks. In [33], a general-sum game-theoretic framework was proposed to explore and evaluate optimal defense strategies for the power grid operator to protect the grid against a combination of cyber and physical attacks.

However, the works in [29–33] rely on a static game formulation in which the dynamics of the power grid are ignored and the interactions between the attacker and the defender are assumed to be one-shot events. In [34], a zero-sum stochastic game was proposed for modeling single transmission line attack-defense scenarios while focusing on deriving the probabilistic strategies of the involved players. While interesting, the stochastic game model of [34] focused only on a single attack (e.g. physical or cyber). Traditionally, power grid planning techniques have accommodated $N-1$ contingency in their scope. Even if the attacker successfully compromises a part of the cyber-physical power grid system, it is quite possible that no load shedding will be caused. However, great power failures could be triggered if the attacker launches coordinated attacks to compromise multiple parts or functions of the power grid in cyber and physical aspects. Compared with single attacks, coordinated attacks, when smartly structured, cannot only have severe physical impacts, but can also potentially nullify the effect of system redundancy and other defense mechanisms. In a recent report by North American Electric Reliability Corporation (NERC), the coordinated attack was identified as one of the three representative high-impact, low-frequency (HILF) threats [35]. Indeed, devising new defense mechanisms against such coordinated attacks is both challenging and desirable. In [36], a stochastic budget allocation game theory was introduced for modeling the attack-defense scenarios in the power grid while factoring in the coordinated cyber-physical attacks. The Nash equilibrium of the formulated dynamic game was derived for guiding the defender to optimally protect power grid elements at different system states.

Smart Grid Cyber-Physical Attack Detection:

Recently, a wealth of efforts have been proposed for the cyber attack detection in the power grid using the *machine leaning techniques*, such as supervised learning, unsupervised learning, and statistics-based learning approaches [37–41]. In [38], a decision tree-based anomaly detection approach was presented to secure the power grid communication network from distributed denial of service (DDoS) attacks. A malware infection detection using Kernel Fisher discriminant analysis was proposed in [39] by comparing malware traffic with normal traffic. An intrusion detection system was developed in [40] for early detection of threats in AMI of the smart grid, where a multi-support vector machine (SVM) classifier was trained. In [41], a Sybil attack detection method based on k-Nearest Neighbours (kNN) classification was introduced for the vehicle-to-grid (V2G) networks. However, all of these machine learning methods need to be evaluated to guide the selection of mechanisms that are most suitable for the Distributed Energy Resource (DER) cyber attack detection. Moreover, techniques should be developed to handle the complex and high-dimensional DER measurement data.

Feature learning is a key to improve the performance of existing machine learning-based attack detection mechanisms, which consists of feature extraction and selection. Feature extraction transforms the original features into a more meaningful representation by reconstructing its inputs and involves reducing the amount of resources required to describe a large dataset. There are two broad categories for feature extraction algorithms, including linear and nonlinear. Linear feature extraction algorithms, such as principal component analysis (PCA) [42], multidimensional scaling [43], and principal coordinates analysis [44], assume the data lies on a lower-dimensional linear subspace and project them on this subspace using matrix factorization. However, nonlinear feature extraction algorithms like self organizing maps (SOMs) [45] and Kohonen maps [46] create a lower dimensional mapping of an input by preserving its topological characteristics.

Performance of attack detection mechanisms is heavily dependent on the choice of applied features, and feature selection is to identify the most informative features from the original and extracted feature sets. Typically, feature selection is partitioned into three classes: *filters*, *wrappers*, and *embedded* methods. Filter methods analyze intrinsic properties of the dataset, ignoring the type of classifier. Conversely, wrappers use classifiers to score a given subset of features, and embedded methods inject the selection process directly into the classification learning process. In this paper, the filter methods are utilized to evaluate different types of classifiers for the DER attack detection. Among the most used filter-based strategies, Relief algorithm [47] estimates the quality of features according to how well their values distinguish between instances that are closer to each other. Another effective yet fast filter method is the Fisher method [48], which computes a score for a feature as the ratio of inter-class separation and intra-class variance, where features are evaluated independently. In [49], a mutual information (MI)-based approach is proposed, and the quality of a given feature is evaluated by the MI between the distribution of the values of this feature and the membership to a particular class.

1.3 Research Objectives and Original Contributions

The research reported in this dissertation is aimed at developing novel game-theoretic models and machine-learning algorithms for solving the smart grid reliability and resilience problems, such as power distribution system reliability forecasting, risk assessment of cyber-physical attacks targeted at the grid, and cyber attack detection in the AMI and renewable resources. Specifically, the main body of the dissertation has been published in several IEEE and other reputed journals and conferences [33, 36, 50–56]. In total, the dissertation has completed the following five major activities:

1) **Hybrid integration of multilayer perceptrons and parametric model for power distribution system reliability forecasting using common weather data**

The main contribution of this objective is to comprehensively investigate the combined effect of various weather parameters on the reliability performance of power system distribution networks. Especially, a multilayer perceptron (MLP)-based framework is proposed to forecast the daily numbers of sustained and momentary power interruptions in one distribution management area using time series of common weather data. Based on the real-time reliability data from the local utility, Florida Power & Light (FPL), and common weather data from National Climatic Data Center (NCDC), a modified extreme learning machine (ELM)-based hierarchical learning algorithm is then introduced to train, validate, and test the proposed framework. Essentially, compared with traditional statistical models, the proposed framework can reduce the mean squared error (MSE) by 8.77% and 61.37% for sustained and momentary power interruption forecasting, respectively. In addition, the sensitivity of each common weather parameter can be derived with respective to the daily numbers of power interruptions.

2) **A survey on application of noncooperative game-theoretic methods to address cyber-physical security threats and challenges in the smart grid**

Noncooperative game theory provides a mathematical framework for analyzing and implementing the smart grid cyber-physical security solutions. However, there is little research in the literature that comprehensively reviews and evaluates the application of noncooperative game theory to the security issues in the smart grid. In this effort, a systematic survey of existing game-theoretic approaches for mitigating security threats is proposed for three main smart grid zones: the power system network infrastructure, AMI, and state estimation. For each zone, the emerging threats and vulnerabilities are identified and summarized, and the potential attacks targeted on both cyber and physical realms are addressed. The current game-theoretic approaches for addressing these security threats are evaluated and compared. Future opportunities and extension of these approaches in the realistic smart grid cyber-physical security problems are also discussed.

3) **Risk assessment of coordinated cyber-physical attacks against the smart grid: a stochastic game approach**

In this approach, to address the dynamic nature of the smart grid protection, a stochastic budget allocation game is proposed to analyze the strategic interactions between a malicious attacker and the grid defender while factoring in the attack and defense budget limitations. At the game equilibrium, the optimal budget allocation strategies of the two players, in terms of attacking/protecting the critical elements of the grid, can be obtained. The information about the successful attack probability to various elements is used to evaluate the risk of the corresponding attack faced by the whole grid at various power system states. Simulation results on the IEEE 9-bus and 118-bus systems have shown that different risks are derived as the attack/defense budget is varied.

4) **Spare feature learning and spatiotemporal correlation for attack detection in power distribution systems integrated with DERs**

This objective presents a multimodal data-driven framework for the attack detection in power distribution systems integrated with DERs. Unlike previous works using only one machine learning classifier, this approach first introduces the spare feature learning techniques into an ensemble classifier to identify the abnormal events including faults and cyber attacks within DER implementations. Finally, the spatiotemporal correlation analysis is utilized for each DER measurement toward the differentiation of the attacked measurements from fault scenarios in the generated abnormal event list. A modified IEEE 34-bus distribution system modeled with photovoltaics (PV) farm, wind turbine generator (WTG), battery energy system, and diesel generator is implemented to simulate the normal, fault, and attack system scenarios, and the numerical results show that the proposed framework achieves the most accurate DER attack detection reported in the literature.

5) **A distributed intelligent framework for electricity theft detection using Benford's law and Stackelberg game**

A Distributed Intelligent Framework for Electricity Theft Detection (DIFETD) is proposed and implemented in this effort. It is equipped with Benford's law for initial but powerful diagnostics on large smart meter data. A Stackelberg game is formulated to analyze the strategic interactions between one utility and multiple electricity thieves, which is applied to data flagged suspicious by Benford's law. Finally, the Stackelberg equilibrium provides sampling rate and threshold to conduct a Likelihood Ratio Test (LRT) to detect potentially fraudulent meters. The capability of the proposed framework was validated against four intelligent theft scenarios with the real consumer power consumption data from FPL. For each smart meter, the successful detection rate is achieved more than 95% and the false alarm is controlled beyond 10%, when the electricity is stolen in 50%.

1.4 Dissertation Organization

The listed contributions in Section 1.3 will be discussed in detail in the remaining chapters, which are structured as follows:

Chapter 2 presents an overview of fundamental game theoretic concepts and current machine learning techniques applied to the reliability and resilience areas of the smart grid. Section 2.1 outlines the classification of game theory, and briefly introduces the definition, solution, and learning algorithms of static and dynamic game theory, respectively. Section 2.2 describes several key machine learning algorithms that are successfully used in the smart grid reliability and resilience evaluation with large datasets.

Chapter 3 proposes a hybrid framework integrating Multilayer Perceptrons (MLPs) and parametric regression models for forecasting the daily numbers of power interruptions in smart grid distribution networks using time series of common weather data. Section 3.1 formally defines the reliability problem and provides a basic introduction to the existing literature. Section 3.2 introduces the reliability metrics and weather parameters collected for analysis. Section 3.3 develops the parametric regression models between the reliability metrics and various weather parameters. Section 3.4 formulates a MLP model for forecasting the daily numbers of power interruptions and introduces a modified Extreme Learning Machine (ELM) based algorithm for training the formulated model. In Section 3.5, the proposed framework is evaluated, and the sensitivity of each weather parameter is analyzed. Section 3.6 concludes the chapter and outlines the future work.

Chapter 4 provides a systematic survey of existing game-theoretic approaches that implemented for mitigating security threats in three main smart grid zones including the power system network infrastructure, AMI, and power system state estimation. Section 4.1 categorizes the smart grid into three main zones and makes an overview of the network security challenges faced by each zone. Section 4.2 evaluates the current game theoretic models for cyber-physical security in power system network infrastructure. Section 4.3 compares the game theoretic models for cyber-physical security of communication network and smart meters in AMI. Section 4.4 introduces the game theoretic models for cyber-physical security in the power system state estimation. To conclude this chapter, we discuss future work and recent progresses in Section 4.5.

Chapter 5 investigates the risk assessment of the coordinated cyber-physical attacks against power grids using a novel game-theoretic approach. Section 5.1 makes an overview of the cyber-physical security issues in the smart grid. Section 5.2 presents the attack-defense scenario in the power grid as well as the formulated stochastic game. Section 5.3 introduces an optimal load shedding technology to quantify the attacker and defender's rewards. Then, Section 5.4 derives the Nash equilibrium of the proposed stochastic game, and computes the risk of the coordinated cyber-physical attack faced by the grid based on the probability of successful attack and corresponding physical impacts. Section 5.5 presents the simulation results while Section 5.6 concludes the chapter.

Chapter 6 presents a multimodal data-driven framework for the attack detection in power distribution systems integrated with a large-scale of distributed energy resources (DERs). Section 6.1 makes an overview of this chapter. Section 6.2 introduces the cyber attack models in DER systems. Section 6.3 describes the proposed DER attack detection framework. Section 6.4 develops a test distribution system. Section 6.5 compares the experimental results of the proposed attack detection framework with existing works, while Section 6.6 concludes the paper and outlines the future work.

Chapter 7 presents a Distributed Intelligent Framework for Electricity Theft Detection (DIFETD) is proposed and implemented in this chapter. Section 7.1 make a summary of this chapter. A summary of related work is provided in Section 7.2. Benford's Analysis for preliminary theft detection is explained in Section 7.3. A Stackelberg game between utility and thieves is proposed in Section 7.4. LRT for theft detection is described in Section 7.5. While Section 7.6 discusses data cleansing and the results, Section 7.7 provides conclusion and future work.

Chapter 8 summarizes the dissertation outcomes, concludes the significance of this research, discuss the results, and finally makes recommendations for the future works.

CHAPTER 2

Game-Theoretic and Machine-Learning Techniques

This chapter presents an overview of fundamental game theoretic concepts and current machine learning techniques applied to the reliability and resilience areas of the smart grid. Section 2.1 outlines the classification of game theory, and briefly introduces the definition, solution, and learning algorithms of static and dynamic game theory, respectively. Section 2.2 describes several key machine learning algorithms that are successfully used in the smart grid reliability and resilience evaluation with large datasets.

2.1 Fundamental Game Theoretic Concepts

Game theory is a branch of applied mathematics that deals with strategic interactions among multiple decision makers, i.e., *players*, in which each player's success in making choices depends on the choices of others [57]. With respect to whether the players can select actions or make decisions collectively or individually, games can be classified into *cooperative* and *noncooperative* games. Due to the conflicting interests between malicious personnel, i.e., *attackers*, and smart grid operators, i.e., *defenders*, this dissertation mainly focuses on noncooperative games that can be used to analyze the strategic decision making processes between attackers and defenders. In the noncooperative game, each attacker or defender's preference ordering among multiple alternatives is captured in an objective function. Attackers try to maximize their objective functions for utility or benefit, while defenders intend to minimize their objective functions for cost or loss. For a nontrivial game, the objective function of an attacker or defender depends on the choices (actions, or equivalently decision variables) of at least one other player, and generally of all the players, and hence players cannot simply optimize their own objective function independent of the choices of the other players.

Table 2.1: Noncooperative Game Classification

Classification	**Player**	**Action Set**	**Utility**	**Utility/ Action Set**	**Utility/Information**	**Time**
Type 1	2	finite	zero-sum	deterministic	complete	static
Type 2	N(≥ 2)	infinite	nonzero-sum	stochastic	incomplete	dynamic

The classification of noncooperative games is shown in Table 2.1. A noncooperative game is *nonzero-sum* if the sum of the players' objective functions cannot be made zero even after appropriate positive scaling and/or translation that do not depend on the players' decision variables. A two-player game is *zero-sum* if the sum of the objective functions of the two players is zero or can be made zero by appropriate positive scaling and translation that do not depend on the decision variables of the players. A game is a *finite* game if each player has only a finite number of alternatives, that is, the players pick their actions out of finite sets (action sets); otherwise the game is an *infinite* game; finite games are also known as matrix games. A game is said to be *deterministic* if the players' actions uniquely determine the outcome, as captured in the objective functions; whereas, if the objective function of at least one player depends on an additional variable (state of nature) with a known probability distribution, then the game is a *stochastic* game. A game is a *complete information* game if the description of the game [that is, the players, the objective functions, and the underlying probability distributions (if stochastic)] is common information to all players; otherwise it is an *incomplete information* game. Finally, noncooperative games can be classified into two categories: *static* games and *dynamic* games. A game is static if each player acts only once, and none of the players has access to information on the actions of any of the other players; otherwise it is a dynamic game. A dynamic game is said to be a differential game if the evolution of the decision process (controlled by the players over time) takes place in continuous time, and generally involves a differential equation. In the following parts, the definition, solution, and learning algorithms of static and dynamic games will be introduced in detail.

2.1.1 Static Game Theory

A static game is one in which the notions of time or information do not affect the action or decision selection of the players [58]. Therefore, in a static setting, a noncooperative game can be seen as a one-shot process in which the players take their actions only once (simultaneously or at different points in time). Here, we provide one general definition for $N(\geq 2)$ players' static noncooperative games, which is shown as follows:

Definition 2.1.1 *A N-player static noncooperative game, $\Xi = \langle \mathcal{N}, \{\mathcal{A}_i\}_{i\in\mathcal{N}}, \{U_i\}_{i\in\mathcal{N}} \rangle$, in normal form, is characterized by three main elements: (1) the players' set $\mathcal{N} := \{1, ..., N\}$, (2) the action set $\mathcal{A}_i$ for each player $i \in \mathcal{N}$, and (3) the utility function U_i for each player $i \in \mathcal{N}$, which reflects the gains and costs from players' action choices.*

In such a game, each player $i \in \mathcal{N}$ intends to choose an action $a_i \in \mathcal{A}_i$ so as to optimize its utility function $U_i(a_i, \boldsymbol{a}_{-i})$ which depends not only on player i's action choice a_i but also on the vector of actions taken by the other players in $\mathcal{N} \setminus i$, denoted by $\boldsymbol{a}_{-i}$. The action selection of N players in such a deterministic manner is called *pure strategies*, denoted by $\boldsymbol{a} = (a_1, ..., a_N) \in \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$. Then, one of the most important objectives of static noncooperative game theory is to derive a *Nash equilibrium* [59], that is, $\boldsymbol{a}^* \in \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$, such that no player i can improve its utility by changing *unilaterally* its actions, given that the actions of the other players are fixed. For the static noncooperative game theory, the Nash equilibrium can be formally defined as follows:

Definition 2.1.2 *A vector of actions $a^* \in \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$ is a Nash equilibrium of a N-player, if and only if $\forall i \in \mathcal{N}$, the following condition holds:*

$$U_i(a_i^*, \boldsymbol{a}_{-i}^*) \geq U_i(a_i, \boldsymbol{a}_{-i}^*), \forall a_i \in \mathcal{A}_i. \tag{2.1}$$

However, a Nash equilibrium in pure strategies is not guaranteed for all static noncooperative games, which opens the door for a *mixed-strategy* Nash equilibrium [60]. A mixed strategy for each player i is a probability distribution over its action set $\mathcal{A}_i$, denoted by $\boldsymbol{\pi}_i$, and a Nash equilibrium is guaranteed to exist in mixed strategies for any finite game.

Numerous learning algorithms have been proposed in the literature for computing Nash equilibrium of static noncooperative games. Two classical iterative algorithms are *best response dynamics* [61] and *fictitious play* [62], in which each player chooses the action that maximizes its utility function given the actions of the other players. A myopic best response strategy was first studied in [63] and refers to the scenario where a firm in a duopoly adjusts its output to maximize its payoff based on the known output of its competitor. The strategy known as fictitious play (employed in finite games), where a player devises a best response based on the history of the other players' actions, was introduced in [64] in the context of mixed-strategy Nash equilibrium in matrix games. The advantage of an iterative algorithm is its simple implementation, however, it suffers from several drawbacks. First, a best response process is only guaranteed to converge to an equilibrium for certain types of utility functions. Second, best response dynamics are highly sensitive to the initial conditions and any change in these conditions could lead to different equilibriums. Third, adopting a best response approach does not always guarantee convergence to an efficient equilibrium.

In contrast, *regret matching* is a type of learning algorithms in which the players attempt to minimize their regret from using a certain action, i.e., the difference between the utility of always playing a certain action and the utility that they achieved by playing their current strategy. An in-depth treatment of regret matching algorithms is found in [65]. Many other types of learning schemes such as reinforcement learning (RL) are also used in various game-theoretic scenarios in order to find a desirable state of the system [66].

2.1.2 Dynamic Game Theory

In contrast to static games, dynamic noncooperative game [67–69] is one in which the players have some information about each others' choices, can act more than once, and time has a central role in the decision making. Note that, when the game is dynamic, one needs to also define, as part of the game, additional components such as information sets, time, or histories (i.e., sets of past actions) which are usually reflected in the utility functions. Dynamic games can be classified into series of games including *repeated games*, *extensive games*, *differential games*, *evolutionary games*, and *stochastic games*. A common framework to study the interactions between attackers and defenders in dynamic smart grid systems is a stochastic game [69]. Here, we provide one general definition for $N(\geq 2)$ players' stochastic smart grid security games, which is shown as follows:

Definition 2.1.3 *A N-player stochastic game, $\Xi = \langle \mathcal{N}, \{\mathcal{A}_i\}_{i\in\mathcal{N}}, \{U_i\}_{i\in\mathcal{N}}, \mathcal{S}, T\rangle$ in normal form, has the following key elements:*

- *The players' set $\mathcal{N} = \{1, ..., N\}$;*
- *The action set $\mathcal{A}_i$ for each player $i \in \mathcal{N}$;*
- *The utility function U_i for each player $i \in \mathcal{N}$, which reflects the gains and costs from players' action choices;*
- *The smart grid state space $\mathcal{S}$, where each state $s \in \mathcal{S}$ is associated with the status of smart grid elements;*
- *The state transition probability $T_{s,s'}(\boldsymbol{a}, \boldsymbol{d})$ from state $s \in \mathcal{S}$ to state $s' \in \mathcal{S}$ under the action selection of N players, denoted by $\boldsymbol{a} = (a_1, ..., a_N) \in \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$.*

In such a stochastic game, players' actions directly affect underlying state variables that influence their utilities. The state variables evolve according to a Markov process in discrete time, and players maximize their infinite horizon expected utility, respectively.

The standard solution concept for stochastic games is *Markov perfect equilibrium* (MPE) [67], where a player's equilibrium strategy depends on the current state of all players. The traditional Q-Learning algorithm for Markov decision processes is extended to two-player zero-sum stochastic games for Minimax-Q Learning in [66]. And the Minimax-Q Learning algorithm is applied for general-sum stochastic games in [70].

However, MPE presents two significant obstacles as an analytical tool, particularly as the number of players grows larger. First is *computability*: the state space expands in dimension with the number of players, and thus the "curse of dimensionality" kicks in, making computation of MPE infeasible in many problems of practical interest. Second is *plausibility*: as the number of players grows larger, it becomes increasingly difficult to believe that individual players track the exact behavior of all other agents. Therefore, *fictitious play* [64] assumes opponents play stationary strategies. The algorithm maintains information about the average value of each action (i.e., is the average expected discounted reward from past experience). The algorithm then selects the action that has done the best in the past. This is nearly identical to single agent value iteration with a uniform weighting of past experience.

Opponent modeling and joint action learners (JALs) [71,72] are RL algorithms, which are multi-agent extensions to the well-studied Q-learning algorithm. Explicit models of the opponents are learned as stationary distributions over their joint action space, which contains the probability the other players will select joint action based on past experience. These distributions combined with learned joint-action values from standard temporal differences are used to select an action. The algorithm has very similar behavior to fictitious play that requires observations of the opponents' actions, but not of their individual rewards. Additionally, its empirical distribution of play may converge to an equilibrium solution, but its action selection is deterministic and cannot play a mixed strategy.

2.2 Machine Learning: Algorithms and Applications

The concept of machine learning refers to the automated detection and extraction of meaningful patterns from large datasets, using statistical techniques [73]. In the smart grid, the bidirectional information flow between the electric utility and its customers, the increasing electricity supply from DERs, and the integration of advanced sensor and metering technologies makes it challenging for the traditional power system analysis, but ideal for the application of machine learning techniques. Based on the learning style, current machine learning techniques can be categorized into the following types:

- *Supervised Learning*: The goal is to develop a model to predict new examples in the test dataset through analyzing examples with known class labels in the training dataset. The derived model can be implemented for the smart grid data classification and regression such as in system monitoring and attack detection.

- *Unsupervised Learning*: The objective is to formulate a model to deduce structures and patterns presented in the training dataset with unlabeled examples. The application areas contain data clustering, dimensionality reduction, and association rule learning. One example is for grouping together data points with similar active/reactive power profiles for power transmission analysis.

- *Semi-Supervised Learning*: For the training dataset including a mixture of labeled and unlabeled examples, this learning algorithm intends to propose a model to learn the structures to organize the data as well as make predictions. The learning algorithms can also be implemented for the smart grid data classification and regression.

- *Reinforcement Learning*: This algorithm learns a policy/strategy of how to act given an observation of the system, wherein each action has an impact on the system, and the system provides feedback that guides the learning process.

In the following section, we briefly review the theoretic models of supervised, unsupervised, semi-supervised, and reinforcement learning. Moreover, we introduce several popular machine leaning algorithms in detail that help in the resilient smart grid design and deployment.

2.2.1 Supervised Learning

Supervised learning involves formulating a mapping between a set of input variables $\mathcal{X}$ and a set of output variables $\mathcal{Y}$, and applying this mapping to predict the outputs for unseen data [74]. Mathematically, the objective is to derive a function $f : \mathcal{X} \rightarrow \mathcal{Y}$ based on a training set $\mathcal{A}_n = \{(\boldsymbol{x}_1, y_1), ..., (\boldsymbol{x}_n, y_n)\}$, which is composed of pairs of input and output points $\boldsymbol{x}_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$. Typically, $\boldsymbol{x}_i \in \mathbb{R}^d$ and $y_i \in \mathbb{R}$. y_i is discrete for classification problems and continuous for regression problems. Let $\mathcal{H}$ denote the set of functions where the solution is sought: $f \in \mathcal{H}$. The supervised learning can be converted into an optimization problem to find the function $f \in \mathcal{H}$ that minimizes the error or loss between the prediction $f(\boldsymbol{x})$ and the desired output y, which is measured by a loss function $L(f(\boldsymbol{x}), y) : \mathcal{Y} \times \mathcal{Y} \rightarrow \mathbb{R}^+$.

In this section, we focus on kernel-based approaches to supervised learning. We first explore one of the simplest algorithms for data classification, termed the nearest neighbor algorithm [75]. We then review the support vector machine (SVM) algorithm which represents the dominant supervised learning technology used for the smart grid data processing, specially in the cyber attack detection. Finally, we discuss the ensemble technique, an important strategy for increasing the stability and accuracy of a classifier whereby a single classifier is replaced by a committee of classifiers.

Nearest Neighbor Algorithm

The nearest neighbor algorithm classifies the example in the test dataset by identifying its nearest neighbor and using this neighbor to determine the class of this example. Given two observations $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ in the training dataset $\mathcal{X}$, the distance between two can be defined as $D(\boldsymbol{x}_1, \boldsymbol{x}_2)$. Here, the function $D(\cdot)$ is defined as an Euclidean distance, where $D(\boldsymbol{x}_1, \boldsymbol{x}_2) = \sqrt{\sum_{i=1}^{d}(x_1^{(i)} - x_2^{(i)})^2}$. Given a test data example $\boldsymbol{x}_t$, the nearest neighbor classifier chooses the class corresponding to the data item in the training set with the shortest distance to the test example. Using the notation we established above, let i^* denote the index of the training example closest (i.e., with minimum distance) to the test example $\boldsymbol{x}_t$. Therefore, i^* can be derived through solving the following problem:

$$i^* = \arg\min_{i=1,\ldots,n} D(\boldsymbol{x}_t, \boldsymbol{x}_i). \tag{2.2}$$

After finding i^*, the nearest neighbor role would assign to the test example the label y_{i^*}, which is the label of the training example $\boldsymbol{x}_{i^*}$ that was closest to the test example $\boldsymbol{x}_t$. In [76], a k-Nearest Neighbor (kNN) algorithm was introduced as an extension of the nearest neighbor algorithm, where the class of the test data example $\boldsymbol{x}_t$ is determined by the majority of samples of the labels for k nearest neighbors.

Support Vector Machine (SVM) Algorithm

For binary classification, we try to formulate a function $f : \mathbb{R}^d \rightarrow \{\pm 1\}$ using the training set $\mathcal{A}_n = \{(\boldsymbol{x}_1, y_1), ..., (\boldsymbol{x}_n, y_n)\}$, where $\boldsymbol{x}_i \in \mathbb{R}^d$ and $y_i \in \{\pm 1\}$, such that f will correctly classify the test data example $\boldsymbol{x}_t$. Assume that the training set $\mathcal{A}_n$ is linearly separable, the linear SVM algorithm [77] is designed based on the class of hyperplanes: $< \boldsymbol{w}, \boldsymbol{x} > +b$ with $y_i(< \boldsymbol{w}, \boldsymbol{x}_i > +b) > 0, \forall i = 1, ..., n$. Therefore, the decision function can be expressed as $f_d(\boldsymbol{x}) = \text{sign}(< \boldsymbol{w}, \boldsymbol{x} > +b)$ with

$$f_d(\boldsymbol{x}_i) = \text{sign}(y_i), i = 1, ..., n. \tag{2.3}$$

The SVM classification method aims at finding the optimal hyperplane based on the maximization of the margin between the training data for both classes. Because the distance between a point $\boldsymbol{x}$ and the hyperplane is $\frac{yf(\boldsymbol{x})}{\|\boldsymbol{w}\|}$, it is easy to show that the optimization problem may be expressed as the following minimization:

$$\begin{aligned} &\min \frac{1}{2}\|\boldsymbol{w}\|^2 \\ &s.t.\ y_i f(\boldsymbol{x}_i) \geq 1, i = 1, ..., n. \end{aligned} \tag{2.4}$$

The support vectors are the training points for which we have an equality in (2.4). They are all equally close to the optimal hyperplane. In the real world, the training data is usually far from linear and the datasets are inseparable. Thus, the nonlinear SVM classifiers were created by applying the kernel trick to maximum-margin hyperplanes in [78].

Ensemble Techniques

Given a set $\mathcal{X} = \{\boldsymbol{x}_1, ..., \boldsymbol{x}_n\}$ of training examples, an ordinary machine learning algorithm outputs a classifier, which is an hypothesis about the true classification function f. The ensemble technique [79] aims to construct a set of classifiers to solve the same classification problem. In particular, an ensemble classifier is implemented to classify $\mathcal{X}$ into -1 and $+1$, in which P subsets of tuples of size $m(< n)$ are created by uniformly sampling from $\mathcal{X}$ with replacement. Therefore, P subsets $\{\mathcal{X}_1, ..., \mathcal{X}_P\}$ are generated, and P classifiers $\{\mathcal{C}_1, ..., \mathcal{C}_P\}$ are built on each subset $\mathcal{X}_i$, $i = 1, .., P$. A final ensemble classifier classifies a test example $\boldsymbol{x}_t$ by giving as output the class predicted most often by $\{\mathcal{C}_1, ..., \mathcal{C}_P\}$. The main discovery is that ensembles are often much more accurate than the individual classifiers that make them up. In addition, the ensemble classifier can be implemented for the parallel computing, in which each subset $\mathcal{X}_i$ resides on a different processor within the parallel computer.

2.2.2 Unsupervised Learning

In unsupervised learning, the machine simply receives the set of training examples $\mathcal{X} = \{\boldsymbol{x}_1, ..., \boldsymbol{x}_n\}$ without supervised target outputs. The goal of unsupervised learning is to build representations of the training examples that can be used for decision making, forecasting future inputs, and efficiently transferring the training dataset to another machine. Therefore, unsupervised learning can be defined as a way to find patterns in the unlabeled dataset. Two popular algorithms of unsupervised learning are Principal Component Analysis (PCA) and data clustering. PCA is a a dimension-reduction tool that can extract the most informational representations or features with a low dimension from a large dataset [80]. Data clustering represents a broad class of methods, such as K-means clustering and hierarchical clustering, for dividing the training examples into groups (clusters) that are meaningful and useful [81].

2.2.3 Semi-supervised Learning

Semi-supervised learning is halfway between supervised and unsupervised learning, where the learning algorithm is provided with both labeled and unlabeled training data [82]. Therefore, the training dataset $\mathcal{X} = \{\boldsymbol{x}_1, ..., \boldsymbol{x}_n\}$ can be divided into two parts: the points $\mathcal{X}_l = \{\boldsymbol{x}_1, ..., \boldsymbol{x}_l\}$, for which labels $\mathcal{Y}_l = \{y_1, ..., y_l\}$ are provided, and the points $\mathcal{X}_u = \{\boldsymbol{x}_1, ..., \boldsymbol{x}_u\}$, the labels of which are not known. Semi-supervised learning addresses the problem that the supervised learning cannot integrate part or all of the available unlabeled data in its learning algorithms. The goal of semi-supervised learning is to maximize the learning performance by combining both labeled and unlabeled data, and develop learning algorithms to take advantage of such a combination. There are some popular semi-supervised learning models, such as self-training, mixture models, co-training and multiview learning, graph-based methods, and semi-supervised support vector machines [83].

2.2.4 Reinforcement Learning

The intrinsic nature of Reinforcement Learning (RL) is learning through interactions, where a machine interacts with its environment by producing a policy π [84]. The derived policy affects the state of the environment, which in turn results in the machine receiving some scalar rewards or losses. The goal of the machine is to find an optimal policy π^* that maximizes/minimizes the total expected rewards/losses over its lifetime, termed the discounted reward/loss. RL is closely related to the field of decision theory, especially the Markov Decision Process (MDP). The MDP is comprised of four main characteristics including: (1) state, (2) policy, (3) transition between states, and (4) reward function. The dynamic programming is a class of algorithms that is able to compute optimal policies in the presence of a perfect model of MDP [85]. Moreover, RL is closely related to game theory, where the machine interacts with some other machines which can also make actions, receive rewards/losses, and learn. Therefore, the goal of the machine is to derive an optimal policy so as to maximize/minimize its rewards/losses based on the other machines' current and future actions.

CHAPTER 3

Hybrid Model for Power Distribution Reliability Forecasting

This chapter proposes a hybrid framework integrating Multilayer Perceptrons (MLPs) and parametric regression models for forecasting the daily numbers of power interruptions in smart grid distribution networks using time series of common weather data. Section 3.1 formally defines the reliability problem and provides a basic introduction to the existing literature. Section 3.2 introduces the reliability metrics and weather parameters collected for analysis. Section 3.3 develops the parametric regression models between the reliability metrics and various weather parameters. Section 3.4 formulates a MLP model for forecasting the daily numbers of power interruptions and introduces a modified Extreme Learning Machine (ELM) based algorithm for training the formulated model. In Section 3.5, the proposed framework is evaluated, and the sensitivity of each weather parameter is analyzed. Section 3.6 concludes the chapter and outlines the future work.

3.1 Overview

The reliability has always been a critical focus area for the design and operation of the electric power grid, where the distribution networks account for up to 90% of all customer reliability problems [86, 87]. Improving the distribution reliability is a key point for increasing customer satisfaction and system performance. However, with the high penetration of renewable resources and increasing electricity demands in distribution networks, meeting reliability objectives in modern grids becomes increasingly challenging [88–91]. According to the Lawrence Berkeley National Laboratory's (LBNL) report in 2016 [5,6], the annual cost for power interruptions to the electricity customers of the United States is estimated to be $110 billions, which increases more than 30% since 2004.

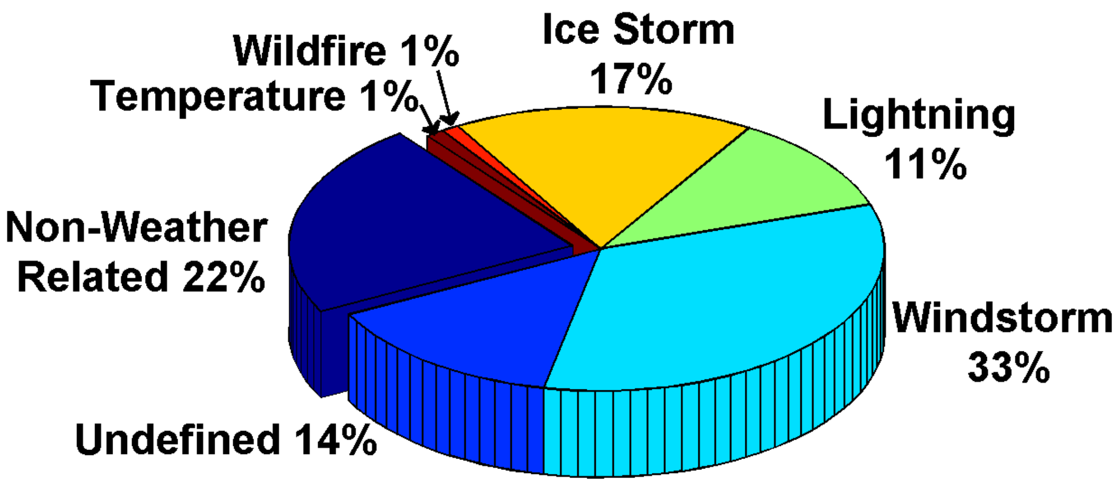


Figure 3.1: The distribution of causes for power interruptions in distribution networks: 178 million customers collected from 1992 to 2011 in the United States.

The power interruptions in distribution networks can be caused by a wide range of factors including equipment failures, animals, trees, and human errors [7, 8]. However, weather conditions, such as windstorm, lightning, ice storm, and high temperature, are usually the important causes of the distribution power interruptions [9–11]. According to the reliability data collected by the United States Department of Energy (DOE) [14] from 1992 to 2011, weather conditions contribute more than 64% of the total number of distribution power interruptions as shown in Figure 3.1. As a result, the accurate reliability forecasting based on time series of weather condition data is both challenging and desirable for the smart grid distribution system design and operation.

In the last decades, a wealth of researchers have investigated the effect of extreme weather conditions, such as floods, hurricanes, and ice storms, on the electric grid reliability performance [20–24]. In [20], a three-state weather model was formulated for the predictive reliability assessment of the electric distribution systems, where the system failure rate was analyzed based on extreme weather conditions. The potential effects of extreme weather conditions and climate changes on power system components operation and reliability were reviewed in [21], and the mitigation framework was outlined for boosting the resilience of electrical networks. In [22], a mathematical framework was presented to assess the risk of extreme weather cases on the power systems, in which the performances of system protection devices were evaluated under extreme events. Additionally, a risk-based defensive islanding algorithm was proposed in [23] for boosting the power grid resilience to extreme weather events. However, all of these works only consider extreme weather conditions. Although severe weather events can cause large amounts of power interruptions, it is not common to consider these events under normal operation conditions and the major of electric customers' interruptions happen under normal weather conditions.

Recently, statistical analysis techniques were introduced in [27, 28] to analyze the relationship between the number of power interruptions on electric distribution networks and common weather parameters, such as temperature, wind, air pressure, and lightning. The number of power interruptions was predicted based on the total sum of the statistical model of each weather parameter. However, the power interruptions related with common weather conditions are essentially the result of combined action of many factors. The power interruption prediction only based on statistical models might be compromising due to the various effects of different weather parameters.

This chapter presents a hybrid framework integrating Multilayer Perceptrons (MLPs) and parametric regression models is for forecasting the daily numbers of power interruptions in smart grid distribution networks using time series of common weather data. The main contributions of this chapter contain:

1. Both polynomial and exponential regression models are implemented to analyze nonlinear relationship between power interruptions and common weather parameters;

2. Derived regression models are integrated as inputs to formulate a MLP neural network to predict the number of power interruptions instead of directly summing together;
3. A modified Extreme Learning Machine (ELM) based algorithm is proposed for training the formulated MLP model using real-time monitored power interruptions data from an electric utility in Florida and common weather data from National Climatic Data Center (NCDC);
4. Sensitivity analysis is implemented to analyze the various impacts of different common weather parameters on the number of power interruptions.

3.2 Reliability and Weather Data Collection

In order to analyze the impacts of common weather conditions on the reliability performances of the smart grid distribution networks, a series of reliability metrics are collected from an electric utility in the United States, serving approximately 10 million people across nearly half of the state of Florida. The reliability metrics collected from the electric utility are comprised of the daily numbers of *sustained interruption* (N), *momentary interruption* (M), *System Average Interruption Duration Index* (SAIDI), *System Average Interruption Frequency Index* (SAIFI), *Momentary Average Interruption Frequency Index* (MAIFI), and *Customer Momentary Experience* (CME). The numbers of N and M play a key point in reliability analysis, and other reliability metrics can be calculated based on these values [92]. Therefore, N and M in one utility management area are selected for reliability analysis in this chapter, and a sample of the daily numbers of N and M is shown in Figure 3.2.

Weather data is mostly collected from NCDC, which provides monthly, daily, and even hourly normal weather data summaries. In addition, a source of weather data like

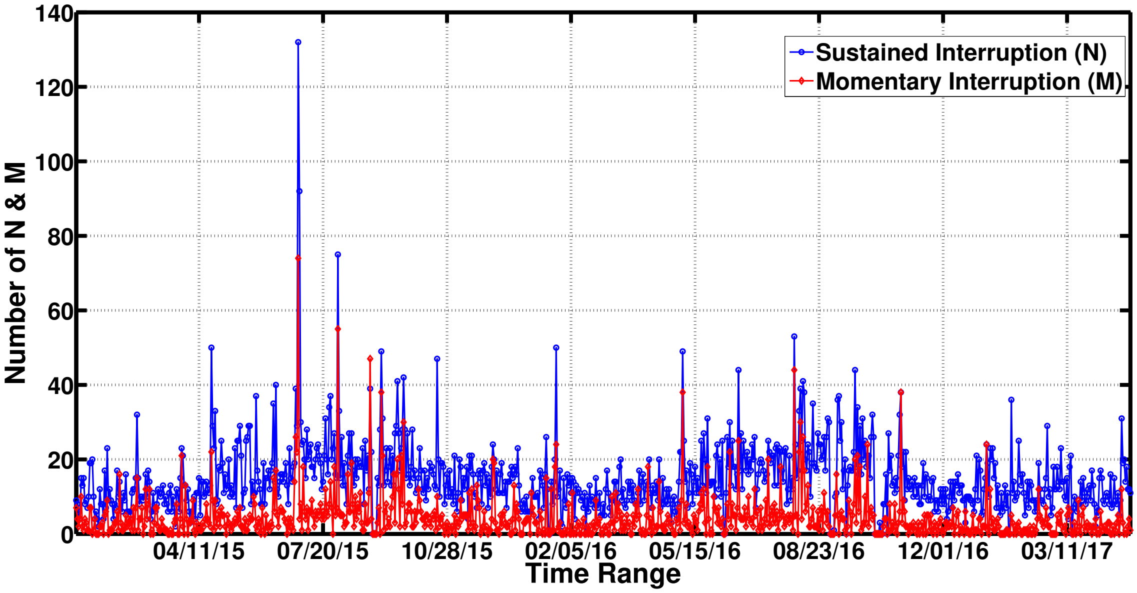


Figure 3.2: Daily numbers of N and M collected from Jan. 1st 2015 to Apr. 30th 2017 in one utility management area.

lightning is provided by the control center of the electric utility, which installs its own weather stations centrally located in various management areas. The selected weather characteristics for analysis contain *temperature*, *precipitation*, *air pressure*, *wind speed*, and *lightning*. All of these data are collected and preprocessed for each utility management area in order to analyze their relationship with the daily numbers of N and M.

The power interruption data can be classified into interruptions with exclusion data and without exclusion data for an entire day. In order to analyze the combined effect of common weather conditions on the system reliability performance, the daily numbers of N and M are selected without exclusion data to avoid extreme events. On the other hand, the weather data is collected hourly to model the data more precisely and improve the location of the weather source. In the following section, the preprocessed power interruptions and weather data will be used for formulating the parametric models to evaluate the effect of each weather parameter on the daily numbers of N and M.

3.3 Parametric Regression Models between Reliability and Weather

In this section, *parametric regression analysis* is introduced to analyze the nonlinear relationship between the number of sustained interruptions and each common weather parameter in one distribution management area. Similarly, the regression analysis can be expanded for the number of momentary interruptions.

For each utility management area, assume that $\boldsymbol{N}$ is the vector of the daily sustained interruptions in one time period, and $\boldsymbol{x}$ is a common weather parameter vector in corresponding time series, the relationship between the two can be represented as: $\boldsymbol{N} = f(\boldsymbol{x}, \boldsymbol{\beta}) + \boldsymbol{\varepsilon}$, where $f(\cdot)$ is the relationship function; $\boldsymbol{\beta}$ is the vector of estimation parameters; and $\boldsymbol{\varepsilon}$ are the unobserved random error satisfying $\varepsilon \sim N(0, \delta^2)$, where δ is the standard deviation. Two most popular regression models can be implemented for this analysis including polynomial and exponential regression. For polynomial regression with the n-th degree, the relationship function can be defined as:

$$f(\boldsymbol{x}, \boldsymbol{\beta}^{\text{pol}}) = \beta_0^{\text{pol}} + \beta_1^{\text{pol}}\boldsymbol{x} + \beta_2^{\text{pol}}\boldsymbol{x}^2 + \cdots + \beta_n^{\text{pol}}\boldsymbol{x}^n. \tag{3.1}$$

Correspondingly, for two-term exponential regression, the relationship function can be determined by:

$$f(\boldsymbol{x}, \boldsymbol{\beta}^{\text{ex}}) = \beta_0^{\text{ex}} + \beta_1^{\text{ex}} \exp(\beta_2^{\text{ex}}\boldsymbol{x}) + \beta_3^{\text{ex}} \exp(\beta_4^{\text{ex}}\boldsymbol{x}). \tag{3.2}$$

Commonly, based on the known samples $(\boldsymbol{N}_k, \boldsymbol{x}_k)$, $k = 1, ..., N_{\text{total}}$, the least square method [93] can be adopted to estimate $\boldsymbol{\beta}$, and the estimation can be expressed by:

$$\sum_{k=1}^{N_{\text{total}}}(\boldsymbol{N} - f(\boldsymbol{x}, \hat{\boldsymbol{\beta}})) = \min_{\boldsymbol{\beta}} \sum_{k=1}^{N_{\text{total}}}(\boldsymbol{N}_k - f(\boldsymbol{x}_k, \boldsymbol{\beta})), \tag{3.3}$$

where $\hat{\boldsymbol{\beta}}$ is the estimation of $\boldsymbol{\beta}$. The goodness-of-fit of polynomial regression with the n-th degree, $n = 1, 2, 3$, and two-term exponential regression for each common weather parameter including *temperature*, *precipitation*, *air pressure*, *wind speed*, and *lightning*

Table 3.1: Goodness-of-Fit of Regression Models for Each Weather Parameter

Weather Parameter	**Performance**	**Polynomial** (1)	**Polynomial** (2)	**Polynomial** (3)	**Exponential** (2)
Maximum Temperature	SSE	7.13E+04	6.68E+04	6.63E+04	7.42E+04
	R-square	0.09367	0.1517	0.1574	0.05683
	Adjusted R-square	0.0926	0.1497	0.1544	0.05349
	RMSE	9.171	8.877	8.853	9.366
Minimum Temperature	SSE	7.47E+04	7.39E+04	7.33E+04	7.38E+04
	R-square	0.05044	0.06093	0.06798	0.06238
	Adjusted R-square	0.04932	0.05872	0.06467	0.05906
	RMSE	9.387	9.34	9.311	9.338
Average Temperature	SSE	7.30E+04	7.06E+04	7.05E+04	7.06E+04
	R-square	0.07222	0.1031	0.104	0.1028
	Adjusted R-square	0.07113	0.101	0.1008	0.09958
	RMSE	9.278	9.128	9.129	9.135
Heat Days	SSE	7.87E+04	7.85E+04	7.85E+04	7.83E+04
	R-square	0.0002128	0.002496	0.002849	0.005259
	Adjusted R-square	-0.0009662	0.0001408	-0.0006875	0.001732
	RMSE	9.632	9.626	9.63	9.619
Cool Days	SSE	7.22E+04	7.08E+04	7.08E+04	7.08E+04
	R-square	0.08255	0.1006	0.1006	0.1006
	Adjusted R-square	0.08147	0.09848	0.09848	0.09848
	RMSE	9.227	9.141	9.141	9.141
Precipitation	SSE	6.69E+04	6.61E+04	6.49E+04	6.43E+04
	R-square	0.08588	0.0963	0.1133	0.1212
	Adjusted R-square	0.08462	0.09381	0.1096	0.1175
	RMSE	9.596	9.547	9.464	9.422
Air Pressure	SSE	7.71E+04	7.66E+04	7.57E+04	7.60E+04
	R-square	0.02001	0.02647	0.03759	0.03367
	Adjusted R-square	0.01886	0.02417	0.03417	0.03024
	RMSE	9.536	9.51	9.461	9.48
Average Wind Speed	SSE	7.62E+04	7.51E+04	7.49E+04	7.48E+04
	R-square	0.03019	0.04404	0.04623	0.04843
	Adjusted R-square	0.02904	0.04177	0.04282	0.04504
	RMSE	9.506	9.444	9.438	9.427
Peak Wind Speed	SSE	7.71E+04	7.66E+04	7.61E+04	7.44E+04
	R-square	0.01996	0.02649	0.03265	0.05445
	Adjusted R-square	0.0188	0.02418	0.02921	0.05108
	RMSE	9.551	9.525	9.501	9.393
Sustainable Wind Speed	SSE	7.77E+04	7.76E+04	7.72E+04	7.74E+04
	R-square	0.01321	0.01411	0.01847	0.01641
	Adjusted R-square	0.01205	0.01178	0.01499	0.01293
	RMSE	9.569	9.57	9.555	9.565
Lightning	SSE	6.60E+04	6.31E+04	6.26E+04	6.35E+04
	R-square	0.1609	0.1987	0.2041	0.1937
	Adjusted R-square	0.16	0.1968	0.2013	0.1908
	RMSE	8.824	8.628	8.604	8.66
Remarks:	**SSE** measures the total deviation of the predicted values from the fit to the observed values. **R-square** is the square of the correlation between the response values and predicted response. **Adjusted R-square** is a modified R-squared that has been adjusted for the number of predictors. **RMSE** is the estimate of the standard deviation of the random component in the data.				

is shown in Table 3.1, where each regression model performance is evaluated through the error metrics including *Sum of Squares Due to Error* (SSE), *R-square*, *Degrees of Freedom Adjusted R-Square*, and *Root Mean Squared Error* (RMSE) defined:

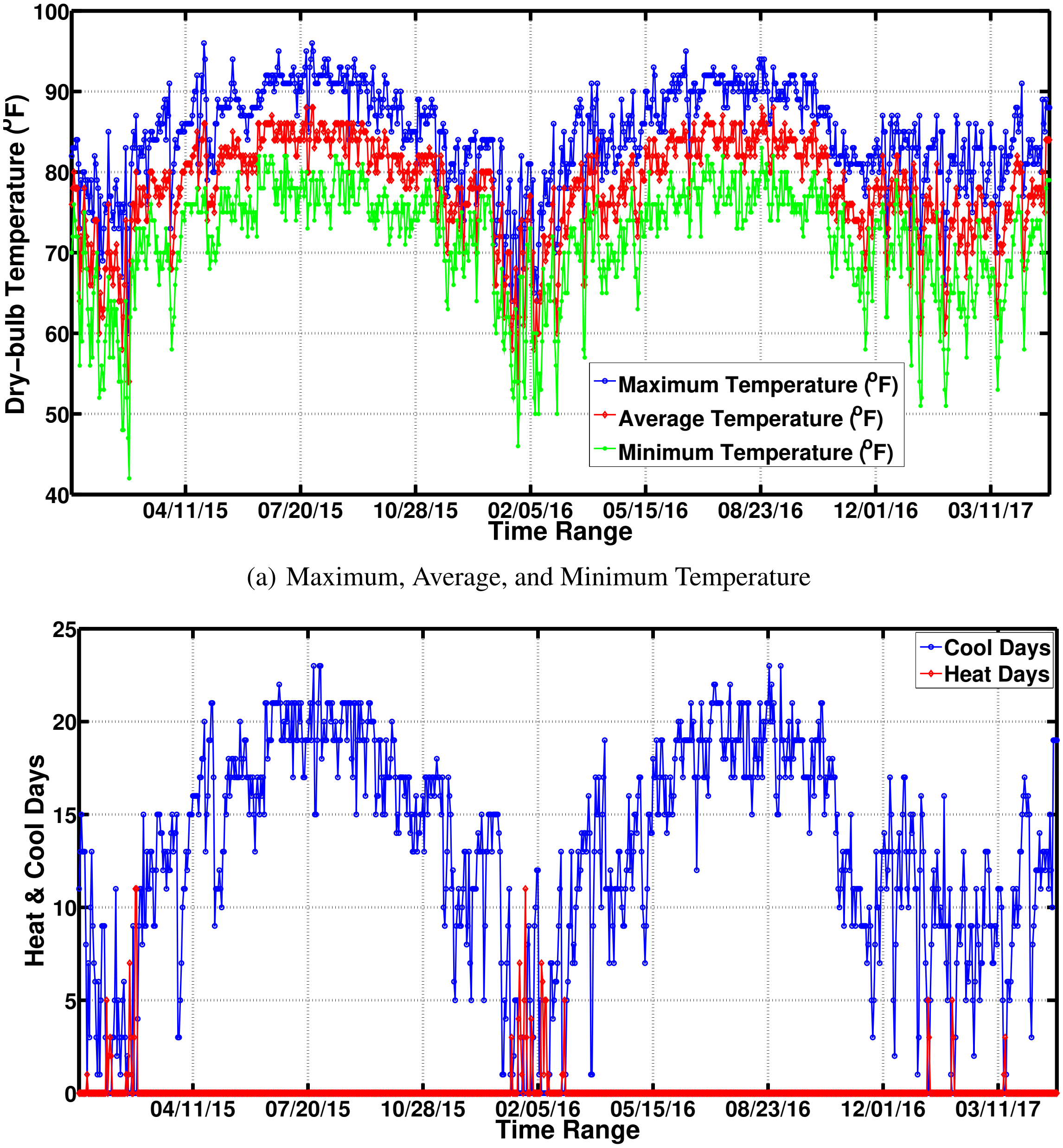
- **SSE** $= \sum_{k=1}^{\boldsymbol{N}_{\text{total}}} \boldsymbol{w}_k(\boldsymbol{x}_k - \boldsymbol{f}_k)^2$ measures the total deviation of the original values from the regression fit, where $\boldsymbol{f}_k$ is the predicted value derived by the regression model, and $\boldsymbol{w}_k$ is the weighting applied to each data point. SSE closer to 0 indicates that the regression model has a smaller fitting error, which is more useful for prediction.
- **R-square** $= 1 - \frac{[\sum_{k=1}^{\boldsymbol{N}_{\text{total}}} \boldsymbol{w}_k(\boldsymbol{x}_k - f_k)^2]}{[\sum_{k=1}^{\boldsymbol{N}_{\text{total}}} w_k(\boldsymbol{x}_k - \boldsymbol{x}_{\text{av}})^2]}$ denotes the square of the correlation between the original and predicted values, where $\boldsymbol{x}_{av}$ is the mean of the original data. R-square has the unit interval $[0, 1]$, where a value closer to 1 represents that a greater proportion of variance is accounted by the regression model.
- **Adjusted R-square** $= 1 - \frac{[\sum_{k=1}^{\boldsymbol{N}_{\text{total}}} \boldsymbol{w}_k(\boldsymbol{x}_k - \boldsymbol{f}_k)^2](\boldsymbol{N}_{\text{total}} - 1)}{[\sum_{k=1}^{\boldsymbol{N}_{\text{total}}} \boldsymbol{w}_k(\boldsymbol{x}_k - \boldsymbol{x}_{\text{av}})^2](v)}$ is a modified type of R-square, where the residual degrees of freedom v is determined by $\boldsymbol{N}_{\text{total}}$ minus the number of fitted coefficients. The adjusted R-square statistic can take on any value less than or equal to 1, where a value closer to 1 implies a better regression fitting.
- **RMSE** $=\sqrt{SSE/v}$ is correlated with the fit standard error and the standard error of the regression model, which is an estimate of the standard deviation of the random component in the data. Similar with SSE, a RMSE value closer to 0 indicates that the regression model is more useful for prediction.

In the subsequent subsections, the regression models between $\boldsymbol{N}$ and various weather parameters are detailed described.

3.3.1 Temperature

Temperature is an important weather parameter impacting on the reliability performance of smart grid distribution networks. An increase of the power interruptions can be caused at relatively low or high temperatures, since the electricity demand will increase due to the heating/cooling requirements of customers. Moreover, high air temperatures may strain power infrastructure devices and reduce transmission capacity [94]. In order to achieve the relationship between temperature and $\boldsymbol{N}$, a series of temperature characteristics including dry-bulb maximum temperature T_{max}, average temperature T_{ave}, minimum temperature T_{min}, heat days H, and cool days C are selected.

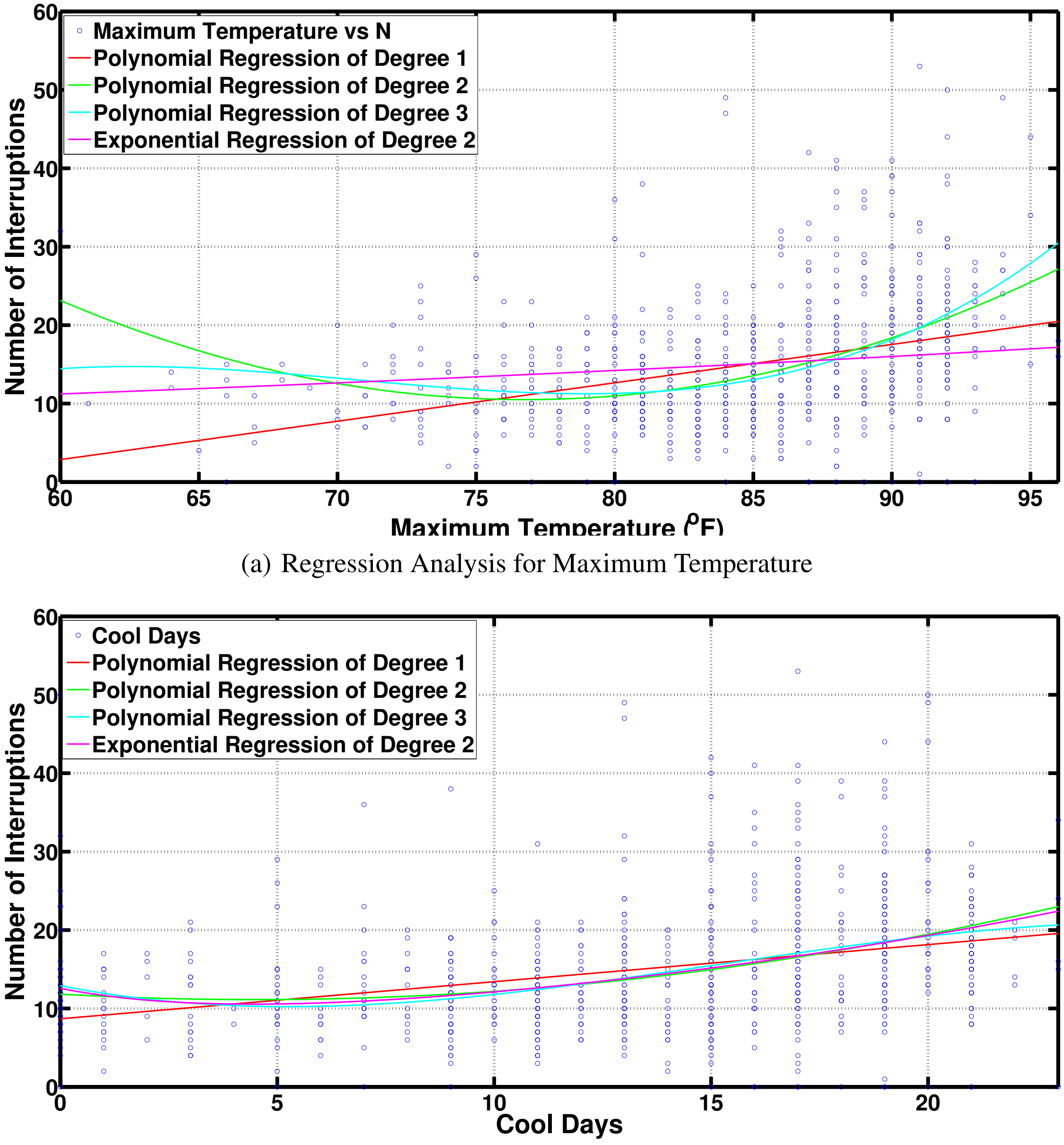
For one utility management area, Figure 3.3(a) shows the variations of T_{max}, T_{ave}, and T_{min}, and Figure 3.3(b) displays the variations of H and C. Polynomial regression with the n-th degree, $n = 1, 2, 3$, and two-term exponential regression are implemented for analyzing the relationship between each temperature characteristic and $\boldsymbol{N}$. Based on the goodness-of-fit results in Table 3.1, for T_{max}, T_{ave}, and T_{min}, polynomial regression with 3-th degree has a better performance with less SSE and RMSE, and greater R-square. Exponential regression with 2 terms has a better performance for H, while, for C, polynomial regression with 2-rd and 3-th degree and exponential regression with 2 terms have similar performances in modeling fitting. Figure 3.4(a) and (b) present the polynomial and exponential regression models adapted for analyzing T_{max} and C, respectively. The relationship function between $N_{T_{\text{max}}}$ and T_{max} can be expressed as: $N_{T_{\text{max}}} = \beta_0^{T_{\text{max}}} + \beta_1^{T_{\text{max}}} T_{\text{max}} + \beta_2^{T_{\text{max}}} {T_{\text{max}}}^2 + \beta_3^{T_{\text{max}}} {T_{\text{max}}}^3$. Correspondingly, the relationship function between N_C and C can be determined by: $N_C = \beta_0^C + \beta_1^C \exp(\beta_2^C C) + \beta_3^C \exp(\beta_4^C C)$.



(a) Maximum, Average, and Minimum Temperature

(b) Heat and Cool Days

Figure 3.3: The collected temperature data including maximum temperature, average temperature, minimum temperature, heat days, and cool days.



(a) Regression Analysis for Maximum Temperature

(b) Regression Analysis for Cool Days

Figure 3.4: The polynomial and exponential regression for analyzing: (a) the number of $N_{T_{\max}}$ respond to maximum temperature $T_{\max}$, (b) the number of N_C respond to cool days C.

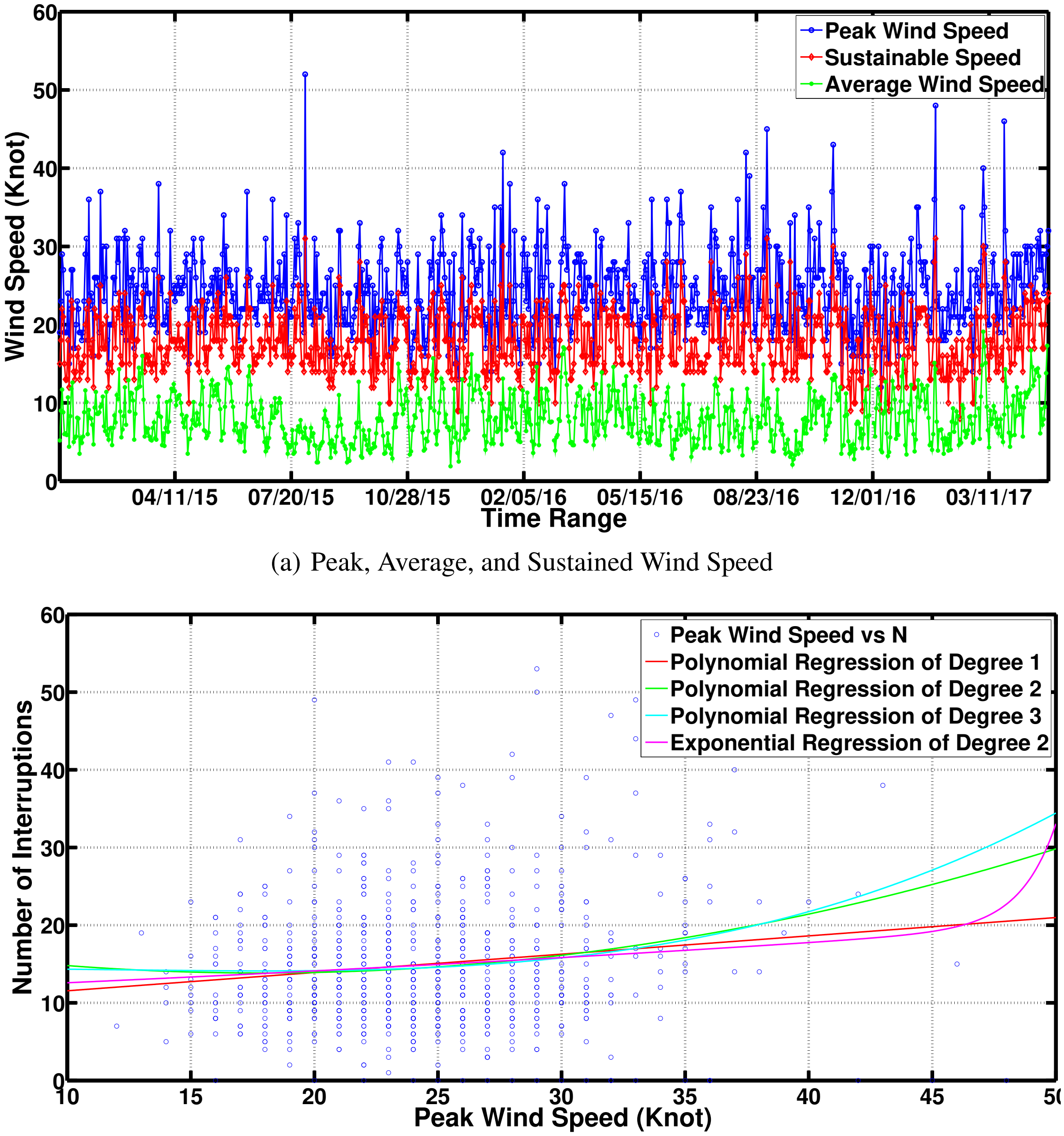
3.3.2 Wind Speed

Wind also plays a key role in the reliability analysis of smart grid distribution networks. The power of wind is directly proportional to the cube of the wind speed. If the wind reaches high speeds, it can cause damages to distribution networks such as entire trees blowing over into power lines, which results in broken conductors, broken crossarms, broken insulators, broken poles, and leaning poles [95]. There are three factors which attribute to the severity of wind speeds: peak wind speed W_{p}, average wind speed W_{a}, and sustained wind speed W_{s}.

Figure 3.5(a) plots the variation of W_{p}, W_{a}, and W_{s} for one utility management area, and Figure 3.5(b) shows the polynomial and exponential regression models fitted for analyzing the number of $N_{W_{\text{p}}}$ corresponding to W_{pea}. Based on the goodness-of-fit results in Table 3.1, exponential regression with 2 terms has a better performance for W_{p} and W_{a}, while W_{s} has a better performance in polynomial regression with 3-th degree. The relationship function modeling of the effect of W_{p} on $N_{W_{\text{p}}}$ can be defined as: $N_{W_{\text{p}}} = \beta_0^{W_{\text{p}}} + \beta_1^{W_{\text{p}}} \exp(\beta_2^{W_{\text{p}}} W_{\text{p}}) + \beta_3^{W_{\text{p}}} \exp(\beta_4^{W_{\text{p}}} W_{\text{p}})$.

3.3.3 Precipitation

Precipitation is any product of the condensation of atmospheric water vapor that falls under gravity, and two main forms of precipitation contain rain P_{rain} and snow P_{snow}. When raining density is large, formerly underground cables, vaults, and manholes may be exposed. Additionally, many power infrastructure equipments may not be sufficient to cater for heavy rain conditions, especially at ultra-high voltage [96]. On the other hand, snow occurs when supercooled rain freezes on contact with tree branches and overhead conductors. Ice buildup on conductors places a heavy physical load on the conductors, which increases the cross-sectional area exposed to the wind [97]. Since little snow falls



(a) Peak, Average, and Sustained Wind Speed

(b) Regression Analysis for Peak Wind Speed

Figure 3.5: (a) Peak wind speed W_p, average wind speed W_a, and sustained wind speed W_s. (b) The polynomial and exponential regression for analyzing the number of N_{W_p} respond to peak wind speed W_p.

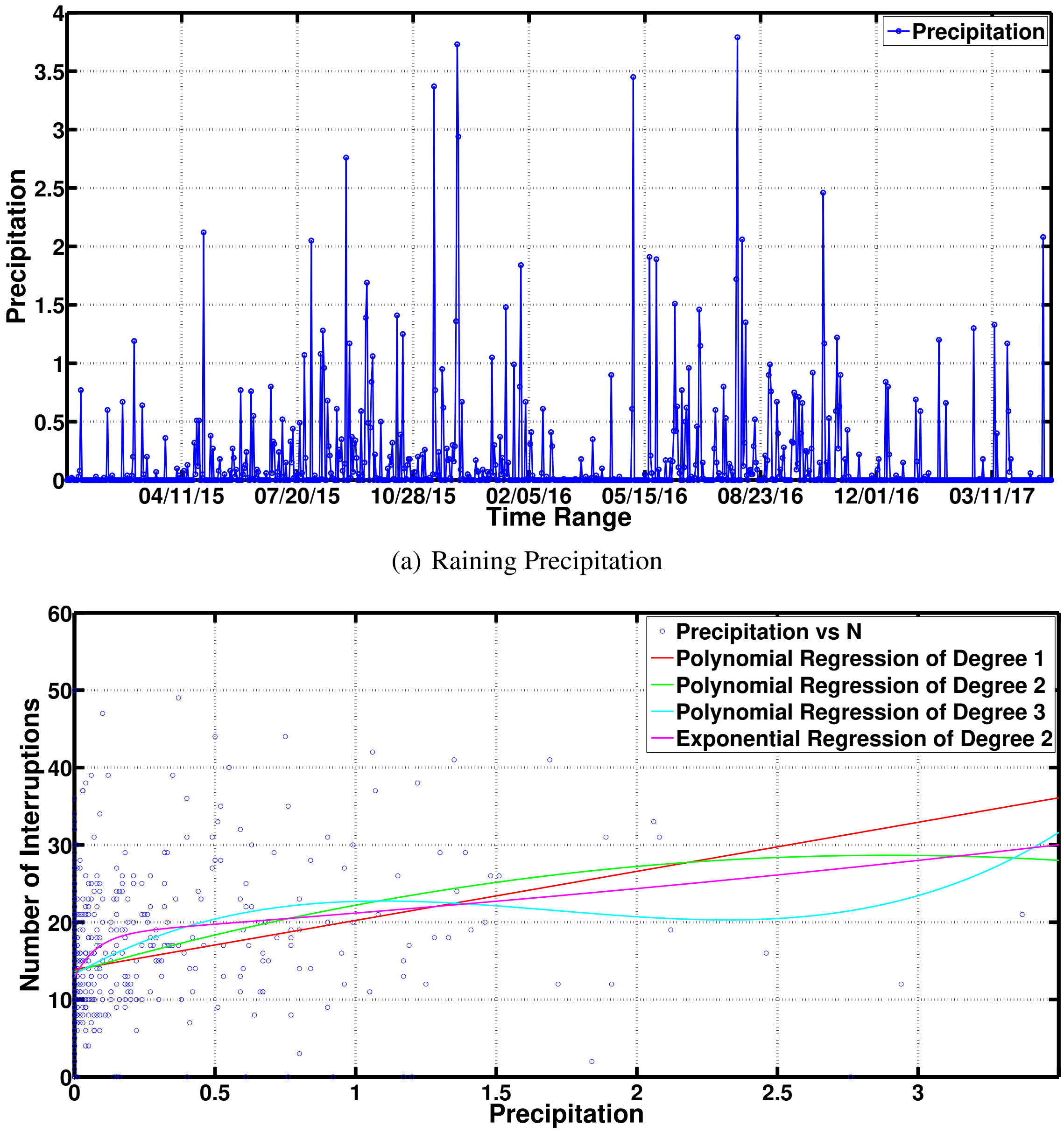
in Florida, the correlation of raining P_{rain} to $N_{P_{\text{ra}}}$ is evaluated in this chapter through polynomial and exponential regression models. As shown in Table 3.1, exponential regression with 2 terms has a better performance with less SSE and RMSE, and greater R-square for P_{rain}. For this purpose, the following equation is developed for modeling the effect of P_{rain} on $N_{P_{\text{ra}}}$: $N_{P_{\text{ra}}} = \beta_0^{\text{ra}} + \beta_1^{\text{ra}} \exp(\beta_2^{\text{ra}} P_{\text{rain}}) + \beta_3^{\text{ra}} \exp(\beta_4^{\text{ra}} P_{\text{rain}})$. Figure 3.6(a) plots the variation of raining precipitation P_{rain} for one utility management area, and Figure 3.6(b) shows the polynomial and exponential regression fittings adapted for analyzing the relationship between P_{rain} and $N_{P_{\text{ra}}}$.

3.3.4 Air Pressure

Air pressure is the pressure within the atmosphere of Earth, which is highly connected with other weather parameters, such as raining, heat storm, and wind speed. The variation of air pressure A for one utility management area is plotted in Figure 3.7(a). The relationship between air pressure A and N_A is analyzed by both polynomial and exponential regression models as shown in Figure 3.7(b). Polynomial regression with 3-th degree has a better performance for A with less SSE and RMSE, and greater R-square according to Table 3.1. Therefore, the relationship function between N_A and A can be expressed as: $N_A = \beta_0^A + \beta_1^A A + \beta_2^A A^2 + \beta_3^A A^3$.

3.3.5 Lightning

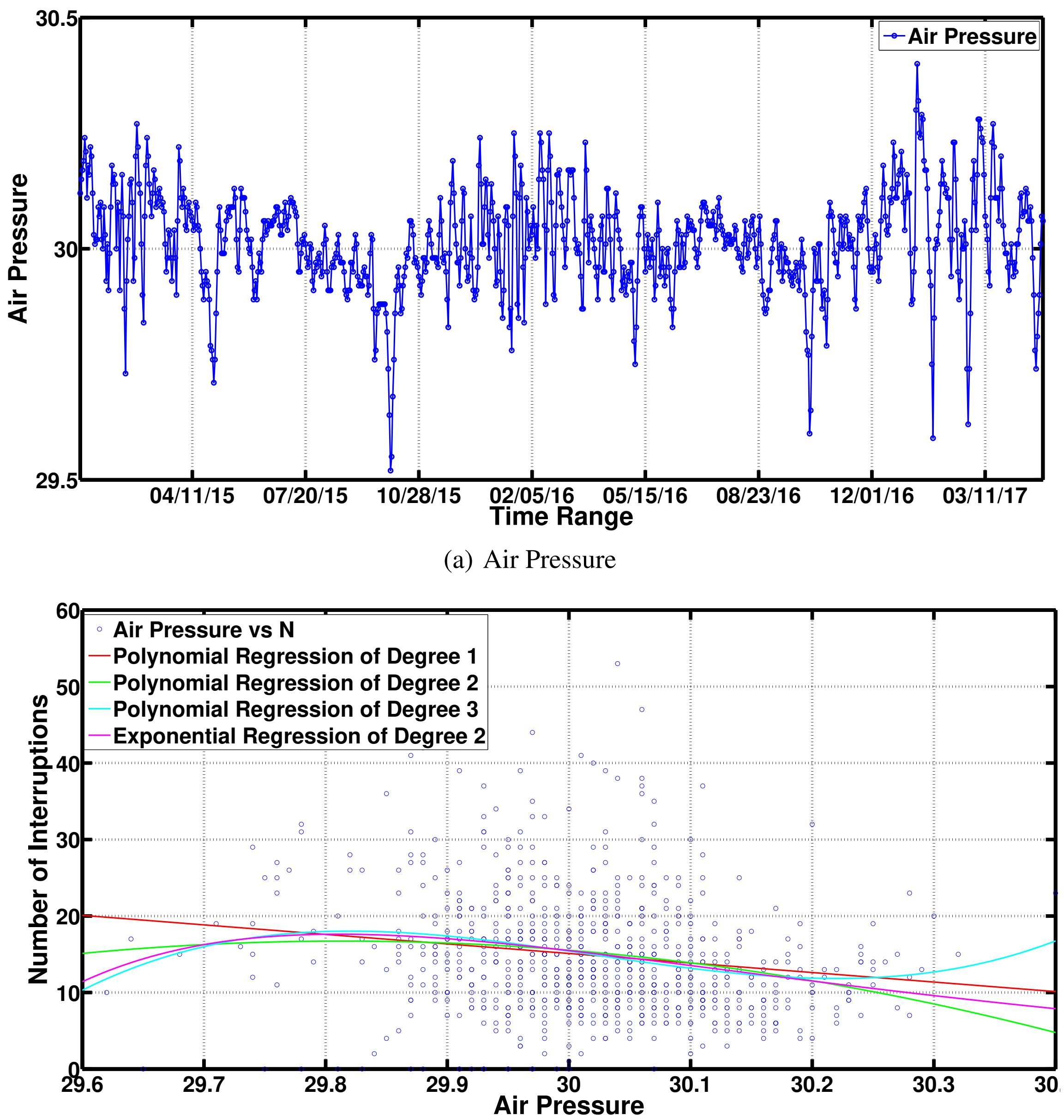
Highly-scaled electrical discharges between the cloud and a piece of earth are called lightning strikes L. This natural phenomenon may strike the phase conductors, the tower or shield wires causing backflash, and a piece of nearby ground generating transient overvoltage. The energy of the lightning flash may exceed the thermal limit of the struck object causing thermal failure [98]. In addition, the combined effects of strong winds and rain



(a) Raining Precipitation

(b) Regression Analysis for Raining Precipitation

Figure 3.6: (a) Raining precipitation P_{rain}. (b) The polynomial and exponential regression for analyzing the number of $N_{P_{\text{ra}}}$ respond to raining precipitation P_{rain}.



(a) Air Pressure

(b) Regression Analysis for Air Pressure

Figure 3.7: (a) Air pressure A. (b) The polynomial and exponential regression for analyzing the number of N_A respond to air pressure A.

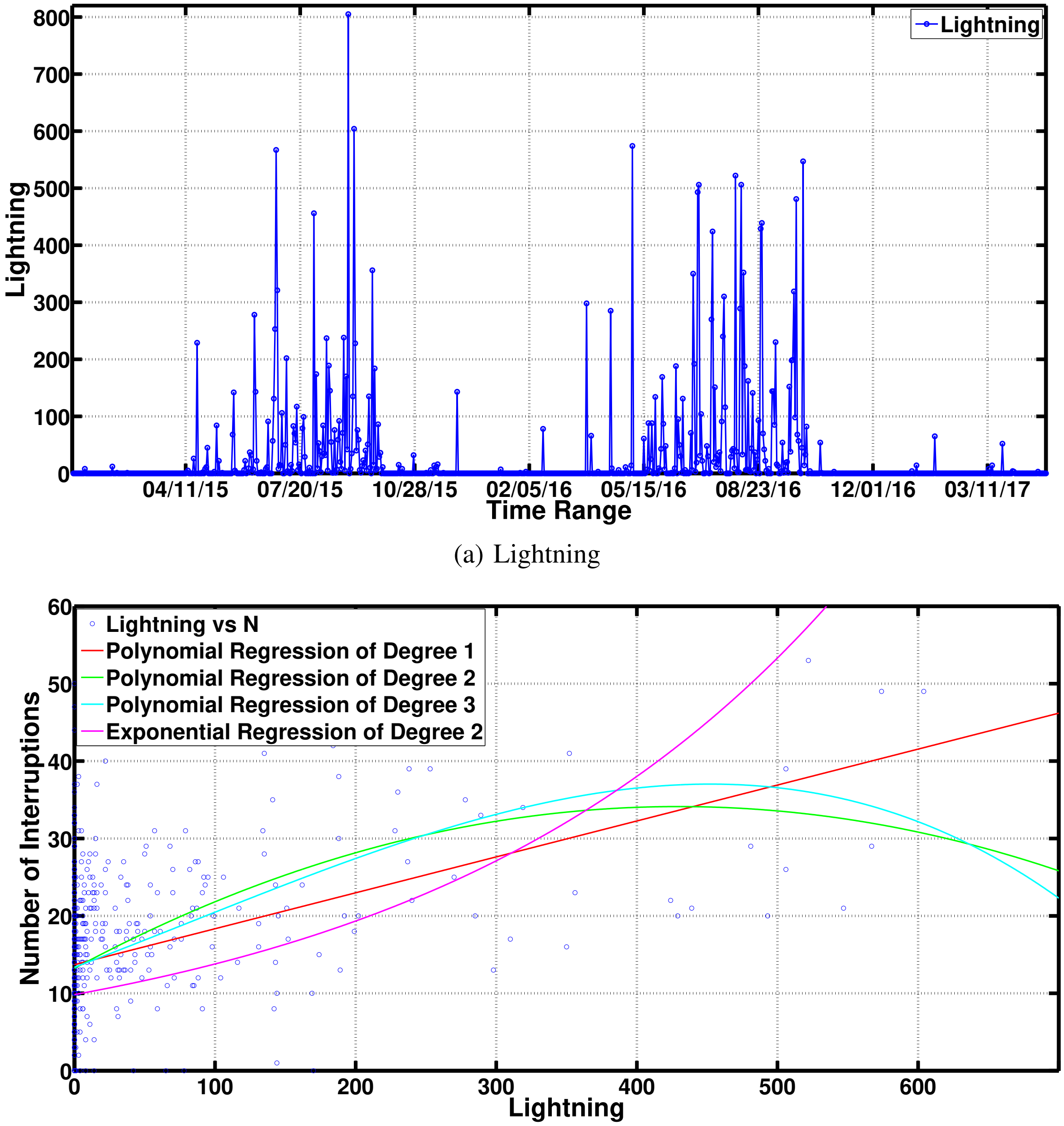
are generally accompanied with L, Thus, L can have a random, though important, effect on the numbers of N_L in distribution networks. Based on the goodness-of-fit performance results in Table 3.1, for lightning L, polynomial regression with 3-th degree has a better performance with less SSE and RMSE, and greater R-square. Therefore, the relationship function between N_L and L can be determined by: $N_L = \beta_0^L + \beta_1^L L + \beta_2^L L^2 + \beta_3^L L^3$. Figure 3.8(a) plots the numbers of L in one utility management area, and both polynomial and exponential regression models are adopted for analysis of the effect of L on N_L as shown in Figure 3.8(b).

3.4 Power Interruption Forecasting Framework

In this section, taking the polynomial and exponential regression models derived for common weather parameters as inputs, a MLP based forecasting framework is developed for forecasting the daily numbers of N and M in smart grid distribution networks. Additionally, a modified ELM based algorithm is proposed to train, validate, and test the proposed framework.

3.4.1 MLP based Forecasting Framework

A typical MLP network structure is composed of input, hidden, and output layers. The input layer neurons receive sample data for analysis and the output layer neurons give the network results out. A MLP network structure is made up by usually one, but occasionally more than one hidden layers between input and output layers. The hidden layer neurons learn the nonlinear relationship between the inputs and outputs. The mathematical expression of the outputs of the MLPs can be defined as follows: $Y = F(b + \sum_{j=1}^{m} v_j [\sum_{i=1}^{n} G(w_{ij} x_i + b_j)])$, where x_i, $i = 1, .., n$, is the input value; Y is the output value; w_{ij} is the weight of connection between the ith input neuron and jth hidden neu-



(a) Lightning

(b) Regression Analysis for Lightning

Figure 3.8: (a) Lightning L. (b) The polynomial and exponential regression for analyzing the number of N_L respond to lightning L.

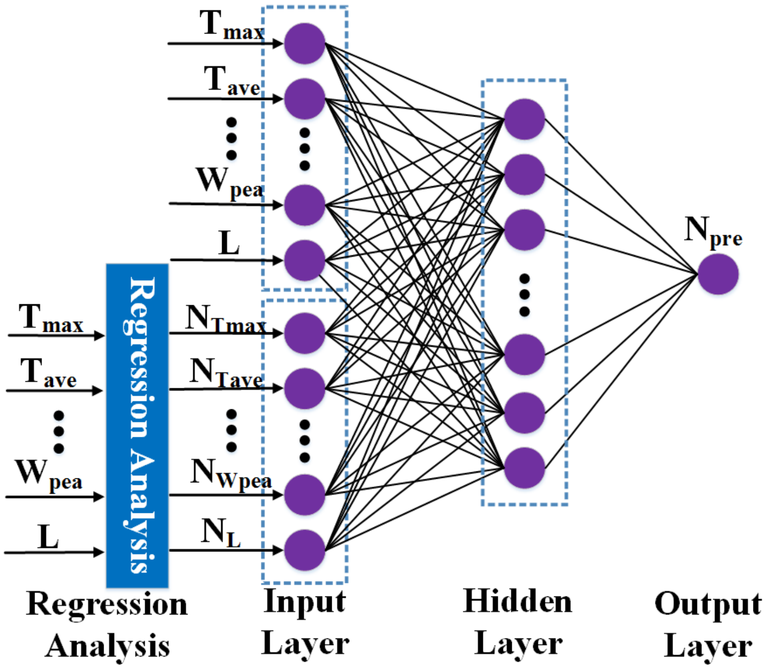


Figure 3.9: Network structure of the proposed MLP based forecasting framework.

ron; v_j is the weight of connection between the jth hidden neuron and output neuron; b and b_j are the bias values of the corresponding output neuron and jth hidden neuron; and $F(\cdot)$ and $G(\cdot)$ are the activation functions of output and hidden neurons, respectively.

However, large MLPs usually generalize poorly due to the time needed for variable preprocessing and the possibility of model overfitting [99]. In this chapter, a hybrid model integrating MLPs and parametric regression models is proposed to analyze the combined effect of common weather parameters on the numbers of N and M. In the proposed framework, the input layer of MLP contains both the common weather parameters, such as T_{max}, T_{ave}, T_{min}, H, C, W_{pea}, W_{ave}, W_{sus}, P_{rain}, A, and L, and corresponding daily numbers of N and M derived by their regression models. The output layer is for the forecasted daily numbers of N and M. To restrict the net capacity, one hidden layer is included in the MLP. The network structure of the MLP based forecasting framework is shown in Figure 3.9.

3.4.2 Extreme Learning Machine Algorithm

ELM is an emerging and efficient algorithm for MLP learning [100], where the model training is transformed into a matrix calculation problem. Assume $F(\cdot)$ to be a constant function, the MLP model then can be represented in the matrix form:

$$\boldsymbol{Y} = \sum_{j=1}^{m} v_j [\sum_{i=1}^{n} G(w_{ij} x_i + b_j)] = \boldsymbol{H}\boldsymbol{v}, \tag{3.4}$$

where $\boldsymbol{H} \in \mathbb{R}^{n \times m}$ is the hidden layer output matrix, and $\boldsymbol{v} = [v_1, ..., v_m]^T$ represents the output weight vector. Since w_{ij}, $i = 1, ..., n$, and b_j are determined randomly for each hidden layer neuron $j = 1, .., m$, the objective of ELM algorithm is to calculate $\boldsymbol{v}$ in order to formulate the MLP model. Given a training set $\{\boldsymbol{X}, \boldsymbol{Y}\}$, where $\boldsymbol{X} = \{x_1, ..., x_n\}$, $\boldsymbol{v}$ can be derived by $\boldsymbol{v} = \boldsymbol{H}^{\dagger}\boldsymbol{Y}$, where $\boldsymbol{H}^{\dagger}$ can be be calculated through orthogonal projection: $\boldsymbol{H}^{\dagger} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T$.

However, ELM algorithm may have a high training error when inappropriate w_{ij} and b_j are selected. In order to boost the training performance of algorithm, a self-adjusting parameter $\lambda = \|Y\|^{\delta}$, $\delta \in [1, 2]$, is introduced into the diagonal elements of $\boldsymbol{H}^T\boldsymbol{H}$: $\boldsymbol{H}^{\dagger} = (\boldsymbol{H}^T\boldsymbol{H} + \lambda)^{-1}\boldsymbol{H}^T$. Therefore, the MLP learning problem is converted into a least square problem defined as:

$$\min_{\boldsymbol{v}} \ \|\boldsymbol{v}\|^{\delta_1} + \lambda\|\boldsymbol{H}\boldsymbol{v} - \boldsymbol{Y}\|^{\delta_2} \tag{3.5}$$

where $\delta_1, \delta_2 > 0$. The modified ELM algorithm intends to minimize both the training error and the norm of output weights, where λ is a parameter to balance the two. The procedures of the modified ELM algorithm can be summarized as Table 3.2. The convergence of the proposed ELM learning algorithm can be proved based on the expansion of *Theorem 3.1* in [101]:

Theorem 3.4.1 *Assume the level set: $L(\boldsymbol{v}^0) = \{\boldsymbol{v} \in \mathbb{R}^m : f(\boldsymbol{v}) \leq f(\boldsymbol{v}^0)\}$ be bounded and $F(\boldsymbol{v}) = \boldsymbol{H}\boldsymbol{v} - \boldsymbol{Y}$ is semismooth over $L(\boldsymbol{v}^0)$. Let $\boldsymbol{v}^k$ be generated by the modified*

Table 3.2: Formulated MLP based Forecasting Framework

```
Parametric Regression Analysis and Modified ELM Algorithm
Phase 1 - Data Collection & Parametric Regression Analysis:
    a) Collect the daily numbers of $N$ and $M$ in one utility MA;
    b) Collect the common weather parameters including $T_{\text{max}}$, $T_{\text{ave}}$,
       $T_{\text{min}}$, $H$, $C$, $W_{\text{pea}}$, $W_{\text{ave}}$, $W_{\text{sus}}$, $P_{\text{rain}}$, $A$, and $L$ for the MA;
       for each common weather parameter do
    1: Implement $f(\boldsymbol{x},\boldsymbol{\beta}^{\text{pol}}) = \beta_0^{\text{pol}} + \beta_1^{\text{pol}}\boldsymbol{x} + \beta_2^{\text{pol}}\boldsymbol{x}^2 + \cdots + \beta_n^{\text{pol}}\boldsymbol{x}^n$,
        $n = 1, 2, 3$, for polynomial regression analysis;
    2: Implement $f(\boldsymbol{x},\boldsymbol{\beta}^{\text{ex}}) = \beta_0^{\text{ex}} + \beta_1^{\text{ex}}\exp(\beta_2^{\text{ex}}\boldsymbol{x}) + \beta_3^{\text{ex}}\exp(\beta_4^{\text{ex}}\boldsymbol{x})$,
        for two-term exponential regression analysis;
    3: Analyze the goodness-of-fit of each derived regression model;
    4: Derive the number of $N$ and $M$ by the optimal regression model.
       end for
Phase 2 - ELM based Learning Algorithm:
    a) For each hidden neuron $j = 1, .., m$, randomly determine its
       input layer weights $w_{ij}$, $i = 1, ..., n$, and the bias value $b_j$;
    b) Calculate the hidden layer output matrix $\boldsymbol{H}$ using both common
        weather parameter data and corresponding the number of $N$ and
        $M$ derived by Phase 1;
    c) Define the self-adjusting parameter $\lambda = \|Y\|^{\delta}$, $\delta \in [1, 2]$;
    d) Obtain the output weight vector $\boldsymbol{v}$ by solving the problem:
       $\boldsymbol{v} = \boldsymbol{H}^{\dagger}\boldsymbol{Y}$, where $\boldsymbol{H}^{\dagger} = (\boldsymbol{H}^T\boldsymbol{H} + \lambda)^{-1}\boldsymbol{H}^T$.
       Or equivalently, $\min_{\boldsymbol{v}}\ \|\boldsymbol{v}\|^{\delta_1} + \lambda\|\boldsymbol{H}\boldsymbol{v} - \boldsymbol{Y}\|^{\delta_2}$.
```

ELM algorithm, then the algorithm terminates in finite iterations or satisfies:

$$lim_{k\to\infty}\|F(\boldsymbol{v}^k)\| = 0.$$

3.5 Evaluation of Proposed Forecasting Framework

The implementation of the proposed forecasting framework contains four main parts including: 1) data collection & preprocessing; 2) parametric regression analysis; 3) MLP based model formulation and training; and 4) sensitivity analysis, in which , in which the flowchart is detailed explained in Figure 3.10.

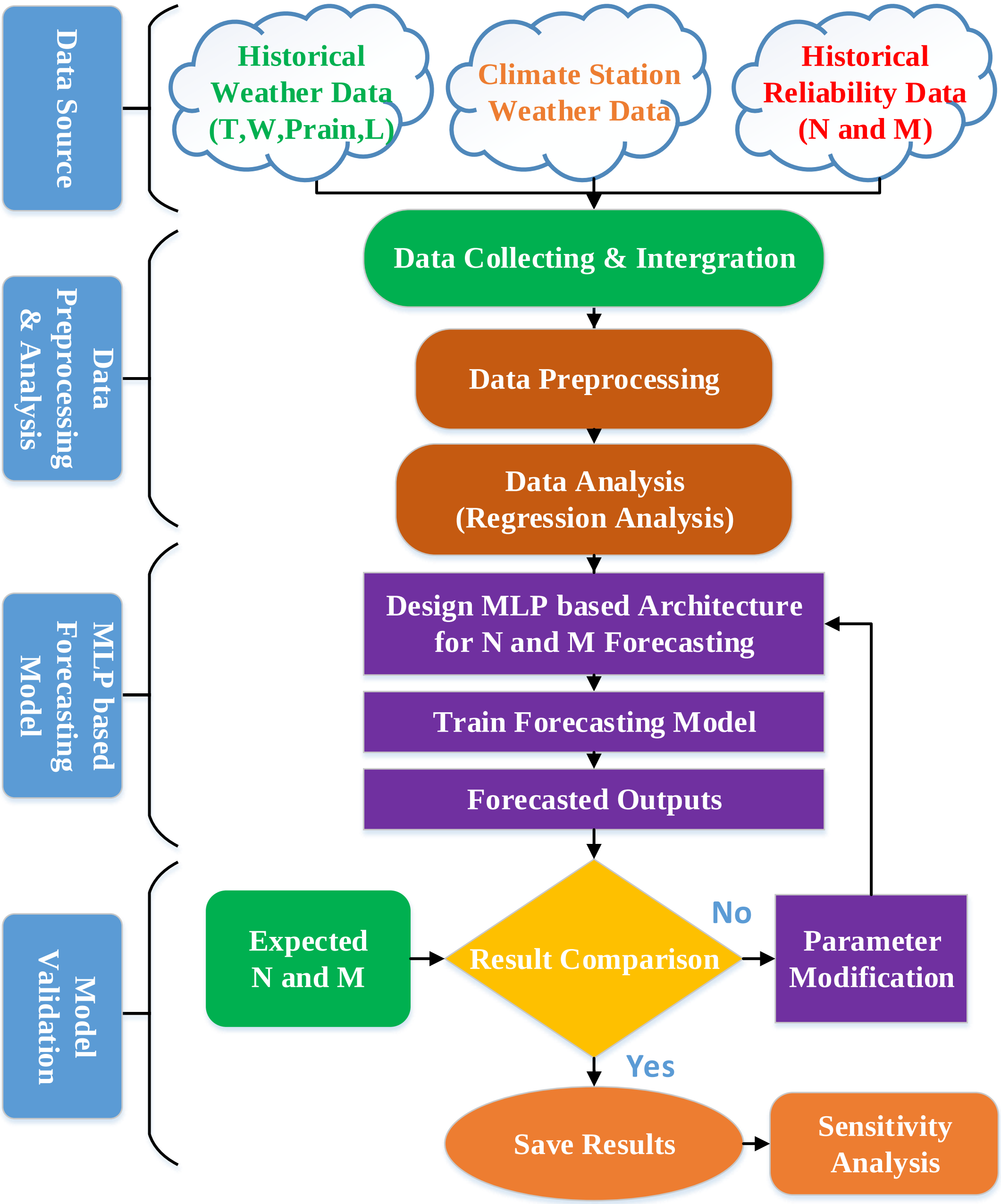


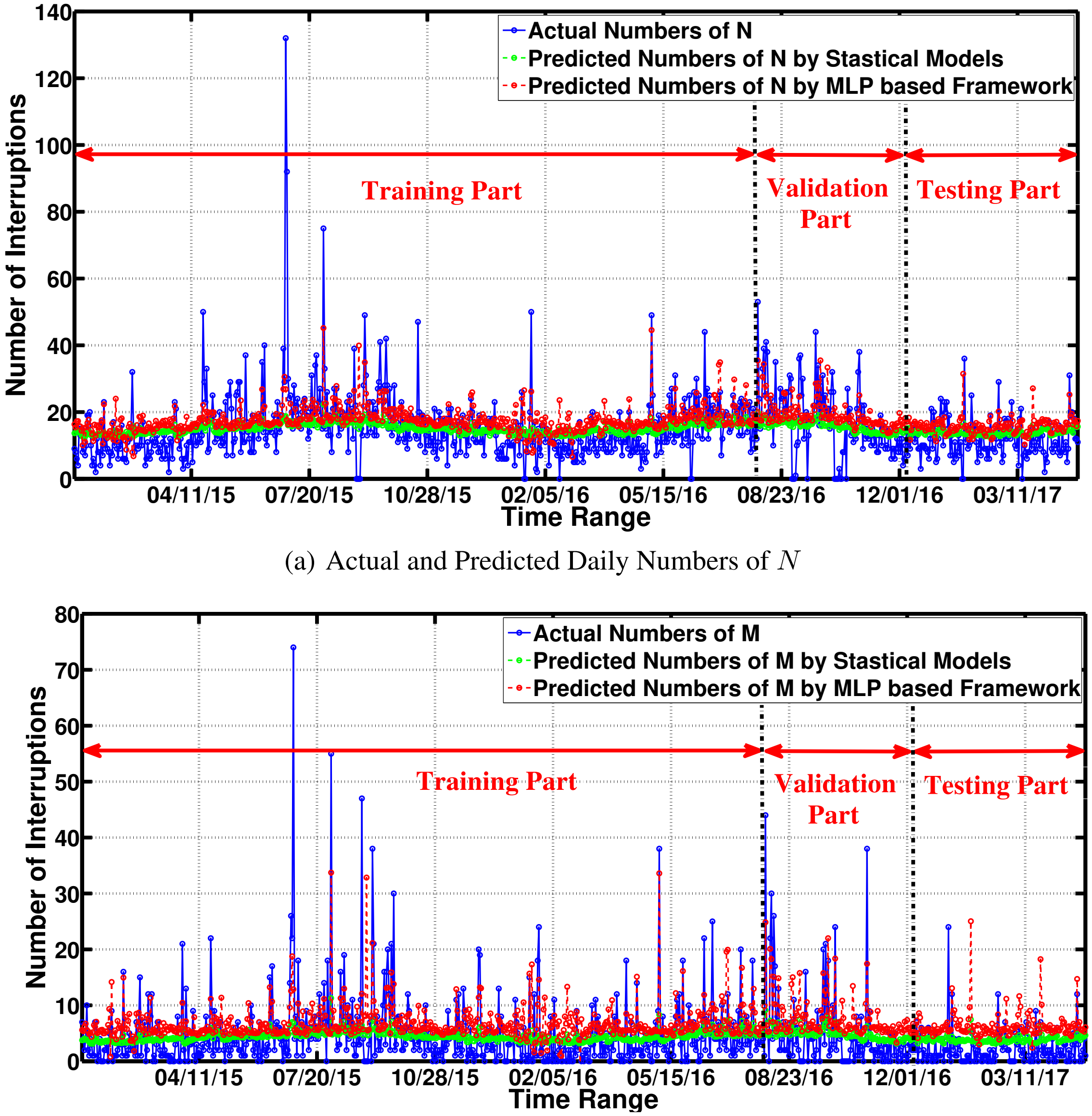
Figure 3.10: The flowchart of the formulated MLP based forecasting model for power distribution networks.

1) *Data Collection & Preprocessing:* The sustained and momentary power interruption data is collected from one utility management area ranging from Jan. 1st 2015 to Apr. 30th 2017. The interval data is recorded daily, annotated with timestamp. Additionally, one climate station, which is nearest to the central point of this management area, is selected for collecting hourly common weather data including T_{max}, T_{ave}, T_{min}, H, C, W_{pea}, W_{ave}, W_{sus}, P_{rain}, and A. The weather data is noted hourly ranging from Jan. 1st 2015 to Apr. 30th 2017. Correspondingly, the hourly lightning strike L data is collected from the control center of the electric utility located inside this management area.

2) *Parametric Regression Analysis:* Both polynomial regression with the n-th degree, $n = 1, 2, 3$, and two-term exponential regression are implemented for the analysis of the numbers of N and M in the management area response to various weather parameters. Based on the goodness-of-fit results in Table 3.1, for T_{max}, T_{ave}, T_{min}, W_{s}, A, and L, polynomial regression with 3-th degree has a better performance with less SSE and RMSE, and greater R-square. Exponential regression with 2 terms has a better performance for H, W_{p}, W_{a}, and P_{ra}, while, for C, polynomial regression with 2-rd and 3-th degrees and two term exponential regression have similar performances in fitting. Based on these regression models, the daily numbers of N and M can be derived by model fitting.

3) *MLP based Forecasting Framework:* The input layer of the formulated MLP network contains all common weather parameters and corresponding daily numbers of N and M derived by their regression models. The hidden layer is set to be one, and the output layer is for the target numbers of N and M. The proposed modified ELM algorithm is used for training, validating, and testing the formulated MLP network, in which 70% of the collected dataset is for the network training, 15% of the dataset is for the network validation, and the remaining 15% of the dataset is for the network testing.

Figure 3.11(a) presents the actual numbers of N and the predicted numbers of N derived by statistical models and the proposed MLP based framework, respectively. In



(a) Actual and Predicted Daily Numbers of N

(b) Actual and Predicted Daily Numbers of M

Figure 3.11: The actual numbers of power interruptions and the predicted numbers of power interruptions derived by statistical models and the proposed MLP based framework. (a) for$N$, (b) for M.

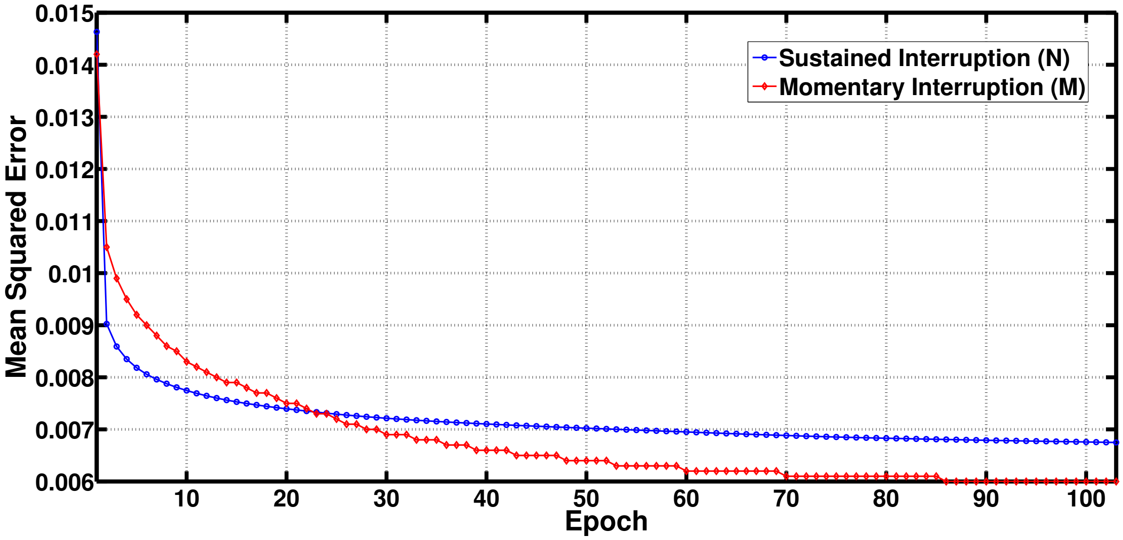


Figure 3.12: Training error of the modified ELM algorithm for forecasting the daily number of N and M.

this figure, we can find that, compared with statistical models, the proposed MLP based framework derives better predicted numbers of N. In particularly, the proposed MLP based framework yields a Mean-Squared Error (MSE) reduction of 8.77% relative to statistical models. Correspondingly, Figure 3.11 (b) compares the predicted numbers of M derived by statistical models and the proposed MLP based framework with the actual numbers of M, respectively. We can also see that the proposed MLP based framework achieves better predicted numbers of M response to statistical models, in which 61.37% MSE reduction yielded by the proposed MLP based framework. Furthermore, the training performance and convergence of the modified ELM algorithm for the MLP based framework are shown in Figure 3.12, in which the y-axis describes the variation of MSE for each epoch.

4) *Sensitivity Analysis:* The sensitivity of the output to various input perturbations is an important issue in the design and implementation of the MLP based forecasting framework. Therefore, the sensitivity analysis is implemented to analyze the impact of each weather parameter on the daily numbers of N and M, respectively. The sensitivity is cal-

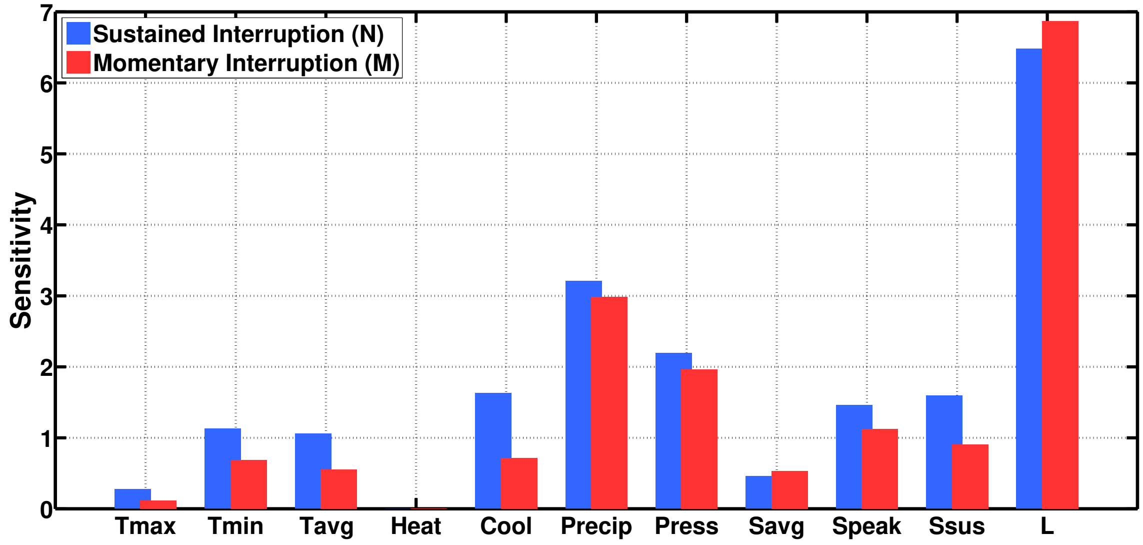


Figure 3.13: Sensitivity analysis of N and M with each weather parameter.

culated by the first-order derivative of system network function with respect to the system parameters, which denotes the degree of influence of parameter variations on the network function. Figure 3.13 presents the sensitivity of each weather parameter response to the daily numbers of N and M, respectively. In this figure, we can find that lightning strike L is the most important weather parameter that has an influence on the daily numbers of N and M, while heat day H has the least impact on the numbers of N and M. This phenomenon can be explained that the most number of N and M was happened ranging from June to September during one year, where is the raining season for the Florida and lightning strike happen most frequently. Since the temperature of Florida is almost kept above 65^oF, heating days has little happened during one year.

3.6 Summary

This chapter presents a MLP based framework to forecast the daily numbers of sustained and momentary interruptions in smart grid distribution networks using time series of common weather data. A modified ELM based learning algorithm is proposed to train, validate, and test the proposed framework, whose convergence is proved. Essentially, compared with traditional statistical models, the proposed framework can reduce MSE by 8.77% and 61.37% for sustained and momentary interruption forecasting, respectively. In addition, we can derive the sensitivity of each common weather parameter with respective to the daily numbers of power interruptions. For the utility management area in Florida, we can find that the lightning strike is the most important common weather parameter impacting on the reliability performance of the smart grid distribution networks, while the heat degree days have the least impacts. In the future, the other factors like power system equipment failure rates and aging of distribution network components can also be integrated as inputs for the proposed framework.

CHAPTER 4

Application of Game Theory for Smart Grid Security

In this chapter, a systematic survey of existing game-theoretic approaches for mitigating security threats is proposed for three main smart grid zones: the power system network infrastructure, advanced metering infrastructure (AMI), and state estimation. Section 4.1 makes an overview of the cyber-phsyical security challenges faced by the three main smart grid zones. Section 4.2 evaluates the current game theoretic models for the cyber-physical security in the power system network infrastructure. Section 4.3 compares the game theoretic models for the cyber-physical security of the communication networks and smart meters in AMI. Section 4.4 introduces the game theoretic models for the cyber-physical security in the power system state estimation. To conclude this chapter, Section 4.5 will discuss future work and recent progresses.

4.1 Overview

The smart grid is the next generation electrical infrastructure integrated with information and communication technologies (ICTs), which are large scale, dynamic cyber-physical systems (CPSs). The ICTs facilitate the grid with effective operation, monitoring and control, enable predictive maintenance and self-healing responses to system disturbances, automate maintenance and operation, and promote expanded deployment of renewable energy sources. However, the large-scale, interconnected nature of smart grid renders the system susceptible to a range of cyber and physical attacks due to a dramatic increase in its attack surface.

Given the presence of risks that could potentially cripple the smart grid as it undergoes an increased shift towards the Internet of Things (IoT) paradigm, identifying and analyzing potential threats that effectively translate risks into successful attacks is essential to achieve a more robust and resilient grid. However, due to the complex and interdependent nature of the different smart grid technologies, various challenges accompany these diagnostic and corrective efforts, such as the dynamic nature of the grid, the impact on the control system, and the synergies between cyber and physical functions. More importantly, and somewhat remarkably, existing CPS security mechanisms are primarily based on mathematical and engineering principles that ignore the human decision making processes of cybercriminals and system administrators. Indeed, cybercriminals are active agents who engage in an intelligent, dynamic decision-making process when selecting a target and executing an attack. Likewise, the defenders, system operators, and engineers also rely on human intelligence in conjunction with available mathematical and software tools. Beyond these limitations, most of the state-of-the-art works often assume that attackers or defenders act individually, which, in a large-scale CPS, can be a restrictive assumption. In this respect, game theory is expected to constitute a key analytical tool for analyzing the strategic interactions between the potential attackers and the smart grid operators. Game theory is a formal analytical tool as well as a conceptual framework with a set of mathematical tools, which enable the study of complex interactions among independent rational players. In recent decades, game theory has been adopted in a wide number of fields, including economics, politics, and psychology. More recently, game theory has also become a central tool in the design and analysis of CPSs such as the smart grid.

In order to design a resilient and secure smart grid, it will have to build on the solid mathematical tools, in which game theory provides a mathematical framework for analyzing and implementing security solutions. Currently, there is little research in the literature that comprehensively reviews and evaluates the application of the game-theoretic models to cyber-physical security issues within the smart grid. The main contribution of this chapter is to propose a systematic survey of existing game-theoretic approaches for mitigating security threats in three main smart grid zones including the power system network infrastructure, AMI, and state estimation. Overall, the goal of this paper is threefold:

- identify and explore the cyber-physical security threats targeted at the three smart grid zones;
- compare the game-theoretic frameworks and solution approaches that can help with analysis of the security of the smart grid as well as devising proper defense strategies;
- discuss the future opportunities and extension of current game theoretic applications in the cyber-physical security of the smart grid.

4.2 Game Theory for Cyber-Physical Security in Smart Grid Zone 1

The emergence of the smart grid, which integrate new communication and information technologies within the power system network infrastructures such as the power generation, transmission, and distribution systems, has opened new cyber security concerns and new points of entry for attackers. Moreover, the growth of the smart grid in both scale and complexity makes it financially and logistically impossible to protect the entire infrastructure. In this section, an overview of the cyber-physical security issues targeted at the power system network infrastructure will be provided. Additionally, the Markov game model for distributed denial of services (DDoS) in automatic generation control (AGC), the three-stage Sequence game for the distribution networks integated with DERs, and the stochastic game for the coordinated cyber-phsyical attack targeted at the transmission system will be provided.

4.2.1 Markov Game for DDoS in Automatic Generation Control

1) Automatic Generation Control Model: AGC is load-frequency control with the additional objective of economic dispatch (distributing the required change in generation among units to minimize costs), which is an indispensable part of the "central nervous system" of a power grid called the energy management system (EMS), and possibly the only automatic closed loop between the IT and power system of a control area; because of this, it is subject to attacks propagated through the IT system.

When system frequency deviates from the nominal frequency by a certain threshold, overfrequency and underfrequency protection relays execute tripping logic defined by a protection plan that varies from operator to operator. Underfrequency relays perform underfrequency load shedding (UFLS), which is the sole concFor our studyern of our study because it results in directly measurable revenue loss. , we adopt Mullen's UFLS scheme. The gist of the scheme is, when the system frequency drops by more than 0.35 Hz below the nominal frequency, to shed this much load: $\triangle P_m - \triangle P_e - 0.3/R$, where $\triangle P_m$ is the change in generator's mechanical power, $\triangle P_e$ is the change in generator's electrical power, and R is the droop characteristic.

The automatic generation controller is an integral controller of gain K_{AGC}. AGC design is an established discipline with designs dating back to the 1950s; a simple integral controller seems to be a logical starting point. The UFLS relay in each area decides on the necessity to shed load, and the amount of load to shed if necessary, using Mullen's algorithm. Once the system frequency has stabilized for at least 30 s, the UFLS relays reconnect the shed loads in the reverse order they were shed. In this sample configuration, the maximum sheddable loads are capped at 4 p.u. and 1 p.u. for the areas 1 and 2 respectively. "p.u." stands for "per unit" and is simply the ratio of an absolute value in some unit to a base/reference value in the same unit. The base load for both areas is taken to be 1000 MW.

It is impossible to exhaust all injection patterns, but there is one basic attack pattern: *constant injection*. If an attacker injects a constant false Δf, then it effectively disables the integral control loop, causing the system frequency to converge to a non-nominal frequency. If the false is positive, then the system will settle on a below-nominal frequency, causing loads to be shed; otherwise, the system will settle on an above-nominal frequency, causing generators to be tripped. Both cases lead to cascading failures. Correspondingly, one basic defense mechanism is *saturation filter*. We can constrain the attack by limiting the Δf input to the integral controller to $[-4.5, 3.5]$ Hz, because at $\Delta f = -4.5$ Hz, not only should all sheddable loads have been shed, but also all generators would be tripped. At $\Delta f = 3.5$ Hz, all generators would be tripped.

2) Game Formulation and Results: The security game between the attacker and the defender is formulated as a stochastic game with a finite state space, and two players that choose their actions from their respective finite action space; or more formally, as a 6-tuple $\langle \mathcal{S}, \mathcal{A}^A, \mathcal{A}^D, M, U^{\mathcal{A}}, U^{\mathcal{D}} \rangle$, where:

- $\mathcal{S} := \{s_1, s_2, ..., s_{N_\mathcal{S}}\}$ is the system's state space, which is associated with the tuple $(\Delta f_1, \Delta f_1)$ consisting of area 1's frequency deviation and area 2's frequency deviation;
- $\mathcal{A}^A := \{a_1, a_2, ..., a_{N_\mathcal{A}}\}$ and $\mathcal{A}^D := \{d_1, d_2, ..., d_{N_\mathcal{D}}\}$ represent the attacker and defender's action space, respectively;
- $M(a, d) = [M_{s_i, s_j}(a, d)]_{N_S \times N_S}$ which represents the system's state transition matrix corresponding to attack action $a \in \mathcal{A}$ and defense action $d \in \mathcal{D}$;
- $U^{\mathcal{A}}(s) := [R^{\mathcal{A}}(a, d, s)]_{N_\mathcal{A} \times N_\mathcal{D}}$ which represents the attacker's expected reward function corresponding to attack action $a \in \mathcal{A}$ against defense action $d \in \mathcal{D}$ in state $s \in \mathcal{S}$;

- $U^{\mathcal{D}}(s) := [R^{\mathcal{D}}(a,d,s)]_{N_{\mathcal{A}} \times N_{\mathcal{D}}}$ which represents the defender's expected reward function corresponding to defense action $d \in \mathcal{D}$ against attack action $a \in \mathcal{A}$ in state $s \in \mathcal{S}$.

For each state $s \in \mathcal{S}$, the attacker (defender) incurs a net gain (net loss), and the attacker's net gain is assumed to be close to the defender's net loss, and hence the security games to be *zero-sum.* The defender's loss is defined including the cost of load shed and the costs of false positives. The cost of the expected total load shed in state s under attack action a and defense action d is defined as $E\{P_{shed}(a,d,s)\}$. And the expected cost of false positives is $c_{fp}p_{fp}$, where c_{fp} is the cost of a false positive in the same unit as load shed, and p_{fp} is the probability of getting a false positive. *Dynamic programming* is implemented to obtain the stationary optimal strategy (solving a zero-sum matrix game at each stage).

4.2.2 Three-Stage Sequence Game for Distribution Networks with DERs

1) Electricity Distribution Networks: Consider a tree network of radial electric distribution systems $\mathcal{G} = (\mathcal{N} \cup \{0\}, \mathcal{E})$, where $\mathcal{N}$ denotes the set of all nodes except the substation (labeled as node 0), and let $N := |\mathcal{N}|$. Let $V_i \in \mathbb{C}$ denote the complex voltage at node i, and $v_i := |V_i|^2$ denote the square of voltage magnitude. We assume that the magnitude of substation voltage $|V_0|$ is constant. Let $I_j \in \mathbb{C}$ denote the current flowing from node i to node j on line $(i,j) \in \mathcal{E}$, and $\ell_j := |I_j|^2$ the square of the magnitude of the current. A distribution line $(i,j) \in \mathcal{E}$ has a complex impedance $z_j = r_j + \mathbf{j}x_j$, where $r_j > 0$ and $x_j > 0$ denote the resistance and inductance of the line (i,j), respectively, and $\mathbf{j} = \sqrt{-1}$.

The voltage regulation requirements of the DN under nominal on attack conditions govern that: $\underline{v}_i \leq v_i \leq \overline{v}_i, \forall i \in \mathcal{N}$, where $\underline{v}_i = |\underline{V}_i|^2$ and $\overline{v}_i = |\overline{V}_i|^2$ are the soft lower and upper bounds for maintaining voltage quality at node i. Additionally, voltage magnitudes under all conditions satisfy: $\underline{\mu}_i \leq v_i \leq \overline{\mu}_i, \forall i \in \mathcal{N}$, where $\underline{\mu}$ and $\overline{\mu}$ are the hard voltage safety bounds for any nodal voltage, and $0 < \underline{\mu} < \min_{i \in \mathcal{N}} \underline{v}_i \leq \max_{i \in \mathcal{N}} \overline{v}_i < \overline{\mu}$.

We consider constant power loads. Let $sc_i := pc_i + \mathbf{j}qc_i$ denote the power consumed by a load at node i, where pc_i and qc_i are the real and reactive components. And let $sg_i := pg_i + \mathbf{j}qg_i$ denote the power generated by the DER connected to node i, where pg_i and qg_i are the real and reactive components, respectively. The 3-phase balanced nonlinear power flow (NPF) on line $(i, j) \in \mathcal{E}$ is given by:

$$\begin{aligned} S_j &= \sum_{k:(j,k)\in\mathcal{E}} S_k + sc_j - sg_j + z_j l_j, \\ v_j &= v_i - 2Re(\overline{z}_j S_j) + |z_j|^2 l_j, \end{aligned} \tag{4.1}$$

where $l_j = |S_j|^2/v_i$, and $S_j = P_j + \mathbf{j}Q_j$ denoting the complex power flowing from node i to node j on line $(i, j) \in \mathcal{E}$.

2) Game Formulation and Results: A 3-stage sequential game between a defender (network operator) and an attacker (external threat agent) is formulated:

- **Stage 1 [Security Investment]:** The defender chooses a security strategy $u \in U_B$ to secure a subset of DERs, where the set of defender actions is: $\mathcal{A}^D := \{d \in \{0,1\}^{\mathcal{N}} \mid \|d\|_0 \leq B\}$, where $B \leq |\mathcal{N}|$ denotes a security budget.
- **Stage 2 [Attack]:** The attacker chooses from the set of DERs that were not secured by the defender in Stage 1, and manipulates their set-points. Let $\Psi_M(d) := \mathcal{S}(d) \times \mathcal{D}_M(d)$ denotes the set of attacker actions for a defender's choice d, where $\mathcal{S}(d) := \prod_{i \in \mathcal{N}_v(d)} \mathcal{S}_i \times \prod_{j \in \mathcal{N}_s(d)} \{0 + 0\mathbf{j}\}$, $\mathcal{D}_M(d) := \{\delta \in \{0,1\}^{\mathcal{N}}\}$, and $M \leq |\mathcal{N}_v|$ denoting the maximum number of DERs that the attacker can compromise. The attacker simultaneously compromises a subset of vulnerable DER nodes by introducing incorrect set-points, and increase the loss L.

- **Stage 3 [Defender Response]:** The defender responds by choosing the set-points of the uncompromised DERs and, if possible, impose load control at one or more nodes according to a strategy $\phi := [sp^d, \gamma] \in \Phi(u, \psi)$. Let $\underline{\gamma}_i \geq 0$ denote the maximum permissible fraction of load control at node i, and define the set of Stage 3 defender actions: $\Phi(d, \psi) := \mathcal{S} \times \Gamma$, where $\Gamma := \prod_{i \in \mathcal{N}} [\underline{\gamma}_i, 1]$. The defender chooses new set-points spd of non-compromised DERs, and load control parameters i to reduce the loss L.

The [DAD] game is a sequential game of perfect information, i.e. each player is perfectly informed about the actions that have been chosen by the previous players. The equilibrium concept is the classical Stackelberg equilibrium. In this game, u_B and $\Phi(\mu, \psi)$ denote the set of defender actions in Stage 1 and 3, respectively; and $\Psi_M(\mu)$ denotes the set of attacker strategies in Stage 2.

4.2.3 Stochastic Game for Coordinated Cyber-Physical Attacks

1) Smart Grid Transmission Networks: Consider a power grid system with $N_{\mathcal{V}}$ buses and $N_{\mathcal{E}}$ branches. This system can be modeled using an undirected graph $\mathcal{G} := (\mathcal{V}, \mathcal{E})$ with $N_{\mathcal{V}}$ vertices and $N_{\mathcal{E}}$ edges. The set of vertices $\mathcal{V} = \{v_1, v_2, ..., v_{N_{\mathcal{V}}}\}$ represents $N_{\mathcal{V}}$ nodes in the graph that can include generation plants, transformers, substation devices, and customers. The set $\mathcal{E} = \{e_1, e_2, ..., e_{N_{\mathcal{E}}}\}$ of edges encompasses $N_{\mathcal{E}}$ edges that correspond to transmission lines. Thus, the total number of elements (vertices and edges) of the system that must be protected against cyber-physical attacks is $N_{\mathcal{G}} = N_{\mathcal{V}} + N_{\mathcal{E}}$.

Consider an attacker that seeks to disrupt the system by distributing its finite attack resources over one or more elements of the graph to maximize the physical impact on the system. The resources owned by the attacker can include a) personnel or hackers that are assigned to the attack, b) technological resources such as advanced tools or malwares to disrupt the power grid, and c) economic resources among others. Due to the resource limitation, we define $C_{\mathcal{A}}$ as the maximum number of attacks that can be carried out at a time, each of which corresponds to a specific attack. For example, the attacker may launch a DoS attack over poorly protected wireless channels to block the communication between power grid sensors and remote estimators. Alternatively, the attacker may plan to launch a physical attack on a high voltage (HV) transformer. Thus, the action space $\mathcal{A}$ of the attacker contains all possible methods of allocating $C_{\mathcal{A}}$ attacks over the $N_{\mathcal{G}}$ elements of the graph.

In order to maximize the system resiliency against such attacks, the defender needs to allocate its limited defense resources over the $N_{\mathcal{G}}$ elements of the graph to reinforce operational elements or to repair disabled elements. Similarly, the defense resources can include a) personnel such as users, administrators, and support personnel, b) technological resources such as advanced tools or softwares to reinforce operational elements or to repair broken elements of the power grid, and c) economic resources such as investments in new infrastructures or nodes, among others. Let $C_{\mathcal{D}}$ be the maximum number of defense mechanisms that can be implemented at a time, each of which is dependent on the type of the attack and the element disrupted. For instance, for false data injection attacks on the automatic generation control system, the defense mechanism can be to implement saturation filters. Alternatively, the defender needs to build some barriers and fortification for preventing physical attacks on critical infrastructures. Briefly, the defender should make sensible decisions about how to allocate finite resources over elements of the graph. Let $\mathcal{D}$ be the action space of the defender, then, it conditions all possible methods to distribute $C_{\mathcal{D}}$ defense mechanisms over the $N_{\mathcal{G}}$ elements of the graph.

In the literature, the physical impact of an attack on the system is measured by the cost of shed load following the failure of elements. In order to analyze the physical impacts of various attacks, attacks on the system can be classified into two categories:

isolated and *coordinated*. The former can only destroy one element of the graph at a time, while the latter can target two or more elements. A coordinated attack that can collapse a combination of elements will naturally have a more detrimental impact, as opposed to a single, isolated attack. For the system impacted by coordinated attacks, load shedding must be performed in order to regain stability.

2) Game Formulation and Results: We now mathematically analyze and identify the interactions between the attacker and the defender using the advanced tools of stochastic, noncooperative game theory. In particular, we formulate a two-player stochastic game in normal form, $\Xi = \langle \mathcal{S}, \mathcal{A}, \mathcal{D}, R^{\mathcal{A}}, R^{\mathcal{D}} \rangle$, in which the players are the attacker and the defender. This game is played over a finite state space and each player has a finite number of actions to choose from. The main components of the game include:

- $\mathcal{S} := \{s_1, s_2, ..., s_{N_{\mathcal{S}}}\}$ represents the transmission network's state space;
- $\mathcal{A} := \{a_1, a_2, ..., a_{N_{\mathcal{A}}}\}$ and $\mathcal{D} := \{d_1, d_2, ..., d_{N_{\mathcal{D}}}\}$ represent the attacker and defender's action space, respectively;
- $R^{\mathcal{A}}(s) := [R^{\mathcal{A}}(a, d, s)]_{N_{\mathcal{A}} \times N_{\mathcal{D}}}$ $(\mathcal{S} \times \mathcal{A} \times \mathcal{D} \rightarrow \mathcal{R})$ which represents the attacker's expected reward function corresponding to attack action $a \in \mathcal{A}$ against defense action $d \in \mathcal{D}$ in state $s \in \mathcal{S}$;
- $R^{\mathcal{D}}(s) := [R^{\mathcal{D}}(a, d, s)]_{N_{\mathcal{A}} \times N_{\mathcal{D}}}$ $(\mathcal{S} \times \mathcal{A} \times \mathcal{D} \rightarrow \mathcal{R})$ as the defender's expected reward function corresponding to defense action $d \in \mathcal{D}$ against attack action $a \in \mathcal{A}$ in state $s \in \mathcal{S}$.

For the power grid composed of $N_{\mathcal{G}}$ elements to be protected, the actions of both the attacker and the defender are constrained by a finite amount of resources. Thus, the attacker and the defender can only implement $C_{\mathcal{A}}$ attacks and $C_{\mathcal{D}}$ defense mechanisms, respectively, at a given time. We define each attack action vector $\boldsymbol{a}_i \in \mathcal{A}$, $i = 1, ..., N_{\mathcal{A}}$, as a method of allocating an attacker's finite resources over $N_{\mathcal{G}}$ elements:

$\boldsymbol{a}_i = [c^{\mathcal{A}}_{i,1}, c^{\mathcal{A}}_{i,2}, ..., c^{\mathcal{A}}_{i,N_{\mathcal{G}}}]^T$, where $\sum_{j=1}^{N_{\mathcal{G}}} c^{\mathcal{A}}_{i,j} = C_{\mathcal{A}}$. $0 \leq c^{\mathcal{A}}_{i,j} \leq C_{\mathcal{A}}$, $j = 1, 2..., N_{\mathcal{G}}$, represents the number of attacks related to action $\boldsymbol{a}_i$ that target element j of the grid. Similarly, each defense action vector $\boldsymbol{d}_i \in \mathcal{D}$, $i = 1, ..., N_{\mathcal{D}}$, conditions one method to distribute its limited defense resources over $N_{\mathcal{G}}$ elements: $\boldsymbol{d}_i = [c^{\mathcal{D}}_{i,1}, c^{\mathcal{D}}_{i,2}, ..., c^{\mathcal{D}}_{i,N_{\mathcal{G}}}]^T$, where $\sum_{j=1}^{N_{\mathcal{G}}} c^{\mathcal{D}}_{i,j} = C_{\mathcal{D}}$. $0 \leq c^{\mathcal{D}}_{i,j} \leq C_{\mathcal{D}}$, $j = 1, 2..., N_{\mathcal{G}}$, denotes the number of defense mechanisms in action $\boldsymbol{d}_i$ that the defender plans to commit to element j of the grid.

In this game, the defender's expected reward is just the negative of the attacker's expected reward, denoted by $R^{\mathcal{D}}(a, d, s) = -R^{\mathcal{A}}(a, d, s)$. The proposed stochastic game Ξ is therefore a *zero-sum stochastic game*. Given a state $s \in S$, the attacker and the defender independently choose actions $a \in \mathcal{A}$ and $d \in \mathcal{D}$, and receive immediate expected rewards $R^{\mathcal{A}}(a, d, s)$ and $R^{\mathcal{D}}(a, d, s)$. The state then transits to the next state s' based on the fixed transition probability $T_{s,s'}(a, d)$. New expected rewards $R^{\mathcal{A}}(a, d, s')$ and $R^{\mathcal{D}}(a, d, s')$ will be obtained in the new state. We have specified the immediate rewards of the attacker and the defender at each stage game, but not how these rewards are aggregated into an overall payoff. To solve this problem, the most commonly used aggregation method is the discounted-sum reward. For an attack action a and a defense action d, the discounted-sum reward of the attacker is the discounted sum of expected rewards at each time step t, with a discount factor $\gamma \in [0, 1)$:

$$Q := \sum_{t=0}^{\infty} \gamma^t R^{\mathcal{A}}(a, d, s(t)), \tag{4.2}$$

where γ^t represents the weight of the immediate reward at the time step t, given by $R^{\mathcal{A}}(a, d, s(t))$, which denotes the relative importance of the immediate reward in the overall payoff. Small values of γ emphasize near-term gains while large values emphasize future rewards. Correspondingly, the defender's discounted-sum reward is the negative of the number.

In this game, the attacker aims to maximize the discounted sum of expected rewards Q, while facing the defender who intends to minimize it. In order to solve for the two players' optimal strategies of a stochastic game in normal form such as Ξ, one popular solution is that of a closed-loop *Nash equilibrium.* A Nash equilibrium is a state of the game such that no player can increase its reward by *unilaterally* deviating from this equilibrium state. Formally, the Nash equilibrium of the proposed stochastic game Ξ is defined as follows:

Definition 4.2.1 *Consider the proposed stochastic game $\Xi = \langle \mathcal{S}, \mathcal{A}, \mathcal{D}, R^{\mathcal{A}}, R^{\mathcal{D}} \rangle$, where expected rewards $R^{\mathcal{A}}$ and $R^{\mathcal{D}}$ are derived by solving the optimal load shedding problem (1), a* Nash equilibrium *solution of the proposed game is a two-tuple of mixed strategies $\{\boldsymbol{\pi}^*_{\mathcal{A}}, \boldsymbol{\pi}^*_{\mathcal{D}}\}$, where $\boldsymbol{\pi}^*_{\mathcal{A}} = \{\boldsymbol{\pi}^*_{\mathcal{A}}(s) | s \in \mathcal{S}\}$ and $\boldsymbol{\pi}^*_{\mathcal{D}} = \{\boldsymbol{\pi}^*_{\mathcal{D}}(s) | s \in \mathcal{S}\}$, such that, for all attack mixed strategies $\boldsymbol{\pi}_{\mathcal{A}}(s)$ and defense mixed strategies $\boldsymbol{\pi}_{\mathcal{D}}(s)$, $s \in \mathcal{S}$, it satisfies the following set of inequalities in state $s_i \in \mathcal{S}$, $i = 1, ..., N_{\mathcal{S}}$:*

$$\begin{aligned} &Q(\boldsymbol{\pi}_{\mathcal{A}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{A}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_{N_{\mathcal{S}}}), \boldsymbol{\pi}_{\mathcal{D}}(s_1), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_{N_{\mathcal{S}}})) \\ \geq\ &Q(\boldsymbol{\pi}_{\mathcal{A}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{A}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_{N_{\mathcal{S}}}), \boldsymbol{\pi}_{\mathcal{D}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{D}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_{N_{\mathcal{S}}})) \\ \geq\ &Q(\boldsymbol{\pi}_{\mathcal{A}}(s_1), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_{N_{\mathcal{S}}}), \boldsymbol{\pi}_{\mathcal{D}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{D}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_{N_{\mathcal{S}}})). \end{aligned} \tag{4.3}$$

4.3 Game Theory for Cyber-Physical Security in Smart Grid Zone 2

The *Advanced Metering Infrastructure* (AMI) is a key component of the Smart Grid Zone 2 as shown in Figure 4.1, which integrates smart meters, information/communications networks and meter data management systems (MDMS). Smart meters of the AMI provide *customers* with accurate load-profile information and billing data to help manage their electricity consumption. MDMS is the portion of the AMI that enables the electric utilities to create a real-time *market.* Furthermore, the power system outages can be detected for *service providers* through meter measurements derived by MDMS. However,

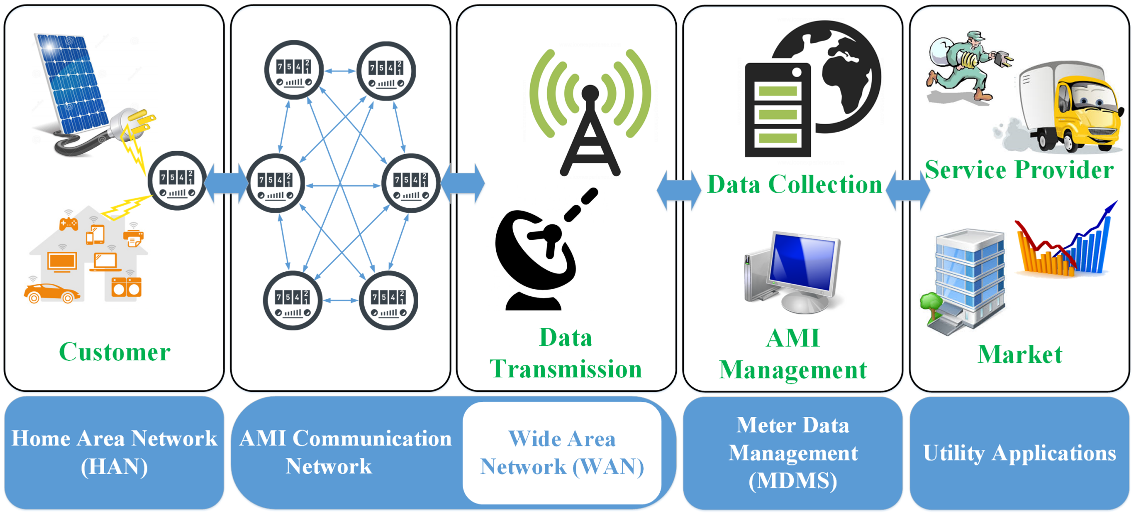


Figure 4.1: The network model of smart grid AMI and its connections with customers, markets and service providers.

the large scalability and cyber-physical nature of the AMI unavoidably exposes the smart meters and the communication network to a range of cyber and physical attacks. In this section, we first provide an overview of the cyber-physical security issues for the AMI. Then, we study, in detail, the application of static noncooperative games for analyzing data confidentiality attacks targeting at the AMI communication network and the use of Stackelberg games for detecting electricity theft in smart meters. We conclude with insights on future game-theoretic approaches for enhancing cyber-physical security in the AMI systems.

4.3.1 Introduction to Cyber-Physical Security Threats in AMI

The AMI enables the two-way communication between the electric utilities and the end customers of power. This, however, opens up two main surfaces for attack vectors and intruders including the *smart meters* and the *AMI communication network*. Smart meters are the primary point of data collection for smart grid energy consumption, which facilitate a dense and large-scale metrology of the smart grid operating characteristics in voltage, frequency, power factor, etc. Moreover, smart meters simplify the automated connection and disconnection of consumers to the smart grid. The design of the smart meter incorporates two network communication radios, and often a local infrared serial port for maintenance, which results in a broadened cyber attack surface. Physical access to the meters adds another attack surface since internal serial links are typically unsecured and based on common protocols. A series of the theoretical and demonstrated cyber and physical attacks target at the smart meters are listed as follows:

- *Meter Manipulation* (**P**) that modifies the smart meter measurements to AMI through physical tampering.
- *Meter Spoof and Energy Fraud Attack* (**P**) that can occur by gaining the smart meter ID through physical access.
- *Denial of Service (DoS)* (**C**) that compromises smart meters such that they are not capable of responding to any request sent by a customer or energy supplier, which can be accomplished through tampering with the routing of the smart meter traffic.
- *False Data Injection Attack (FDIA)* (**C**) that introduces arbitrary and/or certain errors inside a normal smart meter traffic activity causing invalid measurements that are unacceptable in a smart grid network.
- *De-pseudonymization Attack* (**C**) that compromises anonymization and privacy of smart meter data.
- *Man-in-the-middle Attack* (**C**) where rogue agents can place themselves in between end consumer and electric utility.

The vulnerabilities of the AMI communication network can be exploited or disabled by attacks on the underlying communication infrastructure, insertion of false user requests, unauthorized alteration of demand side management schedules and illegal market

Table 4.1: Cyber-Physical Attacks Targeted at AMI

Attack Type		**Attack Target**	
		Smart Meter	**AMI Communication Network**
Physical		• Meter Manipulation • Meter Spoof and Energy Fraud Attack	• Crypto Key Flash Extraction
Cyber	**Availability**	• Denial of Service (DoS)	• Distributed Denial of Service (DDoS)
	Integrity	• False Data Injection Attack (FDIA)	• False Data Injection Attack (FDIA)
	Confidentiality	• De-pseudonymization Attack • Man-in-the-middle Attack	• WiFi/ZigBee Attack • Internet Attack • Data Confidentiality Attack

manipulation; all of which can impact system operations and result in both power shortage, loss of trust and negative economic impacts. The potential and demonstrated attacks aimed at compromising the AMI communication network are listed as follows:

- *Crypto Key Flash Extraction* (**PC**) that accesses AMI device hardware directly with specific tools to extract data.
- *Distributed Denial of Service (DDoS)* (**C**) that compromises AMI data collection units, preventing the normal communication between Wide Area Network (WAN) and Neighbourhood Area Network (NAN).
- *False Data Injection Attack (FDIA)* (**C**) that manipulates power system's state measurements or readings by injecting false load data via AMI/sensors.
- *WiFi/ZigBee Attack* (**C**) that attacks the WiFi/ZigBee networks in Home Area Network (HAN) of the AMI.
- *Internet Attack* (**C**) that compromises the AMI software and systems installed inside the electric utility.
- *Data Confidentiality Attack* (**C**) that attacks device hardware in the AMI in order to compromise data sent from these devices to the electric utility.

A summary of the different types of cyber and physical attacks targeted at smart meters and communication network of the AMI are shown in Table 4.1. To give more insights on these open cyber-physical security problems and related game-theoretic solutions, in what follows, first, we provide a step-by-step tutorial on how static noncooperative game theory can be applied for modeling the interactions between the defender and the attacker implementing data confidentiality attacks in AMI Communication Network.Then, we overview the use of Stackelberg games for detecting potential electricity theft through compromising smart meters. This section is concluded with a brief overview on other existing game-theoretic techniques for protecting the AMI against cyber and physical attacks as well as with a discussion on the future outlook of game theoretic applications in the cyber-physical security of the AMI.

4.3.2 Game Theoretic Models for AMI Communication Network

Due to the sensitivity of importance of the smart meter data, the main security objectives of the AMI communication network is to guarantee data confidentiality. However, the large number of devices deployed in the AMI renders the management of the overall security a challenging task. In this subsection, a two-player noncooperative security game is proposed for the AMI communication network. The attacker's objective is to attack the AMI devices in order to compromise data sent from these devices to the electric utility. Correspondingly, the defender intends to choose which security mode to enable on each device in order to protect the maximum amount of data from the attacker.

1) System Model: Consider the AMI communication network as a tree-pattern architecture $\mathcal{T}$ with one root node, where nodes represent the AMI devices. We refer the root node of $\mathcal{T}$ by 1, and let $\mathcal{V} = \{1, 2, ..., Y\}$ be the set of nodes in $\mathcal{T}$, where Y is the total number of nodes. Each node $i \in \mathcal{V} \setminus \{1\}$ collects data from its children nodes $Ch(i)$, aggregates it, and finally sends it to its parent node $f(i)$. We consider that there exists N aggregation levels, and let L_i be the set of nodes that belong to the i-th aggregation level, where each node can only belong to one aggregation level. Smart meters are denoted by nodes that belong to L_N.

Data on each node i has a value or security asset W_i, which quantifies the loss in data confidentiality if node i is attacked successfully. These values can be quantified as a result of the application of a security risk assessment method [102]. The parent node i collects data from all its children $Ch(i)$. A node could be responsible of processing and analyzing a set of the data collected from its children. The result of this analysis is then sent with the aggregated data from children nodes to the parent node. Therefore, we consider that $W_i \geq \sum_{j \in Ch(i)} W_j$. The value of data on node i is the sum of the value of data generated by the node in addition to the value of data collected from its children. Finally, let $\mathcal{L}(\mathcal{T})$ be the set of leaves of the tree $\mathcal{T}$. We refer by ∇_i^k, the number of children of node $i \in L_m$ at level $k > m$, and W_i^r the security asset of the parent of node $i \in L_m$ at level $r < m$. As notations, let $\nabla_i^k = 1$ and $W_i^k = W_i, \forall i \in L_k$.

For data confidentiality attacks in the AMI communication network, the attacker aims to intercept data by attacking the nodes without being detected. If the attacker wants to intercept data sent by node i, it can either attack node i or attack the parent node of i. We consider that encryption keys are stored in a cryptoprocessor that cannot be accessed by the attacker. The inbound data arrive at a device and is decrypted using the appropriate cryptographic key, processed and then encrypted using a different key. The attacker has no access or control on the decryption and encryption processes. Correspondingly, on each node, the defender can choose one of a set of security modes available on that node. The defender chooses an encryption level of outbound data on each node. For example, if 100 packets are sent from the node, the defender chooses how many packets need to be encrypted. We consider that data on each communication link is encrypted with different encryption keys or using different encryption algorithms. At the root node, data is encrypted for storage after being analyzed.

2) Game Theoretic Formulation and Results: To determine the interactions between the attacker and the defender, a two-player static noncooperative game is formulated in. For the attacker, the strategy is defined as the probability p_i of attacking node i, which is subject to a budget constraint $\sum_i p_i \leq P \leq 1(0 \leq p_i \leq 1, \forall i)$. In contrast, the defender's strategy is defined as the encryption rate s_i of the packets at node i, which is subject to a budget constraint $\sum_i s_i \leq S \leq Y(0 \leq s_i \leq 1, \forall i)$. We consider that on each node, an Intrusion Detection System (IDS) is installed with a detection rate of a. The IDS can be a combination of hardware and software detection capabilities.

In general, defense mechanisms deployed to protect a device depend on the value of data generated, stored, or processed by that device. The efficiency, robustness and therefore the cost of the countermeasures deployed by administrators to protect devices are often proportional to the value of the assets on these devices. The attacker's effort to compromise data on a device increases with defense measures deployed to protect that device which depend on the value of its assets. Therefore, we consider that the cost of attacking and encrypting data on node i are proportional to the value of the data W_i and are given by C_aW_i and C_eW_i respectively, where $0 \leq C_a, C_e \leq 1$.

To intercept data sent by node i, the attacker can choose either to attack node i or its parent node $f(i)$. Therefore, the probability of compromising unencrypted data sent by i with an encryption level of s_i for W_i without being detected is given by $W_i(p_i+p_{f(i)})(1-a)(1-s_i)$. We assume that $1-a > C_a$. Otherwise, the attacker has no incentive to attack since the cost to attack is greater than the payoff when the attack is successful and undetected. The utility functions U_A and U_D of the attacker and the defender respectively are as follows:

$$\begin{aligned} U_A(p,s) =& \sum_{i\in\mathcal{V}}(W_i(p_i+p_{f(i)})(1-a)(1-s_i)-p_iC_aW_i) \\ =& \sum_{i\in\mathcal{V}}(W_ip_i(1-a)(1-s_i)-p_iC_aW_i)+\sum_{i\in\mathcal{V},i\notin L-N}\sum_{j\in Ch(i)}p_iW_i(1-a)(1-s_j) \end{aligned} \tag{4.4}$$

$$U_D(p,s) = -\sum_{i\in\mathcal{V}}(W_ip_i(1-a)(1-s_i)+s_iC_eW_i)-\sum_{i\in\mathcal{V},i\notin L-N}\sum_{j\in Ch(i)}p_iW_i(1-a)(1-s_j) \tag{4.5}$$

The attacker and the defender have complete knowledge of the architecture of the system. The *Nash equilibrium* is considered as the most profitable strategy profile that gives each player the maximum utility given the actions of other players. Let $p=(p_1,...,p_Y)\in\mathcal{P}$ and $s=(s_1,...,s_Y)\in\mathcal{S}$ be the strategy profiles of the attacker and the defender respectively, where $\mathcal{P}$ and $\mathcal{S}$ refer to the strategy spaces of each player. The Nash equilibrium of the proposed game is defined as follows:

Definition 4.3.1 *A Nash equilibrium is a strategy profile $(\boldsymbol{p}^*,\boldsymbol{s}^*)$ in which each player cannot improve his utility by altering his decision unilaterally. More precisely, we have: $U_A(p^*,s^*)\geq U_A(p,s^*),\forall p\in\mathcal{P}$, and $U_D(p^*,s^*)\geq U_A(p^*,s),\forall s\in\mathcal{S}$.*

3) Future Opportunities: The noncooperative game model studied in [102] can be used as a basis to analyze data confidentiality attacks on the AMI communication network. In fact, several future opportunities for extending the work in [102] can be explored:

- Studying the impact of false alarm rates for the detection of attacks on players' behaviors.

- Introducing additional players and strategies into the game that enables analyzing the data confidentiality attack targeted at multiple AMI devices simultaneously, or studying choosing different possible encryption algorithms on each device.
- Proposing dynamic noncooperative game models that can capture the instantaneous state changes in the AMI communication network.
- Analyzing the impact of both the attacker's and defender's information sets on the optimal attack and defense strategy selections.
- Proposing a practical implementation that can be used as an AMI communication testbed to evaluate the defender's Nash equilibrium strategies against the data confidentiality attacks.

In the security domain, the defenders often deploy defense countermeasures based on the value of the assets available to protect and potential threats from attackers. Due to strict defense budgets, defenders must consider the possible actions of attackers while intelligently allocate defense resources. Clearly, noncooperative games could become a foundation for analyzing this type of interactions between attackers and defenders, and eventually identify the optimal defense strategy.

4.3.3 Game Theoretic Methods for Smart Meters

The proliferation and cyber-physical nature of smart meters have rendered them vulnerable to both cyber and physical attacks. Particularly, *electricity theft*, such as Meter Manipulation and FDIA, where malicious attackers alter usage measurements collected by smart meters, is a major challenge of these attacks [103–105]. According to the U.S. Energy Information Administration, in 2016, between 1.5 and 2% of electricity in the U.S. was lost due to theft, costing utilities as much as $\$6$ billion annually. Traditional research on electricity theft detection has focused on employing specific devices, like wireless sensors and balance meters, which have a high electricity theft detection accuracy [106,107]. In [106], an AMI intrusion detection system was proposed to accurately detect electricity theft, where anti-tampering sensors were embedded into smart meters. A set of trusted balanced meters were implemented in the distribution network of smart grid in order to detect electricity theft [107]. Although these research works do reduce the risks due to unmeasured and non-billed usage of electricity, they do not identify specific meters being compromised. Furthermore, these methods significantly increase the cost of deploying and operating millions of smart meters.

Additionally, statistics and machine learning have been used to train a classifier based on detailed electricity usage measurements [108–110]. Average historical electricity usage under the same conditions was used for constructing an electricity theft detector; an alarm was raised if the average usage was below a predefined detection threshold. Principal Component Analysis (PCA) based anomaly detection was proposed in [108], where anomalies were deviations from the normal usage behavior. In [109], usage data was proved to be non-stationary, and Auto-Regressive Integrated Moving Average (ARIMA) forecasting methods were proposed to validate readings. A Consumption Pattern-Based Energy Theft Detector (CPBETD) that employed a multi-class Support Vector Machine (SVM) for each customer was formulated in [110]. However, these works ignored the attack models of potential thieves, and the effectiveness of anomaly detector was only evaluated based on a dataset of attack examples.

1) Game Formulation and Results: Consider an electric utility serving a set of customers, denoted by $\mathcal{N} := \{1, ..., N\}$. Assuming these customers have a similar preference of electricity usage, they can be separated into two classes: *normal customers* and *thieves*. Let $\mathcal{M} := \{1, ..., M\} \subseteq \mathcal{N}$ be the set of thieves among the N customers of an electric utility. Then, a single leader, multi-follower Stackelberg game is formulated in [111] between the utility and M thieves to characterize and analyze strategic interactions between the two. In this game, a subset from N customers is chosen for an anomaly detection test $\mathcal{D}$, aiming to reduce NTLs. Based on the limited sampling rate l, the utility intends to maximize detection probability and minimize false positives, while the thieves interact with one another using a non-cooperative game to identify optimal quantities of electricity to steal in response to the utility's detection strategy.

The noncooperative game of M thieves is formulated, $\Xi := \langle \mathcal{M}, (\mathcal{A}_i)_{i\in\mathcal{M}}, (R_i)_{i\in\mathcal{M}} \rangle$, where $\mathcal{M}$ is the set of M thieves. $\mathcal{A}_i$ is the set of actions available to thief $i \in \mathcal{M}$, where $\boldsymbol{a}_i \in \mathcal{A}_i$ is represented by the expected amount of consumed and stolen electricity by thief i, denoted by q_i and q_i^S, respectively. Additionally, $R_i(\boldsymbol{a}_i)$ is the reward function of thief i under action $\boldsymbol{a}_i$. Thus, thief i selects an action $\boldsymbol{a}_i := \{q_i, q_i^S\}$ that maximizes its reward R_i, which can be defined as below:

$$R_i(q_i, q_i^S) := B(q_i^S) - p_i^D(l, q_i^S)P(q_i^S), \tag{4.6}$$

where $B(\cdot)$ represents the utility's electricity billing function; $B(q_i^S)$ gives the amount of the electricity bill that is not paid by thief i; $p_i^D(l, q_i^S)$ denotes the probability of thief i being detected when the sampling rate is l and the amount of stolen electricity is q_i^S; and $P(q_i^S)$ indicates the penalty function activated upon the successful detection of thief i for stealing a power of q_i^S.

One popular solution of the thieves' game is the Generalized Nash Equilibrium (GNE):

Definition 4.3.2 *Consider the noncooperative game $\Xi := \langle \mathcal{M}, (\mathcal{A}_i)_{i\in\mathcal{M}}, (R_i)_{i\in\mathcal{M}} \rangle$. GNE is a state of the game in which each electricity thief aims at maximizing its rewards. As a response to optimal chosen actions of other thieves, a thief aims at choosing the actions, in the restricting subset dictated by the choice of other thieves that maximizes their own reward.*

Under the derived GNE of M thieves, the utility needs to selects a defense action, $\mathbf{a}_0$, that maximizes its reward, R_0. It is assumed that the utility's defense action is determined by two variables including: (1) Detection mechanism, $\mathcal{D}$, used to identify electricity theft, and (2) Customer sampling rate, l. The objective of the utility is to maximize the following problem:

$$\max_{\mathcal{D},l} \quad R_0 := \sum_{i \in \mathcal{M}} p_i^D(l, q_i^S) P(q_i^S), \quad \text{s.t.} \quad 0 \leq p_i^E(l, q_i^S) \leq p_{i\max}^E, \quad 0 \leq l \leq l_{\max}, \tag{4.7}$$

where q_i^S is derived from the GNE of the proposed noncooperative game Ξ; $p_i^E(l, q_i^S)$ represents the false alarm probability for thief i; $p_{i\max}^D$ gives the constraint of the false alarm probability for thief i; and $l_{\max}$ indicates sampling rate limitation for the utility. The Stackelberg solution concept is adequate for games with hierarchy in which the leader enforces its strategy and the followers respond, rationally (i.e. optimally), to the leader's strategy. The optimal response of M thieves to an action $\mathbf{a}_0$ by the utility is written as $\mathcal{A}^{\text{theft}}(\mathbf{a}_0) = \{\mathbf{a}_1^*, ..., \mathbf{a}_M^*\}$. This optimal strategy denotes the equilibrium strategy profile of the attackers as a response to the defender's strategy. In this regard, $\mathbf{a}_0^* \in \mathcal{A}_0$ is a *Stackelberg equilibrium* if it minimizes the utility's reward function, R_0. In other words,

$$R_0(\mathbf{a}_0^*, \mathcal{A}^{\text{theft}}) \leq R_0(\mathbf{a}_0, \mathcal{A}^{\text{theft}}), \forall \mathbf{a}_0 \in \mathcal{A}_0. \tag{4.8}$$

In the Stackelberg equilibrium, the optimal customer sampling rate l and the threshold selected for the the detection mechanism $\mathcal{D}$ can be derived; then they determine the detection probability p_i^D and false alarm probability p_i^E, $i \in \mathcal{N}$. In the thieves' game, M thieves make their decisions simultaneously at each step of the evolutionary process, playing a GNE between themselves. A multimodal Genetic Algorithm is implemented for computing the Stackelberg equilibrium for the utility.

2) Further Opportunities: Essentially, the work in [111] establishes how the Stackerlberg game theory can be used to study the adversarial nature of the electricity theft problem. The game-theoretic framework proposed in this work can help analyze equilibrium consumer and distributor choices in scenarios where the assumptions on consumer utilities and distributor's profit function are applicable. Moreover, one can envision several future directions that build upon [111], as follows:

- Investigating the impact of the privacy-preserving demand response on the optimal sampling rate selection.
- Exploring how the sampling interval of smart meters affects the ability of the distribution utility to identify anomalies and electricity theft.
- Developing utility functions that capture not only the expected electricity stolen, but also the prices during energy trade and the costs for the communication overhead.
- Analyzing the interactions between the M electricity thieves using classical cooperative games.
- Proposing effective algorithms that can identify optimal and stable associations between the electric utility that acts a leader and millions of electricity thieves as followers.

Beyond [111], the application of Stackerlberg games for detecting electricity theft is also discussed in [112], in which the objective of the attacker is set to find the optimal amount of electricity stolen, while minimizing the expected probability being detected. A summary of the different applications of game theory for cyber-physical security in the AMI is shown in Table 4.2.

4.4 Game Theory for Cyber-Physical Security in Smart Grid Zone 3

The *State Estimation* (SE) of the smart grid is an essential function for the wide area system monitoring and control in the Smart Grid Zone 3, which is an important part

Table 4.2: Summary of Game Theoretic Techniques for Security in AMI.

Application	**Game Theoretic Features**	**Main Future Extensions**
Data Confidentiality Attack in AMI Communication Network [102]	• Two-player (Attacker vs Defender) • Finite Action Set • Nonzero-sum Utility • Deterministic • Complete Information • Static game	• Studying the impact of false alarm rates for the detection of attacks on players' behaviors. • Introducing additional players and strategies into the game. • Proposing dynamic noncooperative game models. • Analyzing the impact of the attacker and defender's information sets. • Proposing a practical AMI communication testbed for evaluation.
Electricity Theft in Smart Meters [111]	• Multiple-player (Defender vs Multiple Attackers) • Finite Action Set • Nonzero-sum Utility • Deterministic • Complete Information • Stackerlberg game	• Investigating the impact of the privacy-preserving demand response. • Exploring the impact of the sampling interval of electricity theft. • Developing utility functions that capture the price change in the market. • Analyzing the cooperative interactions between the M electricity thieves. • Proposing effective algorithms for game including millions of electricity thieves.

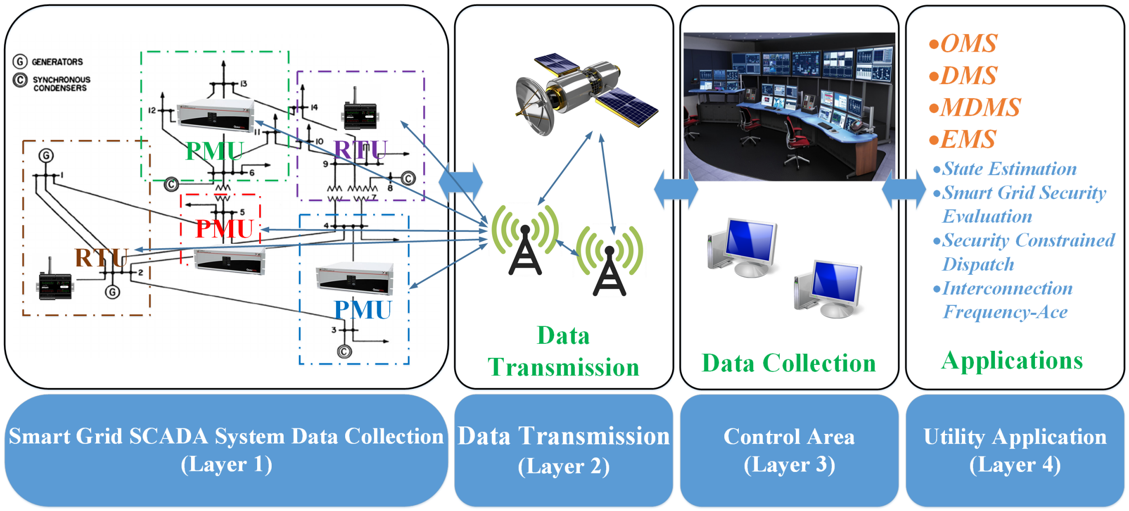

GENERATORS
SYNCHRONOUS CONDENSERS
PMU
RTU
PMU
RTU
PMU
Data Transmission
Data Collection
•OMS
•DMS
•MDMS
•EMS
•State Estimation
•Smart Grid Security Evaluation
•Security Constrained Dispatch
•Interconnection Frequency-Ace
Applications
Smart Grid SCADA System Data Collection (Layer 1)
Data Transmission (Layer 2)
Control Area (Layer 3)
Utility Application (Layer 4)

Figure 4.2: The network model of smart grid state estimation and its connections with system monitoring and control.

of the modern Energy Management System (EMS), as shown in Figure 4.2. The smart grid SE uses the redundancy of measurement data provided by SCADA to improve the accuracy of data, automatically exclude error messages caused by random interference, and estimate or forecast the running state of the system. In this section, an overview of the mathematical model of SE and the false data inject attack targeted at SE will be provided. Then, the application of Stackelberg games for analyzing FDIAs in the smart grid SE will be studied in detail. Finally, insights on future game-theoretic approaches for enhancing cyber-physical security within the SE systems will be discussed.

4.4.1 Introduction to Security Threats in State Estimation

A smart grid SE uses multiple power measurements collected throughout the grid to estimate the system states. The relation between the measurement vector $\boldsymbol{z}$, and the vector of system states $\boldsymbol{\theta}$, in a linearized SE model can be expressed as $\boldsymbol{z} = \boldsymbol{H}\boldsymbol{\theta} + \boldsymbol{e}$, where $\boldsymbol{H}$ is the measurement Jacobian matrix and $\boldsymbol{e}$ is the vector of random errors assumed to follow a normal distribution $N(0, \boldsymbol{R})$. Using a Weighted Least Square (WLS) estimator, the estimated system states are given by $\hat{\boldsymbol{\theta}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z}$. Using the estimated states, an estimate of the measurement vector can be calculated as $\hat{\boldsymbol{z}} = \boldsymbol{H}\hat{\boldsymbol{\theta}} = \boldsymbol{S}\boldsymbol{z}$, and residual $\boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = (\boldsymbol{I}_n - \boldsymbol{S})\boldsymbol{z} = \boldsymbol{W}\boldsymbol{z}$, where $\boldsymbol{I}_n$ is the identity matrix of size $(n \times n)$, and n is the total number of collected measurements.

The WLS estimator is the maximum likelihood estimator for locating the system states, but the estimated system states have zero robustness against faulty data, either caused by random network errors or malicious attacks. Evidently, a secure and efficient power system requires an accurate state estimation that truthfully reflects the system operating state. The state estimator commonly uses a bad data detection (BDD) mechanism to filter fault data, which typically implements the Chi-squares test over the sum of the squares of the residuals. $\|\boldsymbol{r}\|_2^2 = \sum_{i=1}^{n} r_i^2$ follows a χ^2 distribution with $n - N_\theta$ degrees of freedom, where N_θ is the number of states to be estimated; the residuals must satisfy $\|\boldsymbol{r}\|_2 \leq \tau$, where τ is a detection threshold. Hence, for a measurement set to be considered free from bad data, the residuals must satisfy $\|\boldsymbol{r}\|_2 \leq \tau$, where τ is a detection threshold.

However, BDD is unable to detect some structured collaborating injection attacks that are disguised as normal measurements. One common cyber attack in smart grids is FDIA, which distorts the measurements collected by the system operator through either physical device compromise or remote cyber-data injection. Due to its ability to compromise the state estimation, an adversary capable of false-date injecting can have devastating effects, such as exploiting profits from electricity price manipulation in the power market and causing a regional blackout, which could potentially induce financial chaos. The Stackelberg game-theoretic approach in [113] is described in detail in order to give more insight about cyber-physical security problems.

4.4.2 Stackelberg Game for False Data Injection Attacks in SE

1) Game Formulation and Results: Consider M attackers implementing a FDIA targeted at the smart grid SE, and the defender intends to secure a set of measurements in order to decrease the aggregate effect of the FDIA on the system. In [113], a single leader, multi-follower Stackelberg game between the defender and the M attackers is formulated to capture and analyze their strategic interactions. In this game, the defender acts as a leader who selects a set of measurements to defend the SE from the potential FDIA attacks. The M attackers interact with one another by using a followers' noncooperative game to identify the optimal FDIA attack based on the defender's strategy.

The noncooperative game between M attackers is formulated in its normal form as follows: $\Xi = \langle \mathcal{M}, \{\mathcal{Z}_m\}_{m\in\mathcal{M}}, \{U_m\}_{m\in\mathcal{M}}\rangle$, where $\mathcal{M}$ is the set of M attackers, $\mathcal{Z}_m$ is the set of FDIA actions available to attacker $m \in \mathcal{M}$, and U_m is the utility function of attacker m. Thus, each attacker, $m \in \mathcal{M}$, selects an attack vector, $z_m \in \mathcal{Z}_m$, that maximizes its utility, U_m. For each attacker m, let $\mathcal{K}_m$ denote the subset of measurements that can be attacked by m. Hence, $\mathcal{Z}_m$ can be represented by a column vector with elements equal to 0 except for those in $\mathcal{K}_m$ which can take values within a compact range reflecting the range of magnitude of the attack.

The utility function U_m for each attacker m can be defined as the financial benefit obtained by virtual bidding. In virtual bidding, attacker m buys and sells P_m MW at buses i_m and j_m in day ahead, respectively, while, conversely, attacker m sells and buys P_m MW at, buses i_m and j_m, respectively. Thus, the goal of attacker $m \in \mathcal{M}$ is to optimize:

$$\begin{aligned} \max_{z_m \in \mathcal{Z}_m} \quad & U_m(z_m, z_m^{-1}) = [(\mu_{i_m}^{RT} - \mu_{i_m}^{DA}) + (\mu_{j_m}^{DA} - \mu_{j_m}^{RT})]P_m - c_m(z_m), \\ \text{s.t.} \quad & \|\boldsymbol{W} z_m\|_2 + \sum_{l=1, l\neq m}^{M} \|\boldsymbol{W} z_l\|_2 \leq \epsilon_m, \end{aligned} \tag{4.9}$$

where $c_m(z_m)$ is the cost of attack, and z_m^{-1} is the strategy vector of all players except m.

Based on the equilibrium of the followers, the grid defender selects a defense vector $\boldsymbol{a}_0$ that determines which measurements to be secured from the FDIA attacks. The objective of the defender is to minimize a cost function that captures the variation between the day ahead and real-time prices on all buses in the system:

$$\begin{aligned} \min_{\boldsymbol{a}_0 \in \mathcal{A}_0} \quad & U_0(\boldsymbol{a}_m, \boldsymbol{a}_{-0}) = P_L \sqrt{\frac{1}{N} \sum_{i=1}^{N} (\mu_{i_m}^{RT} - \mu_{i_m}^{DA})^2} + c_0(\boldsymbol{a}_0), \\ \text{s.t.} \quad & \|\boldsymbol{a}_0\|_2 \leq B_0, \end{aligned} \tag{4.10}$$

where $c_0(\boldsymbol{a}_0)$ is the cost of defense, P_L is the total system load, and B_0 is the limit on the number of measurements that the operator can defend simultaneously.

The Stackelberg solution concept is adequate for games with a hierarchy in which the leader enforces its strategy and the followers respond, rationally (i.e., optimally), to the leader's strategy. The optimal response of the attackers to action $\boldsymbol{a}_0$ played by the defender is denoted by $\mathcal{R}^{\text{att}}(\boldsymbol{a}_0) \triangleq \{z_1^*(\boldsymbol{a}_0), ..., z_M^*(\boldsymbol{a}_0)\}$. This optimal strategy denotes the equilibrium strategy profile of the attackers as a response to the defender's strategy. In this regard, $\boldsymbol{a}_0^* \in \mathcal{A}_0$ is a Stackelberg equilibrium if it minimizes the leader's (i.e., defender's) utility function U_0. In other words,

$$U_0(\boldsymbol{a}_0^*, \mathcal{R}^{\text{att}}(\boldsymbol{a}_0^*)) \leq U_0(\boldsymbol{a}_0, \mathcal{R}^{\text{att}}(\boldsymbol{a}_0)), \forall \boldsymbol{a}_0 \in \mathcal{A}_0. \tag{4.11}$$

2) Further Opportunities: The work in [113] provides a Stackerlberg game theoretic approach in order to analyze the strategic interactions between the defender and multiple attackers, which intend to inject FDIA into the smart grid SE. Based on this work, several future directions can be pursed, such as:

- Investigating the multiple-stage sequence game by integrating the defender's FDIA mitigation strategy if the attack is successfully detected.
- Developing utility functions that capture not only the expected price changes during energy trade, but also the physical impact for the grid operation.

- Analyzing the interactions between the M FDIA attackers by using classical cooperative games.

4.5 Summary

In this survey, a comprehensive overview on the applications of noncooperative game theory for analyzing the cyber-physical security of the smart grid, which was divided into three zones, was provided. The smart grid analysis was carefully drawn from a broad range of cyber and physical security issues spanning key elements such as the network layer, AMI and state estimation. In each zone, the main cyber-physical security threats were presented and an elaborate discussion on how noncooperative game theory can be applied to address these challenges was presented. Moreover, several future directions for extending these approaches and adopting advanced game theoretic techniques was provided, so as to reduce the gap between theoretical models and practical implementations of future smart grids. Essentially, from the surveyed works, it can be clearly noted that noncooperative game theory has a strong potential to provide solutions for pertinent cyber-physical security problems within the smart grid; however, these theoretic applications face many design challenges. It can also noted that many of the existing works have focused on classical static noncooperative games. Hence, for future works, it is of interest to investigate dynamic game models (both in cooperative and noncooperative settings) and their applications within smart grid systems.

CHAPTER 5

Risk Assessment of Coordinated Cyber-Physical Attacks in Smart Grid

In this chapter, the risk assessment of the coordinated cyber-physical attacks against power grids is investigated using a novel game-theoretic approach. Section 5.1 makes an overview of the cyber-physical security issues in the smart grid. Section 5.2 presents the attack-defense scenario in the power grid as well as the formulated stochastic game. Section 5.3 introduces an optimal load shedding technology to quantify the attacker and defender's rewards. Then, Section 5.4 derives the Nash equilibrium of the proposed stochastic game, and computes the risk of the coordinated cyber-physical attack faced by the grid based on the probability of successful attack and corresponding physical impacts. Section 5.5 presents the simulation results while Section 5.6 concludes the chapter.

5.1 Overview

The modern electric power grid constitutes the backbone of any nation's economy. The cyber-physical nature of its critical infrastructures facilitates its effective operation, monitoring and control, but renders it to be a high priority target for a range of malicious attacks in cyber and physical domains [114]. Indeed, the security of the grid is not guaranteed at all times, and some element failures can cause significant problems for the producers and consumers of electricity. For example, the Blackout on August 14, 2003 [115] showed that even a single transmission line outage has cascading effects on an area with an estimate of 50 million people and 61,800 megawatts (MW) of electric load in the Northeastern and Midwestern United States and the Canadian province of Ontario. The North American Electric Reliability Corporation (NERC) traditionally requires that the bulk electric power grid in an operation state should be able to transition into another operation state in case of one element failure, commonly referenced as the N-1 contingency criteria [116].

Compared with accidental single element failures, the well-organized *coordinated cyber-physical attacks* can not only lead to severe physical damages to the grid, but may also potentially nullify the functionality of existing defense mechanisms. A class of coordinated cyber-physical attacks was presented in [117] whereby physical transmission line attacks and corresponding false data injection attacks were considered. False data injection attacks, as a special case of cyber attacks, can be implemented into the power grid state estimation to mask the line outages caused by these physical attacks, and potentially exasperate outages to trigger cascading failures. As a result, risk analysis of coordinated attacks and devising defense countermeasures are both challenging and desirable.

Risk assessment is identified as a critical part of the security framework by most power grid standards and guidelines [118]. *Attack graph* is a common starting point for most of the work in this area [50, 119–121]. An attack graph-based framework was developed in [120] to assess the risk faced by the power grid control systems, in which the cyber attack targeted at control systems was graphed in a tree structure, and the risk was quantified according to existing defense mechanisms. In [121], a privilege graph was introduced to analyze all potential attack paths that can be exploited by the attacker in the advanced metering infrastructure (AMI) system, and an exposure metric was derived for evaluating the vulnerability of the system. In [122], a mathematical risk assessment framework was proposed as an alternative to attack graphs for analyzing coordinated cyber attacks against the supervisory control and data acquisition (SCADA) system of the power grid. This work defined the risk of coordinated cyber attacks as the product of probability of successful cyber intrusion and resulting power grid impacts.

Furthermore, due to the multi-faced decision making process involved in the power grid protection against coordinated cyber-physical attacks, a noncooperative game-theoretic approach was introduced in [123] to analyze the interactions between an intelligent attacker and the grid defender. Also, the attack probability to various elements of the grid at the game's equilibrium was used to assess the risk associated with them. In [124], a zero-sum static game between a malicious attacker and the grid operator was proposed to compute optimal defense budget allocation strategies that seek to protect physical infrastructures of the power grid against physical attacks. Risk faced by each physical infrastructure was determined by corresponding defense budget allocation. In [125], a general-sum game-theoretic framework was proposed to explore and evaluate strategies for the power grid defender to protect the grid against a variety of physical and cyber attacks, where the attack and defense resource limitations were considered. Optimal attack/defense resource allocation strategies at the game's equilibrium were used for risk analysis of each power grid element.

However, the works in [123–125] depend on static game frameworks, in which the interactions and decision making processes between the attacker and defender are assumed to be one-shot events. In [36, 51], the dynamic game theory was introduced for modeling the attack-defense scenarios in the power grid while factoring in the dynamic nature of the power grid protection. The Nash equilibrium of the formulated dynamic game was derived for guiding the grid defender to optimally protect power grid elements at different system states.

The main contribution of this chapter is to develop a new game-theoretic framework for assessing the risk faced by a power grid in terms of coordinated cyber-physical attacks. In order to characterize the dynamic nature of the grid protection, this problem is formulated as a stochastic budget allocation game between a malicious attacker and the grid defender. An optimal load shedding problem is proposed to quantify the amount of shed load under coordinated attacks representing their physical impacts on the power grid. Taking these physical impacts as the two players' rewards, a novel learning algorithm is devised to enable the two players to reach the Nash equilibrium of the game while maximizing their respective minimum rewards in a sequence of stages. The attacker's budget allocation strategies at such game's equilibrium are implemented to assess the vulnerability associated with each grid element. Furthermore, the risk of a coordinated cyber-physical attack faced by the whole power grid at various states can be evaluated based on the information about the successful attack probability to various elements. Simulation results using the IEEE 9-bus system are presented to illustrate the proposed framework and deriving different risk under different attack/defense budget limitations.

5.2 Problem Statement and Game Formulation

In this section, we first present the problem of power grid protection against coordinated cyber-physical attacks and then, formulate a stochastic budget allocation game between the attacker and defender. Main notations are listed in Table 5.1.

5.2.1 Problem Statement

We consider an electric power grid system consisting of N_B buses including N_g generation buses and N_l load buses and N_T transmission lines. The network topology of this system can be abstracted as a digraph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ with size N_B denotes the set of all power buses (vertices), and $\mathcal{E}$ denotes the set of N_T transmission lines (edges). The total number of elements (vertices and edges) of the system that must be defended against coordinated cyber-physical attacks is $N_G = N_B + N_T$.

A malicious attacker aims to disrupt the system by allocating its limited attack budgets over N_G system elements, in order to bring the maximum physical damage to the system. The budgets possessed by the attacker can contain 1) human budgets such as hackers and terrorists, 2) technological budgets such as electrical tools and malwares, and 3) economic

Table 5.1: Summary of Notations

Symbol	Description
i	a power grid element's index
N_B	the number of power buses
N_g	the number of generation buses
N_l	the number of load buses
N_T	the number of transmission lines
N_G	the total number of system elements to be protected
$\mathcal{G}$	electric power grid digraph
$\mathcal{V}$	vertex set of power grid digraph
$\mathcal{E}$	edge set of power grid digraph
$\mathcal{A}(\mathcal{D})$	attacker's (defender's) action space
$\boldsymbol{a}(\boldsymbol{d})$	attacker's (defender's) action vector
$\Pi_{\mathcal{A}}(\Pi_{\mathcal{D}})$	attacker's (defender's) mixed strategy space
$\boldsymbol{\pi}_{\mathcal{A}}(\boldsymbol{\pi}_{\mathcal{D}})$	attacker's (defender's) mixed strategy
$B^{\mathcal{A}}(B^{\mathcal{D}})$	the maximum attack (defense) budget
$b_i^{\mathcal{A}}(b_i^{\mathcal{D}})$	attack (defense) budget implemented for element i
$R^{\mathcal{A}}(R^{\mathcal{D}})$	attacker's (defender's) expected reward
$\mathcal{S}$	power grid state space
s	a power grid's state
T	state transition probability
p_i^{fail}	fail probability of normal element i
p_i^{rec}	recovery probability of failed element i
γ	discount factor to the overall reward
Q	the discounted-sum reward

budgets. Let $\mathcal{A}$ be the action space of the attacker, and $B^{\mathcal{A}}$ be the maximum budget that can be implemented for attacking N_G system elements at a time. Each attack action $\boldsymbol{a} \in \mathcal{A}$ can be defined as a vector of allocating $B^{\mathcal{A}}$ budgets over N_G system elements: $\boldsymbol{a} = [b_1^{\mathcal{A}}, b_2^{\mathcal{A}}, ..., b_{N_G}^{\mathcal{A}}]^T$, each element denotes the budget that action $\boldsymbol{a}$ implements for the corresponding element, and $\sum_{i=1}^{N_G} b_i^{\mathcal{A}} = B^{\mathcal{A}}$. For example, the attacker may allocate a part of technological budgets on launching a false data injection attack over poorly protected wireless channels to block the communication between command control center and remote senors. Alternatively, the attacker may plan to distribute several economic budgets on a physical attack on high voltage (HV) transmission lines.

Correspondingly, in order to minimize the risk of the attacks against the system, the system defender (administrator) needs to distribute its finite defense budgets over N_G system elements to protect normal elements or to repair broken elements. The budgets possessed by the defender can contain: 1) human budgets such as users, administrators, and maintenance staff, b) technological budgets such as advanced operation systems and monitoring softwares, and c) economic budgets. Let $\mathcal{D}$ be the action space of the defender, and $B^{\mathcal{D}}$ be the maximum defense budget that can be implemented at a time. Then, each defense action $\boldsymbol{d} \in \mathcal{D}$ conditions one vector to distribute its limited defense budgets over N_G elements of the system: $\boldsymbol{d} = [b_1^{\mathcal{D}}, b_2^{\mathcal{D}}, ..., b_{N_G}^{\mathcal{D}}]^T$, whose element is the defense budget in action $\boldsymbol{d}$ that committed to the corresponding element, and $\sum_{j=1}^{N_G} b_j^{\mathcal{D}} = B_{\mathcal{D}}$. Therefore, the attacker's (defender's) action space $\mathcal{A}$ ($\mathcal{D}$) includes all possible methods of allocating its limited budgets over N_G system elements.

5.2.2 Game Formulation

The interactions and decision making processes between the attacker and defender are analyzed using the *dynamic noncooperative game theory* [57, 67–69, 126]. In particular, we formulate a two-player, discrete time stochastic budget allocation game $\Xi = \langle \mathcal{S}, \mathcal{A}, \mathcal{D}, R^{\mathcal{A}}, R^{\mathcal{D}}, T \rangle$, whose key elements are shown as follows:

- $\mathcal{S}$: Power grid state space, where each state $s \in \mathcal{S}$ is associated with the status of N_G grid elements.
- $\mathcal{A}$: Action space of the attacker, where each attack action $\boldsymbol{a} \in \mathcal{A}$ represents a method of allocating the attack budget over N_G grid elements.
- $\mathcal{D}$: Action space of the defender, where each defense action $\boldsymbol{d} \in \mathcal{D}$ conditions a defense budget allocation over N_G grid elements.

- $\Pi(\mathcal{A})$ $(\Pi(\mathcal{D}))$: Mixed strategy space of the attacker (defender), where each mixed strategy $\boldsymbol{\pi}_{\mathcal{A}} \in \Pi(\mathcal{A})$ $(\boldsymbol{\pi}_{\mathcal{D}} \in \Pi(\mathcal{D}))$ yields a probability distribution over action space $\mathcal{A}$ $(\mathcal{D})$.
- $R^{\mathcal{A}}(s, \boldsymbol{a}, \boldsymbol{d})$ $(R^{\mathcal{D}}(s, \boldsymbol{a}, \boldsymbol{d}))$: Reward function for the attacker (defender), under a pair of attack and defense actions $(\boldsymbol{a}, \boldsymbol{d})$ at state $s \in \mathcal{S}$.
- $T_{s,s'}(\boldsymbol{a}, \boldsymbol{d})$: State transition probability from state $s \in \mathcal{S}$ to state $s' \in \mathcal{S}$ under a pair of attack and defense actions $(\boldsymbol{a}, \boldsymbol{d})$.
- $p_i^{\text{fail}}(\boldsymbol{a}, \boldsymbol{d})$: Fail probability for normal element i failing under a pair of attack and defense actions $(\boldsymbol{a}, \boldsymbol{d})$.
- $p_i^{\text{rec}}(\boldsymbol{a}, \boldsymbol{d})$: Recovery probability for failed element i recovering under a pair of attack and defense actions $(\boldsymbol{a}, \boldsymbol{d})$.

The game is played over a finite state space $\mathcal{S}$, where each state is an enumeration of the status of N_G power grid elements in order. For instance, if we use ”1” and ”0” to denote the normal and failed statuses, respectively. Two states then can be defined as: state s_1: {1,1,...,1,1} for all elements being operated normally, and state s_2: {0,0,1,...,1,1} for all elements being operated normally except elements 1 and 2. The state transition probability $T_{s,s'}(a, d)$ is derived from corresponding probabilities $p_i^{\text{fail}}(a, d)$ and $p_i^{\text{rec}}(a, d)$, $i = 1, ..., N_G$, based on state s and s'. For example, $T_{s_1,s_2}(a, d) = p_1^{\text{fail}}(a, d) \times (1 - p_2^{\text{fail}}(a, d)) \times (1 - p_3^{\text{fail}}(a, d)) \times \cdots \times (1 - p_{N_G}^{\text{fail}}(a, d))$.

This game proceeds in time steps. In each time step of the game, the attacker takes an action $\boldsymbol{a} \in \mathcal{A}$, and, at the same time, the defender takes an action $\boldsymbol{d} \in \mathcal{D}$. The pair of players' actions $(\boldsymbol{a}, \boldsymbol{d})$ will bring a reward for each player at the current state $s \in \mathcal{S}$. Assume the attacker seeks to maximize the physical damage towards the system under the pair of actions $(\boldsymbol{a}, \boldsymbol{d})$, while the defender intends to minimize this damage. The attacker's reward will be the negative of the defender's reward at each time step, where $R^{\mathcal{A}}(s, \boldsymbol{a}, \boldsymbol{d}) = -R^{\mathcal{D}}(s, \boldsymbol{a}, \boldsymbol{d})$.

Thus far, the immediate rewards at each time step are defined for both players, but the proposed stochastic game Ξ still proceeds. In order to quantify the attacker and defender's overall rewards in Ξ, two players' immediate rewards derived at each time step should be aggregated together. A popularly used method for aggregating these immediate rewards is the discounted-sum method [127]. For a pair of attack and defense actions $(\boldsymbol{a}, \boldsymbol{d})$, the overall reward of the attacker can be defined the discounted sum of immediate rewards at each time step, with a discount factor $\gamma \in (0, 1)$:

$$Q^{\mathcal{A}} = \sum_{t=0}^{\infty} \gamma^t R^{\mathcal{A}}(s(t), \boldsymbol{a}, \boldsymbol{d}), \tag{5.1}$$

where γ^t represents the relative importance of the reward at the time step t in the overall reward $Q^{\mathcal{A}}$. Since the defender's reward is the negative of the attacker's reward at each time step, the defender's overall reward is just the negative of the attacker's overall reward, where $Q^{\mathcal{D}}(s, \boldsymbol{a}, \boldsymbol{d}) = -Q^{\mathcal{A}}(s, \boldsymbol{a}, \boldsymbol{d})$. Therefore, the proposed stochastic game Ξ is a *zero-sum stochastic game*.

The attacker and defender's optimal strategies for the proposed stochastic game Ξ are characterized by the concept of a closed-loop *Nash equilibrium* [68, 126]:

Definition 5.2.1 *The pair of attack and defense mixed strategies $(\boldsymbol{\pi}^*_{\mathcal{A}}, \boldsymbol{\pi}^*_{\mathcal{D}})$ is said to be a closed-loop Nash equilibrium of the proposed stochastic game $\Xi = \langle \mathcal{S}, \mathcal{A}, \mathcal{D}, R^{\mathcal{A}}, R^{\mathcal{D}}, T \rangle$, if, for all attack and defense strategies $\boldsymbol{\pi}(\mathcal{A}) \in \boldsymbol{\Pi}(\mathcal{A})$ and $\boldsymbol{\pi}_{\mathcal{D}} \in \boldsymbol{\Pi}_{\mathcal{D}}$, we have in state*

$s_i \in \mathcal{S}$, $i = 1, ..., N_{\mathcal{S}}$:

$$\begin{cases} \quad Q^{\mathcal{A}}(\boldsymbol{\pi}_{\mathcal{A}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{A}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_{N_{\mathcal{S}}}), \\ \qquad \boldsymbol{\pi}_{\mathcal{D}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{D}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_{N_{\mathcal{S}}})) \\ \geq Q^{\mathcal{A}}(\boldsymbol{\pi}_{\mathcal{A}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{A}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_{N_{\mathcal{S}}}), \\ \qquad \boldsymbol{\pi}_{\mathcal{D}}(s_1), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_{N_{\mathcal{S}}})), \\ \quad Q^{\mathcal{D}}(\boldsymbol{\pi}_{\mathcal{A}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{A}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_{N_{\mathcal{S}}}), \\ \qquad \boldsymbol{\pi}_{\mathcal{D}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{D}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_{N_{\mathcal{S}}})) \\ \geq Q^{\mathcal{D}}(\boldsymbol{\pi}_{\mathcal{A}}(s_1), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{A}}(s_{N_{\mathcal{S}}}), \\ \qquad \boldsymbol{\pi}_{\mathcal{D}}(s_1), ..., \boldsymbol{\pi}^*_{\mathcal{D}}(s_i), ..., \boldsymbol{\pi}_{\mathcal{D}}(s_{N_{\mathcal{S}}})). \end{cases} \tag{5.2}$$

The existence of a closed-loop Nash equilibrium for stochastic games is known only in some very special cases [128]. However, for the proposed stochastic game Ξ, if the attacker and defender's mixed strategies are limited to *stationary strategies*, we can present the existence of a closed-loop Nash equilibrium. First, the stationary strategy is defined as follows:

Definition 5.2.2 *For the proposed stochastic game $\Xi = \langle \mathcal{S}, \mathcal{A}, \mathcal{D}, R^{\mathcal{A}}, R^{\mathcal{D}}, T \rangle$, a stationary strategy is one in which the rule of choosing a mixed strategy is the same in each system state $s \in \mathcal{S}$, where the attacker and defender's mixed strategies satisfy for $\forall s \in \mathcal{S}$, $\boldsymbol{\pi}_{\mathcal{A}}(s) = \boldsymbol{\pi}_{\mathcal{A}}(s(t))$, and $\boldsymbol{\pi}_{\mathcal{D}}(s) = \boldsymbol{\pi}_{\mathcal{D}}(s(t))$, $\forall t$.*

Now, we can present the existence of Nash equilibrium in stationary strategies for the proposed stochastic game Ξ.

Theorem 5.2.3 *For the proposed stochastic game $\Xi = \langle \mathcal{S}, \mathcal{A}, \mathcal{D}, R^{\mathcal{A}}, R^{\mathcal{D}}, T \rangle$, if it satisfies that action sets $\mathcal{A}$ and $\mathcal{D}$ are finite and state transitions T are dominated by some probability measures on $\mathcal{S}$, there exists a stationary Nash equilibrium for each discount factor $\gamma \in (0, 1)$.*

This theorem was proved in a more general form in [129], in which the players' rewards and the discount factor γ may rely on time, and the state space $\mathcal{S}$ is a measurable space. If we assume that action sets $\mathcal{A}$ and $\mathcal{D}$ are finite and transition probabilities T are dominated by some probability measures on $\mathcal{S}$, the proposed stochastic game Ξ becomes as a special case of stochastic games given in [129].

5.3 Optimal Load Shedding

We now calculate the attack and defender's rewards $R^{\mathcal{A}}$ and $R^{\mathcal{D}}$ at each time step of the proposed stochastic game Ξ, which are determined by the physical damage under the pair of attack and defense actions $(\boldsymbol{a}, \boldsymbol{d})$. In the literature [130–132], such physical damage can be quantified by the cost of load that must be shed due to element failures, in which some load must to be cut off to avoid a cascading failure. For the power grid composed of N_B buses including N_g generation buses and N_l load buses, let $\boldsymbol{p} = [\boldsymbol{p}_g; \boldsymbol{p}_l]$ be the power distribution over N_B buses, where $\boldsymbol{p}_g \geq \mathbf{0}$ represents the power generation over N_g generation buses and $\boldsymbol{p}_l \leq \mathbf{0}$ represents the load distribution over N_l load buses. Additionally, let $\boldsymbol{z} = [\boldsymbol{z}_g; \boldsymbol{z}_l]$ be the power assignment changes over N_B buses due to element failures, where $\boldsymbol{z}_g$ represents the re-dispatched power at N_g generation buses and $\boldsymbol{z}_l$ represents load to be shed at N_l load buses. Finally, let $\boldsymbol{u}_l$ be the load cost vector of load buses, an optimal load shedding strategy then can be derived by solving the following optimization problem:

$$\begin{aligned}
\min_{\boldsymbol{z},\boldsymbol{\theta}} \quad & L = {\boldsymbol{u}_l}^T \boldsymbol{z}_l, \\
\text{s.t.} \quad & \boldsymbol{\Gamma}^T \boldsymbol{B} \sin(\boldsymbol{\Gamma}\boldsymbol{\theta}) - (\boldsymbol{p} + \boldsymbol{z}) = 0, \\
& \boldsymbol{p}_{\text{gmin}} \leq \boldsymbol{p}_g + \boldsymbol{z}_g \leq \boldsymbol{p}_{\text{gmax}}, \\
& \boldsymbol{z}_{\text{gmin}} \leq \boldsymbol{z}_g \leq \boldsymbol{z}_{\text{gmax}}, \\
& \boldsymbol{p}_l \leq \boldsymbol{p}_l + \boldsymbol{z}_l \leq \boldsymbol{p}_{\text{lmax}}, \\
& \boldsymbol{\theta}_{\min} \leq \boldsymbol{\Gamma}\boldsymbol{\theta} \leq \boldsymbol{\theta}_{\max}, \\
& \boldsymbol{c}_{\min} \leq \boldsymbol{B} \sin(\boldsymbol{\Gamma}\boldsymbol{\theta}) \leq \boldsymbol{c}_{\max},
\end{aligned} \tag{5.3}$$

where $\boldsymbol{p}_{\text{gmin}} \geq \mathbf{0}$ and $\boldsymbol{p}_{\text{gmax}} \geq \mathbf{0}$ represent, respectively, the minimum and maximum outputs at given generation buses. $\boldsymbol{z}_{\text{gmin}} \leq \mathbf{0}$ represents the maximum power can be reduced at given generation buses for a time step, and $\boldsymbol{z}_{\text{gmax}} \geq \mathbf{0}$ represents the maximum power can be increased at given generation buses for a time step. $\boldsymbol{p}_{\text{lmax}} \leq \mathbf{0}$ refers to important load that cannot be shed at given load buses. $\boldsymbol{\theta}$ is the phase angle at each bus. $\boldsymbol{\theta}_{\min}$ and $\boldsymbol{\theta}_{\max}$ represent the minimized and maximized limitations of the phase angle at each bus, respectively. $\boldsymbol{\Gamma}$ is the incidence matrix for the topology of the power grid, and $\boldsymbol{B}$ is the diagonal matrix whose diagonal entries correspond to line admittances. $\boldsymbol{c}_{\min}$ and $\boldsymbol{c}_{\max}$ independently represent the minimized and maximized power limitations of each branch.

The first constraint of the formulated problem gives the physical power flow equations that must be satisfied during the load shedding, where the voltages at N_B buses are assumed to be fixed. For N_g generation buses, the minimum output of some generation buses is an important constraint because of the cogeneration, where they must generate certain power to ensure the heat supply. Additionally, the output of each power plant cannot exceed its maximum output. Therefore, the second constraint gives the limitations for generation buses about their minimum and maximum outputs. Additionally, the ramping capability also exists in generation buses because the power plants need certain time to increase or decrease their outputs. The constraint for the ramping capability of generation buses is given in the third constraint. For N_l load buses, in order to ensure the uninterrupted power supply to certain load, there may be some important load can not be shed at any time for load buses, which is shown by $\boldsymbol{p}_l + \boldsymbol{z}_l \leq \boldsymbol{p}_{\text{lmax}}$ of the fourth constraint. And $\boldsymbol{p}_l \leq \boldsymbol{p}_l + \boldsymbol{z}_l$ in the fourth constraint ensures that the load at given load buses can only be shed, not added. In order to keep the power grid in a stable state, the phase at N_B buses and N_T transmission line flows are also required to be in certain range, which are given in the fifth and sixth constraint, respectively.

For a given time step t, a pair of attack and defense actions $(\boldsymbol{a}, \boldsymbol{d})$ will cause the state (topology) change of the power grid, which is represented by the incidence matrix $\boldsymbol{\Gamma}$. Therefore, the incidence matrix $\boldsymbol{\Gamma}$ should be updated according to the current power grid state. For different power grid states, we can derive different incidence matrices to represent the topology of the power grid. Then, the cost of shed load under the attack, denoted by L, will be equal to $\boldsymbol{u}_l{}^T \boldsymbol{z}_l$ derived by solving (7.3). The attacker's reward is then given by $R^{\mathcal{A}}(s(t), \boldsymbol{a}, \boldsymbol{d}) = \sum_{s' \in \mathcal{S}} T_{s,s'}(\boldsymbol{a}, \boldsymbol{d}) L(s')$, and the defender's reward $R^{\mathcal{D}}(s, \boldsymbol{a}, \boldsymbol{d})$ is just negative of $R^{\mathcal{A}}(s, \boldsymbol{a}, \boldsymbol{d})$.

5.4 Game Solution and Risk Assessment

With the two players' rewards computed, the proposed stochastic game Ξ can be solved by characterizing the closed-loop Nash equilibrium for each state $s \in \mathcal{S}$. At the Nash equilibrium, one player's strategy is the optimal strategy to maximize the minimum overall rewards under the other player's optimal strategy, and the optimal attack and defense budgets allocated at N_G power grid elements can be derived. Moreover, the probability of successful attack $\boldsymbol{a} \in \mathcal{A}$ can be derived according to the two players' optimal budget

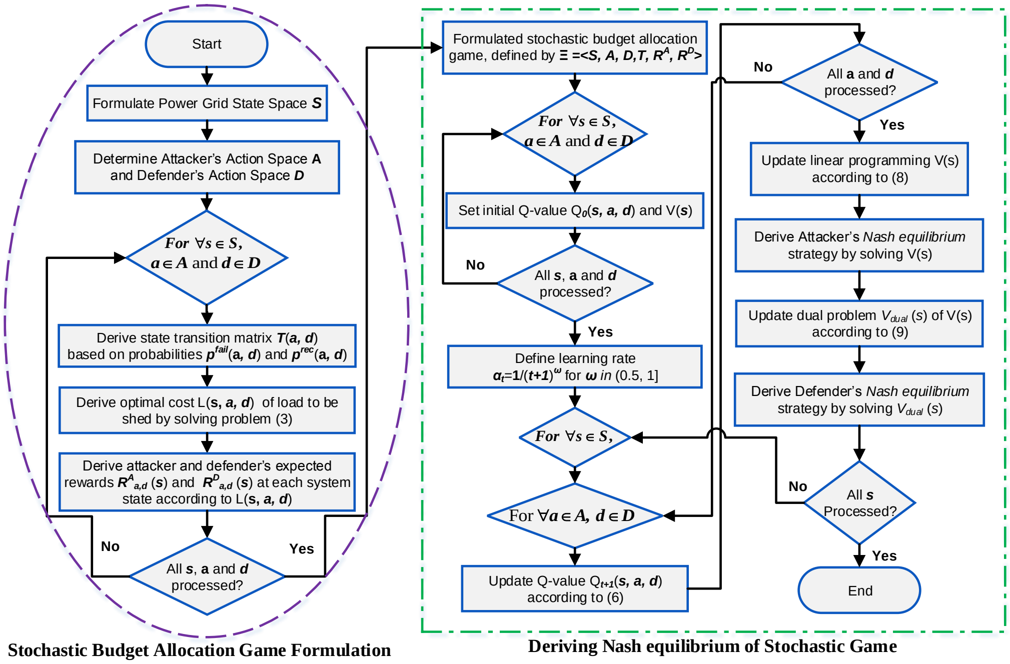

Start
Formulate Power Grid State Space S
Determine Attacker's Action Space $\mathbf{A}$ and Defender's Action Space D
For $\forall s \in S$, $a \in A$ and $d \in D$
Derive state transition matrix $T(a, d)$ based on probabilities $p^{fail}(a, d)$ and $p^{rec}(a, d)$
Derive optimal cost $L(s, a, d)$ of load to be shed by solving problem (3)
Derive attacker and defender's expected rewards $R^{A}_{a,d}(s)$ and $R^{D}_{a,d}(s)$ at each system state according to $L(s, a, d)$
No
Yes
All s, $\mathbf{a}$ and d processed?
Stochastic Budget Allocation Game Formulation
Formulated stochastic budget allocation game, defined by Ξ =<S, A, D,T, R^{A}, R^{D}>
For $\forall s \in S$, $a \in A$ and $d \in D$
Set initial Q-value $Q_0(s, a, d)$ and $V(s)$
No
All s, $\mathbf{a}$ and d processed?
Yes
Define learning rate $\alpha_t=1/(t+1)^{\omega}$ for ω in (0.5, 1]
For $\forall s \in S$,
For $\forall a \in A$, $d \in D$
Update Q-value $Q_{t+1}(s, a, d)$ according to (6)
No
All $\mathbf{a}$ and d processed?
Yes
Update linear programming V(s) according to (8)
Derive Attacker's Nash equilibrium strategy by solving V(s)
Update dual problem $V_{dual}(s)$ of V(s) according to (9)
Derive Defender's Nash equilibrium strategy by solving $V_{dual}(s)$
No
All s Processed?
Yes
End
Deriving Nash equilibrium of Stochastic Game

Figure 5.1: Flowchart of the proposed algorithm for deriving the Nash equilibrium of the stochastic budget allocation game Ξ.

allocation strategies at the Nash equilibrium of the game. The risk of the coordinated cyber-physical attack faced by the power grid is then defined as the product of the probability of successful attack and its corresponding physical impact on the grid.

5.4.1 Game Solution

Since the proposed stochastic game Ξ is a zero-sum game, we can first derive one player's mixed strategies at the Nash equilibrium, and the other's mixed strategies can be derived in the same way. Here, we first focus on the attacker, and assume the following overall reward Q as $Q^{\mathcal{A}}$. As shown in [126], the attacker's Nash equilibrium strategies can be derived recursively through the following dynamic iterations. Given an initial overall reward Q_0, the optimal overall reward Q^* for the attacker can be derived iteratively as follows:

$$Q_{t+1}(s,\boldsymbol{a},\boldsymbol{d}) = R^{\mathcal{A}}(s,\boldsymbol{a},\boldsymbol{d}) + \gamma \sum_{s'\in\mathcal{S}} T_{s,s'}(\boldsymbol{a},\boldsymbol{d})V(s'), \tag{5.4}$$

$$V(s') = \max_{\boldsymbol{\pi}_{\mathcal{A}}} \min_{\boldsymbol{d}} \boldsymbol{\pi}_{\mathcal{A}}^{T}(s')Q_t(s',\boldsymbol{a},\boldsymbol{d}). \tag{5.5}$$

The attacker's stationary strategy $\boldsymbol{\pi}_{\mathcal{A}}^{*}(s), \forall s \in \mathcal{S}$ derived by (5.5) is the optimal strategy at Nash equilibrium. However, one of the drawbacks of this method is that, during each iteration, the Q-value is only updated by immediate rewards derived at the current time step, but immediate rewards derived at previous steps are ignored. Therefore, the algorithm's computational complexity grows exponentially with the bus and transmission line size of the power grid, and will make it impractical for grids with reasonable sizes to be solved by this algorithm. This chapter introduces a changeable learning rate $\alpha_t = 1/(t+1)^{\omega}$ in [67] for each time step t, for $\omega \in (0.1, 1)$, into the above algorithm. Using the learning rate α_t, two new recursions are defined for computing the optimal discounted sum of expected rewards Q^* at time step t, as follows:

$$\begin{aligned} Q_{t+1}(s,\boldsymbol{a},\boldsymbol{d}) = (1-\alpha_t)Q_t(s,\boldsymbol{a},\boldsymbol{d}) + \alpha_t(R^{\mathcal{A}}(s,\boldsymbol{a},\boldsymbol{d}) \\ +\gamma \sum_{s'\in\mathcal{S}} T_{s,s'}(a,d) \times V(s')), \end{aligned} \tag{5.6}$$

$$V(s') = \max_{\boldsymbol{\pi}_{\mathcal{A}}} \min_{\boldsymbol{d}} \boldsymbol{\pi}_{\mathcal{A}}^{T}(s')Q_t(s',\boldsymbol{a},\boldsymbol{d}), \tag{5.7}$$

for a given initial condition Q_0. (5.7) can be formulated as a linear constrained optimization problem. And the attacker's stationary strategy $\boldsymbol{\pi}_{\mathcal{A}}^{*}(s)$, $\forall s \in \mathcal{S}$ derived by the following problem is the Nash equilibrium strategy:

$$\begin{aligned} \max_{\boldsymbol{\pi}_{\mathcal{A}}} \quad & V(s'), \\ \text{s.t.} \quad & \boldsymbol{\pi}_{\mathcal{A}}^{T}(s')Q_t(s',\boldsymbol{a},\boldsymbol{d}) \geq V(s'), \forall \boldsymbol{d} \in \mathcal{D}. \end{aligned} \tag{5.8}$$

The fixed points of (5.6) and (5.7), V^* and Q^*, lead to the optimal maxmin solution for the attacker. Correspondingly, the defender's Nash equilibrium strategy $\boldsymbol{\pi}_{\mathcal{D}}^{*}(s)$, $\forall s \in \mathcal{S}$

can be obtained by solving the dual of the linear constraint optimization (5.8):

$$\begin{aligned} \min_{\boldsymbol{\pi}_{\mathcal{D}}} \quad & V_{\text{dual}}(s'), \\ \text{s.t.} \quad & \boldsymbol{\pi}_{\mathcal{D}}^{T}(s')Q_t(s',\boldsymbol{a},\boldsymbol{d}) \leq V_{\text{dual}}(s'), \forall \boldsymbol{a} \in \mathcal{A}. \end{aligned} \tag{5.9}$$

For the proposed stochastic games Ξ, the strong max-min property in [**?**] proves that strong duality applies and $V_{\text{dual}}(s')$ is equal to $V(s')$. Therefore, the tuple of stationary strategies ($\boldsymbol{\pi}_{\mathcal{A}}^{*}(s)$,$\boldsymbol{\pi}_{\mathcal{D}}^{*}(s)$), $\forall s \in \mathcal{S}$, obtained by (5.8) and (5.9) is the Nash equilibrium that we are looking for each system state of the power grid. The flowchart of computing the Nash equilibrium of the proposed stochastic game Ξ is detailed presented in Fig. 5.1.

However, in order to derive the pure strategy Nash equilibrium, a ε-greedy technology is introduced to select the attack/defense action at each time step. With ε-greedy, the attacker (defender) selects at each time step a random action with a fixed probability, $0 < \varepsilon < 1$, instead of selecting greedily one of the learned optimal actions with respect to the Q-function:

$$\boldsymbol{a}(\boldsymbol{d}) = \begin{cases} \text{random action from } \mathcal{A}(\mathcal{D}), if\ \xi < \varepsilon, \\ \text{optimal solution of problem } (5.8)((5.9)),\ otherwise, \end{cases} \tag{5.10}$$

where $0 \leq \xi \leq 1$ is a uniform random number drawn at each time step.

The risk faced by the power grid is defined as the product of the probability of successful attacks and corresponding physical impacts on the grid, which can be taken as the cost of the shed load under the given attack action. Since the tuple of Nash equilibrium strategies ($\boldsymbol{\pi}_{\mathcal{A}}^{*}(s)$,$\boldsymbol{\pi}_{\mathcal{D}}^{*}(s)$) gives the optimal attack and defense action selection strategy over the two players' action spaces, the probability $Pr(s,\boldsymbol{a})$ of successful attack action $\boldsymbol{a} \in \mathcal{A}_{att}$ at state s can be defined as follows:

$$Pr(s,\boldsymbol{a}) = \sum_{\boldsymbol{d} \in \mathcal{D}} \boldsymbol{\pi}_{\mathcal{A}}^{*}(s,\boldsymbol{a})\boldsymbol{\pi}_{\mathcal{D}}^{*}(s,\boldsymbol{d}) \prod_{i \in T} p_i^{\text{fail}}(\boldsymbol{a},\boldsymbol{d}), \tag{5.11}$$

where $\boldsymbol{\pi}_{\mathcal{A}}^{*}(s,\boldsymbol{a})$ and $\boldsymbol{\pi}_{\mathcal{D}}^{*}(s,\boldsymbol{d})$ represents the probability of selecting attack action $\boldsymbol{a}$ and defense action $\boldsymbol{d}$ in the tuple of Nash equilibrium strategies ($\boldsymbol{\pi}_{\mathcal{A}}^{*}(s)$,$\boldsymbol{\pi}_{\mathcal{D}}^{*}(s)$) at state s, respectively. T represents the set of grid elements targeted by attack action $\boldsymbol{a}$. The risk faced by the power grid at state s is therefore shown as follows:

$$\Gamma(s) = \sum_{\boldsymbol{a} \in \mathcal{A}} Pr(s, \boldsymbol{a}) L(\boldsymbol{a}), \tag{5.12}$$

where $L(\boldsymbol{a})$ is the cost of load that must be shed under successful attack action $\boldsymbol{a}$, which is derived by solving (7.3).

5.4.2 Risk Assessment

For a given state $s \in \mathcal{S}$, with the tuple of Nash equilibrium strategies ($\boldsymbol{\pi}^*_{\mathcal{A}}(s)$,$\boldsymbol{\pi}^*_{\mathcal{D}}(s)$) computed, the optimal defense budget allocation for element i of the power grid at the Nash equilibrium of the proposed game Ξ can be formulated as follows:

$$B_i^{\mathcal{D}}(s) = \sum_{d \in \mathcal{D}} b_i^{\mathcal{D}}(\boldsymbol{d}) \boldsymbol{\pi}^*_{\mathcal{D}}(s, \boldsymbol{d}), \tag{5.13}$$

where $i = 1, ..., N_G$, and $b_i^{\mathcal{D}}(\boldsymbol{d})$ represents the defense budget implemented for element i in defense action $\boldsymbol{d}$. Similarly, the optimal attack budget allocation for grid element i at the game equilibrium can be formulated for state s shown as follows:

$$B_i^{\mathcal{A}}(s) = \sum_{a \in \mathcal{A}} b_i^{\mathcal{A}}(\boldsymbol{a}) \boldsymbol{\pi}^*_{\mathcal{A}}(s, \boldsymbol{a}), \tag{5.14}$$

where $i = 1, ..., N_G$, and $b_i^{\mathcal{A}}(\boldsymbol{a})$ represents the attack budget implemented for element i in attack action $\boldsymbol{a}$. Therefore, the vulnerability of the power grid can be assessed with respect to the ranking of grid components regarding the attack budget ratio $B_i^{\mathcal{A}}/B^{\mathcal{A}}$ being allocated.

5.5 Simulation Results and Analysis

To illustrate the application of the stochastic game theoretic approach to the risk assessment of coordinated cyber-physical attacks, the IEEE 9-bus system [133] is taken as the test system. We consider that the attacker can take both physical attacks and denial-of-service (DoS) attacks to disrupt the transmission lines of the system, while the defender must implement proper defense mechanisms such as building barriers and implementing filters, to reinforce normal transmission lines and repair broken lines. For clarity, conciseness, and easy illustration of this case study, the attack and defense budgets, independently denoted by $B_{\mathcal{A}}$ and $B_{\mathcal{D}}$, are considered as dimensionless quantities, i.e., quantities without any physical units. In the test system, 6 types of *single attacks* and 15 types of *coordinated attacks* are investigated. The amount of shed load following each of successful attacks is listed in Table 5.2. Table 5.2 shows that coordinated attacks can lead to more load to be shed than single attacks, and attack 7-9, 13-15, 17 and 19-21 are ten coordinated attacks that can cause more physical damages on the grid than other coordinated attacks. Thus, the attack action space $\mathcal{A}$ contains above ten coordinated attacks, where a_1 for Line 1 and 2, a_2 for Line 1 and 3, a_3 for Line 1 and 4, a_4 for Line 2 and 4, a_5 for Line 2 and 5, a_6 for Line 2 and 6, a_7 for Line 3 and 5, a_8 for Line 4 and 5, a_9 for Line 4 and 6, and a_{10} for Line 5 and 6. Similarly, the defense action space $\mathcal{D}$ includes ten corresponding defense actions.

With the two players' action spaces and rewards computed, we intend to derive the *Nash equilibrium* of the proposed stochastic game in stationary strategies for each state of the power grid. Here, eleven grid states are considered including state s_1: $\{$1,1,1,1,1,1$\}$, state s_2: $\{$0,0,1,1,1,1$\}$, state s_3: $\{$0,1,0,1,1,1$\}$, state s_4: $\{$0,1,1,0,1,1$\}$, state s_5: $\{$1,0,1,0,1,1$\}$, state s_6: $\{$1,0,1,1,0,1$\}$, state s_7: $\{$1,0,1,1,1,0$\}$, state s_8: $\{$1,1,0,1,0,1$\}$, state s_9: $\{$1,1,1,0,0,1$\}$, state s_{10}: $\{$1,1,1,0,1,0$\}$, and state s_{11}: $\{$1,1,1,1,0,0$\}$, where ”1” and ”0” independently denote the normal or failed status of transmission lines in order. Given the discount number $\gamma = 0.5$, here, we assume that $B_{\mathcal{A}} = B_{\mathcal{D}} = 10$, and $p_i^{\text{fail}} = [b_i^{\mathcal{A}}/(1 + b_i^{\mathcal{A}})] \times [1/(1 + b_i^{\mathcal{D}})]$ and $p_i^{\text{rec}} = [b_i^{\mathcal{D}}/(1 + b_i^{\mathcal{D}})] \times [1/(1 + b_i^{\mathcal{A}})]$, where $b_i^{\mathcal{A}(\mathcal{D})}$ represents the attack (defense) budget implemented on Line i.

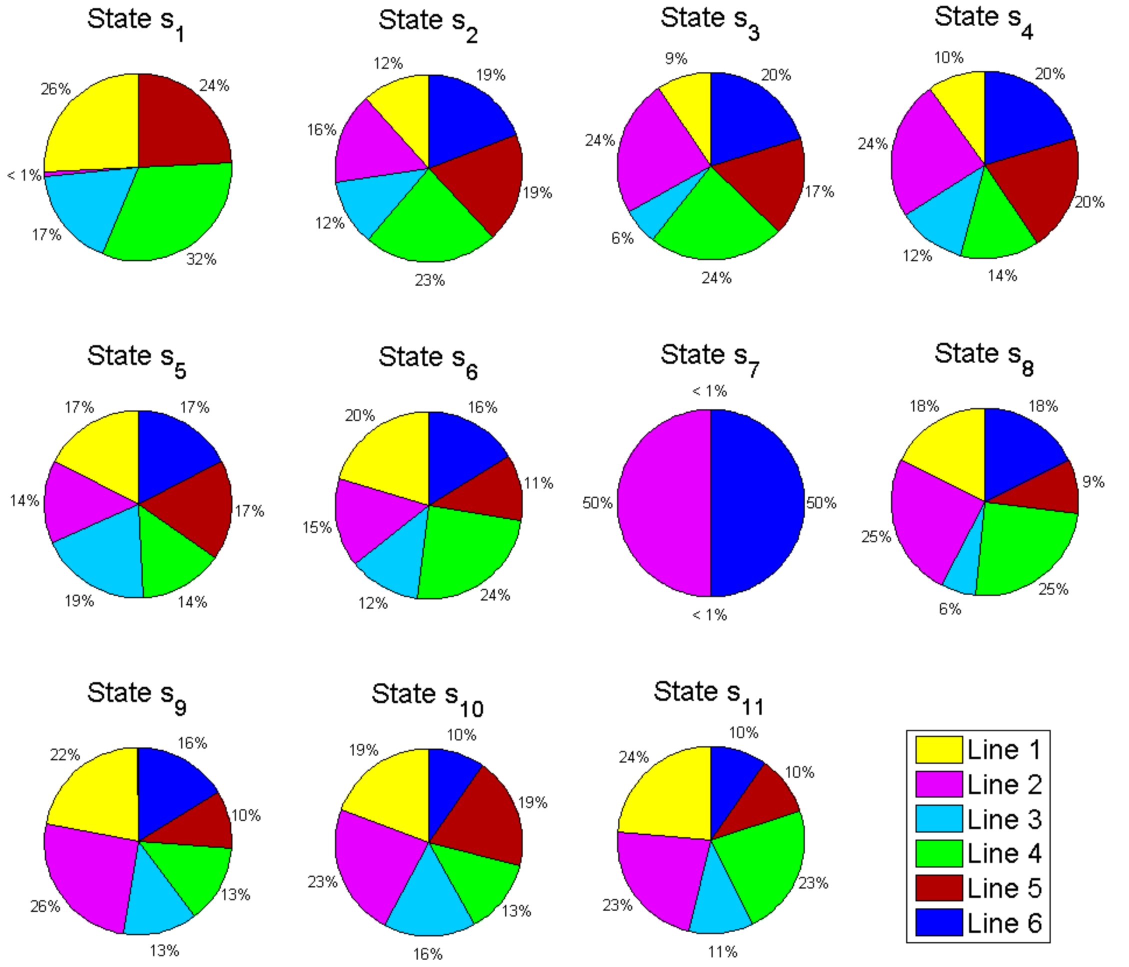


Figure 5.2: The defense budget allocation strategies for the test system at the Nash equilibrium of the proposed game from state s_1 to state s_{11}.

Table 5.2: Shed Load due to Attacks in the IEEE 9-Bus System

Attack No.	Attack Target	Shed Load	Attack No.	Attack Target	Shed Load
		(MW)			(MW)
1	Line 1	0	12	Line 2 and 3	0
2	Line 2	0	13(a_4)	Line 2 and 4	352
3	Line 3	0	14(a_5)	Line 2 and 5	132
4	Line 4	0	15(a_6)	Line 2 and 6	27
5	Line 5	0	16	Line 3 and 4	0
6	Line 6	0	17(a_7)	Line 3 and 5	361
7(a_1)	Line 1 and 2	120	18	Line 3 and 6	0
8(a_2)	Line 1 and 3	376	19(a_8)	Line 4 and 5	220
9(a_3)	Line 1 and 4	232	20(a_9)	Line 4 and 6	328
10	Line 1 and 5	0	21(a_{10})	Line 5 and 6	135
11	Line 1 and 6	0			

Fig. 5.2 presents the defender's optimal budget allocation strategies for the test system at the *Nash equilibrium* of the proposed game from state s_1 to state s_{11}. In this figure, we can see that different defense budget allocation strategies are derived in various system states. For instance, at state s_1, the defender focuses on distributing its budgets on Lines 1, 3, 4 and 5, which are critical transmission lines that can cause more than 300 MW of load must be shed if failed. In contrast, the defender shifts its focus to Lines 2 and 6 at state s_7, which can only lead to 27 MW of load to be shed if failed. This observation can be explained according to the difference between state s_1 and s_7. At state s_1, all transmission lines of the grid are operated normally. Thus, the defender should implement more budgets on protecting critical transmission lines that can lead to severe physical damages if failed. However, at state s_7, Lines 2 and 6 have already been out of service. Although Lines 2 and 6 can cause less physical impacts on the system if failed, the defender need to implement more budgets on repairing them to avert a cascading failure on other transmission lines. Furthermore, in all broken states from s_2 to s_{11}, Lines 2 and 6 are implemented of more than 26% budgets, while, in normal state s_1, none budget is distributed on these two lines. This observation shows that Lines 2 and 6 would took important roles if some

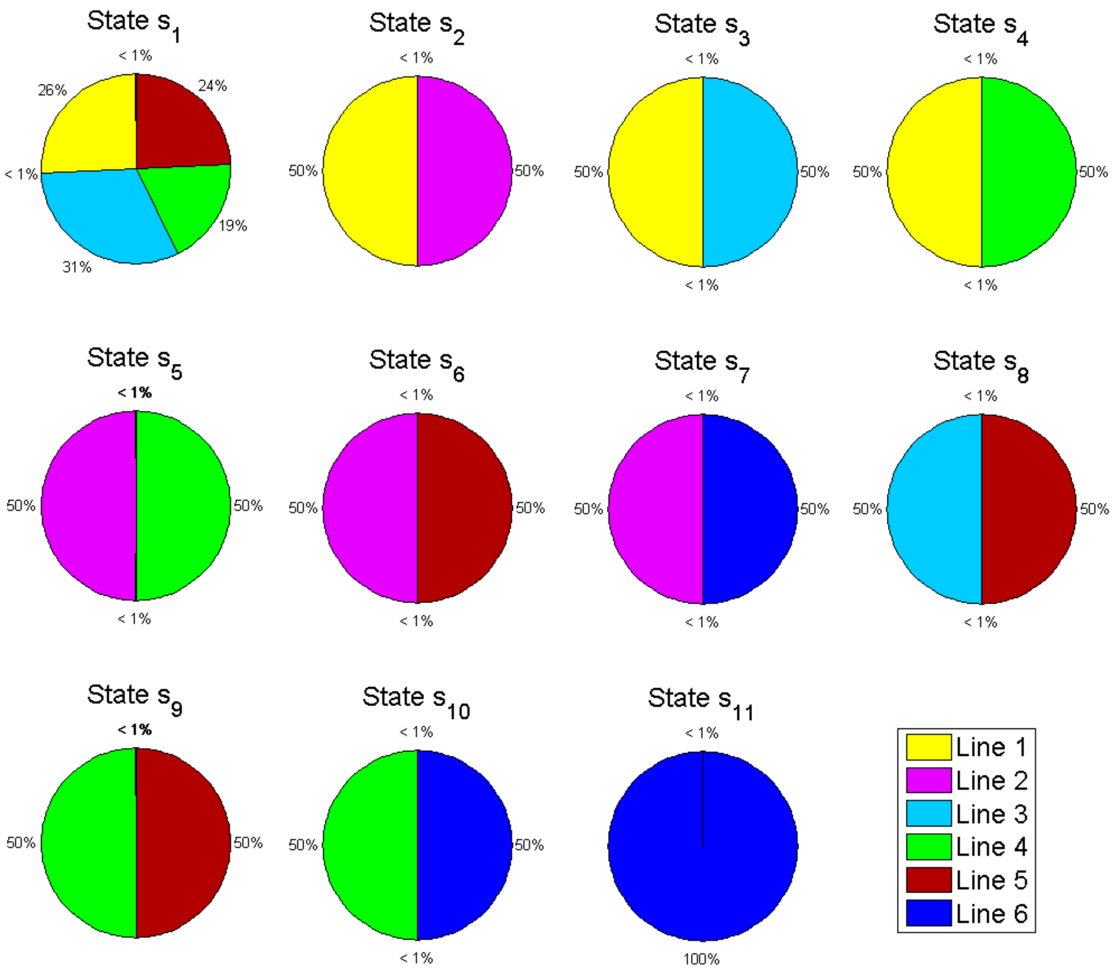


Figure 5.3: The attack budget allocation strategies for the test system at the Nash equilibrium of the proposed game from state s_1 to state s_{11}.

test system lines broken.

Fig. 5.3 presents the attacker's optimal budget allocation strategies for the test system at the *Nash equilibrium* of the proposed game from state s_1 to state s_{11}. In Fig. 5.3, we can also find that the attack budget allocation strategies at the Nash equilibrium varies with different system states. However, compared with the defender's optimal budget allocation strategies, the attacker implements its budgets on only one or two transmission lines from state s_2 to s_{11}, which are broken states. This observation can be explained based on less attack budgets are owned by the attacker for allocation. Therefore, the attacker should implement more budgets on limited critical transmission lines to increase the probability of the successful attack action. Furthermore, from state s_2 to s_{11}, the attacker distributes its main budgets on broken transmission lines to disrupting the repair of the broken transmission lines. For instance, at state s_2, the attacker distribute its almost 50% budget on Lines 1 and 50% budget on Lines 2. And the attacker shifts its focus to Lines 1 and 3 at state s_3.

The attacker and defender's Nash equilibrium strategies from state s_1 to state s_{11} for the test system have been derived by solving the proposed stochastic game. The two players' optimal budget allocation strategies can be used to assess and quantify the associated risk faced by the test system for the corresponding state. Here, we assume that $B_{\mathcal{A}} = B_{\mathcal{D}} = 10$, and Fig. 5.4 presents the quantified risks faced by the test system from state s_1 to state s_{11} with various discount factors γ. In this figure, the x-axis represents the discount factor γ ranging from 0 to 0.9, and the y-axis shows the corresponding risk (MW). In this figure, we can see that different quantified risks are derived as we vary γ. Small values of γ emphasize near-term gains while large values emphasize future rewards. If $\gamma = 0$, the proposed stochastic game becomes a static game, where only the current state is considered. For instance, at states s_2, s_4, s_6, s_7, and s_9, as we increase γ from 0 (static game) to 0.9 (stochastic game), the risk reduction reaches up to 87.99%, 87.89%, 87.57%, 82.76%, and 87.41%. Although, at states s_5, s_8, and s_{10}, the risk is increased as we increase γ from 0 to 0.9, the risk increase only reaches up to 2.76%, 0.22%, and 1.47%.

The attack and defense budgets, denoted by $B^{\mathcal{A}}$ and $B^{\mathcal{D}}$ are also key contributors to the risk variation. Given the discount factor $\gamma = 0.5$, Fig. 5.5 presents the risk variation at state s_1 of the proposed game for the test system with respect to various budgets of the attacker and defender. In this figure, we can see that the risk faced by the grid diminishes

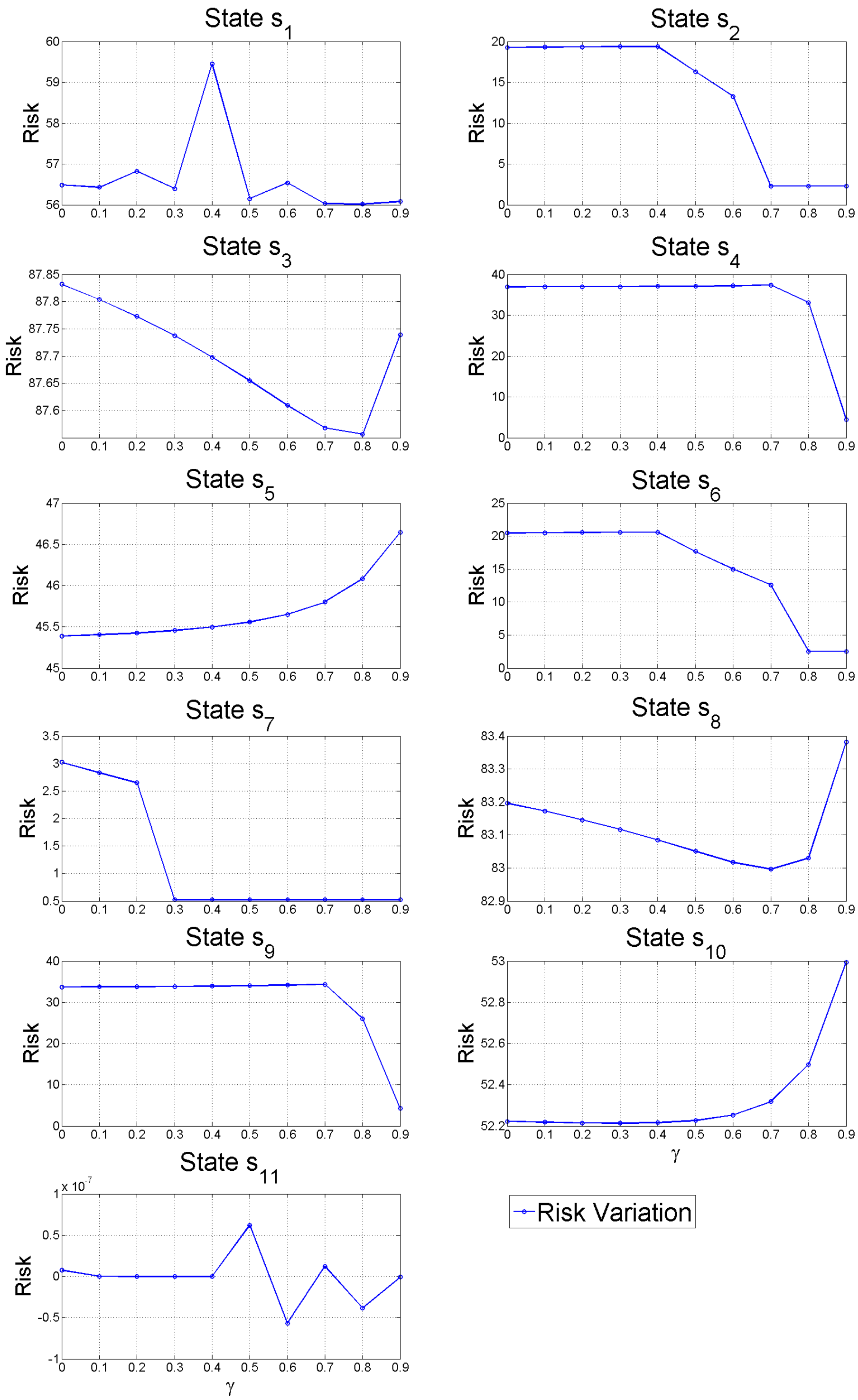


Figure 5.4: The risk in each of eleven states for the test system with the discount factor γ ranging from 0 to 0.9.

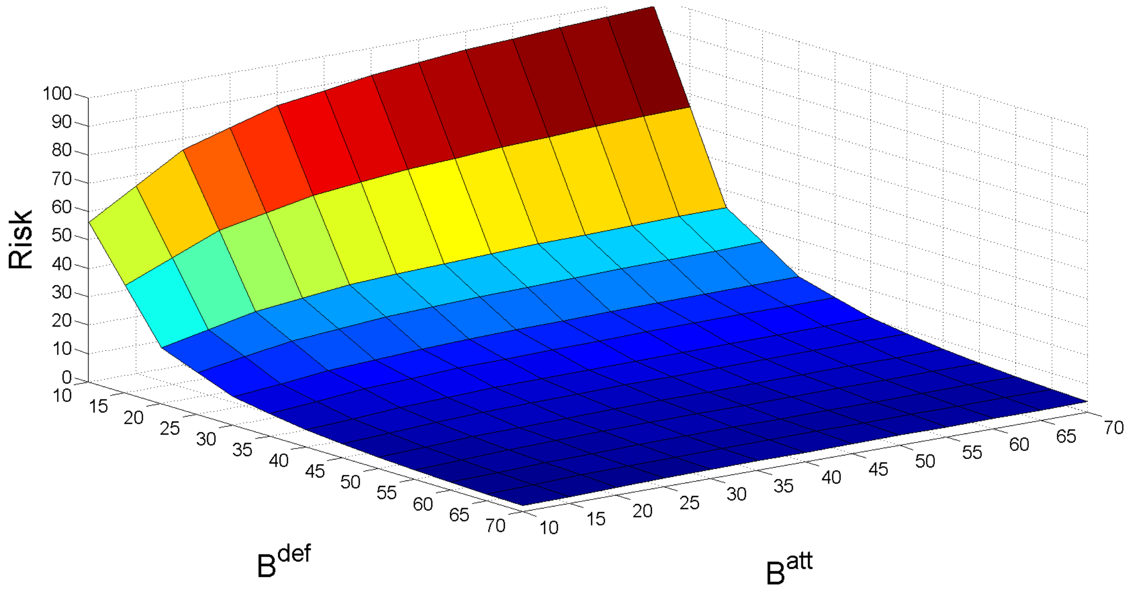


Figure 5.5: The risk at state s_1 of the proposed game for the test system with respect to the various budgets of the attacker and defender that can be implemented at a time.

accordingly with the increase of $B^{\mathcal{D}}$. However, the reduction rate of the risk will be gradually decreased. For instance, for $B^{\mathcal{A}} = 10$, the increase of $B^{\mathcal{D}}$ from 10 to 40 yields 13.09 times of risk reduction than the increase of $B^{\mathcal{D}}$ from 40 to 70. On the contrary, to increase the probability of successful attacks and corresponding risks, the increase of B^{att} is much less effective. For example, for $B^{\mathcal{D}} = 70$, the addition of $B^{\mathcal{A}}$ from 10 to 40 yields the almost same risk increase with the addition of $B^{\mathcal{D}}$ from 40 to 70. The above quantitative analysis provides a basis for the investment of the defense budget $B^{\mathcal{D}}$ and optimal defense budget allocations.

5.6 Summary

In this chapter, we have presented a novel game-theoretic approach for the risk assessment of coordinated cyber-physical attacks against power grids, while considering the finite budget owned by the attacker and defender that will have an important influence on the assessment. We have formulated a two-player zero-sum stochastic game between the attacker and defender in which each player seeks to maximize its respective minimum rewards under the opponent's optimal strategy. In order to quantify their rewards, the optimal load shedding technology is introduced to determine the minimum cost of shed load. Using these quantified rewards as inputs, the attacker and defender's Nash equilibrium strategies about its budget allocation are derived by solving the proposed stochastic game. At the Nash equilibrium of the game, the optimal attack and defense budget allocation strategies can be obtained, in terms of attacking/protecting the critical elements of the grid. The probability of successful attacks and corresponding physical impacts on the grid can be used to assess the risk for various states of the power grid, and the optimal defense budget allocation is formulated in terms of the corresponding risk. The IEEE 9-bus grid is used as the test system, and simulation results have shown that different risks are derived as we vary the attack/defense budget.

CHAPTER 6

Multimodal Data-Driven Framework for DER Attack Detection

This chapter presents a multimodal data-driven framework for the attack detection in power distribution systems integrated with a large-scale of distributed energy resources (DERs). Section 6.1 makes an overview of this chapter. Section 6.2 introduces the cyber attack models in DER systems. Section 6.3 describes the proposed DER attack detection framework. Section 6.4 develops a test distribution system. Section 6.5 compares the experimental results of the proposed attack detection framework with existing works, while Section 6.6 concludes the chapter and outlines the future work.

6.1 Overview

The power grid architecture is currently evolving from a utility-centric structure to a distributed cyber-physical system (CPS) integrated with a large-scale of distributed energy resources (DERs) [134]. The implementation of DERs requires electric utilities to coordinate grid control functions with customers and other energy providers, which demands a wide-area communication for remotely controlling customer owned DERs. While smart meters and advanced metering infrastructure (AMI) already significantly expand the utilities' attack surfaces, DER deployments present additional risks due to the tremendous number of devices and access points that operate outside the typical utility's administrative domain. Therefore, cyber attacks could exploit vulnerabilities in the end-user devices such as smart meters and renewable energy resources, thereby compromising the power grid. Moreover, the high scalability of DER deployments and the existence of uncertainties in power distribution systems make the quick and accurate detection of DER cyber attacks challenging [135].

To detect targeted cyber attacks and achieve attack resilience, there is a requirement for continuous monitoring of DERs and their interactions with power distribution systems in real-time [136]. The anomalies within the physical systems can be used for the DER cyber attack detection. If cyber attacks are beginning to manipulate the operation of DERs, a variety of smart meters and micro-PMUs on power distribution systems can be utilized to evaluate which DER devices and customers are misoperating and what malicious functions they are performing. Additionally, historical data describing the DER operation can help identify anomalies and potential attacks. As a result, it is useful and effective to predict the DER system states and detect potential cyber attacks through measurement data-driven approaches.

Recently, a wealth of efforts have been proposed for the cyber attack detection in the power grid using the advanced data analytics, such as supervised learning, unsupervised learning, and statistics-based learning approaches [38–41]. In [38], a decision tree based anomaly detection approach was presented to secure the power grid communication network from distributed denial of service (DDoS) attacks. A malware infection detection using Kernel Fisher discriminant analysis was proposed in [39] by comparing malware traffic with normal traffic. An intrusion detection system was developed in [40] for early detection of threats in AMI of smart grid, where a multi-support vector machine (SVM) classifier was trained. In [41], a Sybil attack detection method based on k-Nearest Neighbours (kNN) classification was introduced for the vehicle-to-grid (V2G) networks. However, all of these machine learning methods need to be evaluated to guide the selection of mechanisms that are most suitable for the DER cyber attack detection. Moreover, techniques should be developed to handle the complex and high dimensional DER measurement data, whereas maintain the accuracy of the attack detection mechanisms.

Feature learning is a key to improve the performance of existing data analytics based attack detection mechanisms, which consists of feature extraction and selection. Feature extraction transforms the original features into a more meaningful representation by reconstructing its inputs and involves reducing the amount of resources required to describe a large dataset. There are two broad categories for feature extraction algorithms including linear and nonlinear. Linear feature extraction algorithms, such as principal component analysis (PCA) [42], multidimensional scaling [43], and principal coordinates analysis [44], assume the data lies on a lower-dimensional linear subspace and projects them on this subspace using matrix factorization. However, nonlinear feature extraction algorithms like self organizing maps (SOMs) [45] and Kohonen maps [46] create a lower dimensional mapping of an input by preserving its topological characteristics.

Performance of attack detection mechanisms is heavily dependent on the choice of applied features, and feature selection is to identify the most informative features from the original and extracted feature sets. Typically, feature selection is partitioned into three classes: *filters*, *wrappers*, and *embedded* methods. Filter methods analyze intrinsic properties of dataset ignoring the type of classifier. Conversely, wrappers use classifiers to score a given subset of features, and embedded methods inject the selection process directly into the classification learning process. In this chapter, the filter methods are utilized to evaluate different types of classifiers for the DER attack detection. Among the most used filter-based strategies, Relief algorithm [47] estimates the quality of features according to how well their values distinguish between instances that are closer to each other. Another effective yet fast filter method is the Fisher method [48], which computes a score for a feature as the ratio of inter-class separation and intra-class variance, where features are evaluated independently. In [49], a mutual information (MI) based approach is proposed, and the quality of a given feature is evaluated by the MI between the distribution of the values of this feature and the membership to a particular class.

This chapter introduces a novel sparse feature extraction and a modified filter based feature selection into an ensemble classifier, and formulates a multimodal data-driven detection framework for identifying the abnormal events within DER implementation. In order to differentiate the attacked DER measurements from fault scenarios in the generated abnormal event list, the spatiotemporal correlation analysis is finally applied to each measurement to quantify the differentiable characteristics of this measurement from other correlated measurements. The main contributions of the chapter contain:

- Develop a two layer stacked denoising autoencoder (SAE) for feature extraction, and construct the low dimensional abstract features from the original DER measurement data;
- Propose a modified Relief based feature selection algorithm to identify the most relevant features;
- Train a decision tree based ensemble classifier using the selected features for identifying the abnormal events in DER measurement data;
- Implement a spatiotemporal correlation based approach for each DER measurement to classify the cyber attacks and system faults in the generated abnormal event list;
- Formulate a test distribution system integrated with DERs for simulating the normal, fault, and attack scenarios, and compare the attack detection performance of the proposed framework with existing works.

6.2 DER System Model and Adversary Model

6.2.1 DER System Model

A CPS architecture is developed to model the cyber-physical integration of DER systems into the power grid, as depicted in Fig. 6.1, which consists of four main domains: 1) transmission operation and control, 2) distribution utility communication and control, 3) DER devices and controllers, and 4) third parties. The high penetration of DERs in Domain 3 leads to a large number of distributed energy devices, such as smart inverters and battery controllers, which could vastly outnumber the utility owned and controlled resources. In addition, the DERs span multiple security administrative domains, meaning that the utility may only be able to monitor the security posture of devices up to the smart meter while DER owners in Domain 4 control and manage their devices themselves. Furthermore, a variety of communication networks (e.g., utility wide area network (WAN)) used to control the DERs will likely be interconnected with DER local area network (LAN) and related IT networks, thereby increasing the attack surfaces. All of these features introduce many new threats to both DER instances and the broader grid, and potential attacks listed in Fig. 6.1 include:

- *Attack 1*: Malicious commands to DERs over utility WAN;
- *Attacks 2-3*: Malware or unauthorized control over DER control devices to manipulate their operation;
- *Attacks 4-6*: Additional attack vectors to access DER components through interconnected networks;
- *Attack 7*: Novice system owners and administrators;
- *Attack 8*: Compromised wide-area monitoring, protection, and control (WAMPAC) applications negatively influence the operation of a large number of DERs.

In the physical layer of the architecture, the DERs in the distribution system include solar PV, battery energy storage systems, diesel generators, and electric vehicles (EVs), while wind turbine generators (wind farms) are connected at the sub-transmission and transmission levels. In addition, in power flow calculations, all DER devices except diesel generators are modeled as constant active (P) and reactive (Q) power generators connected at the corresponding bus. The diesel generators are treated as constant active power (P)

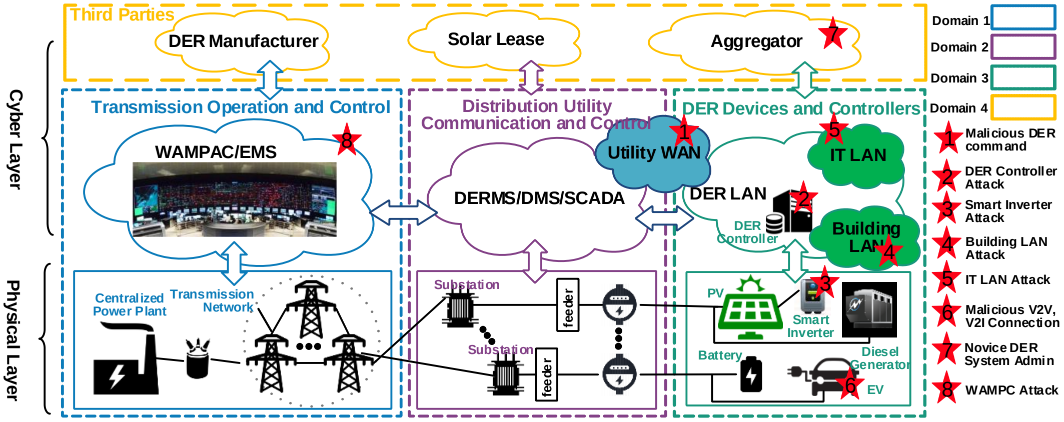


Figure 6.1: CPS architecture of the power grid integrated with a large-scale of distributed energy resources (DERs) and its cyber security risk.

and constant voltage (V) bus. The PCC point with the bulk grid is considered as the slack bus. In the cyber layer, the control architectures and communication networks of the DER implementation directly determine the risk exposure from cyber attacks. Multiple devices are involved in controlling DERs, especially smart inverters, DER controllers, and battery controllers. Models can be developed using cyber-architectural languages such as data flow diagrams or the architectural analysis and design language. Specific properties of DER control and communication that need to be modelled include: (1) communication protocols (e.g., IEEE 1815 (DNP3), IEC 61850-7-420, SEP (Smart Energy Profile) 2.0, and SunSpec Modbus) tailored for the control of DER devices; (2) unicast, multicast, and broadcast communication topologies for DER messages; (3) different messaging patterns such as request reply, publish subscribe, push-pull, exclusive pair, and client-server; and (4) smart inverter control functions including volt/var management, frequency/watt management, status reporting, and time synchronization.

6.2.2 Adversary Model

Consider a power distribution system integrated with DERs, and let $\mathcal{M}$ be the set of DER devices in this system, where $|\mathcal{M}| = m$. Assume that the control center collects the DER measurements of different physical quantities (e.g., voltages and currents) from $\mathcal{M}$ for a time period $\boldsymbol{T}$. Hence, the collected time series measurement set can be defined as $\mathcal{X} := \{\boldsymbol{x}^{(t)} | t \in \boldsymbol{T}\}$, where $\boldsymbol{x}^{(t)}$ is an m-dimensional vector $[x_1^{(t)}, ..., x_m^{(t)}]^T \in \mathbb{R}^m$, and its elements correspond to m DER device measurements. An attacker could compromise a subset of DER devices and manipulate their measurements such that any operational decision made based on these measurements could trigger unwarranted control actions for the true system state. There are various types of cyber attacks targeted at DERs. In the following parts, four specific cyber attack models are presented consisting of denial-of-service (DoS) attack, fault replay attack, data manipulation attack, and device misconfiguration attack.

Assume that the attacker has limited resources and could only compromise m_A DER devices for a time period $\boldsymbol{T}_A \subseteq \boldsymbol{T}$. Define the set of compromised DER devices as $\mathcal{M}_A \subseteq \mathcal{M}$, where $|\mathcal{M}_A| = m_A$. For *DoS attacks*, the attacker could jam the communication channels, attack networking protocols, and flood the network traffic to make the DER measurement packets sent from sensors to be lost. Hence, $\forall t \in \boldsymbol{T}_A$, DER device i measurement $x_i^{(t)}$, $i \in \mathcal{M}_A$, is set to be NA. *Fault replay attacks* attempt to emulate a valid fault by alerting system measurements followed by sending an illicit trip command to relays at the ends of the lines. This attack may lead to confusion and potentially cause an operator to take invalid control actions. For each compromised DER device $i \in \mathcal{M}_A$, the fault replay attack involves replacing the measurement $x_i^{(t)}$, $t \in \boldsymbol{T}_A$, by a historical valid fault measurement.

Correspondingly, *data manipulation attacks* refer to inject false data into the DER measurements by hacking into the communication network. Here, two types of data manipulation attacks are studied: 1) for each DER device $i \in \mathcal{M}_A$, a zero-mean white noise is added into the measurement sequence: $\{x_i^{(t)} + \epsilon | t \in \boldsymbol{T}_A\}$; 2) a uniformly distributed random number in the interval (a, b) is injected into the measurement of DER device $i \in \mathcal{M}_A$: $\{x_i^{(t)} + \text{rand}(a, b) | t \in \boldsymbol{T}_A\}$. In addition, an attacker can manipulate the *droop characteristic* or *references setpoints* of DER control systems, which can cause changes in the outputs of DERs or system frequency. For example, a scaling attack parameter λ_A is injected into the device i measurement to change the magnitude: $\{(1 + \lambda_A)x_i^{(t)} | t \in \boldsymbol{T}_A\}$, where $i \in \mathcal{M}_A$.

All of these cyber attacks could cause instabilities in the underlying physical system or force the system to operate at uneconomical operating conditions due to non-optimal control actions. This chapter aims to formulate a data-driven framework to identify the compromised DER devices based on the collected measurements, and provide a performance analysis on the proposed DER attack detection mechanism.

6.3 DER Attack Detection Framework

In this section, we formulate a multimodel DER attack detection framework, whose main objective is to: 1) reduce the cost of DER measurement collection; 2) improve detection rates and reduce false alarms; and 3) control the attack detector training time. As depicted in Figure 6.2, the basic procedure of the multimodel attack detection framework consists of:

1. DER measurement data collection and preprocessing;
2. *Sparse feature extraction*;
3. *Filter based feature selection*;
4. DER anomaly detector training and postprocessing;

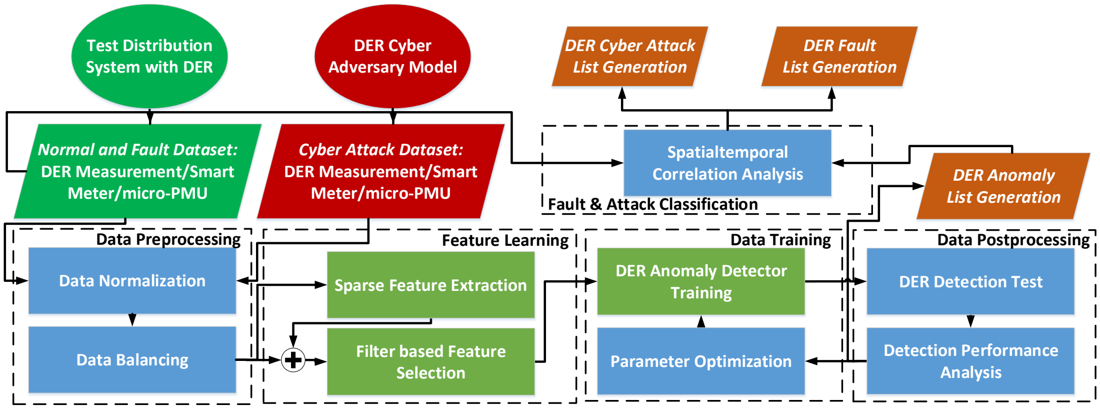

Test Distribution System with DER
DER Cyber Adversary Model
DER Cyber Attack List Generation
DER Fault List Generation
Normal and Fault Dataset: DER Measurement/Smart Meter/micro-PMU
Cyber Attack Dataset: DER Measurement/Smart Meter/micro-PMU
Spatialtemporal Correlation Analysis
Fault & Attack Classification
DER Anomaly List Generation
Data Preprocessing
Data Normalization
Data Balancing
Feature Learning
Sparse Feature Extraction
Filter based Feature Selection
Data Training
DER Anomaly Detector Training
Parameter Optimization
Data Postprocessing
DER Detection Test
Detection Performance Analysis

Figure 6.2: Flowchart for the multimodel DER attack detection framework.

5. DER anomaly list generation;

6. *Spatialtemporal correlation analysis for anomalies*;

7. DER cyber attack and fault scenarios classification.

In particular, the SAE is introduced for the sparse feature extraction, and a Relief based feature selection algorithm is proposed to select the most relevant features with a lower dimensionality from the total of input and extracted feature sets.

6.3.1 SAE based Feature Extraction

An autoencoder mainly contains two parts including an encoder and a decoder. Given a measurement point $\boldsymbol{x}^{(t)} \in \mathcal{X}$ with m DER features, the encoder first maps it to a $m'(< m)$-dimensional hidden representation (feature) $\boldsymbol{y}^{(t)} \in \mathbb{R}^{m'}$ through a deterministic mapping $\boldsymbol{y}^{(t)} = s_f(\boldsymbol{W}\boldsymbol{x}^{(t)} + \boldsymbol{b})$, where $s_f(\cdot)$ is a nonlinear activation function parameterized by a $m' \times m$ weight matrix $\boldsymbol{W}$ and a bias vector $\boldsymbol{b} \in \mathbb{R}^{m'}$. The derived latent representation $\boldsymbol{y}^{(t)}$ is then mapped by the decoder back to a reconstructed vector $\boldsymbol{z}^{(t)} \in \mathbb{R}^m$ in input space: $\boldsymbol{z}^{(t)} = s_g(\boldsymbol{W}'\boldsymbol{y}^{(t)} + \boldsymbol{b}')$, where $s_g(\cdot)$ is the decoder's activation function parameterized by a $m \times m'$ weight matrix $\boldsymbol{W}'$ and a bias vector $\boldsymbol{b}' \in \mathbb{R}^m$. In this chapter, the autoencoder is assumed to have tied weights, where $\boldsymbol{W}' = \boldsymbol{W}^T$. Each $\boldsymbol{x}^{(t)} \in \mathcal{X}$ is thus mapped to a corresponding $\boldsymbol{y}^{(t)}$ and a reconstruction $\boldsymbol{z}^{(t)}$. The parameters $\boldsymbol{\theta} = \{\boldsymbol{W}, \boldsymbol{b}, \boldsymbol{b}'\}$ of the autoencoder is optimized through minimizing the reconstruction loss $L(\boldsymbol{x}^{(t)}, \boldsymbol{z}^{(t)})$:

$$\boldsymbol{\theta}^* = \arg\min_{\boldsymbol{\theta}} L(\boldsymbol{x}^{(t)}, \boldsymbol{z}^{(t)}) = \min_{\boldsymbol{\theta}} L(\boldsymbol{x}^{(t)}, s_g(s_f(\boldsymbol{x}^{(t)}))), \tag{6.1}$$

where loss $L(\boldsymbol{x}^{(t)}, \boldsymbol{z}^{(t)})$ is defined from cross-entropy:

$$L = -\frac{1}{T}\sum_{t=1}^{T}\sum_{i=1}^{m}[x_i^{(t)} \log(z_i^{(t)}) + (1 - x_i^{(t)}) \log(1 - z_i^{(t)})]. \tag{6.2}$$

Due to the large scalability of the power distribution system integrated with DERs, the anomalies caused by limited attack resources usually lie in sparse regions of the extracted feature space $\boldsymbol{Y} := \{\boldsymbol{y}^{(t)} | t \in \boldsymbol{T}\}$. In order to keep the sparsity of the autoencoder, the average output of each extracted feature j: $\hat{\rho}_j = \frac{1}{T}\sum_{t=1}^{T} y_j^{(t)}$, $j = 1, ..., m'$, is enforced to a sparsity parameter ρ_0 close to zero. To achieve this, a sparsity regularization based on Kullback-Leibler (KL) divergence is added into the optimization objective (6.1) that penalizes $\hat{\rho}_j$ deviating significantly from ρ_0:

$$\boldsymbol{\theta}^* = \arg\min_{\boldsymbol{\theta}} L(\boldsymbol{x}^{(t)}, \boldsymbol{z}^{(t)}) + \lambda_S \sum_{j=1}^{m'} \mathrm{KL}(\rho_0 \| \hat{\rho}_j), \tag{6.3}$$

where $\mathrm{KL}(\rho_0 \| \hat{\rho}_j) = \rho_0 \mathrm{log}\, \frac{\rho_0}{\hat{\rho}_j} + (1 - \rho_{)}) \log \frac{1-\rho_0}{1-\hat{\rho}_j}$, and parameter λ_S controls the weight of the sparsity regularization.

Furthermore, to enforce robustness to partially destroyed or missing DER measurements, a modified denoising autoencoder is trained to reconstruct a repaired input from a corrupted version, which is done by first corrupting the initial input $\boldsymbol{x}^{(t)}$ into $\tilde{\boldsymbol{x}}^{(t)}$ by means of a stochastic mapping $\tilde{\boldsymbol{x}}^{(t)} \sim q_{\mathcal{D}}(\tilde{\boldsymbol{x}}^{(t)} | \boldsymbol{x}^{(t)})$. Corrupted input $\tilde{\boldsymbol{x}}^{(t)}$ is then mapped, as with the basic autoencoder, to a hidden representation $\tilde{\boldsymbol{y}}^{(t)} = s_f(\boldsymbol{W}\tilde{\boldsymbol{x}}^{(t)} + \boldsymbol{b})$, from which we reconstruct $\tilde{\boldsymbol{z}}^{(t)} = s_g(\boldsymbol{W}'\tilde{\boldsymbol{y}}^{(t)} + \boldsymbol{b}')$. The overall objective function of the de-

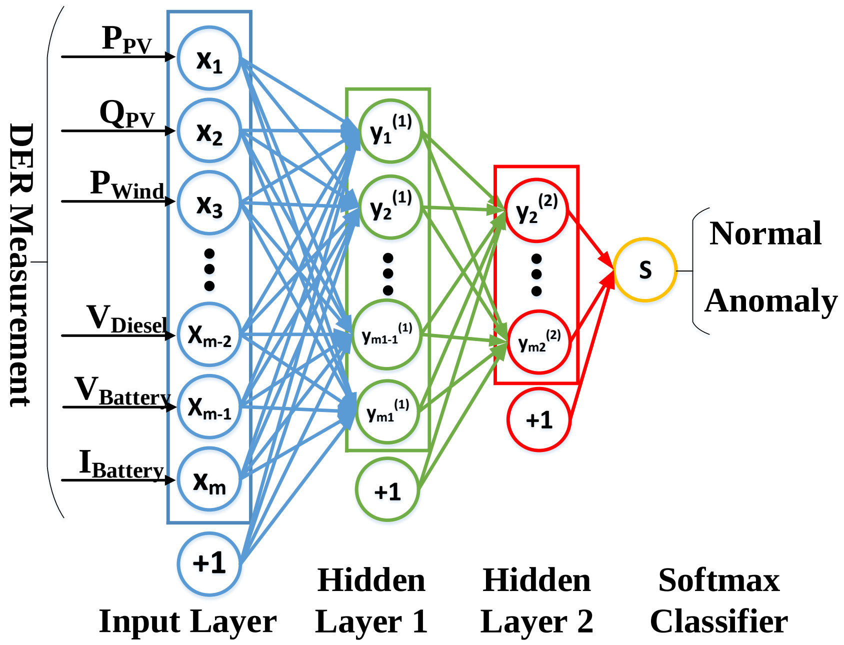


Figure 6.3: Network Architecture of SAE for Feature Extraction.

noising (sparse) autoencoder is:

$$\begin{aligned} \boldsymbol{\theta}^* = \arg\min_{\boldsymbol{\theta}} \quad & L(\boldsymbol{x}^{(t)}, \tilde{\boldsymbol{z}}^{(t)}) + \lambda \sum_{j=1}^{m'} \mathrm{KL}(\rho \| \tilde{\rho}_j), \\ s.t. \qquad & \tilde{\boldsymbol{x}}^{(t)} \sim q_{\mathcal{D}}(\tilde{\boldsymbol{x}}^{(t)} | \boldsymbol{x}^{(t)}), \end{aligned} \tag{6.4}$$

where $\tilde{\rho}_j = \frac{1}{T} \sum_{t=1}^{T} \tilde{y}_j^{(t)}$, $j = 1, ..., m'$, and $q_{\mathcal{D}}(\tilde{\boldsymbol{x}}^{(t)} | \boldsymbol{x}^{(t)})$ denotes $\tilde{\boldsymbol{x}}^{(t)} = \boldsymbol{x}^{(t)} + \varepsilon$, where ε is a zero-sum white Gaussian noise, $\tilde{\boldsymbol{x}}^{(t)} \sim N(0, \delta^2)$, and δ is the standard deviation of $\boldsymbol{x}^{(t)}$.

The SAE is a neural network consisting of multiple layers of denoising autoencoders, which can generate different levels of new features by adding hidden layers. In this chapter, we construct two layer SAE as shown in Fig. 6.3, where two denoising autoencoders are trained in a layer-wise manner. The input vector $\boldsymbol{x}^{(t)} \in \mathcal{X}$ is fed to *Input Layer* for training *Hidden Layer 1* of the first autoencoder. The outputs of the first autoencoder are propagated to *Hidden Layer 2* for deriving the second autoencoder. The overall process of encoding is $\boldsymbol{y}^{(t)} = s_{f1}(s_{f2}(\boldsymbol{W}\boldsymbol{x}^{(t)}+\boldsymbol{b}))$, where $s_{fi}(\cdot), i = 1, 2$, is the encoding function of Hidden Layer i. Correspondingly, the decoding process is: $\boldsymbol{z}^{(t)} = s_{g1}(s_{g2}(\boldsymbol{W}'\boldsymbol{y}^{(t)} + \boldsymbol{b}'))$, where $s_{gi}(\cdot), i = 1, 2$, is the decoding function of Hidden Layer i. The neurons of Hidden Layer 2 are used as extracted features of DER measurements, and *Final Layer* implements the softmax function for identifying the abnormal measurements based on the extracted features.

6.3.2 Relief based Feature Selection

Due to the increasing dimensionality of DER features, feature selection plays a critical role in the attack detection for reducing computational complexity and enhancing detection performance. The key idea of *Relief* based algorithms is to estimate each feature weight based on its ability to differentiate between neighboring features. Define the DER feature set to be $\mathcal{D} := \{\boldsymbol{d}^{(t)} | t \in \boldsymbol{T}\}$, where $\boldsymbol{d}^{(t)} = (\boldsymbol{x}^{(t)}, \boldsymbol{y}^{(t)}) \in \mathbb{R}^{m+m'}$ is composed of the original measurement $\boldsymbol{x}^{(t)} \in \mathcal{X}$ and its extracted feature $\boldsymbol{y}^{(t)} \in \boldsymbol{Y}$ through SAE. Given a randomly selected feature vector $\boldsymbol{d}^{(t)} = [d_1^{(t)}, ..., d_{m+m'}^{(t)}]^T$, the Relief algorithm first searches for its two nearest neighbors: one from the same class, termed the nearest hit NH($\boldsymbol{d}^{(t)}$), and the other from the different class, called the nearest miss NM($\boldsymbol{d}^{(t)}$). Let the feature weight vector to be $\boldsymbol{w} = [w_1, ..., w_{m+m'}]^T$ and the margin of $\boldsymbol{d}^{(t)}$ to be $\rho_d^{(t)} = \sum_{i=1}^{m+m'} |d_i^{(t)} - \text{NM}_i(\boldsymbol{d}^{(t)})| - \sum_{i=1}^{m+m'} |d_i^{(t)} - \text{NH}_i(\boldsymbol{d}^{(t)})|$. The optimal weight vector $\boldsymbol{w}^*$ then can be derived through maximizing the averaged margin computed with respect to $\boldsymbol{w}$:

$$\begin{aligned} \boldsymbol{w}^* = \arg\max_{\boldsymbol{w}} \quad & \frac{1}{T}\sum_{t=1}^{T}\Big(\sum_{i=1}^{m+m'}\big(w_i|d_i^{(t)} - \text{NM}_i(\boldsymbol{d}^{(t)})|\big) \\ & \qquad - \sum_{i=1}^{m+m'}\big(w_i|d_i^{(t)} - \text{NH}_i(\boldsymbol{d}^{(t)})|\big)\Big), \\ s.t. \qquad & \|\boldsymbol{w}\|_2^2 = 1, \boldsymbol{w} \geq 0, \end{aligned} \tag{6.5}$$

where the constraints correspond to the boundary of $\boldsymbol{w}$. However, the objective function of (6.5) only considers the nearest neighbors for calculating the averaged margin. Thus, the performance of Relief algorithm may be greatly deteriorated when a large amount of irrelevant features included in the dataset.

To increase the algorithm reliability, a modified objective function is proposed by searching for all hits/misses of each feature vector $\boldsymbol{d}^{(t)} \in \mathcal{D}$ instead of only the nearest hit/miss. We first define $\mathcal{M}^{(t)} = \{t'|\text{label}(\boldsymbol{d}^{(t')}) \neq \text{label}(\boldsymbol{d}^{(t)})\}$ and $\mathcal{H}^{(t)} = \{t'|\text{label}(\boldsymbol{d}^{(t')}) = \text{label}(\boldsymbol{d}^{(t)}), t' \neq t\}$ as the miss and hit sets of $\boldsymbol{d}^{(t)}$, respectively. By using the pairwise distances that have been computed when searching for the nearest hit and miss, the probability of $\boldsymbol{d}^{(t')}$, $\forall t' \in \mathcal{M}^{(t)}$, being the nearest miss of $\boldsymbol{d}^{(t)}$ can be defined as:

$$P_M(t'|\boldsymbol{d}^{(t)}, \boldsymbol{w}) = \frac{\sum_{i=1}^{m+m'} \left(w_i|d_i^{(t)} - d_i^{(t')}|\right)}{\sum_{t'' \in \boldsymbol{M}^{(t)}} \sum_{i=1}^{m+m'} \left(w_i|d_i^{(t)} - d_i^{(t'')}|\right)}. \tag{6.6}$$

Similarly, $\forall t' \in \mathcal{H}^{(t)}$, the probability of $\boldsymbol{d}^{(t')}$ being the nearest hit of $\boldsymbol{d}^{(t)}$ can be defined as:

$$P_H(t'|\boldsymbol{d}^{(t)}, \boldsymbol{w}) = \frac{\sum_{i=1}^{m+m'} \left(w_i|d_i^{(t)} - d_i^{(t')}|\right)}{\sum_{t'' \in \boldsymbol{H}^{(t)}} \sum_{i=1}^{m+m'} \left(w_i|d_i^{(t)} - d_i^{(t'')}|\right)}. \tag{6.7}$$

Finally, $\boldsymbol{w}$ can be derived by solving the following problem:

$$\begin{aligned} \boldsymbol{w}^* = \arg\max_{\boldsymbol{w}} \quad & \frac{1}{T}\sum_{t=1}^{T}\Big(\sum_{t' \in \boldsymbol{M}^{(t)}} P_M(t'|\boldsymbol{d}^{(t)}, \boldsymbol{w}) \\ & - \sum_{t' \in \boldsymbol{H}^{(t)}} P_H(t'|\boldsymbol{d}^{(t)}, \boldsymbol{w})\Big), \\ s.t. \quad & \|\boldsymbol{w}\|_2^2 = 1, \boldsymbol{w} \geq 0. \end{aligned} \tag{6.8}$$

The feature weight w_i, $i = 1, ..., m + m'$, is updated after integrating all of the feature vectors in $\mathcal{D}$. In order to select the important features, a threshold $\sigma > 0$ is selected, and the feature satisfying $w > \sigma$ is collected for DER anomaly detection.

Let $\mathcal{S} = \{s_1, s_2, ..., s_N\}$ be the index set of the selected N DER features, the selected feature set then can be defined as $\mathcal{D}_S = \{\{d_s^{(t)}|s \in \boldsymbol{S}\}|t \in \boldsymbol{T}\}$. An ensemble classifier is implemented to classify $\mathcal{D}_S$ into “Normal” and “Anomaly”, in which P subsets of tuples of size $n(< N)$ are created by uniformly sampling from $\mathcal{D}_S$ with replacement. Therefore, P subsets $\{\mathcal{D}_1, ..., \mathcal{D}_P\}$ are generated and P decision tree classifiers $\{\mathcal{C}_1, ..., \mathcal{C}_P\}$ are built on each subset $\mathcal{D}_i$, $i = 1, .., P$. A final ensemble classifier classifies a DER feature example $\{d_s^{(t)} | s \in \boldsymbol{S}\}$ by giving as output the class predicted most often by $\{\mathcal{C}_1, ..., \mathcal{C}_P\}$. In addition, the ensemble classifier can be implemented for the parallel computing, in which each subset $\mathcal{D}_i$ resides on a different processor within the parallel computer.

6.3.3 DER Fault and Cyber Attack Classification

Situation awareness of the anomaly event such as a system fault or cyber attack is critical for utility operators to make a reaction. Specially, this chapter propose a *spatiotemporal correlation* based approach to accurately extract patterns of system faults and cyber attacks from the generated DER anomaly list derived by the ensemble classifier. Spatiotemporal correlation is a natural property found in various physical phenomena including power system fault scenarios, since the system components are typically continuous over both the time and spatial domains. For the spatial domain, the DERs, such as PV farm and battery storage, deployed in a nearby area are interdependent in such a way that the fault of one DER device would affect the power quality of other independent devices and may cause the faults of other DERs. In addition, these spatial correlations should be similar to those that have occurred in the past, that is, these DER devices are temporally correlated.

Define the anomaly measurement set to be $\mathcal{X}_D = \{\boldsymbol{x}^{(t)} | t \in \boldsymbol{T}_D\}$, where $\boldsymbol{T}_D \subseteq \boldsymbol{T}$ denotes for the anomaly period. Each anomaly $\boldsymbol{x}^{(t)} \in \mathcal{X}_D$ is an m-dimensional vector corresponding to m DER devices. Given two DER devices ($i, j \in \mathcal{M}$), the correlation coefficient ρ_{ij} between two is:

$$\rho_{ij} = \frac{\sum_{t\in\boldsymbol{T}_D}(x_{Di}^{(t)} - \mu_i)\sum_{t\in\boldsymbol{T}_D}(x_{Dj}^{(t)} - \mu_j)}{\sqrt{\sum_{t\in\boldsymbol{T}_D}(x_i^{(t)} - \mu_i)^2}\sqrt{\sum_{t\in\boldsymbol{T}_D}(x_j^{(t)} - \mu_j)^2}}, \tag{6.9}$$

where μ_i and μ_j are the means of device measurement $\{x_i^{(t)}|t \in \boldsymbol{T}_D\}$ and $\{x_j^{(t)}|t \in \boldsymbol{T}_D\}$, respectively. In this approach, we first define a correlation sphere $\mathcal{G}$ satisfying that, for each DER device pair $(i, j) \in \mathcal{G}$, the correlation coefficient ρ_{ij} between two is greater than a constant threshold $\tau \in (0, 1)$. Thus, the correlation neighbor set $\mathcal{N}_i$ of device $i \in \mathcal{G}$ contains all the DER devices in $\mathcal{G}$ excluding i. The definition of correlation sphere can guarantee that all of DER devices in $\mathcal{G}$ are spatially and temporally correlated in fault scenarios. However, in the DER cyber attack scenarios, assume that the attacker has limited resources and cannot access all DER devices in $\mathcal{G}$, therefore, the attacked DER device will not be correlated with the other DER devices in its neighbor set. Given a DER device $i \in \mathcal{G}$, let $|\mathcal{N}_i|$ be the number of DER devices in its neighbor set, and $|\mathcal{N}_i^D|$ be the correlated DER device number in $\mathcal{X}_D$. If $\frac{|\mathcal{N}_i^D|}{|\mathcal{N}_i|} > 50\%$, DER device i is classified into a fault scenarios. Otherwise, its measurement is under cyber attacks.

6.4 Test System and Dataset Formulation

A test distribution system, shown in Fig. 6.4, is used for simulating system scenarios and formulating corresponding DER measurement datasets. The developed test system is a modified version of the IEEE 34-bus system. The test distribution system is integrated with four types of DERs including PV farm, wind turbine generator (wind farm), utility scale battery energy system, and diesel generator, where DERs are connected to a distribution node via a transformer having rating equal to the volts-ampere (VA) rating of DERs. In the test system, the nominal voltage level is set to be 12.47 kV L-L; *PV farm* is rated at 5 MW with modeled MPPT controller, DC-DC converter, and a three-phase

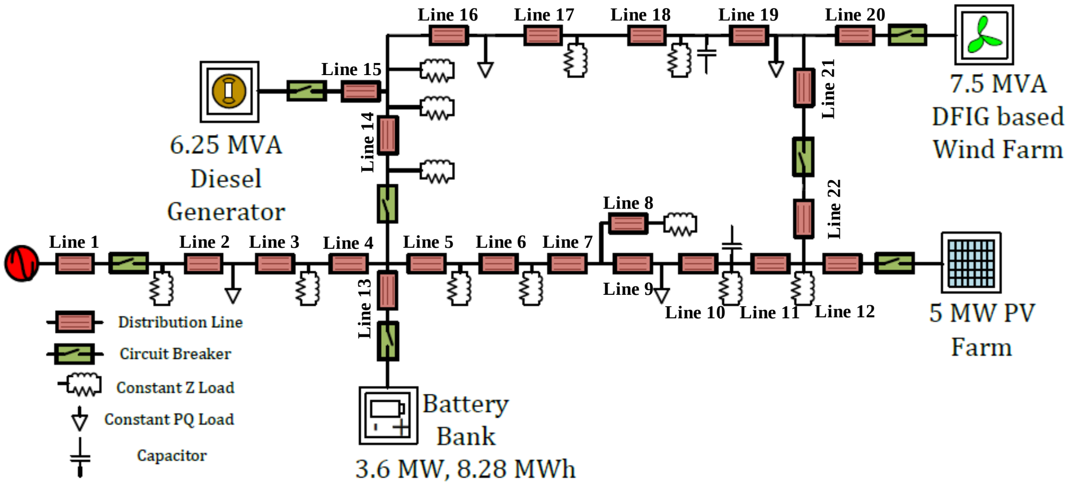


Figure 6.4: The test distribution system integrated with four types of DERs.

inverter; *wind farm* is modeled using a single doubly fed induction generator of 7.5 MVA capacitor including major components, such as rotor-side converter (RSC), grid-side converter (GSC), pitch controller, and two mass model for wind turbines; *battery bank* is rated at 360 kW, 828 kWh with terminal voltage of 720 V dc, and the *battery inverter* is rated at 540 kVA to provide enough reactive power support to the feeder; *diesel generator* is rated at 6.25 MVA with diesel engine governor, and IEEE AC1A type excitation system. The battery inverter, PV inverter, and wind generator have the provision operated in one of the following three modes of control:

1. *Voltage control mode*: With the voltage setpoint decided by the grid operator and the DER tries to maintain its point of common coupling voltage at the desired setpoint.
2. *Reactive power control mode*: With the reactive power set point decided by the grid operator and the DER tracks the reactive power setpoint.
3. *Power factor control mode*: With the power factor at the DER point of common coupling decided by the grid operator and the DER tracks the power factor setpoint.

Table 6.1: Simulated Scenarios For Test Distribution System

State	No.	Scenario Description
Normal	S1	Normal system operation and no event occurring.
Fault	S2	Three phase fault on Line 1.
	S3	Three phase fault on Line 16.
	S4	Two three phase faults on both Line 1 and 16.
Cyber Attack	S5-S9	Five types of attacks on PV farm power measurement.
	S10-S14	Five types of attacks on wind farm RMS measurement.
	S15-S19	Five types of attacks on battery power measurement.
	S20-S24	Five types of attacks on diesel power measurement.
	S25-S29	Five types of attacks on distribution node measurement.

In addition, the system is designed to operate in both radial system and loop configuration, and has a provision to operate in both islanded and grid connected modes.

The system scenarios simulated by the test system are utilized to train and validate the proposed DER attack detection framework, which have been grouped into three categories: 1) normal operation; 2) three phase line-to-ground faults; and 3) cyber attacks. Given a initial system state, Table 6.1 lists the 29 simulated system scenarios, where each scenario is named with capital “S” along with a number. For scenario S1, the test distribution system is in the normal operation state without abnormal events occurring. Three phase line-to-ground faults are injected into the distribution lines for fault scenarios S2-S4 simulation. Specially, S2 represents a scenario, in which a three phase fault is injected into Line 1, and S3 shows the scenario that a three phase fault occurs on Line 16. Two three phase faults are instantaneously injected into both Line 1 and 16 for S4.

For scenarios S5-S29, the five types of cyber attacks proposed in Section II, including DoS attack, fault replay attack, two types of data manipulation attack, and device misconfiguration attack, are simulated for the distribution node and each DER in the test distribution system. Especially, S5-S9 simulate five types of cyber attacks on the PV farm power measurement, respectively. S10-S14 inject five types of cyber attacks targeted at the root mean square (RMS) measurement of WTG. S15-S19 represent five types of cyber attacks on the battery bank power measurement. S20-S24 describe five types of cyber attacks for the diesel generator power measurement. In addition, S25-S29 show five types of cyber attacks on the distribution node power measurement. Taking the real power measurement of the distribution node as example, Fig. **??** presents its normal measurement (S1), fault measurement (S2), DoS attack (S25), fault replay attack (S26), two types of data manipulation attacks (S27-S28), and device misconfiguration attack (S29), respectively.

The collected dataset consists of data logs associated with 2×10^5 simulated instances for each system scenario. Each data log is a CSV file with labeled tuples including 21 types of measurement data and a time stamp. The 21 data sources are collected from the distribution node and four types of DERs including PV farm, WTG, battery energy system, and diesel generator. The real $\&$ reactive power measurements and three phase V-I measurements are collected for the distribution node and PV farm. The RMS measurement is selected for WTG. For battery energy system, the real $\&$ reactive power measurements, the State of Charge (SoC) measurement, RMS measurement, and grid real $\&$ reactive power measurements are gathered together. The real $\&$ reactive power measurements and RMS measurement are collected for the diesel generator. In addition, relay information, breaker events, snort alerts, and control panel alerted are logged for the dataset. The simulation timestep is set to be 50 μs, and all logged data is merged into a single dataset.

6.5 Numerical Experiment

This section evaluates the performance of the proposed DER attack detection framework using the test dataset, in which the dataset of fault and cyber attack scenarios is labeled as “Anomaly”, while the dataset simulated in normal conditions is named as “Normal”. First, the dataset is preprocessed through normalization and balancing. The SAE based feature extraction and Relief based feature selection are then introduced for an ensemble classifier for DER anomaly detection. Finally, the spatiotemporal correlation approach is implemented to classify faults and cyber attacks in the generated anomaly list.

6.5.1 Data Preprocessing and Detection Evaluation Metrics

1) Data Normalization: The DER measurements contained in the test dataset are generally diverse in a flexible value, therefore, the preprocessing phase first implements data normalization to transform all measurement ranges to be equal. The mean range method is adopted, in which each device measurement $\boldsymbol{x}_i = [x_i^{(1)}, ..., x_i^{(T)}]^T$, $i \in \mathcal{M}$, is linearly normalized in $[0, 1]$ in order to avoid the undue influence of different scales. Given a measurement point $x_i^{(t)} \in \boldsymbol{x}_i$, the normalized measurement $z_i^{(t)}$ can be derived by: $z_i^{(t)} = \frac{x_i^{(t)} - \min(\boldsymbol{x}_i)}{\max(\boldsymbol{x}_i) - \min(\boldsymbol{x}_i)}$, where $\min(\boldsymbol{x}_i)$ and $\max(\boldsymbol{x}_i)$ are the minimum and maximum values of device i measurement, respectively.

2) Data Balancing: In the test dataset, abnormal instances from scenarios S2-S29 significantly outnumber normal instances in S1, and the ratio between two is 28:1, which is not a good representation of real situations. In addition, this property might be biased to the attack detection model and affect its performance. To alleviate this, we balance the dataset by randomly selecting the abnormal instances, and make the ratio between normal and abnormal instances to be 1:1, which is an appropriate proportion for the model training phase.

3) Evaluation Metrics: In order to compare the performance of the proposed DER attack detection framework with existing detection mechanisms, the following evaluation metrics are implemented: *Accuracy* (Acc), *Detection Rate* (DR), *Precision*, *False Alarm Rate* (FAR), F_1 *Score*, *Matthews Correlation Coefficient* (Mcc),*CPU Time of Model Building* (T_B), and *Prediction Speed* (S_p). In these metrics, Acc($\%$) represents the overall effectiveness of an algorithm. DR($\%$) refers to the number of anomaly detected divided by the total number of abnormal instances, while Precision($\%$) counts the number of anomaly detected among the total number of instances classified as anomaly. FAR($\%$) is the number of normal instances mistakenly classified as anomaly divided by the total number of normal instances. F_1($\%$) measures the harmonic mean of Precision and DR. Mcc($\%$) represents the correlation coefficient between the detected and observed data. The proposed DER attack detection framework aims to achieve a high Acc, DR, Precision, F_1, Mcc, and S_p, and simultaneously maintain low FAR and T_B.

The metrics can be defined by the following equations:

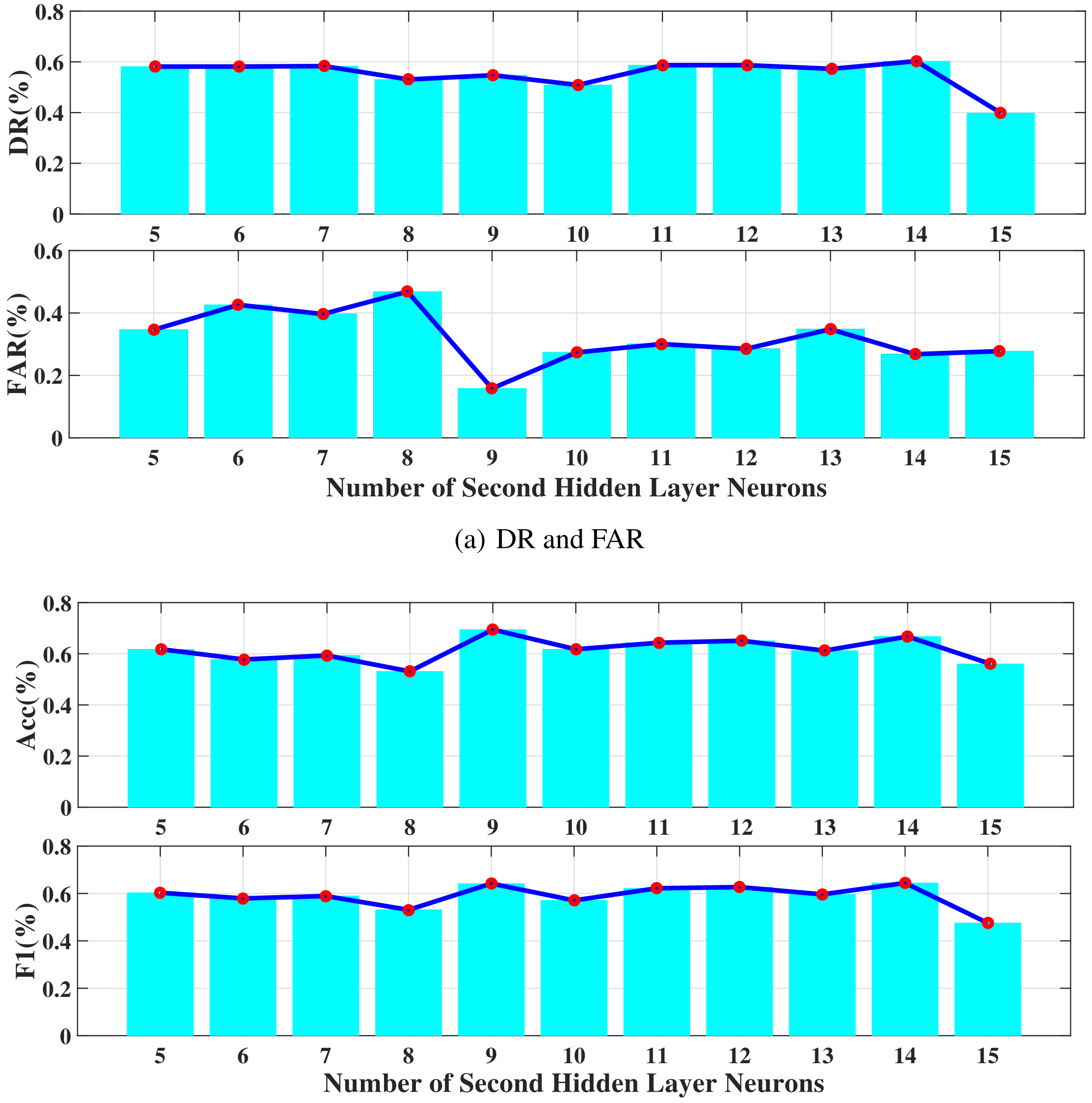
$$\begin{aligned}
&Acc = \frac{TP+TN}{TP+TN+FP+FN}(\%),\\
&DR = \frac{TP}{TP+FN}(\%),\\
&FAR = \frac{FP}{TN+FP}(\%),\\
&F_1 = \frac{2TP}{2TP+FP+FN},\\
&Mcc = \frac{TP\times TN - FP\times FN}{\sqrt[2]{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}},
\end{aligned} \tag{6.10}$$

where TP is the number of intrusions correctly classified as an attack, TN is the number of normal instances correctly classified as a benign packet, FN is the number of intrusions incorrectly classified as a benign packet, and FP is the number of normal instances incorrectly classified as an attack.

6.5.2 Sparse Feature Extraction and Selection

1) SAE based Feature Extraction: The SAE architecture with two hidden layers is utilized to extract the new features from the preprocessed dataset, in which the features generated from the first encoder layer are employed as the training data in the second encoder layer. Meanwhile, the size of each hidden layer is decreased accordingly such that the encoder in the second encoder layer learns an even smaller representation of the input data. The classification layer with the softmax activation function is then implemented in the final step. Although there is no strict rule for determining the number of hidden neurons, it is generally selected from 70% to 90% of the input neurons [137]. In the formulated SAE architecture, the first hidden layer is set to have 20 neurons. The SAE architecture is then introduced for classifying the preprocessed dataset, and its performance is compared for different numbers of second hidden layer neurons. The evaluation metrics including *Detection Rate* (DR), *False Alarm Rate* (FAR), *Accuracy* (Acc), and F_1 *Score* are shown in Fig. 6.5 for the SAE architecture with varying the number of second hidden layer neurons from 5 to 15. In Fig. 6.5(a), the formulated SAE architecture achieves similar DR around 60% when the second hidden layer neurons are selected from 5 to 14, while it only derives 40% DR when 15 second hidden layer neurons are defined. However, when the second hidden layer is set to have 9 neurons, the least FAR of 15.8% is derived. Meanwhile, in Fig. 6.5(b), the SAE architecture achieves the highest Acc (69.5%) and F_1 (64.1%) for 9 second hidden layer neurons. As a result, the SAE architecture is chosen with 21:20:9:2 topology.

2) Feature Selection: The preprocessed test dataset is then integrated with extracted features from the second hidden layer of the SAE architecture. In the integrated dataset, even though each instance is represented by various features, not all of these features are needed to build an attack detection model. Therefore, it is important to identify the most informative features from the integrated dataset to achieve higher performance. The



(a) DR and FAR

(b) Acc and F_1

Figure 6.5: The evaluation metrics of DR, FAR, Acc, and F_1 for the formulated SAE architecture with various numbers of second hidden layer neurons ranging from 5 to 15. (a) for DR(%) and FAR(%), (b) for Acc(%) and F_1(%).

proposed modified Relief based algorithm (MRelief) is compared with 7 state-of-the-art algorithms for feature selection:

- Latent feature selection (LFS);
- Infinite latent feature selection (Inf-FS);
- Feature selection via eigenvector centrality (EC-FS);
- Distributed mutual information feature selection (DisMI);
- Unsupervised multi-cluster data feature selection (MC-FS);
- Generalized Fisher score for feature selection (Fisher);
- L1 regularized discriminative feature selection (L1-FS).

Based on the feature ranking/weight derived by these algorithms, the first 15 features are selected as inputs from each algorithm for training and evaluating a decision tree based ensemble classifier independently. The anomaly detection performance is measured by DR, FAR, Acc, and F_1. Table 6.2 lists the feature selection algorithms compared, where we note their *types* as filters and wrappers. The feature ranking/weight for total 30 features and the classification evaluation metrics are also reported. From the table, we can find that MRelief achieves the best anomaly detection performance with the highest DR, Acc, and F_1 of 99.48%, 99.69%, and 99.69%, respectively. At the same time, the lowest FAR (0.1%) is derived. In addition, based on the feature ranking/weight derived by these algorithms, we can see that some features are essential for DER anomaly detection, such as the power measurement data of the battery bank (Feature 19 and 20). This phenomenon can be explained that the power of the battery bank will change significantly when some faults or failures occur.

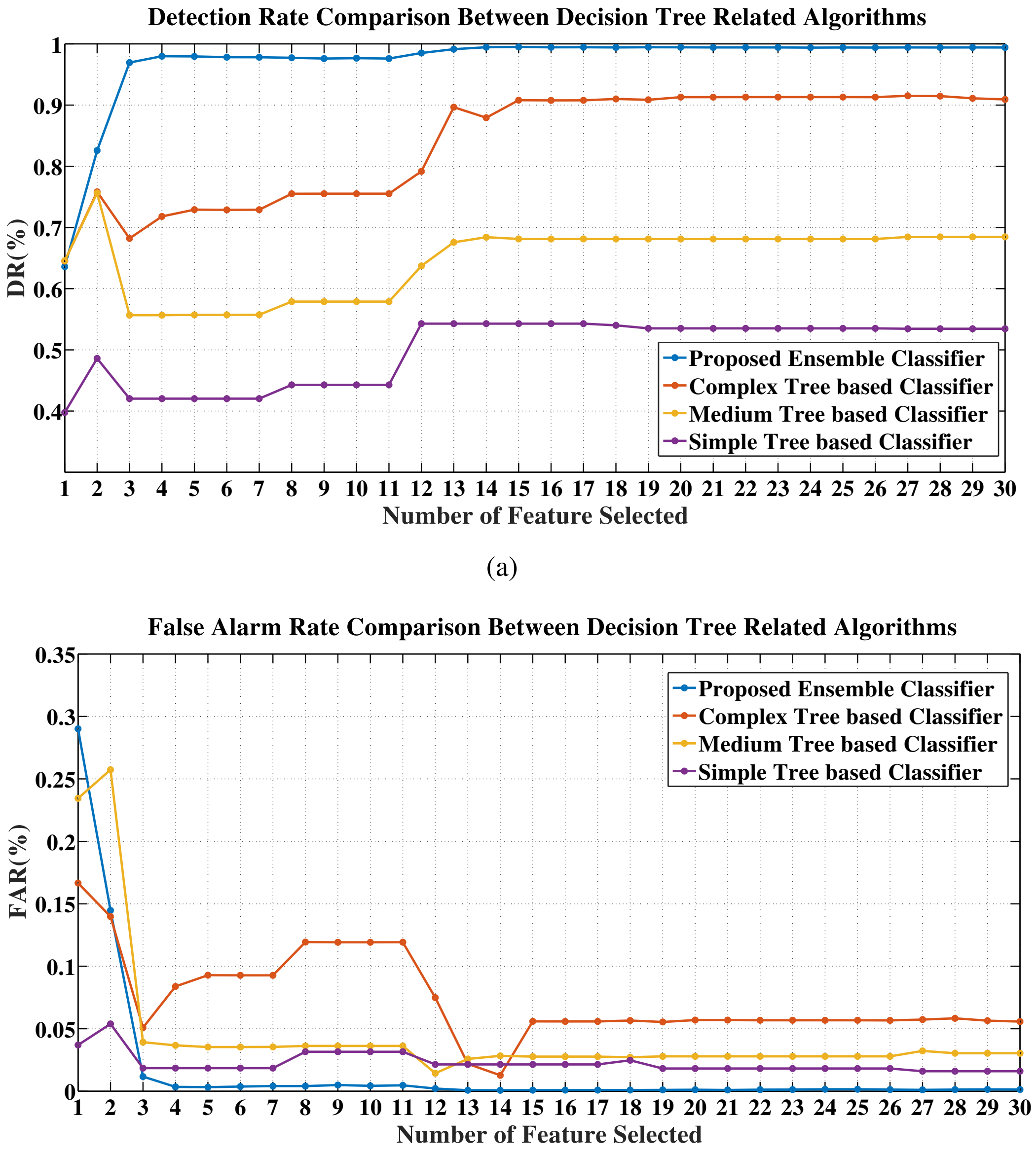
Table 6.2: Anomaly Detection Comparison of Feature Selection Methods

Method	**Type**	**Feature Ranking/Weight**	**DR(%)**	**FAR(%)**	**Acc(%)**	F_1**(%)**
MRelief	filter	**19,20,6,5,1,9,4,2,8,3,7,11,16,17,27**,12,15,10,18,13,28,22,25,26,23,21,24,14,29,30	**99.48**	**0.10**	**99.69**	**99.69**
LFS [138]	filter	**11,21,24,13,28,18,12,27,10,4,7,16,3,17,8**,22,14,9,26,25,23,2,1,6,5,29,20,30,15,19	97.43	2.91	97.25	97.26
Inf-FS [138]	filter	**19,20,11,5,21,23,22,2,24,1,26,25,6,9,8**,3,7,4,10,16,27,12,18,13,30,17,28,14,29,15	98.39	0.209	99.09	99.08
EC-FS [139]	filter	**19,20,11,21,23,22,24,25,26,5,2,1,6,9,8**,3,7,4,27,12,10,16,18,13,30,17,28,14,29,15	98.37	0.19	99.09	99.08
DisMI [49]	filter	**11,19,20,27,12,2,5,1,6,9,8,3,7,4,30**,16,13,17,10,18,28,14,15,29,22,23,21,25,26,24	99.41	0.12	99.64	99.64
MC-FS [140]	filter	**4,8,7,26,23,21,24,25,22,2,1,3,6,12,27**,5,9,10,19,20,18,17,11,28,13,30,14,15,16,29	96.87	2.20	97.33	97.32
Fisher [48]	filter	**5,19,2,1,20,6,9,8,3,7,4,11,10,27,18**,12,13,28,16,14,17,30,29,15,24,21,22,25,23,26	99.32	0.13	97.32	97.32
L1-FS [141]	wrapper	**3,1,9,5,7,6,2,4,8,12,27,24,19,25,20**,22,23,17,21,26,13,15,11,28,14,16,10,18,29,30	98.35	0.19	99.08	99.06

6.5.3 Comparisons With State-of-the-Art Methods

Based on the feature ranking derived by the MRelief, we compare the anomaly detection performance of the proposed ensemble classifier with three other decision tree based classifiers including: 1) simple tree with 4 branch nodes, 2) medium tree with 20 branch nodes, and 3) complex tree with 100 branch nodes. Fig. 6.6 plots the DR and FAR for the four decision tree based classifiers with varying the number of selected features from 1 to 30. From this figure, we can find that the proposed ensemble classifier achieves higher DR and lower FAR compared with other three classifiers, when more than 2 features are selected for training the classification model. Especially, in Fig. 6.6(a), the proposed ensemble classifier achieves 99.48% DR after 15 features are selected, while the complex tree obtains 90.8%, the medium tree derives 68.12%, and the simple tree only acquires 54.29%. Meanwhile, as shown in Fig. 6.6(b), the proposed ensemble classifier achieves 0.1% FAR after 15 features are selected, which is lower than 5.59% of the complex tree, 2.83% of the medium tree, and 2.17% of the simple tree. Additionally, in Fig. 6.6(a), with the increasing of branch nodes, the decision tree based classifier can derive higher DR. However, when more than 3 features are selected, the simple tree based classifier can obtain lower FAR than medium and complex tree based classifiers, as depicted in Fig. 6.6(b).

We also compare the performance of the proposed ensemble classifier based DER attack detection method against existing classification methods, such as *Quadratic Dis-*



(a)

(b)

Figure 6.6: The DR(%) and FAR(%) comparison between the decision tree based classifiers with various numbers of feature selected based on the feature ranking derived by MRelief. (a) for DR; (b) for FAR.

Table 6.3: Anomaly Detection Comparison With Existing Methods

Model Type	**DR(%)**	**FAR(%)**	**Acc(%)**	$\boldsymbol{F_1}$**(%)**	$\boldsymbol{T_B}$**(s)**
Proposed Detection	**99.48**	**0.10**	**99.69**	**99.69**	82.82
Quadratic [39]	50.06	20.48	64.79	58.71	**1.84**
Logistic [142]	56.07	17.11	69.48	64.75	4.89
SVM [40]	98.61	0.36	99.13	99.13	938.92
kNN [41]	98.33	0.62	98.85	98.85	171.4

criminant Analysis, *Logistic Regression Classifier*, *SVM*, and *Nearest Neighbor Classifier*, and their evaluation metrics, like DR, FAR, Acc, F_1, and the computing time for model building (T_B), are provided in Table 6.3. Compared with other four existing algorithms, we can see that the proposed DER attack detection algorithm shows the best performance by achieving the highest DR (99.48$\%$), Acc (99.69$\%$) and F_1 (99.69$\%$), and the lowest FAR (0.1%). Even though the nearest neighbor classifier and SVM algorithm derive the competitive detection results, their T_B are 2.07 and 11.34 times longer than the proposed DER attack detection algorithm, respectively. The quadratic discriminant analysis and logistic regression classifier consume less T_B, whereas they only achieve Acc of 64.79% and 69.48%, which are not satisfactory for accurate DER attack detection.

6.5.4 DER Fault and Cyber Attack Classification

Based on the spatiotemporal correlation in scenario S1, we define a correlation sphere $\mathcal{G}$ including the real $\&$ reactive power measurements (P_0,Q_0) at the distribution node, the real $\&$ reactive power measurements (P_G,Q_G) and RMS measurement (RMS$_G$) for the diesel generator, the RMS measurement data (RMS$_W$) for the wind generator, and the real $\&$ reactive power measurements (P_P,Q_P) for the PV farm. Therefore, we can define the neighbor set of P_P as: $\mathcal{N}_{P_P} = \{P_0, Q_0, P_G, Q_G, \text{RMS}_G, \text{RMS}_W, Q_P\}$. In the fault scenarios S2-S4, the correlation ratio $\frac{|\mathcal{N}^C_{P_P}|}{|\mathcal{N}_{P_P}|}$ for P_P is 100%, 57.14%, 100%, respectively.

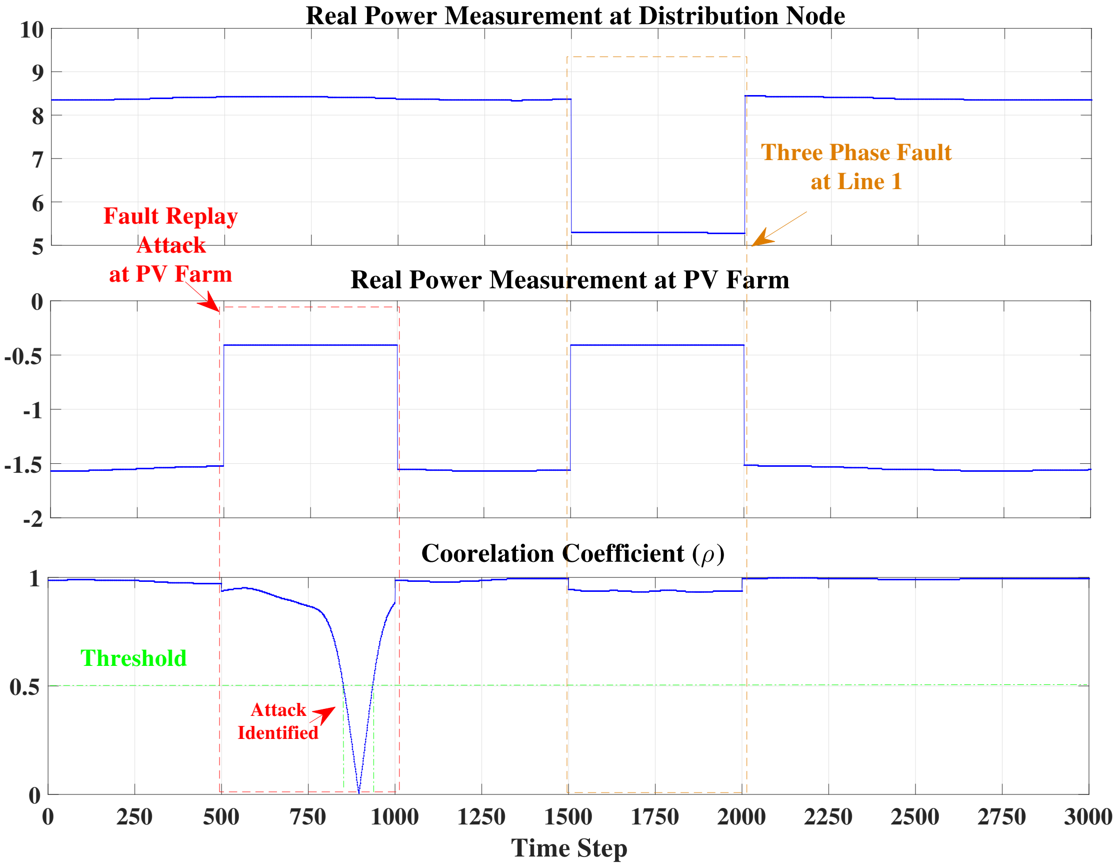


Figure 6.7: P_0 measurement, P_P measurement, and their coorelation coefficient ρ_{ij} change from time step 1 to 3000, where cyber attack occurs at PV farm from 500 to 1000, and a three phase fault occurs on Line 1 from 1500 to 2000.

However, for cyber attack scenarios S5-S9, the correlation ratio is only 14.29%, which is less than 50%. Since the cyber attacks are injected into the PV power measurements in S5-S9, P_P is only spatiotemporally correlated with Q_P except other measurements in $\mathcal{N}_{P_P}$. In order to describe the spatiotemporal correlation approach in time series, we introduce the measurements P_0 and P_P from time step 1 to 3000, where a fault replay attack is injected into P_P from time step 500 to 1000. Assume that a three phase line-to-ground fault occurs on Line 1 from time step 1500 to 2000, Fig. 6.7 plots the measurements (P_0,P_P) and their coorelation coefficient ρ_{ij} change from time step 1 to 3000. From this figure, we can see that ρ_{ij} decreases below 0.5 during the cyber attack period from 500 to 1000, whereas it keeps around 0.9 during the fault period from 1500 to 2000.

6.6 Summary

In this chapter, we introduced a novel DER cyber attack detection framework that integrates spare feature learning and spatiotemporal correlation analysis. First, a two-layer SAE architecture was formulated to extract the abstract representations from large-volume DER measurement datasets. The MRelief feature selection was then developed to provide the feature ranking for both original measurements and extracted representations. Furthermore, we combined the SAE architecture and MRelief with a decision tree based ensemble classifier for identifying the abnormal events in the DER measurement dataset. The normal, fault, and cyber attack system scenarios simulated by the IEEE 34-bus test distribution system are utilized for training the proposed ensemble classifier. Compared with existing detection methods such as decision tree, quadratic discriminant analysis, logistic regression classifier, SVM, and nearest neighbor classifier, the proposed DER anomaly detection framework achieved the best performance of 99.48% DR, 99.69% Acc, 99.69% F_1, and only 0.1% FAR. Finally, a spatiotemporal correlation sphere is developed for PV farm in the test distribution system for classifying the fault scenarios and the potential cyber attacks in the generated abnormal event list.

CHAPTER 7

A Distributed Intelligent Framework for Electricity Theft Detection

Electricity theft is a major contributor of non-technical losses in the distribution systems of the smart grid. However, owing to the resource-limitations of smart meters and the privacy requirement of electricity usage data, theft detection has become a challenging task for electric utilities. To address this problem, a Distributed Intelligent Framework for Electricity Theft Detection (DIFETD) is proposed and implemented in this chapter. Section 7.1 make a summary of this chapter. A summary of related work is provided in Section 7.2. Benford's Analysis for preliminary theft detection is explained in Section 7.3. A Stackelberg game between utility and thieves is proposed in Section 7.4. LRT for theft detection is described in Section 7.5. While Section 7.6 discusses data cleansing and the results, Section 7.7 provides conclusion and future work.

7.1 Overview

The transformation of the traditional power grid into a smart grid capable of advanced computing and communication functions, self-healing, and autonomy is expected to guarantee an improved efficiency, reliability, and security [143–145]. Advanced Metering Infrastructure (AMI) is a key component of the smart grid, which brings together technologies deployed at the customer to the utility level and supports smart meters capable of bidirectional communication [146]. However, proliferation of smart meters has rendered the distribution system vulnerable to cyber-attacks [147, 148]. Particularly, electricity theft is a major challenge for utilities, where malicious attackers alter usage measurements collected by smart meters. According to the U.S. Energy Information Administration in 2016, between 1.5 and 2% of electricity in the U.S. is lost due to theft, costing utilities as much as $\$6$ billion annually [33, 149]. Although most traditional theft detection methods consider both technical as well as Non-Technical Losses (NTLs), this chapter focuses on NTLs caused by deliberate acts to manipulate electricity usage data by actors called electricity thieves, referred to in this chapter as *thieves*.

The main contribution of this chapter is the development and implementation of a data-driven Distributed Intelligent Framework for Electricity Theft Detection (DIFETD) for smart meters. The proposed method first uses Benford's Analysis [150] to study the distribution of significant digits in a machine-generated data. The analysis is based on Benford's Law which states that the frequency of occurrence of the first significant digit in a machine generated and natural data is around 30.1%, which is much higher than the expected value of 11.1% [151]. The analysis compares the Probability Density Function (PDF) of the leading significant digits of the structured electricity usage data with the baseline curve to which it must ideally adhere. Any violation therein signifies the occurrence of suspected theft. The baseline curve is the PDF of the leading significant digits of Fibonacci series which strictly conforms to Benford's Law [152]. Therefore, the Benford's Analysis provides the first but important diagnostic of the dataset.

Additionally, the proposed method provides a mathematical approach to maximize theft detection probability with minimum false positives. As shown in Fig. 7.1, for any AMI data that fails Benford's Analysis, the following steps are executed: **1)** Implementation of Maximum Likelihood Estimator (MLE) for training historical usage data of customers and development of the adversary model of multiple thieves; **2)** Formulation of a Stackelberg game where the utility aims to maximize theft detection probability while limiting false positives and the thieves engage in a non-cooperative strategic game by stealing different amounts of electricity to maximize the trade-off between rewards and probability of being detected; and **3)** Application of the proposed game to obtain a Stackelberg equilibrium from which the customer sampling rate l and a threshold value are derived. Likelihood Ratio Test (LRT) at the sampling rate l and the derived threshold value

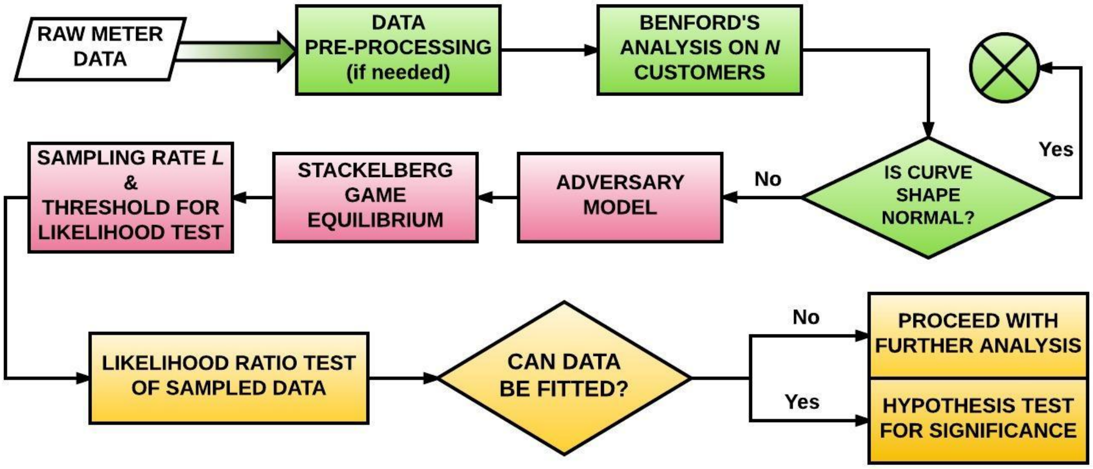

RAW METER DATA
DATA PRE-PROCESSING (if needed)
BENFORD'S ANALYSIS ON *N* CUSTOMERS
IS CURVE SHAPE NORMAL?
Yes
No
ADVERSARY MODEL
STACKELBERG GAME EQUILIBRIUM
SAMPLING RATE *L* & THRESHOLD FOR LIKELIHOOD TEST
LIKELIHOOD RATIO TEST OF SAMPLED DATA
CAN DATA BE FITTED?
No
PROCEED WITH FURTHER ANALYSIS
Yes
HYPOTHESIS TEST FOR SIGNIFICANCE

Figure 7.1: Schematic of the proposed data-driven Distributed Intelligent Framework for Electricity Theft Detection (DIFETD).

is implemented for classifying each customer into normal customers or thieves. Therefore, the specific meters being compromised are identified for final checking. It ensures faster resolution, minimal latency, and identification of suspicious meters from which associated customers could be discovered. The proposed method was implemented using real-world AMI interval data collected from an electric utility in Florida, USA, that contained multiple suspected electricity thefts. It is noteworthy that the terms *attack* and *theft* are used interchangeably.

7.2 Related Work

The significance of cybersecurity for smart meters has been a well-researched topic in the literature, where the focus is on ensuring power availability at all times.Traditional research on electricity theft detection has focused on employing specific devices, like wireless sensors and balance meters, to provide a high electricity theft detection accuracy [153, 154]. In [153], an AMI intrusion detection system was proposed to accurately detect electricity theft, where anti-tampering sensors were embedded into smart meters. A set of trusted balanced meters were implemented in the distribution network of smart grid to detect electricity theft [154]. Although these research works reduce the risks due to unmeasured and non-billed usage of electricity, they do not identify specific meters being compromised. Further, these methods significantly increase the cost of deploying and operating millions of smart meters.

Despite cyber-physical vulnerabilities of smart meters, the high-resolution data is a promising tool to complement traditional tools for theft detection, and is also considered one of the preliminary tools for auditors [155–158]. A Fast NTL Fraud Detection (FNFD) method using Recursive Least Squares (RLS) was proposed by [159] to detect frauds in real-time, and its performance was shown to be better than Intrusion Detection Systems, Binary Coded Grouping-based Inspection (BCGI) [160], NTL Fraud Detector (NFD) and Difference-comparison-based detection [161]. However, it's performance for real data was not accounted for, nor was its convergence speed. Considering not all datasets conform to Benford's Law, a model-based Digits Analysis was proposed using log-Pearson Type IV model [162].

Additionally, statistics and machine learning have been used to train a classifier based on detailed electricity usage measurements [163–166]. In [163], average historical electricity usage under the same conditions was used for constructing an electricity theft detector, and an alarm was raised if the average usage was below a predefined detection threshold. Principal Component Analysis (PCA) based anomaly detection was proposed in [164], where anomalies were deviations from the normal usage behavior. In [165], usage data was proved to be non-stationary, and Auto-Regressive Integrated Moving Average (ARIMA) forecasting methods were proposed to validate readings. A Consumption Pattern-Based Energy Theft Detector (CPBETD) that employed a multi-class Support Vector Machine (SVM) for each customer was formulated in [166]. However, these works ignored the attack model of potential thieves, and the effectiveness of anomaly detector was only evaluated based on a dataset of attack examples.

The problem of electricity theft detection was formulated as a game between the utility and the thieves in [167], in which the utility intended to maximize the detection probability and minimize the investment in monitoring fraud, while each electricity thief was to steal a certain amount of electricity and minimize the probability being detected. However, these works assume all electricity thieves as a player, and the competition between thieves was ignored. If thieves add high loads to the distribution networks and steal electricity at the same time, the resulting power surges and electrical system failures can cause power outages, causing thefts to be detected.

7.3 Benford's Analysis

The first step in the proposed framework is Benford's Analysis, as depicted by Fig. 7.1 [168]. Consider an electric utility serving a set of customers, denoted by $\mathcal{N} := \{1, ..., N\}$. Assuming these customers have a similar preference of electricity usage however some customers have the ability to tamper with the smart meter data, they can be separated into two classes, such as normal customers and thieves. The goal of this analysis is to determine whether the electricity usage data belonging to these $\mathcal{N}$ customers is potentially tampered with or not.

It has been empirically proven by statisticians and mathematicians that PDF of the leading significant digits of a data which is either randomly distributed or is a result of mathematical operations on multiple randomly distributed data that is most likely to follow a trend as illustrated in Fig. 7.2 [169–171]. This is counter-intuitive to the presumption that the PDF of such digits should be uniformly distributed with a percentage of occurrence around 11% each. Electricity usage falls under this category because it is

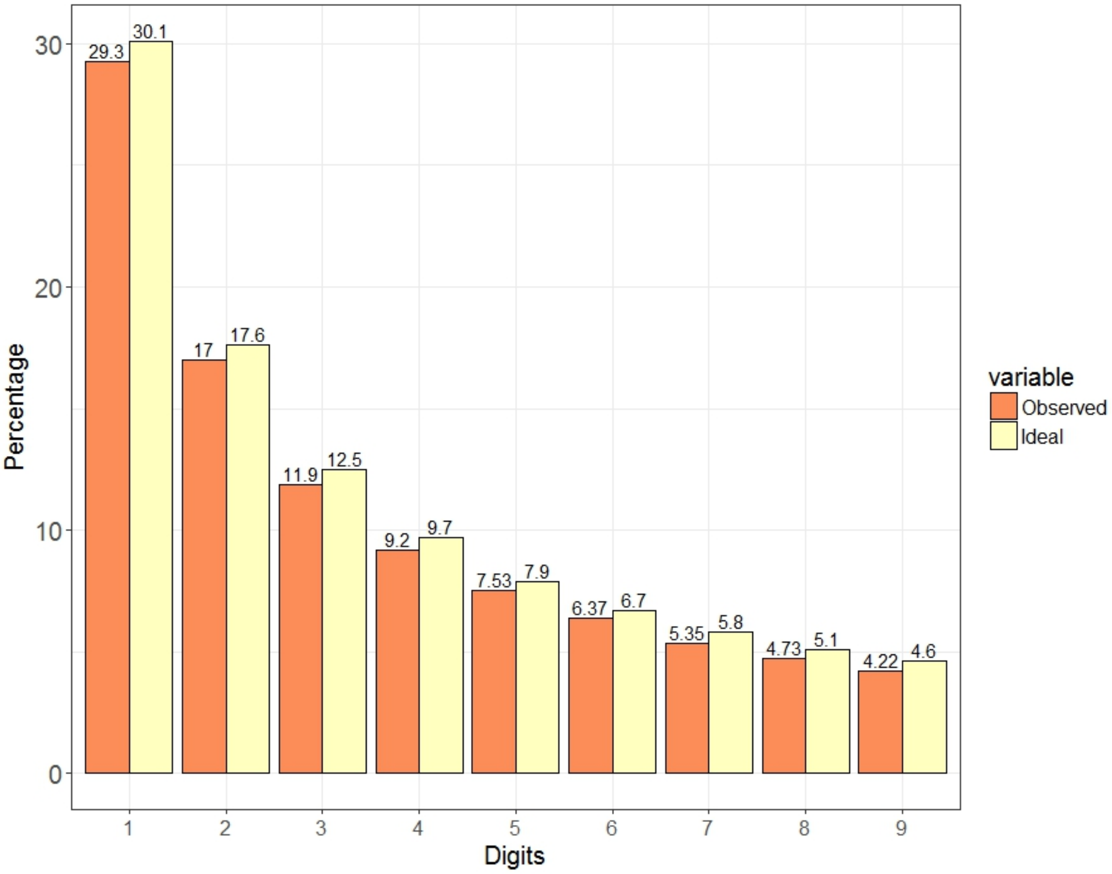


Figure 7.2: Ideal vs. observed Benford's distribution for normal meter dataset.

derived by the product of voltage and current, both of which are randomly distributed. Thus, by virtue of this property, this data is expected to conform to Benford's Law. A mathematical representation of Benford's Law for first significant digits in decimal (base 10) system can be written as [172]:

$$\mathcal{P}(d) = log_{10}(d+1) - log_{10}(d) = log_{10}(1+\frac{1}{d}), \tag{7.1}$$

where d is the first (leading) significant digit of the data and $\mathcal{P}(\cdot)$ denotes the PDF of the leading digit. PDF of the leading digits of Fibonacci series is used as the baseline since real-world data does not conform with zero error. The frequency of occurrence of the leading significant digits is expressed in percent for better intuition in Fig. 7.2. Also shown in the same figure is the PDF of the leading significant digit frequency for preprocessed meter data. It can be seen that this data is close to the ideal trend with a small, acceptable deviation. A smart meter data that is tampered by humans is expected to have a PDF that violates Benford's Law.

7.4 Game Model for Strategic Interactions between Utility and Thieves

Let $\mathcal{M} := \{1, ..., M\} \subseteq \mathcal{N}$ be the set of thieves among the N customers of an electric utility. Then, a single leader, multi-follower Stackelberg game can be formulated between the utility and M thieves to characterize and analyze strategic interactions between the two. In this game, a subset from N customers is chosen for an anomaly detection test $\mathcal{D}$, aiming to reduce NTLs. Based on the limited sampling rate l, the utility intends to maximize detection probability and minimize false positives, while the thieves interact with one another using a non-cooperative game to identify optimal quantities of electricity to steal in response to the utility's detection strategy. In the following subsection, the thieves' game is first analyzed before finding the Stackelberg game solution.

7.4.1 Thieves' Non-cooperative Game Formulation

A non-cooperative game is formulated in this section to analyze optimal decision making of M thieves in response to any arbitrary utility's action. This game is formulated in normal form, $\Xi := \langle \mathcal{M}, (\mathcal{A}_i)_{i\in\mathcal{M}}, (R_i)_{i\in\mathcal{M}} \rangle$, where $\mathcal{M}$ is the set of M thieves. $\mathcal{A}_i$ is the set of actions available to thief $i \in \mathcal{M}$, where $\boldsymbol{a}_i \in \mathcal{A}_i$ is represented by the expected amount of consumed and stolen electricity by thief i, denoted by q_i and q_i^S, respectively. Additionally, $R_i(\boldsymbol{a}_i)$ is the reward function of thief i under action $\boldsymbol{a}_i$. Thus, thief i selects an action $\boldsymbol{a}_i := \{q_i, q_i^S\}$ that maximizes its reward R_i, which can be defined as below:

$$R_i(q_i, q_i^S) := B(q_i^S) - p_i^D(l, q_i^S)P(q_i^S), \tag{7.2}$$

where $B(\cdot)$ represents the utility's electricity billing function; $B(q_i^S)$ gives the amount of electricity bill that is not paid by thief i; $p_i^D(l, q_i^S)$ denotes the probability of thief i being detected when the sampling rate is l and the amount of stolen electricity is q_i^S; and $P(q_i^S)$ indicates the penalty function activated upon the successful detection of thief i for stealing a power of q_i^S.

The reward function of each thief reflects the financial benefit obtained by stealing electricity. Thus, for a given sampling rate l and theft detection mechanism $\mathcal{D}$, the goal of thief i is to optimize the following problem (**Problem 1**):

$$\begin{aligned} \max_{\boldsymbol{a}_i \in \mathcal{A}_i} \quad & R_i(\boldsymbol{a}_i, \boldsymbol{a}_{-i}) \\ \text{s.t.} \quad & 0 \le p_i^D(l, q_i^S) \le p_{i\text{max}}^D, \\ & 0 \le q_i^S \le q_i, \\ & 0 \le q_i \le q_{\text{max}}, \\ & 0 \le \sum_{i=1}^{M} q_i \le q_{\text{Tmax}}, \end{aligned} \tag{7.3}$$

where $\boldsymbol{a}_{-i}$ denotes the actions of all thieves except thief i. In order to control the risk, $p_{i\text{max}}^D$ represents the upper bound for the probability of being detected for thief i. q_{max} indicates the electricity usage limitation for thief i. Similarly, q_{Tmax} gives the total electricity usage constraint for the community. Following this formulation, one popular solution of the thieves' game is the Generalized Nash Equilibrium (GNE) [126]:

Definition 7.4.1 *Consider the proposed noncooperative game* $\Xi := \langle \mathcal{M}, (\mathcal{A}_i)_{i\in\mathcal{M}}, (R_i)_{i\in\mathcal{M}} \rangle$. *GNE is a state of the game in which each electricity thief aims at maximizing Problem 1. As a response to optimal chosen actions of other thieves, a thief aims at choosing the actions, in the restricting subset dictated by the choice of other thieves that maximizes their own reward.*

To find a GNE that can be reached by the thieves, the distributed learning algorithm using the framework of learning automata [126] is implemented, in which each thief only knows its own action space and its own reward after choosing an action.

7.4.2 Utility's Side Analysis

Under the derived GNE of M thieves, the utility needs to selects a defense action $\mathbf{a}_0$ that maximizes its reward R_0. It is assumed that the utility's defense action is determined by two variables including: (1) Detection mechanism, $\mathcal{D}$, used to identify electricity theft, and (2) Customer sampling rate, l.

The objective of the utility is to maximize the following problem (**Problem 2**):

$$\begin{aligned} \max_{\mathcal{D},l} \quad & R_0 := \sum_{i\in\mathcal{M}} p_i^D(l, q_i^S) P(q_i^S), \\ \text{s.t.} \quad & 0 \leq p_i^E(l, q_i^S) \leq p_{i\text{max}}^E, \\ & 0 \leq l \leq l_{\text{max}}, \end{aligned} \tag{7.4}$$

where q_i^S is derived from the GNE of the proposed noncooperative game Ξ; $p_i^E(l, q_i^S)$ represents the false alarm probability for thief i; $p_{i\text{max}}^D$ gives the constraint of the false alarm probability for thief i; and l_{max} indicates sampling rate limitation for the utility. The

Stackelberg solution concept is adequate for games with hierarchy in which the leader enforces its strategy and the followers respond, rationally (i.e. optimally), to the leader's strategy. The optimal response of M thieves to an action $\mathbf{a}_0$ by the utility is written as $\mathcal{A}^{\text{theft}}(\mathbf{a}_0) = \{\mathbf{a}_1^*, ..., \mathbf{a}_M^*\}$. This optimal strategy denotes the equilibrium strategy profile of the attackers as a response to the defender's strategy. In this regard, $\mathbf{a}_0^* \in \mathcal{A}_0$ is a Stackelberg equilibrium [57] if it minimizes the utility's reward function R_0. In other words,

$$R_0(\mathbf{a}_0^*, \mathcal{A}^{\text{theft}}) \leq R_0(\mathbf{a}_0, \mathcal{A}^{\text{theft}}), \forall \mathbf{a}_0 \in \mathcal{A}_0. \tag{7.5}$$

In the Stackelberg equilibrium, the optimal customer sampling rate l and the threshold selected for the the detection mechanism $\mathcal{D}$ can be derived; they determine the detection probability p_i^D and false alarm probability p_i^E, $i \in \mathcal{N}$. In the thieves' game, M thieves make their decisions simultaneously at each step of the evolutionary process, playing a GNE between themselves. A multimodal Genetic Algorithm [57] is implemented for computing the Stackelberg equilibrium for the utility.

7.5 Likelihood Ratio Test

Following the scenario that the smart meter data from a community fails Benford's Analysis, the proposed DIEFTED implements the Likelihood Ratio Test (LRT) for further scrutiny in order to identify potentially fraudulent meters within this community using results from the Stackelberg game. For each customer $i \in \mathcal{N}$, the utility collects a time series of electricity usage measurements, denoted by x_t^i, from time 1 to time T. It is assumed that the collected meter measurements x_t^i, $t = 1, .., T$, are independently drawn from identically distributed random variables following the PDF of f_i^0. Then, the expected value of x_t^i for customer i is q_i. In other words, it is the expected amount of electricity consumed by customer i at one time step. However, if customer i is an electricity thief, they may have comprised their smart meter and thus can propagate a falsified time series, $\hat{x}_t^i$, to lower their billable energy. Let the fraudulent meter measurements, $\hat{x}_t^i$, follow the PDF of f_i^1 and thus the expected value of $\hat{x}_t^i$ is $q_i - q_i^S$, which is the expected amount of electricity billed by customer i. Therefore, a binary hypothesis testing problem can be formulated as follows:

$$\begin{aligned} &\mathcal{H}_0 : x_t^i \sim f_i^0, \mathbb{E}[x_t^i] = q_i, \\ &\mathcal{H}_1 : x_t^i \sim f_i^1, \mathbb{E}[x_t^i] = q_i - q_i^S, \end{aligned} \tag{7.6}$$

where $t = 1, .., T$. The null hypothesis $\mathcal{H}_0$ indicates that customer i's time series follows the PDF of normal customers, while the alternative hypothesis $\mathcal{H}_1$ states that customer i's time series follows the PDF of thieves.

For customer i, let the time series for a normal customer follow lognormal distribution with scale parameter μ_i^0 and shape parameter δ_i^0. Also let the time series for a thief follow lognormal distribution with scale parameter μ_i^1 and shape parameter δ_i^1. Therefore, the LRT can be expressed as:

$$\begin{aligned} \Lambda =& \ln \frac{\prod_{t=1}^K f_i^n(x_t^i)}{\prod_{t=1}^K f_i^f(x_t^i)} \\ =& \sum_{t=1}^T \ln(|\frac{\delta_i^1}{\delta_i^o}| \times e^{\frac{(\ln(x_t^i)-\mu_i^1)^2}{2\delta_i^{1\,2}} - \frac{(\ln(x_t^i)-\mu_i^0)^2}{2\delta_i^{0\,2}}}) \gtrless \gamma, \end{aligned} \tag{7.7}$$

where γ represents the threshold to classify customer i as ”Normal” or ”Thief”. If $\Lambda > \gamma$, customer i is considered Normal, and a Thief otherwise. If $\delta_i^0 = \delta_i^1 = \delta$, then:

$$\Lambda = \sum_{t=1}^T \frac{(2 \ln x_t^i - \mu_i^1 - \mu_i^0)(\mu_i^0 - \mu_i^1)}{2\delta^2} \gtrless \gamma. \tag{7.8}$$

where $t = 1, .., T$. The null hypothesis $\mathcal{H}_0$ indicates that customer i's time series follows the PDF of normal customers, while the alternative hypothesis $\mathcal{H}_1$ states that customer i's time series follows the PDF of thieves.

For customer i, let the time series for a normal customer follow lognormal distribution with scale parameter μ_i^0 and shape parameter δ_i^0. Also let the time series for a thief follow lognormal distribution with scale parameter μ_i^1 and shape parameter δ_i^1. Therefore, the LRT can be expressed as:

$$\begin{aligned}\Lambda &= \ln \frac{\prod_{t=1}^{K} f_i^n(x_t^i)}{\prod_{t=1}^{K} f_i^f(x_t^i)} \\ &= \sum_{t=1}^{T} \ln(|\frac{\delta_i^1}{\delta_i^o}| \times e^{\frac{(\ln(x_t^i)-\mu_i^1)^2}{2{\delta_i^1}^2} - \frac{(\ln(x_t^i)-\mu_i^0)^2}{2{\delta_i^0}^2}}) \gtrless \gamma,\end{aligned} \tag{7.9}$$

where γ represents the threshold to classify customer i as ”Normal” or ”Thief”. If $\Lambda > \gamma$, customer i is considered Normal, and a Thief otherwise. If $\delta_i^0 = \delta_i^1 = \delta$, then:

$$\Lambda = \sum_{t=1}^{T} \frac{(2\ln x_t^i - \mu_i^1 - \mu_i^0)(\mu_i^0 - \mu_i^1)}{2\delta^2} \gtrless \gamma. \tag{7.10}$$

Therefore, LRT can be simplified as $\sum_{t=1}^{T} \ln x_t^i \gtrless \tau$, where $\tau = \frac{2\gamma\delta^2}{\mu_i^0 - \mu_i^1} + \frac{T(\mu_i^0+\mu_i^1)}{2}$. Under this assumption, successful detection probability p_i^D and the false alarm probability p_i^E are defined as follows:

$$\begin{aligned}p_i^D &= \Pr\{x_t^i < e^\tau | H_1\} = \int_0^{e^\tau} f_i^1(x)dx, \\ p_i^E &= \Pr\{x_t^i < e^\tau | H_0\} = \int_0^{e^\tau} f_i^0(x)dx,\end{aligned} \tag{7.11}$$

where $f_i^0(x)$ is the lognormal PDF of the time series consumed by the normal customer with scale parameter μ_i^0 and shape parameter δ_i, and $f_i^1(x)$ is the lognormal PDF of the time series consumed by the thief with scale parameter μ_i^1 and shape parameter δ_i. Based on historical time-series on normal customers, the parameters μ_i^0 and δ_i can be determined by the Maximum Likelihood Estimator (MLE), where $\mathbb{E}[X] = e^{\mu_i^0+\delta_i^2/2} = q_i$, and $Var[X] = e^{2\mu_i^0+\delta_i^2}(e^{\delta_i^2} - 1)$. For a thief, $\mathbb{E}[\hat{X}] = e^{\mu_i^1+\delta_i^2/2} = q_i - q_i^S$, and $Var[\hat{X}] = e^{2\mu_i^1+\delta_i^2}(e^{\delta_i^2} - 1)$.

The descriptive parameters for one meter’s interval usage data is illustrated in Fig. 7.3 using a Cullen and Frey Graph that plots kurtosis against skewness [173]. While Kurtosis is a measure of how heavy-tailed the distribution of a given data is, Skewness is

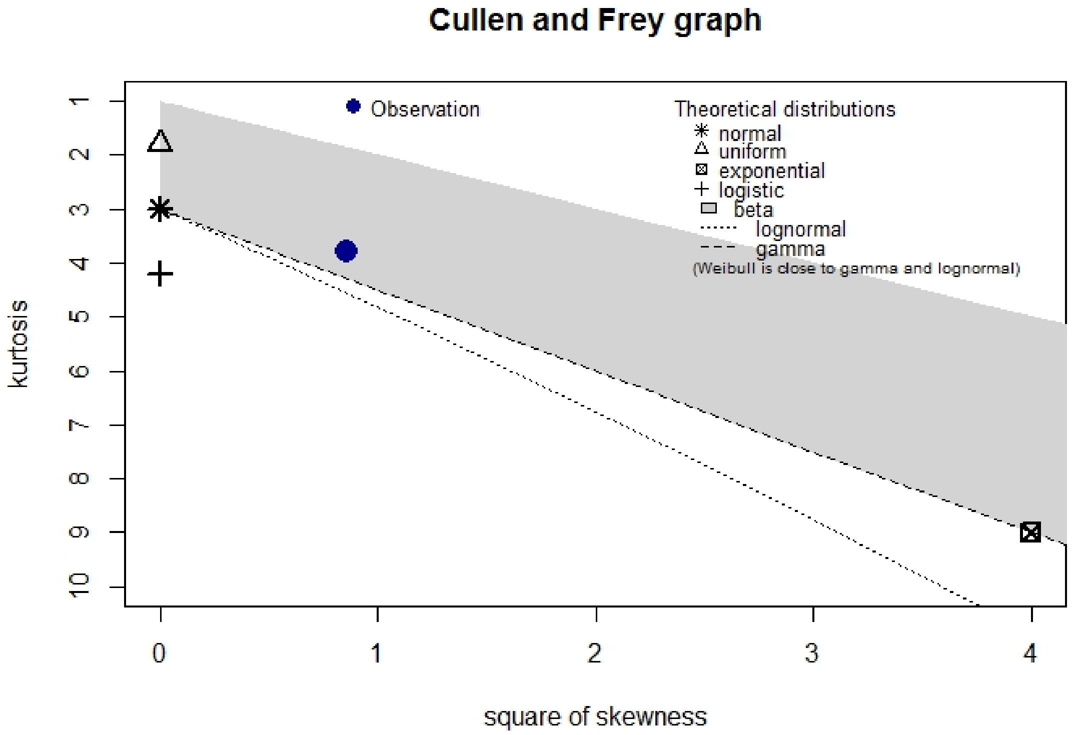


Figure 7.3: Skewness vs. Kurtosis for the data of one meter.

a measure of its symmetry. For example, the PDF of an ideal normally distributed data has a Skewness of 0 and a Kurtosis of 3. It can be seen from the figure that the PDF of the considered dataset, denoted by a blue colored filled circle, is likely to show a fit for lognormal distribution denoted by the dotted line. A similar Kurtosis-Skewness plot was obtained for data from majority of the other meters. It was further deduced that data from all meters were within the shaded region, implying they were all likely to show a fit for beta distribution. These observations are again evident in the PDF of the data shown in the top-left of Fig. 7.4.

The Quantile-Quantile (Q-Q) and Probability-Probability (P-P) plots shown in the top and bottom right of the same figure illustrate the agreement between the theoretical and empirical quantiles and probabilities, respectively. The empirical data is drawn

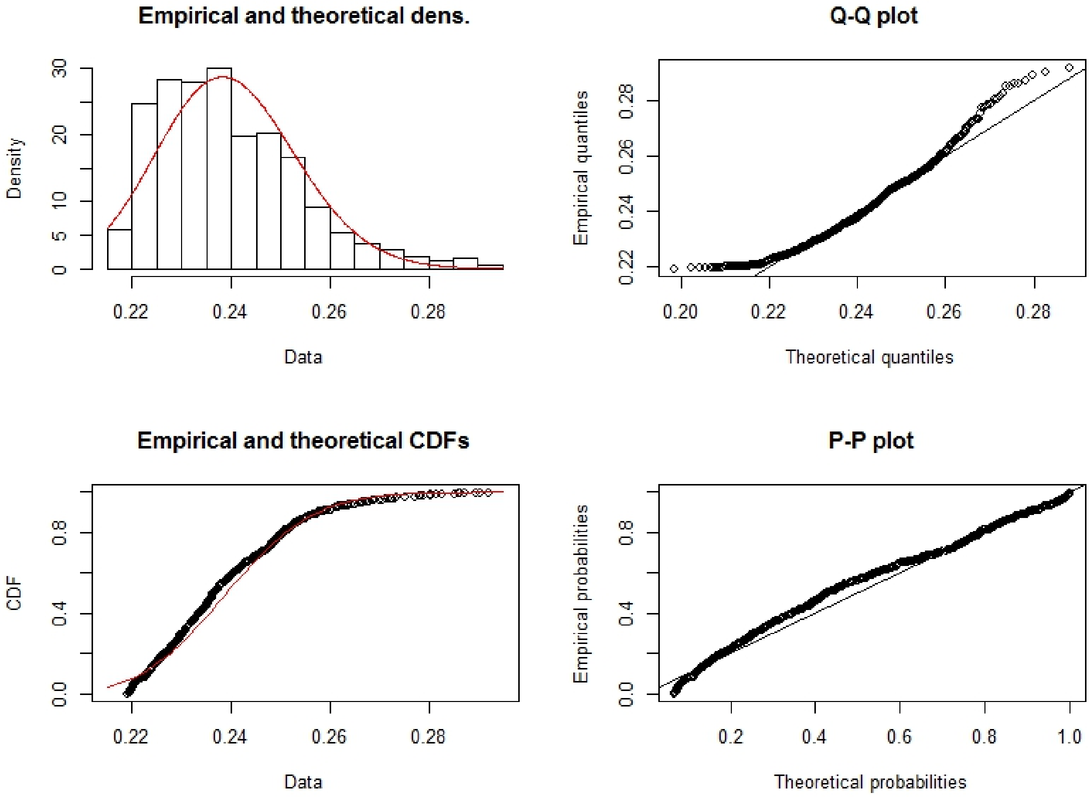


Figure 7.4: Fitting meter data to a lognormal distribution using MLE.

from the sample observations while the theoretical data belongs to the known lognormal distribution. While Q-Q plot compares the quantiles, P-P plot compares the Cumulative Distribution Functions (CDFs), which is affirmed by the agreement between the theoretical and empirical CDFs shown in the bottom-left of Fig. 7.4. It can be concluded both mathematically as well statistically that lognormal distribution can be viewed as the most likely fit for the smart meter interval data.

7.6 Results and Discussion

In order to implement the proposed DIFETD, real-world data from 103 AMI smart meters was collected from an electric utility in Florida, for the month of May, 2013. The interval data was recorded every one hour, annotated with timestamp. It is to be noted that the sample of 103 meters was chosen to demonstrate the feasibility of the proposed framework alone, and that in the future, the number of meters would be scaled to validate the framework against real-world test cases.

Data Preprocessing

Raw data was available as DAT Header files containing values separated by semicolon delimiters (;). Appropriate preprocessing steps were implemented since the data was in a non-numeric format and contained non-intuitive header format. The resulting dataset was structured, time-series and multivariate in nature. In order to maintain privacy of the consumers, original meter IDs were renamed $Meter1$ through $Meter103$.

Theft Scenario Construction

This subsection considers the different electricity theft scenarios that will be used to demonstrate the feasibility of the proposed framework. It is to be noted that, while the attbp]

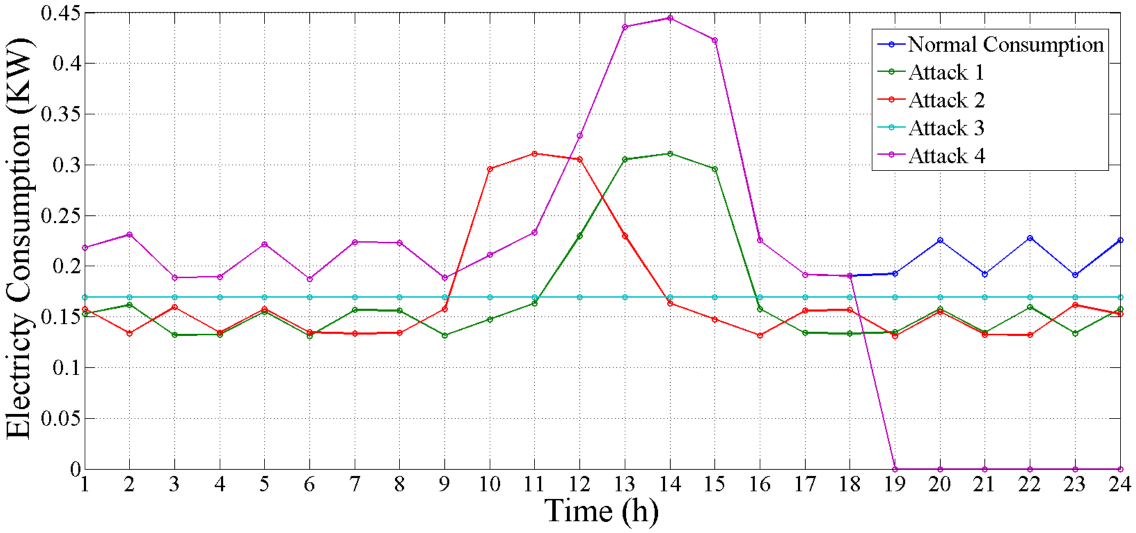


Figure 7.5: An example of the normal daily electricity usage and four theft scenarios.

tacks were synthetically generated, their distributions are randomized to ensure the exact percolation of the attacks into the meter data is still unknown. This ensures a minimization of any inherent bias the proposed framework might have and keeps the overall data structure intact (as would be the case in reality). Consider the electricity bill function as $B(q) = Bq$, and the fine penalty as $B(q) = P$, with $p^D_{i\max} = 0.5$ and $p^E_{i\max} = 0.3, \forall i \in \mathcal{N}$, and $l_{\max} = 0.7$. Therefore, the Stackelberg equilibrium can be derived. Based on the derived q^S_i in the game equilibrium, for each meter measurement x_t, $t = 1, .., 744$, in the dataset, four electricity theft scenarios can be formulated:

1. $A^1_t = (q_i - q^S_i)/q_i \times (x_t)$;
2. $A^2_t = (q_i - q^S_i)/q_i \times (x_{744-t})$;
3. $A^3_t = (q_i - q^S_i)/q_i \times \mathbb{E}[x_t]$;
4. $A^4_t = [x_1, ..., x_{t_1}, 0, ..., 0]$, where t_1 is the earliest time satisfies $\sum_1^{t_1} x_t \geq q_i - q^S_i$.

One customer's daily electricity usage and the four suspected scenarios of electricity theft are shown in Fig. 7.5.

Benford's Analysis

To validate the data's adherence to Benford's Law, several Goodness of Fit (GoF) tests have been proposed in the literature. Of them, Pearson's Chi-Square test and Euclidian distance are two of the widely considered methods to test for significance. These tests assume a null hypothesis ($\mathcal{H}_0$) of the data conforming to the Law, and an alternate hypothesis ($\mathcal{H}_1$) representing the conclusion otherwise. As the sample size grows larger, as is the case in this study, the significance level represented by p-value decreases substantially, approaching zero. Furthermore, threshold of significance, denoted by α is arbitrarily set to a value of 0.05 in most studies. However, even a slight difference between the mean of the two groups of data becomes statistically significant for such a large sample size. Hence, it is necessary to justify hypothesis testing with a measure of how big the effect of size is. Cohen's distance is used as an effect of size measure to evaluate the difference between the mean of two groups. Here, group 1 comprises the Fibonacci series that precisely conforms to the Benford's Law curve. It is used as the baseline, while group 2 comprises different types of meter data: normal, and those subject to Attacks 1 through 4 as described in Section 7.6. Illustrated by Fig. 7.6, it can be seen that the difference in mean between Normal and the baseline is 0, implying that there is no effect of size between the two. However, the Cohen's d-value increases relatively significantly when the data is subject to the Attacks 1 through 4. Greater the d-value, more obvious is the difference between the normal and abnormal datasets. The small d-values implicitly suggest that the four attacks considered are quite intelligent, probably perpetrated by an attacker who is aware of typical electricity usage profiles.

Benford's Analysis for normal data against that compromised by the four attacks is depicted by Fig. 7.7. It can be seen that the PDFs of the leading significant digits of data manipulated by Attacks 1 through 4 (colored orange, yellow, green and blue, respectively) show significant deviations from the expected PDF represented by the normal data (col-

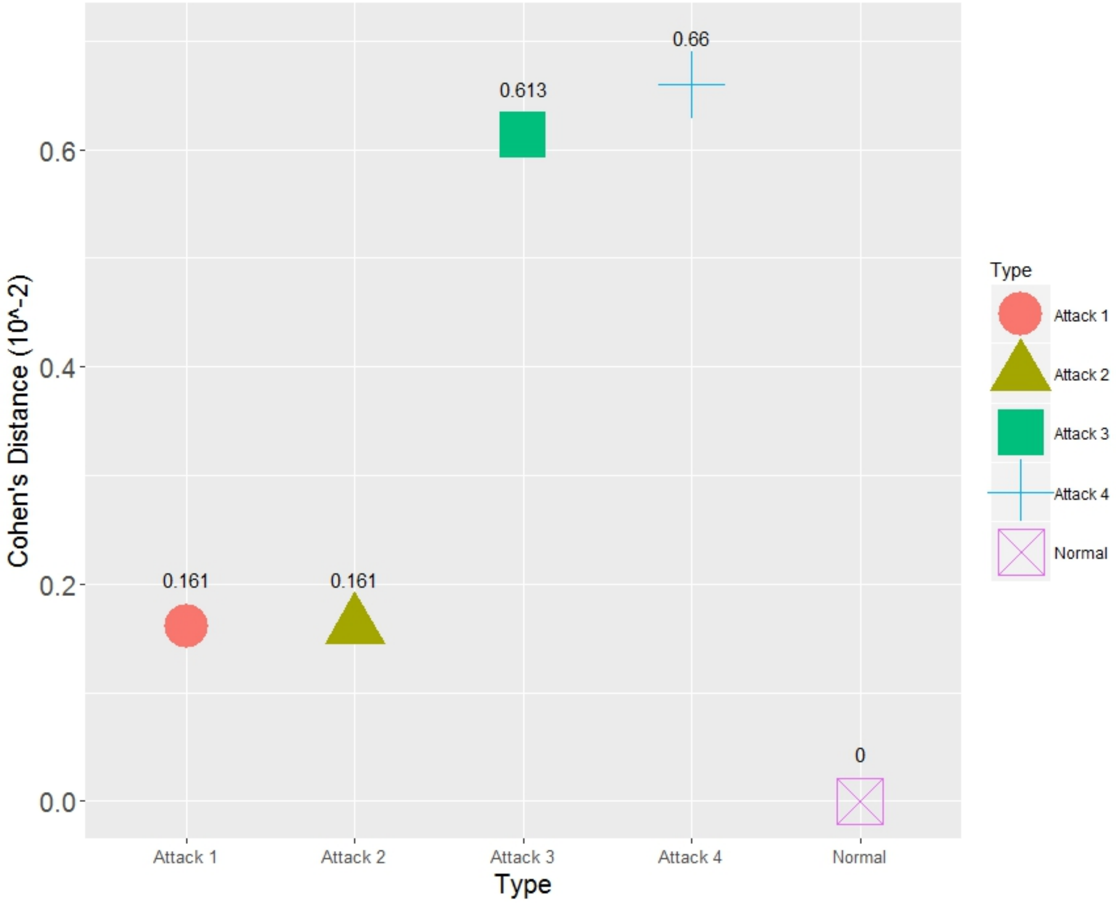


Figure 7.6: Cohen’s distance showing effect of size measure for normal and tampered data against ideal dataset.

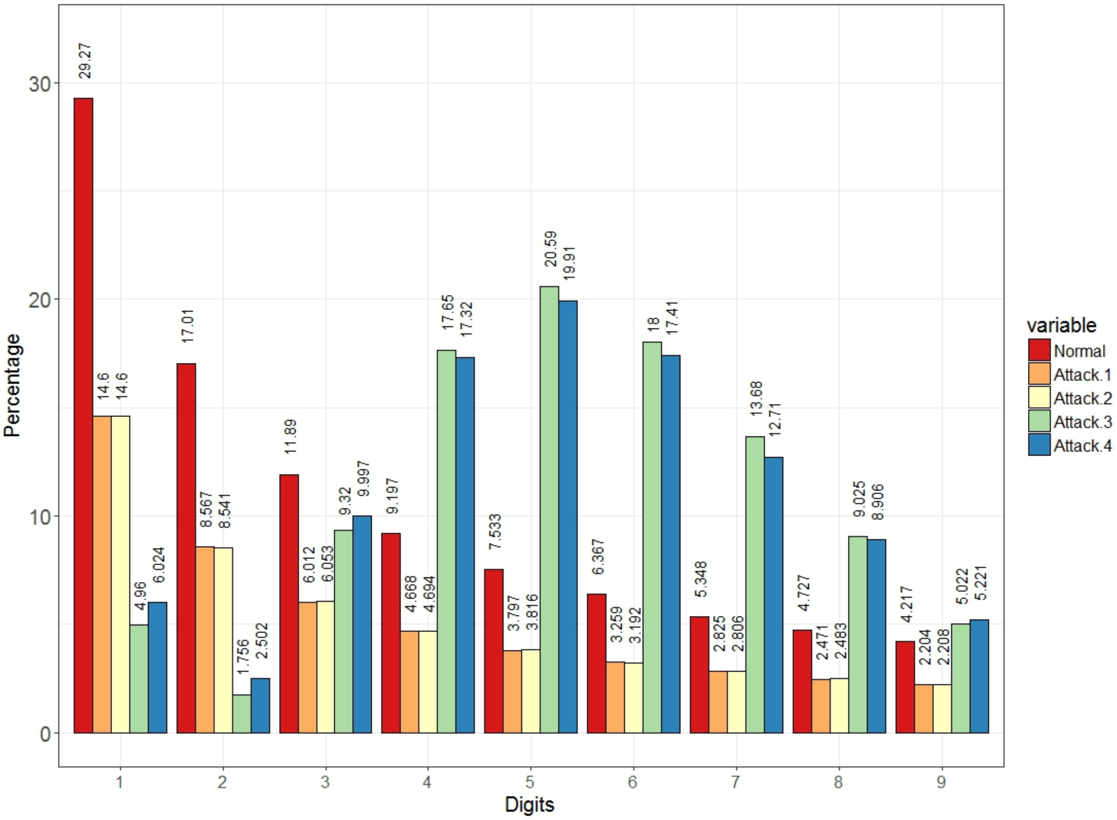


Figure 7.7: Benford analysis for normal and tampered data against ideal dataset.

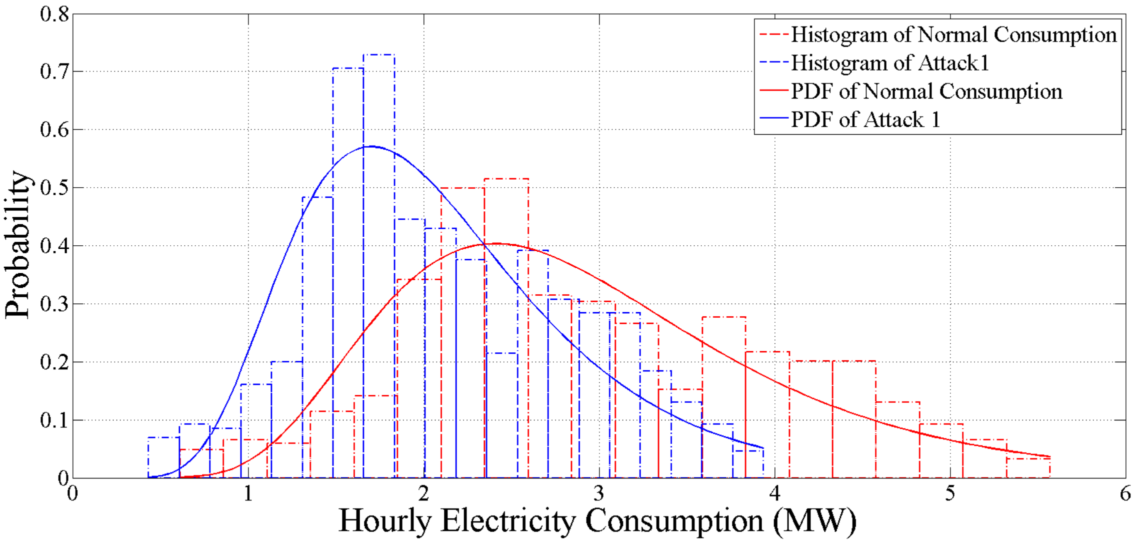


Figure 7.8: The LRT between normal daily electricity usage and Attack 1.

ored red). This deviation signifies the comparison step shown in Fig. 7.1. This, hence, illustrates the power of Benford's Analysis in determining whether the data is potentially tampered with in some form. However, this analysis fails to pin-point specific meters that are manipulated. Thus, this analysis provides a crucial preliminary high-level picture for the operators and analysts to study the meter data of $\mathcal{N}$ consumers and decipher anomalies in them for the next stage. If flagged by this analysis, the data is sent to the next stage of the proposed DIFETD.

Likelihood Ratio Test

The lognormal PDF of a normal customer and a thief was trained using normal electricity usage and attack patterns, respectively. Figure 7.8 gives one normal customer's lognormal PDF and corresponding malicious lognormal PDF. Figure 7.9 shows the Receiver Operating Characteristic (ROC) curve of the LRT for different levels of stealing by thieves, where $q^S/q = 30\%, ..., 70\%$. In this figure, it can be seen that, with increase of the percent of electricity being stole, the LRT test exhibits better performance. For instance,

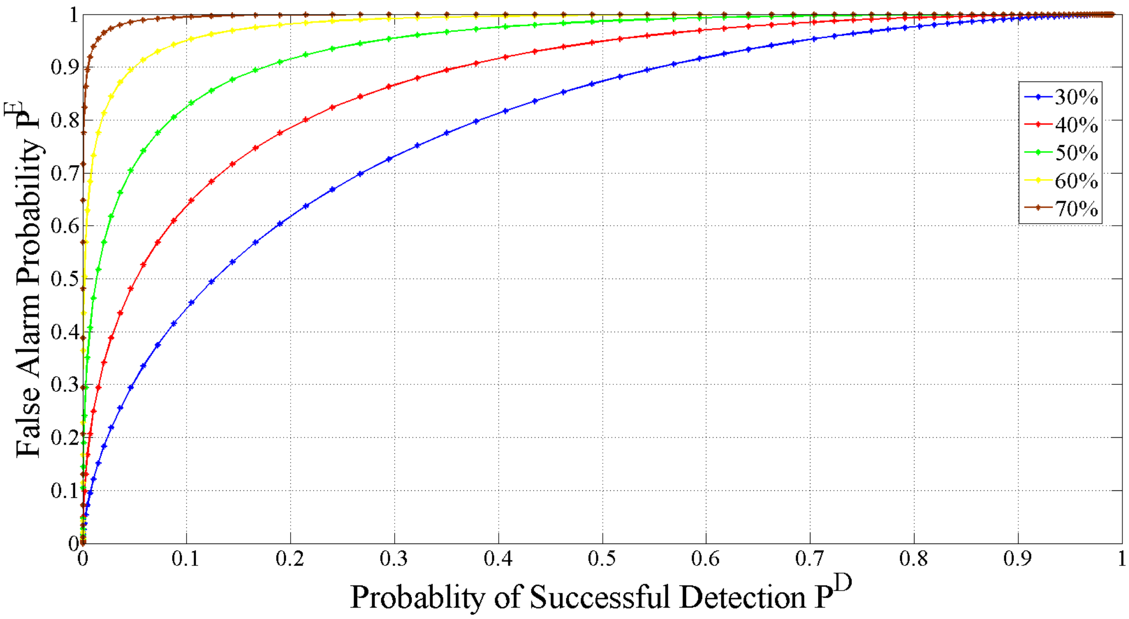


Figure 7.9: The ROC Curve (probability of successful detection versus false alarm probability) of the LRT for different levels of stealing by thieves.

when $q^S/q = 30\%$, the probability of successful detection probability p^D is close to the false alarm probability p^E. However, when $q^S/q = 70\%$, the probability of successful detection probability p^D is close to 1, which is much larger than p^E.

7.7 Summary

Electricity theft is a major concern for utilities all over the world, since it accounts for billions of dollars in losses every year. Considering crucial power system applications such as demand response and state estimation utilize smart meter data, undetected thefts such as FDI could pose serious threats to the reliable operation of smart grid distribution network, raising resiliency concerns. Thus, electricity theft can be considered a very key precursor to the issue of resiliency in smart grid. To address this growing concern, DIFETD is proposed in this chapter to detect electricity theft in smart meters using Benford's Analysis for preliminary diagnostics and Stackelberg game for strategic interactions between one utility and multiple thieves. The game equilibrium provides optimal sampling rate and threshold value for LRT. The capability of the proposed framework was validated against four intelligent theft scenarios with real usage data. For each smart meter, the successful detection rate is achieved more than 95% and the false alarm is controlled beyond 10%, if the electricity is stolen in 50%. In the future, more sophisticated types of theft scenarios on a community of more number of smart meters will be used to evaluate the performance of the proposed work. Here, realistic attack data will be used to validate the framework, and the number of meter samples drawn will be further increased to demonstrate the real-world complexity and how the proposed framework handles it. Further, the uncertainty in theft detection will be considered in the adversary model formulation, in order to detect specific fraudulent meters.

CHAPTER 8

Conclusion and Future Work

8.1 Conclusion

Security and resilience issues that arise in the smart grid constitute a pivotal concern in modern critical infrastructures. In this dissertation, we have discussed new mathematical methods and analytical tools for addressing the reliability and resilience aspects of the smart grid. Regarding the smart grid reliability, statistical analysis techniques were introduced in [27, 28] to analyze the relationship between the number of power interruptions on electric distribution networks and common weather parameters, such as temperature, wind, air pressure, and lightning. The number of power interruptions was predicted based on the total sum of the statistical model of each weather parameter. However, the power interruptions related with common weather conditions are essentially the result of combined action of many factors. The power interruption prediction only based on statistical models might be compromising due to the various effects of different weather parameters.

Chapter 3 has presented a MLP based framework to forecast the daily numbers of sustained and momentary interruptions in smart grid distribution networks using time series of common weather data. Essentially, compared with traditional statistical models, the proposed framework reduced MSE by 8.77% and 61.37% for sustained and momentary interruption forecasting, respectively. A modified ELM based learning algorithm was proposed to train, validate, and test the formulated framework, whose convergence was proved. In addition, we derived the sensitivity of each common weather parameter with respect to the daily numbers of power interruptions based on the formulated framework. For the utility management area in Florida, we can find that the lightning strike was the most important common weather parameter impacting the reliability performance of the smart grid distribution networks, while the heating day had the least impact.

Appropriate implementation of this framework leads to save time by predicting the number of power interruptions. Whenever the number of interruptions is forecasted based on historical weather data, power system equipment failure rates, and aging of distribution network components, the utilities can prevent a major percent of these events by establishing preventive maintenance programs. Hence, the number of interruptions will be reduced considerably because they are not unexpected and the system operator is equipped to face such problems and solve them immediately and without any delay. This awareness of the power distribution network situation helps to achieve an acceptable level of reliability and the improvement of reliability is one of the main objectives of moving to smart grid. The proposed method is implementable on the future power system. In the proposed approach, the variable weather conditions are also considered. The capability of considering the weather conditions in the reliability calculations in terms of interruption prediction is one of the significant breakthroughs of Chapter 3.

A comprehensive overview on the applications of noncooperative game theory for analyzing the cyber-physical security of the smart grid has been presented in Chapter 4. The smart grid analysis was carefully drawn from a broad range of cyber and physical security issues spanning key elements such as network infrastructure, AMI, and state estimation. In each zone, we have identified the main cyber-physical security threats and presented an elaborate discussion on how noncooperative game theory can be applied to address these challenges. Moreover, we proposed several future directions for extending these approaches and adopting advanced game theoretic techniques, so as to reduce the gap between theoretical models and practical implementations of future smart grids. From the surveyed works, we can clearly see that game theory has strong potential to provide solutions for pertinent cyber-physical security problems in the smart grid but also faces many design challenges. However, we also note that many of the existing works have focused on classical static noncooperative games. Hence, in future work, it is of interest to investigate dynamic game models (both in cooperative and noncooperative settings) and their applications in smart grid systems. In this context, dynamic game theory could be a cornerstone for capturing these parameters and designing better algorithms for improving the cyber and physical aspects of the future smart grid.

In Chapter 5, we proposed a novel game-theoretic approach for the risk assessment of coordinated cyber-physical attacks against power grids, while considering the finite budget owned by the attacker and defender that will have an important influence on the assessment. We have formulated a two-player zero-sum stochastic game between the attacker and defender in which each player seeks to maximize its respective minimum rewards under the opponent's optimal strategy. In order to quantify their rewards, the optimal load shedding technology was introduced to determine the minimum cost of shed load. Using these quantified rewards as inputs, the attacker and defender's Nash equilibrium strategies about its budget allocation were derived by solving the proposed stochastic game. At the Nash equilibrium of the game, the optimal attack and defense budget allocation strategies can be obtained, in terms of attacking/protecting the critical elements of the grid. The probability of successful attacks and corresponding physical impacts on the grid can be used to assess the risk for various states of the power grid, and the optimal defense budget allocation is formulated in terms of the corresponding risk. The IEEE 9-bus grid wasis used as the test system, and simulation results have shown that different risks are derived as we vary the attack/defense budget. In addition, compared with the traditional static game models, the proposed stochastic game-theoretic approach can reduce the test system risk by more than 30% for each system state. This proposed game theoretic framework provided a way for the optimal management of the shared critical infrastructure resources be resilient to failures in any of the power system.

In Chapter 6, we introduced a novel DER cyber attack detection framework that integrates spare feature learning and spatiotemporal correlation analysis. First, a two-layer SAE architecture was formulated to extract the abstract representations from large-volume DER measurement datasets. The MRelief feature selection was then developed to provide the feature ranking for both original measurements and extracted representations. Furthermore, we combined the SAE architecture and MRelief with a decision tree-based ensemble classifier for identifying the abnormal events in the DER measurement dataset. The normal, fault, and cyber attack system scenarios simulated by the IEEE 34-bus test distribution system are utilized for training the proposed ensemble classifier. Compared with existing detection methods such as decision tree, quadratic discriminant analysis, logistic regression classifier, SVM, and nearest neighbor classifier, the proposed DER anomaly detection framework achieved the best performance of 99.48% DR, 99.69% Acc, 99.69% F_1, and only 0.1% FAR. Finally, a spatiotemporal correlation sphere is developed for PV farm in the test distribution system for classifying the fault scenarios and the potential cyber attacks in the generated abnormal event list.

In Chapter 7, to address this growing concern for electricity theft, DIFETD was proposed in this paper to detect electricity theft in smart meters using Benford's Analysis for preliminary diagnostics and Stackelberg game for strategic interactions between one utility and multiple thieves. The game equilibrium provides optimal sampling rate and threshold value for LRT. The capability of the proposed framework was validated against four intelligent theft scenarios with real usage data. For each smart meter, the successful detection rate is achieved more than 95% and the false alarm is controlled beyond 10%, if the electricity is stolen in 50%. Electricity theft is a major concern for utilities all over the world, since it accounts for billions of dollars in losses every year. Considering crucial power system applications such as demand response and state estimation utilize smart meter data, undetected thefts such as FDIA could pose serious threats to the reliable operation of smart grid distribution network, raising resiliency concerns. Thus, electricity theft can be considered a very key precursor to the issue of resiliency in smart grid. The proposed DIFETD provided a model to investigate distributor monitoring choices when customers are strategic, and a known fraction of consumers engages in stealing.

8.2 Recommendations for Future Work

The reliable power system operation is a major goal for electric utilities, which requires the accurate reliability forecasting to minimize the duration of power interruptions. The weather conditions, including both common weather parameters and extreme weather events, are usually the leading causes for power interruptions in the smart grid, especially for its distribution networks. However, the proposed hybrid power distribution reliability forecasting model in Chapter 3 only investigated the combined effect of common weather parameters on the reliability performance of distribution networks. Due to essential needs for understanding and recognizing the power system reliability performance under extreme weather events such as hurricanes and windstorms, it is recommended to consider the extreme weather condition based power system reliability forecasting as the future work. Specially, a Bidirectional LSTM based framework can be proposed to forecast the numbers of sustained and momentary power interruptions in one distribution management area under extreme weather events.

The stochastic game theoretic framework proposed in Chapter 5 can be used as a basis to analyze the coordinated cyber-physical attacks targeted at the smart grid. However, the proposed framework can be extended by considering the bounded rationality of the players and the coordination between the cyber attackers. In fact, several future opportunities for extending this work can be explored:

- Introducing additional players and strategies into the game that enables analyzing the cyber-physical attack targeted at multiple smart grid elements simultaneously;

- Analyzing the impact of both the attacker's and defender's information sets on the optimal attack and defense strategy selections;
- Proposing a practical implementation that can be used as a smart grid testbed to evaluate the defender's Nash equilibrium strategies against the data confidentiality attacks.

Regarding the DER cyber attack detection mechanism in Chapter 6 and theft detection framework in Chapter 7, the simulated attack scenarios are implemented for evaluating the performance of the proposed work. However, in the future work, realistic attack data can be used to validate the framework. Further, the operation and information technology support personnel at utility command and control centers constantly detect suspicious events and/or extreme conditions across the smart grid. Already overwhelmed by routine mandatory tasks such as guidelines compliance and patching that if ignored could incur penalties, they have little time to understand the large volumes of machine-generated data associated with the events, generated by intrusion detection systems, firewalls, and other security tools. Lack of powerful classification and anomaly detection tools, and non-contextual visualization of such critical but inadequately processed data, reduces the situational awareness, thereby increasing the likelihood of erroneous or sub-optimal decisions that could prove opportunities to well-evolved attackers. The future work focuses on proposing a tri-modular framework which shifts low-performance processing speed and data contextualization from users to high-performance processing using software, thereby providing users with actionable information. The framework provides three modules, Data Module ($\mathcal{DM}$): Kafka, Spark, and R to ingest streams of heterogeneous data; Classification Module ($\mathcal{CM}$): a Long Short-Term Memory (LSTM) model to classify processed data at each time-step; and Action Module ($\mathcal{AM}$): naturalistic and rational models for time-critical and non-time-critical decision-making, respectively.

BIBLIOGRAPHY

[1] S. Tan, D. De, W. Z. Song, J. Yang, and S. K. Das, “Survey of security advances in smart grid: A data driven approach,” *IEEE Communications Surveys Tutorials*, vol. 19, pp. 397–422, Firstquarter 2017.

[2] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” *IEEE Communications Surveys Tutorials*, vol. 16, pp. 1933–1954, Fourthquarter 2014.

[3] D. He, S. Chan, and M. Guizani, “Win-win security approaches for smart grid communications networks,” *IEEE Network*, vol. 31, pp. 122–128, November 2017.

[4] W. Saad, Z. Han, H. V. Poor, and T. Basar, “Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications,” *IEEE Signal Process. Mag.*, vol. 29, pp. 86–105, Sept. 2012.

[5] J. H. Eto, “The national cost pf power interruptions to electricity customers - an early peek at LBNL’s 2016 updated estimate,” tech. rep., Lawrence Berkeley National Laboratory (LBNL), Dec. 2016.

[6] K. H. LaCommare and J. H. Eto, “Understanding the cost of power interruptions to U.S. electricity consumers,” tech. rep., Lawrence Berkeley National Laboratory (LBNL), Sep. 2004.

[7] R. E. Brown, *Electric Power Distribution Reliability*. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2009.

[8] H. Mirsaeedi, A. Fereidunian, S. M. Mohammadi-Hosseininejad, P. Dehghanian, and H. Lesani, “Long-term maintenance scheduling and budgeting in electricity distribution systems equipped with automatic switches,” *IEEE Trans. Ind. Informat.*, vol. PP, no. 99, pp. 1–1, 2017.

[9] R. J. Campbell, “Weather-related power outages and electric system resiliency,” tech. rep., Congressional Research Service, Aug. 2012.

[10] G. Li, P. Zhang, P. B. Luh, W. Li, Z. Bie, C. Serna, and Z. Zhao, “Risk analysis for distribution systems in the northeast U.S. under wind storms,” *IEEE Trans. Pow. Syst.*, vol. 29, pp. 889–898, Mar. 2014.

[11] C. Chen, J. Wang, F. Qiu, and D. Zhao, “Resilient distribution system by microgrids formation after natural disasters,” *IEEE Trans. Smart Grid*, vol. 7, pp. 958–966, Mar. 2016.

[12] I. Parvez, A. Islam, and F. Kaleem, “A key management-based two-level encryption method for ami,” in *PES General Meeting— Conference & Exposition, 2014 IEEE*, pp. 1–5, IEEE, 2014.

[13] I. Parvez, F. Abdul, and A. I. Sarwat, “A location based key management system for advanced metering infrastructure of smart grid,” in *Green Technologies Conference (GreenTech), 2016 IEEE*, pp. 62–67, IEEE, 2016.

[14] President’s Council of Economic Advisers, “Economic benefits of increasing electric grid resilience to weather outages,” tech. rep., Executive Office of the President, Aug. 2013.

[15] J. Hay and N. Mimura, “The changing nature of extreme weather and climate events: risks to sustainable development,” *Geomatics, Natural Hazards and Risk*, vol. 1, no. 1, pp. 3–18, 2010.

[16] A. O’Connor, “Florida’s hurricane Irma recovery: The cost, the challenges, the lessons,” November 2017.

[17] R. A. Serrano and E. Halper, “Sophisticated but low-tech power grid attack baffles authorities,” *Los Angeles Times*, Feb. 2014.

[18] S. Greengard, “The new face of war,” *Commun. ACM*, vol. 53, pp. 20–522, Dec. 2010.

[19] S.Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” in *Proc. 37th IEEE Conf. Ind. Electron. Soc.*, (Melbourne, Australia), Nov. 2011.

[20] R. Billinton and C. Wu, “Predictive reliability assessment of distribution systems including extreme adverse weather,” in *2001 Canadian Conference on Electrical and Computer Engineering*, vol. 2, pp. 719–724, 2001.

[21] M. Panteli and P. Mancarella, “Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies,” *Electr. Pow. Syst. Res.*, vol. 127, 2015.

[22] X. Liu, M. Shahidehpour, Y. Cao, Z. Li, and W. Tian, "Risk assessment in extreme events considering the reliability of protection systems," *IEEE Trans. Smart Grid*, vol. 6, Mar. 2015.

[23] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Boosting the power grid resilience to extreme weather events using defensive islanding," *IEEE Trans. Smart Grid*, vol. 7, Nov. 2016.

[24] J. Coelho, S. M. Nassar, E. Gauche, V. W. Ricardo, H. L. Queiroz, M. de Lima, and M. C. Lourenco, "Reliability diagnosis of distribution system under adverse weather conditions," in *2003 IEEE Bologna Power Tech Conference Proceedings*, vol. 4, Jun. 2003.

[25] Y. Tang, C. Ten, C. Wang, and G. Parker, "Extraction of energy information from analog meters using image processing," *IEEE Transactions on Smart Grid*, vol. 6, pp. 2032–2040, July 2015.

[26] Y. Tang, C. Ten, and L. E. Brown, "Switching reconfiguration of fraud detection within an electrical distribution network," in *2017 Resilience Week (RWS)*, pp. 206–212, Sept 2017.

[27] A. I. Sarwat, A. Domijan, M. H. Amini, A. Damnjanovic, and A. Moghadasi, "Smart grid reliability assessment utilizing boolean driven markov process and variable weather conditions," in *2015 North American Power Symposium (NAPS)*, pp. 1–6, Oct. 2015.

[28] A. I. Sarwat., M. Amini, A. Domijan, A. Damnjanovic, and F. Kaleem, "Weather-based interruption prediction in the smart grid utilizing chronological data," *J. Mod. Pow. Syst. Cl. Ener.*, vol. 4, pp. 308–315, Apr. 2016.

[29] A. J. Holmgren, E. Jenelius, and J. Westin, "Evaluating strategies for defending electrical power networks against antagonistic attacks," *IEEE Trans. Power Syst.*, vol. 22, Feb. 2007.

[30] P.-Y. Chen, S. M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, 2012.

[31] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, pp. 2831–2836, Oct. 2015.

[32] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, 2015.

[33] I. Parvez, A. I. Sarwat, L. Wei, and A. Sundararajan, "Securing metering infrastructure of smart grid: A machine learning and geo-location based perspective," *Energies*, vol. 9, no. 69, 2016.

[34] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Trans. Power Syst.*, vol. 28, pp. 1676–1686, May 2013.

[35] NERC, "The highimpact, low-frequency event risk to the North American Bulk Power System," 2009.

[36] L. Wei, A. I. Sarwat, and W. Saad, "Risk Assessment of Coordinated Cyber-Physical Attacks Against Power Grids: A Stochastic Game Approach," in *Proc. 51st IEEE IAS Annu. Meeting*, Otc. 2016.

[37] Y. Tang, S. Zhao, C. Ten, and K. Zhang, "Enhancement of distribution load modeling using statistical hybrid regression," in *2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–5, April 2017.

[38] S. Lakshminarasimman, S. Ruswin, and K. Sundarakantham, "Detecting DDoS attacks using decision tree algorithm," in *2017 4th Int. Conf. Signal Process., Commun. and Netw. (ICSCN)*, pp. 1–6, March 2017.

[39] M. Ichino, Y. Ohtsuki, M. Hatada, and H. Yoshiura, "Detection of malware infection using score level fusion with Kernel Fisher discriminant analysis," in *2013 IEEE 2nd Global Conf. Consum. Electron. (GCCE)*, pp. 536–537, Oct 2013.

[40] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," in *2017 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, pp. 1–7, Jan 2017.

[41] P. Gu, R. Khatoun, Y. Begriche, and A. Serhrouchni, "K-nearest neighbours classification based sybil attack detection in vehicular networks," in *2017 3rd Int. Conf. Mobi. Sec. Serv. (MobiSecServ)*, pp. 1–6, Feb 2017.

[42] L. Cai, N. F. Thornhill, S. Kuenzel, and B. C. Pal, "Wide-area monitoring of power systems using principal component analysis and k-nearest neighbor analysis," *IEEE Trans. Power Syst.*, pp. 1–1, 2018.

[43] P. Y. Lee, C. M. Yu, T. Dargahi, M. Conti, and G. Bianchi, "Mdsclone: Multidimensional scaling aided clone detection in internet of things," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2031–2046, Aug 2018.

[44] N. Tsagkarakis, P. P. Markopoulos, G. Sklivanitis, and D. A. Pados, "L1-norm principal-component analysis of complex data," *IEEE Trans. Signal Process.*, pp. 1–1, 2018.

[45] J. H. Chen, M. C. Su, S. I. Lin, and D. Y. Huang, "Som-optimized neurofuzzy classifiers for measuring expatriation willingness," *IEEE Intell. Syst.*, vol. 32, pp. 28–34, September 2017.

[46] S. P. Lim and H. Haron, "Cube kohonen self-organizing map (cksom) model with new equations in organizing unstructured data," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 24, pp. 1414–1424, Sept 2013.

[47] M. Liu, L. Xu, J. Yi, and J. Huang, "A feature gene selection method based on ReliefF and PSO," in *2018 10th Int. Conf. Measuring Technol. Mechatronics Autom. (ICMTMA)*, pp. 298–301, Feb 2018.

[48] M. Liu, W. Yang, J. Chen, and X. Chen, "An orthogonal Fisher transformation-based unmixing method toward estimating fractional vegetation cover in semiarid areas," *IEEE Geosci. Remote Sens. Lett.*, vol. 14, pp. 449–453, March 2017.

[49] S. Li, P. Wang, and L. Goel, "A novel wavelet-based ensemble method for short-term load forecasting with hybrid neural networks and feature selection," *IEEE Trans. Power Syst.*, vol. 31, pp. 1788–1798, May 2016.

[50] L. Wei, A. H. Moghadasi, A. Sundararajan, and A. Sarwat, "Defending mechanisms for protecting power systems against intelligent attacks," in *Proc. IEEE 10th SoSE Conf.*, (San Antonio, the United States), May 2015.

[51] L. Wei, A. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[52] L. Wei, A. Sundararajan, A. I. Sarwat, S. Biswas, and E. Ibrahim, "A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game," in *Resilience Week (RWS), 2017*, pp. 5–11, IEEE, 2017.

[53] J. Lu, L. Wei, M. M. Pour, Y. Mekonnen, and A. I. Sarwat, “Modeling discharge characteristics for predicting battery remaining life,” in *Transportation Electrification Conference and Expo (ITEC), 2017 IEEE*, pp. 468–473, IEEE, 2017.

[54] L. Wei, L. P. Rondon, A. Moghadasi, and A. I. Sarwat, “Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid,” *arXiv preprint arXiv:1805.07422*, 2018.

[55] A. Anzalchi, A. Sundararajan, L. Wei, A. Moghadasi, and A. Sarwat, “Future directions to the application of distributed fog computing in smart grid systems,” in *Smart Grid Analytics for Sustainability and Urbanization*, pp. 162–195, IGI Global, 2018.

[56] A. Sundararajan, L. Wei, T. Khan, A. I. Sarwat, and D. Rodrigo, “A tri-modular framework to minimize smart grid cyber-attack cognitive gap in utility control centers,” in *2018 Resilience Week (RWS)*, pp. 117–123, IEEE, 2018.

[57] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory*. Philadelphia, PA: SIAM Series in Classics in Applied Mathematics, 1999.

[58] Z. Han, D. Niyato, W. Saad, T. Baar, and A. Hjrungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. New York, NY, USA: Cambridge University Press, 1st ed., 2012.

[59] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.

[60] R. B. Myerson, *Game Theory: Analysis of Conflict*. Harvard University Press, 1st paperback edition ed., Sept. 1997.

[61] M. Feldman and T. Tamir, “Convergence of best-response dynamics in games with conflicting congestion effects,” in *Internet and Network Economics* (P. W. Goldberg, ed.), (Berlin, Heidelberg), pp. 496–503, Springer Berlin Heidelberg, 2012.

[62] D. P. Foster and H. Young, “On the nonconvergence of fictitious play in coordination games,” *Games and Economic Behavior*, vol. 25, no. 1, pp. 79 – 96, 1998.

[63] M. Kosfeld, E. Droste, and M. Voorneveld, “A myopic adjustment process leading to best-reply matching,” *Games and Economic Behavior*, vol. 40, no. 2, pp. 270 – 298, 2002.

[64] D. Fudenberg and D. Levine, “Learning in games,” *European Economic Review*, vol. 42, no. 3, pp. 631 – 639, 1998.

[65] J. Chen, Q. Yu, B. Chai, Y. Sun, Y. Fan, and X. . Shen, “Dynamic channel assignment for wireless sensor networks: A regret matching based approach,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 95–106, Jan 2015.

[66] M. L. Littman, “Markov games as a framework for multi-agent reinforcement learning,” in *Machine Learning Proceedings 1994* (W. W. Cohen and H. Hirsh, eds.), pp. 157 – 163, San Francisco (CA): Morgan Kaufmann, 1994.

[67] A. Neyman and S. Sorin, *Stochastic Games and Applications*. New York: Kluwer Academic, July 1999.

[68] A. P. Maitra and W. D. Sudderth, *Discrete Gambling and Stochastic Games*. New York: Sringer-Verlag, 1996.

[69] T. E. S. Raghaven, T. S. Ferguson, T. Parthasarathy, and O. Vrieze, *Stochastic Games and Related Topics: In Honor of Professor L. S. Shapley*. New York: Springer Netherlands, 1991.

[70] J. Hu and M. P. Wellman, “Nash q-learning for general-sum stochastic games,” *J. Mach. Learn. Res.*, vol. 4, pp. 1039–1069, Dec. 2003.

[71] D. Carmel and S. Markovitch, “Opponent modeling in multi-agent systems,” in *Adaption and Learning in Multi-Agent Systems* (G. Weiß and S. Sen, eds.), (Berlin, Heidelberg), pp. 40–52, Springer Berlin Heidelberg, 1996.

[72] D. Banerjee and S. Sen, “Reaching pareto-optimality in prisoner’s dilemma using conditional joint action learning,” *Autonomous Agents and Multi-Agent Systems*, vol. 15, pp. 91–108, Aug 2007.

[73] N. M. Nasrabadi, “Pattern recognition and machine learning,” *Journal of Electronic Imaging*, vol. 16, 2007.

[74] S. Marsland, *Machine Learning: An Algorithmic Perspective*. Chapman & Hall/CRC, 1st ed., 2009.

[75] A. Kataria and M. D. Singh, “A review of data classification using k-nearest neighbour algorithm,” June 2013.

[76] T. Cover and P. Hart, “Nearest neighbor pattern classification,” *IEEE Transactions on Information Theory*, vol. 13, pp. 21–27, January 1967.

[77] C. J. Burges, “A tutorial on support vector machines for pattern recognition,” *Data Mining and Knowledge Discovery*, vol. 2, pp. 121–167, Jun 1998.

[78] M. A. Hearst, S. T. Dumais, E. Osuna, J. Platt, and B. Scholkopf, “Support vector machines,” *IEEE Intelligent Systems and their Applications*, vol. 13, pp. 18–28, July 1998.

[79] T. G. Dietterich, “Ensemble methods in machine learning,” in *Multiple Classifier Systems*, (Berlin, Heidelberg), pp. 1–15, Springer Berlin Heidelberg, 2000.

[80] H. Zou, T. Hastie, and R. Tibshirani, “Sparse principal component analysis,” *Journal of Computational and Graphical Statistics*, vol. 15, no. 2, pp. 265–286, 2006.

[81] J. Jacques and C. Preda, “Functional data clustering: a survey,” *Advances in Data Analysis and Classification*, vol. 8, pp. 231–255, Sep 2014.

[82] M. F. A. Hady and F. Schwenker, *Semi-supervised Learning*, pp. 215–239. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[83] X. Zhu, A. B. Goldberg, R. Brachman, and T. Dietterich, *Introduction to Semi-Supervised Learning*. Morgan and Claypool Publishers, 2009.

[84] J. Kober and J. Peters, *Reinforcement Learning in Robotics: A Survey*, pp. 579–610. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[85] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, “Deep reinforcement learning: A brief survey,” *IEEE Signal Processing Magazine*, vol. 34, pp. 26–38, Nov 2017.

[86] A. Heidari, Z. Dong, D. Zhang, P. Siano, and J. Aghaei, “Mixed-integer nonlinear programming formulation for distribution networks reliability optimization,” *IEEE Trans. Ind. Informat.*, vol. PP, no. 99, pp. 1–1, 2017.

[87] I. Hernando-Gil, I. S. Ilie, and S. Z. Djokic, “Reliability planning of active distribution systems incorporating regulator requirements and network-reliability equivalents,” *IET Gener. Transm. Distrib.*, vol. 10, no. 1, pp. 93–106, 2016.

[88] A. Kavousi-Fard, M. A. Rostami, and T. Niknam, “Reliability-oriented reconfiguration of vehicle-to-grid networks,” *IEEE Trans. Ind. Informat.*, vol. 11, pp. 682–691, Jun. 2015.

[89] M. A. Rostami, A. Kavousi-Fard, and T. Niknam, “Expected cost minimization of smart grids with plug-in hybrid electric vehicles using optimal distribution feeder reconfiguration,” *IEEE Trans. Ind. Informat.*, vol. 11, pp. 388–397, Apr. 2015.

[90] T. Strasser, F. Andrén, J. Kathan, C. Cecati, C. Buccella, P. Siano, P. Leitão, G. Zhabelova, V. Vyatkin, P. Vrba, and V. Mařík, “A review of architectures and concepts for intelligence in future electric energy systems,” *IEEE Trans. Ind. Electron.*, vol. 62, pp. 2424–2438, Apr. 2015.

[91] K. Moslehi and R. Kumar, “Smart grid - a reliability perspective,” in *2010 Innovative Smart Grid Technologies (ISGT)*, pp. 1–8, Jan. 2010.

[92] “IEEE Guide for Electric Power Distribution Reliability Indices - Redline,” *IEEE Std 1366-2012 (Revision of IEEE Std 1366-2003)*, pp. 1–92, May 2012.

[93] T. V. Dao, S. Chaitusaney, and H. T. N. Nguyen, “Linear least-squares method for conservation voltage reduction in distribution systems with photovoltaic inverters,” *IEEE Trans. Smart Grid*, vol. 8, pp. 1252–1263, May 2017.

[94] C. Pace, J. Hernandez-Ambato, L. Fragomeni, G. Consentino, A. D’Ignoti, S. Galiano, and A. Grimaldi, “A new effective methodology for semiconductor power devices HTRB testing,” *IEEE Trans. Ind. Electron.*, vol. 64, pp. 4857–4865, June 2017.

[95] H. Li, J. Guo, and J. Liang, “Application of new wind speed model in power system reliability assessment,” in *2015 50th International Universities Power Engineering Conference (UPEC)*, pp. 1–6, Sept 2015.

[96] A. Lisnianski and H. Ben Haim, “Short-term reliability evaluation for power stations by using Lz-transform,” *J. Mod. Pow. Syst. Cl. Ener.*, vol. 1, pp. 110–117, Sep 2013.

[97] H. Yang, C. Y. Chung, J. Zhao, and Z. Dong, “A probability model of ice storm damages to transmission facilities,” *IEEE Trans. Power Del.*, vol. 28, pp. 557–565, April 2013.

[98] C. Romualdo-Torres, M. Ramirez-Gonzaez, and A. Escamilla-Paz, “Lightning outage transmission line reliability improvement with surge arresters,” in *2016*

IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pp. 1–5, May 2016.

[99] Y.-C. Lai, Y.-A. Huang, and H.-Y. Chu, “Estimation of rail capacity using regression and neural network,” *Neural Comput. Appl.*, vol. 25, pp. 2067–2077, Dec 2014.

[100] Y. Zhang, Y. Xu, Z. Y. Dong, Z. Xu, and K. P. Wong, “Intelligent early warning of power system dynamic insecurity risk: Toward optimal accuracy-earliness tradeoff,” *IEEE Trans. Ind. Informat.*, vol. 13, pp. 2544–2554, Oct 2017.

[101] L. Qi, X. Xiao, and L. Zhang, “A parameter-self-adjusting levenberg-marquardt method for solving nonsmooth equations,” *J. Comp. Math*, vol. 34, no. 3, 2016.

[102] Z. Ismail, J. Leneutre, D. Bateman, and L. Chen, “A game theoretical analysis of data confidentiality attacks on smart-grid ami,” *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1486–1499, July 2014.

[103] A. Sundararajan, A. Pons, and A. Sarwat, “A generic framework for eeg-based biometric authentication,” in *12th International Conference on Information Technology-New Generations (ITNG)*, (Las Vegas), Apr. 2015.

[104] A. Anzalchi and A. Sarwat, “A survey on security assessment of metering infrastructure in smart grid systems,” in *IEEE Southeast Conference*, (Fort Lauderdale), 2015.

[105] I. Parvez, A. Sundararajan, and A. Sarwat, “Frequency band for han and nan communication in smart grid,” in *IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG)*, (Orlando), Dec. 2014.

[106] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, “A multi-sensor energy theft detection framework for advanced metering infrastructures,” *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1319–1330, July 2013.

[107] E. de Buda, “System for accurately detecting electricity theft,” January 2010.

[108] V. Badrinath Krishna, G. A. Weaver, and W. H. Sanders, *PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure*, pp. 70–85. Cham: Springer International Publishing, 2015.

[109] V. Badrinath Krishna, R. K. Iyer, and W. H. Sanders, *ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids*, pp. 199–210. Cham: Springer International Publishing, 2016.

[110] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in ami using customers' consumption patterns," *IEEE Transactions on Smart Grid*, vol. 7, pp. 216–226, Jan 2016.

[111] S. Amin, G. A. Schwartz, A. A. Cardenas, and S. S. Sastry, "Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure," *IEEE Control Systems*, vol. 35, pp. 66–81, Feb 2015.

[112] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in ami systems," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1830–1837, Oct 2012.

[113] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Transactions on Smart Grid*, vol. 7, pp. 2038–2049, July 2016.

[114] W. Saad, Z. Han, H. V. Poor, and T. Basar, "Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications," *IEEE Signal Process. Mag.*, vol. 29, pp. 86–105, Sept. 2012.

[115] ELCON, "The economic impacts of the august 2003 blackout," Feb. 2004.

[116] NERC, "Reliability concepts.," Nov. 2015.

[117] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–1, 2015.

[118] M. Anthony, R. Arno, N. Dowling, and R. Schuerger, "Reliability analysis for power to fire pump using fault tree and rbd," *IEEE Trans. Ind. Appl.*, vol. 49, pp. 997–1003, March 2013.

[119] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Trans. Power Syst.*, vol. 30, pp. 223–232, Jan 2015.

[120] C. W. Ten, G. Manimaran, and C. C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” *IEEE Trans. Syst., Man, and Cybern. A, Syst., Humans*, vol. 40, pp. 853–865, July 2010.

[121] A. Hahn and M. Govindarasu, “Cyber attack exposure evaluation framework for the smart grid,” *IEEE Trans. Smart Grid*, vol. 2, pp. 835–843, Dec. 2011.

[122] S. Sridhar, M. Govindarasu, and C.-C. Liu, “Risk analysis of coordinated cyber attacks on power grid,” in *Control and Optimization Methods for Electric Smart Grids*, vol. 3, (New York, USA: Springer), pp. 275–294, Nov. 2011.

[123] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini, “Risk assessment of malicious attacks against power systems,” *IEEE Trans. Syst., Man, and Cybern. A, Syst., Humans*, vol. 39, pp. 1074 – 1085, Sept. 2009.

[124] A. J. Holmgren, E. Jenelius, and J. Westin, “Evaluating strategies for defending electrical power networks against antagonistic attacks,” *IEEE Trans. Power Syst.*, vol. 22, Feb. 2007.

[125] L. Wei, A. H. Moghadasi, A. Sundararajan, and A. Sarwat, “Defending mechanisms for protecting power systems against intelligent attacks,” in *Proc. IEEE 10th SoSE Conf.*, (San Antonio, the United States), May 2015.

[126] E. Alpaydin, *Introduction to Machine Learning*. MIT Press, Aug. 2012.

[127] NERC, “The highimpact, low-frequency event risk to the North American Bulk Power System,” Nov. 2009.

[128] K. Chatterjee and A. Tarlecki, *Computer Science Logic*. Springer Berlin Heidelberg Press, 2004.

[129] L. Shapley, “Stochastic games,” in *Proc. Nat. Acad. Sci. USA*, vol. 39, pp. 1095–1100, 1953.

[130] A. Pinar, J. Meza, V. Donde, and B. Lessieutre, “Optimization strategies for the vulnerability analysis of the electric power grid,” *SIAM J. Optimiz.*, vol. 20, no. 4, pp. 1786–1810, 2010.

[131] B. Otomega and T. V. Cutsem, “Undervoltage load shedding using distributed controllers,” *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1898–1907, 2007.

[132] V. C. Nikolaidis, C. D. Vournas, G. A. Fotopoulos, G. P. Christoforidis, E. Kalfaoglou, and A. Koronides, “Automatic load shedding schemes against voltage stability in the hellenic system,” in *Proc. IEEE PES Gen. Meet.*, (Tampa, FL), June 2007.

[133] P. M. Anderson and A. A. Fouad, *Power system control and stability*. Delhi, India: Galgotia, 1981.

[134] J. Qi, A. Hahn, X. Lu, J. Wang, and C. C. Liu, “Cybersecurity for distributed energy resources and smart inverters,” *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, 2016.

[135] D. Munoz-Alvarez, J. F. Garcia-Franco, and L. Tong, “On the efficiency of connection charges - part II: Integration of distributed energy resources,” *IEEE Trans. Power Syst.*, pp. 1–1, 2017.

[136] A. Ameli, A. Hooshyar, E. El-Saadany, and A. Youssef, “Attack detection and identification for automatic generation control systems,” *IEEE Trans. Power Syst.*, pp. 1–1, 2018.

[137] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, “Deep abstraction and weighted feature selection for wi-fi impersonation detection,” *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 621–636, March 2018.

[138] N. Chen, J. Zhu, F. Sun, and B. Zhang, “Learning harmonium models with infinite latent features,” *IEEE Trans. Neural Netw. Learning Syst.*, vol. 25, pp. 520–532, March 2014.

[139] M. A. Karim, J. Currie, and T. T. Lie, “Dynamic event detection using a distributed feature selection based machine learning approach in a self healing microgrid,” *IEEE Trans. Power Syst.*, pp. 1–1, 2018.

[140] L. Wang and H. Shen, “Improved data streams classification with fast unsupervised feature selection,” in *2016 17th Int. Conf. Parallel Distrib. Comput., Appl. and Technol. (PDCAT)*, pp. 221–226, Dec 2016.

[141] Y. Yang, H. T. Shen, Z. Ma, Z. Huang, and X. Zhou, “L2,1-norm regularized discriminative feature selection for unsupervised learning,” in *the 22nd Int. Joint Conf. AI*, pp. 1589–1594, 2011.

[142] M. Ohsaki, P. Wang, K. Matsuda, S. Katagiri, H. Watanabe, and A. Ralescu, "Confusion-matrix-based kernel logistic regression for imbalanced data classification," *IEEE Trans. Knowl. Data Eng*, vol. 29, pp. 1806–1819, Sept 2017.

[143] W. Saad, Z. Han, H. V. Poor, and T. Basar, "Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications," *IEEE Signal Process. Mag.*, vol. 29, pp. 86–105, Sept. 2012.

[144] L. Wei, A. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[145] I. Parvez, M. Jamei, A. Sundararajan, and A. I. Sarwat, "Rss based loop-free compass routing protocol for data communication in advanced metering infrastructure (ami) of smart grid," in *2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG)*, pp. 1–6, Dec 2014.

[146] I. Parvez, A. I. Sarwat, L. Wei, and A. Sundararajan, "Securing metering infrastructure of smart grid: A machine learning and localization based key management approach," *Energies*, vol. 9, no. 9, 2016.

[147] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology*, vol. 19, pp. 105–120, April 2014.

[148] L. Wei, A. I. Sarwat, and W. Saad, "Risk assessment of coordinated cyber-physical attacks against power grids: A stochastic game approach," in *2016 IEEE Industry Applications Society Annual Meeting*, pp. 1–7, Oct 2016.

[149] U. S. EIA, "Internatioanl energy outlook 2016," May 2016.

[150] A. Jamain, "Benford's law," *Imperial College of London*, 2001.

[151] S. Newcomb, "Note on the frequency of use of the different digits in natural numbers," *American Journal of Mathematics*, vol. 4, no. 1, pp. 39–40, 1881.

[152] O. Kafri, "Entropy principle in direct derivation of benford's law," *Varicom Communication*, 2009.

[153] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, “A multi-sensor energy theft detection framework for advanced metering infrastructures,” *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1319–1330, July 2013.

[154] E. de Buda, “System for accurately detecting electricity theft,” January 2010.

[155] C. Durtschi, W. Hillison, and C. Pacini, “The effective use of benford’s law to assist in detecting fraud in accounting data,” *Journal of Forensic Accounting*, vol. V, pp. 17–34, 2004.

[156] R. Joannes-Boyau, T. Bodin, A. Scheffers, M. Sambridge, and S. May, “Using benford’s law to investigate natural hazard dataset homogeneity,” *Nature Scientific Reports*, 2015.

[157] G. Bella and F. Grigoli, “Power it up: Strengthening the electricity sector to improve efficiency and support economic activity,” *IMF Working Paper Technical Report*, 2016.

[158] T. Mir, “Citations to articles citing benford’s law: a benford analysis,” *arXiv*, Feb. 2016.

[159] W. Han and Y. Xiao, “Fnfd: A fast scheme to detect and verify non-technical loss fraud in smart grid,” *Proc. 2016 ACM International on Workshop on Traffic Measurements for Cybersecurity*, pp. 24–34, 2016.

[160] X. Xia, W. Liang, Y. Xiao, and M. Zheng, “Bgci: A fast approach to detect malicious meters in neighborhood area smart grid,” in *IEEE International Conference on Communications*, (London, UK), June 2015.

[161] X. Xia, W. Liang, Y. Xiao, M. Zheng, and Z. Xiao, “Difference-comparison-based approach for malicious meter inspection in neighborhood area smart grids,” in *Proc. 50th International Conference on Communications*, (London, UK), June 2015.

[162] C. Winter, M. Schneider, and Y. Yannikos, “Model-based digit analysis for fraud detection overcomes limitations of benford analysis,” *2012 Seventh International Conference on Availability, Reliability and Security*, 2012.

[163] E. Telecom., “Fighting electricity theft with advanced metering infrastructure,” March 2011.

[164] V. Badrinath Krishna, G. A. Weaver, and W. H. Sanders, *PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure*, pp. 70–85. Cham: Springer International Publishing, 2015.

[165] V. Badrinath Krishna, R. K. Iyer, and W. H. Sanders, *ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids*, pp. 199–210. Cham: Springer International Publishing, 2016.

[166] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in ami using customers' consumption patterns," *IEEE Transactions on Smart Grid*, vol. 7, pp. 216–226, Jan 2016.

[167] S. Amin, G. A. Schwartz, A. A. Cardenas, and S. S. Sastry, "Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure," *IEEE Control Systems*, vol. 35, pp. 66–81, Feb 2015.

[168] W. K. T. Cho and B. J. Gaines, "Breaking the (benford) law: Statistical fraud detection in campaign finance," *The American Statistician*, vol. 61, pp. 218–223, Aug. 2007.

[169] P. D. Scott and M. Fasli, "Benford's law: An empirical investigation and a novel explanation," *CSM Technical Report 349*, 2001.

[170] S. Miller, *Benford's Law: Theory and Applications*. Princeton Press, 2015.

[171] T. Sugiarto, "Application of first digits 'benford' law: A case study of an indonesian company," *International Journal of Management & Organizational Studies*, vol. 5, June 2016.

[172] F. Benford, "The law of anomalous numbers," in *Proc. American Philosophical Society*, vol. 78, 1938.

[173] A. Cullen and H. Frey, *The Use of Probabilistic Techniques in Exposure Assessment: A Handbook for Dealing with Variability and Uncertainty in Models and Inputs*. New York, NY: Plenum Press, Plenum Publishing Corporation, 1999.

VITA

LONGFEI WEI

	Born, Tangshan, Hebei Province, China
2007-2011	B.S., Mathematics and Applied Mathematics Hebei University of Technology Tianjin, China
2011-2014	M.S., Applied Mathematics Hebei University of Technology Tianjin, China
2014-2018	Doctoral Candidate, Electrical Engineering Florida International University Miami, Florida

PUBLICATIONS AND PRESENTATIONS

L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, (2016). Stochastic games for power grid protection against coordinated cyber-physical attacks. IEEE Transactions on Smart Grid, 9(2), 684–694.

I. Parvez, A. I. Sarwat, L. Wei, and A. Sundararajan, (2016). Securing metering infrastructure of smart grid: a machine learning and localization based key management approach. Energies, 9(9), 691–709.

L. Wei and A. I. Sarwat, Hybrid integration of multilayer perceptrons and parametric models for reliability forecasting in the smart grid. Submitted to IEEE Transactions on Industry Informatics, Under Review.

L. Wei, R. Singh, and A. I. Sarwat, Spare feature learning and spatiotemporal correlation for attack detection in power distribution systems integrated with DERs. Submitted to IEEE Transactions on Power System, Under Review.

M. Moghaddami, L. Wei, and A. I. Sarwat, Generalized Physics-Based Multi-Objective Design Optimization of Magnetic Structures for Inductive Charging Systems. Submitted to the IEEE Transactions on Industrial Electronics, Under Review.

A. Sundararajan, T. Olowu, L. Wei, S. Rahman, and A. I. Sarwat, Impacts of Partial Solar Eclipse on Distribution Grid-Tied Photovoltaic Systems and Management Areas: A Case Study. Submitted to International Journal of Electrical Power and Energy Systems, Under Review.

L. Wei, L. P. Rondon, A. Moghadasi, and A. I. Sarwat, (2018, April). Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid. In 2018 IEEE PES T&D conference (pp. 1–7).

L. Wei, A. Sundararajan, and A. I. Sarwat, (2018, to be appear). Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid. In 2018 resilience week (RWS) (pp. 1–7).

L. Wei, A. Sundararajan, A. I. Sarwat, S. Biswas, and E. Ibrahim, (2017, September). A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game. In 2017 resilience week (RWS) (pp. 5–11)

J. Lu, L. Wei, M. M. Pour, Y. Mekonnen, and A. I. Sarwat, (2017, June). Modeling discharge characteristics for predicting battery remaining life. In 2017 IEEE transportation electrification conference and expo (ITEC) (pp. 468–473).

L. Wei, A. I. Sarwat, and W. Saad, (2016, October). Risk assessment of coordinated cyber-physical attacks against power grids: a stochastic game approach. In 2016 IEEE industry applications society annual meeting (pp. 1–7).

L. Wei, A. H.Moghadasi, A. Sundararajan, and A. I. Sarwat, (2015, May). Defending mechanisms for protecting power systems against intelligent attacks. In 2015 10th system of systems engineering conference (SoSE) (pp. 12–17).

A. Anzalchi, A. Sundararajan, L. Wei, A. Moghadasi, and A. Sarwat, (2018, June). Future directions to the application of distributed fog computing in smart grid systems. IGI Global.

L. Wei, A. Anzalchi, A. Sundararajan, and A. Moghadasi, Electric Power Reliability & Analytics Center (EPRAC) for High Penetration Distributed Renewable Resource Modern Grid System, presented at Engineering Center, FIU, Miami, FL, Nov. 2016.

L. Wei, A. Anzalchi, A. Sundararajan, and A. Moghadasi, Electric Power Reliability & Analytics Center (EPRAC) for High Penetration Distributed Renewable Resource Modern Grid System, presented at Florida Power & Light (FPL), Juno Beach, FL, Aug. 2017.

L. Wei, Game-Theoretic Methods and its Application for Cyber-Physical Security in Smart Grids, presented at American Mathematical Society (AMS) Student Chapter Event, FAU, Boca, FL, Nov. 2017.

L. Wei, A. Sundararajan, S. Rahman, T. Olayemi, and M. Jafari, Electric Power Reliability & Analytics Center (EPRAC) for High Penetration Distributed Renewable Resource Modern Grid System, presented at Florida Power & Light (FPL), Jupiter, FL, Apr. 2018.