2017

Smart Grid Security Against Massive Blackouts

Jun Yan
University of Rhode Island, junyan018@gmail.com

SMART GRID SECURITY AGAINST MASSIVE BLACKOUTS

BY

JUN YAN

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

ELECTRICAL ENGINEERING

UNIVERSITY OF RHODE ISLAND

2017

DOCTOR OF PHILOSOPHY DISSERTATION

OF

JUN YAN

APPROVED:

Dissertation Committee:

Major Professor Haibo He

Yan Sun

Pete August

Nasser H. Zawia

DEAN OF THE GRADUATE SCHOOL

UNIVERSITY OF RHODE ISLAND

2017

ABSTRACT

The security of the smart grid is a grand challenge across cyber and physical domains. As an emerging critical infrastructure that integrates information and communication technologies (ICT) into power and energy systems (PES) with improved efficiency, reliability, and sustainability, the smart grid encompasses a transcontinental network of interdependent and interoperating cyber-physical systems (CPS) through the computerization, interconnection, and communication of systems and devices. Across the closely interwoven cyber-physical spaces, the vulnerability and exposure of critical systems and processes have been on the rise: malicious attackers may penetrate through access points in the cyberspace and exploit vulnerabilities in the physical systems, posing major threats to disrupt the delivery of electricity through massive cascading blackouts. Risks and impacts of such attacks have been demonstrated by intensive research efforts as well as real-world incidences recently, drawing increasing concerns from the government, the industry, and the public.

This dissertation will investigate the cyber-physical security of smart grid against potential massive blackouts. The work is composed of three synergistic tasks: 1) understand the mechanisms behind major cascading blackouts; 2) identify critical attack vectors that could initiate the cascading process; 3) develop effective strategies to enhance the resilience of the grid. The dissertation will first assess operational and structural vulnerabilities in massive cascading blackouts through steady state and complex network models, respectively. It will then examine malicious attacks that exploit the vulnerabilities through compromised control and measurements, where advanced machine learning algorithms are employed to identify critical attack vectors that would trigger massive cascades. Simulations results on IEEE standard benchmarks are evaluated and revealed the impact of sophisticated attacks. The dissertation aims to facilitate our awareness and preparedness toward an attack-resilient smart grid of the future.

ACKNOWLEDGMENTS

During this journey, I have received unimaginable support from numerous individuals and organizations. Dr. Haibo He, has been a mentor, colleague, and friend with every guidance and support that I could ask for. I have also benefited immensely from my doctoral committee members, Dr. Yan (Lindsay) Sun, Dr. Pete August, Dr. Lisa DiPippo, and Dr. Tao Wei, whose invaluable time and advice have helped me made it through. I would also like to thank Dr. Sigrid Berka, for her support from the IEP program that allows me to start this incredible journey.

I have enjoyed six wonderful years in the Computational Intelligence and Self-Adaptive System (CISA) laboratory, thanks to an exceptional group of fellow colleagues. Thank you, Zhen, Bo, Jing, Xiangnan, for your feedback, friendliness, and fun that make this journey brilliant and memorable. I am so grateful to have worked with and learned tremendously from so many outstanding scholars and colleagues around the globe at the CISA lab.

I would also like to give special thanks to my great colleague, roommate, and friend, Yufei Tang. I believe our mutual support and friendship will last long, long into the future.

This journey would not be possible without the unbreakable love and support from my parents, Weihua Song and Haoning Yan. And I could not be more blessed to have the company of my wife, Yingying Zhang, for her incredible wisdom, enthusiastic endeavor, and unconditional love are beyond compare.

The research has been supported by the National Science Foundation (NSF) under Grants CNS 1117314, ECCS 1053717, and CMMI 1526835, and by the Army Research Office (ARO) under Grant W911NF-12-1-0378.

TABLE OF CONTENTS

Page

Page

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

CHAPTER 1

Introduction to Cyber-Physical Security of Smart Grid

1.1 Overview of the Smart Grid

1.1.1 The Existing Electrical Power Infrastructure

Electricity is one of the substantial foundations of the modern life. Playing an expanding critical role in maintaining the functioning of our society and sustaining its prosperity, the electrical power infrastructure has gradually evolved over the last century into a transcontinental network of interconnected and interacting systems. Shown in Figure 1, the cyber-physical power grid in North American has become one of the largest systems humans have ever built [1] and arguably one of the most complex and challenging to operate.

According to the National Institute of Standards and Technologies (NIST), the monolithic electrical power infrastructure can be categorized into seven domains: generation, transmission, distribution, operation, electricity markets, service providers, and customers [2]. In a traditional model of physical power systems, power plants generate the electricity from various resources, and the electricity is delivered to the customers via the transmission and distribution networks, where substations and transmission/power lines constitute the major components in such networks. Regional power grids have been constructed, operated, and networked geographically in the major interconnections that ensure the delivery of electricity for customers across the continent.

On top of this physical systems, a cyber infrastructure for the monitoring, control, and communication of the grid has been established, mostly on proprietary facilities, to maintain and regulate power grid operations. Control centers host energy management systems (EMS) that monitor and control the grid through the supervisory control and data acquisition (SCADA) system. The SCADA is composed of master and remote terminal units, i.e., MTUs and RTUs, which are located at the control center and

field substations, respectively. The MTUs and RTUs exchange control commands and sensory measurements through an array of communication networks to maintain and operate the grid. The sensory measurements, primarily consisting of raw data of voltage, current, and frequency in the field, are collected by deployed sensors, pre-processed and aggregated at the RTUs, and transmitted to MTUs. The information is further processed in control rooms and visualized through the human-machine interface (HMI), based on which control commands are determined and issued. The MTUs then send down the commands to the RTUs, which execute the code to operate actuators and adjust dynamics of the system. In this process, regional grids, predominantly owned and operated by local utility providers, are supervised and coordinated by regional transmission organizations (RTO) and independent system operators (ISO). The hierarchical collective efforts ensure overall system reliability, social utility, and economic benefits through the production, delivery, and consumption of electricity.

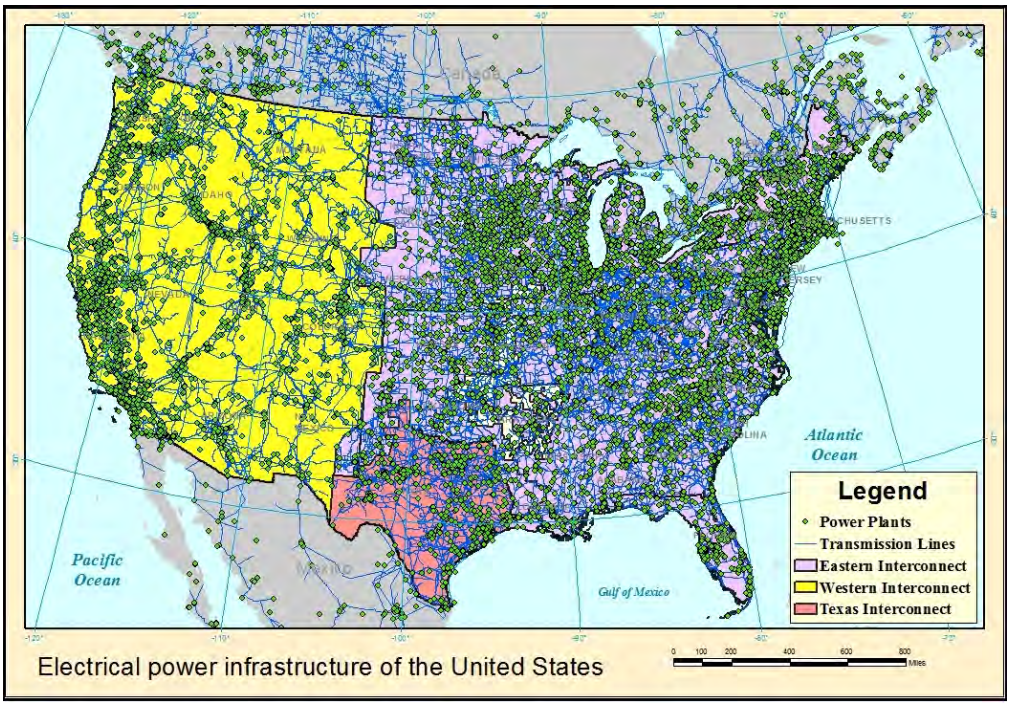


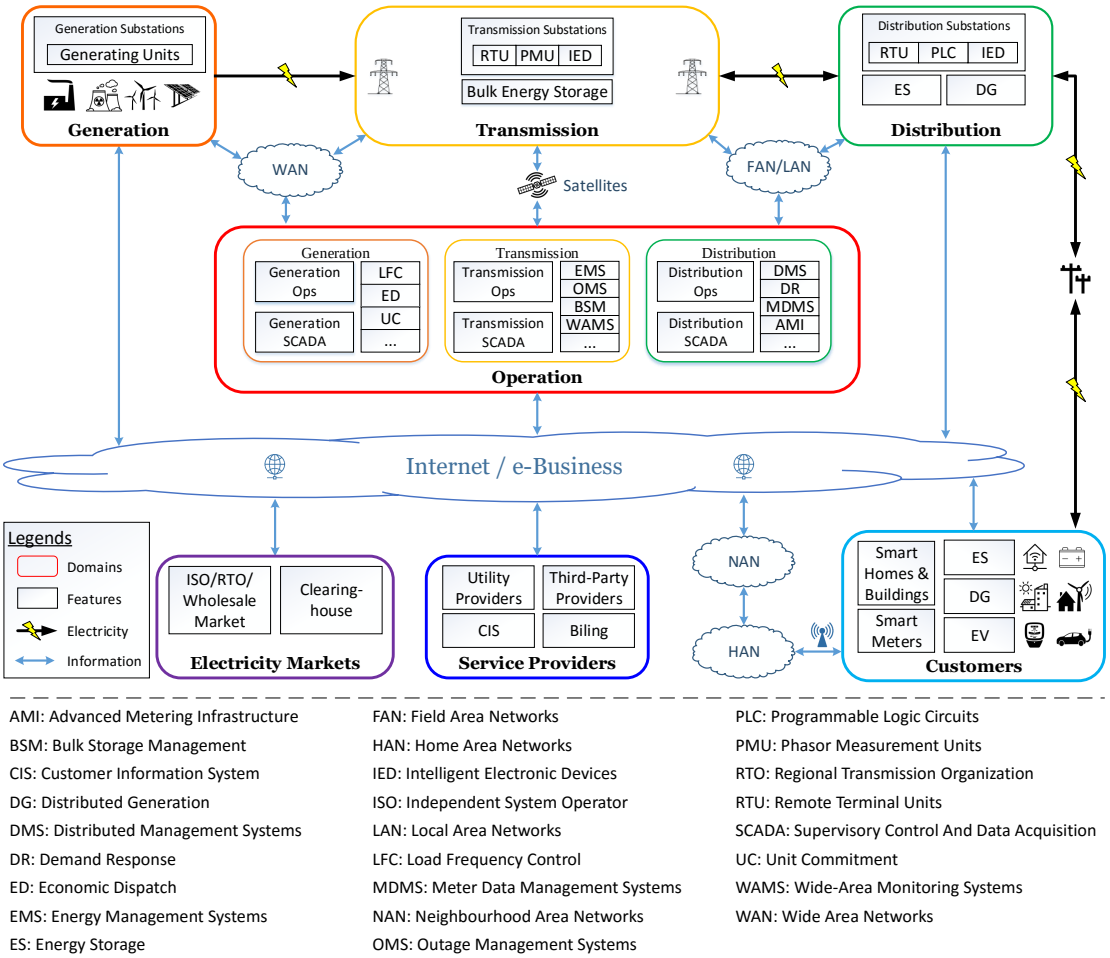
Figure 1. The electrical power infrastructure in the United States.

1.1.2 The Emerging Smart Grid

Since the millennium, increasing challenges as well as innovative solutions in both the physical and the cyber spaces have been transforming the electrical power infrastructure into a new generation known as the *smart grid* [3, 4, 5]. Evolving along with the emerging challenges and advancements, the smart grid stands out as an advanced infrastructure to supply electrical power with significantly increased efficiency, reliability, and sustainability. One of the key innovations therein is the incorporation of modern information and communication technologies (ICT) to computerize and network the existing power systems. This incorporation, or integration, allows better accommodation of a combination of latest changes and challenges across generation supply, transmission operation, demand variation, energy storage, renewable energies, distributed resources, and market deregulation, among others. Consequently, the critical electrical power infrastructure has become a cyber-physically integrated network of systems, as illustrated in Figure 2 [6].

From the power engineering perspective, the physical power grids are undergoing radical transformations. On the generation side, the growing integration of renewable energies (RES) brings one of the most significant improvements of the sustainability and economics of electrical power generation. According to the U.S. Energy Information Administration [7], the percentage of renewable energies has grown from to 8.5% in 2007 to 14.9% in 2016 over the last decade. This growth, contributed by installation and operation of utility-scale renewable generations like wind farms, solar photovoltaic, and solar thermal plants, is projected to continue in the years to come thanks to efforts in states like New York, Texas, and California [8].

In the transmission systems, long-distance transmission lines are being planned and installed to deliver electricity from remote generation sites to populated metropolitans as well as to increase interchange between different balancing authorities. A 2016



AMI: Advanced Metering Infrastructure
BSM: Bulk Storage Management
CIS: Customer Information System
DG: Distributed Generation
DMS: Distributed Management Systems
DR: Demand Response
ED: Economic Dispatch
EMS: Energy Management Systems
ES: Energy Storage
FAN: Field Area Networks
HAN: Home Area Networks
IED: Intelligent Electronic Devices
ISO: Independent System Operator
LAN: Local Area Networks
LFC: Load Frequency Control
MDMS: Meter Data Management Systems
NAN: Neighbourhood Area Networks
OMS: Outage Management Systems
PLC: Programmable Logic Circuits
PMU: Phasor Measurement Units
RTO: Regional Transmission Organization
RTU: Remote Terminal Units
SCADA: Supervisory Control And Data Acquisition
UC: Unit Commitment
WAMS: Wide-Area Monitoring Systems
WAN: Wide Area Networks

Figure 2. Cyber-physical architecture of the smart grid.

report from Edison Electric Institute showed a record-breaking investment of at least $41 billion in transmission from 2016 to 2019 [9]. Meanwhile, short-distance and local transmission are also being developed to compensate the loss and cost of long-distance transmission. Advancements in transmission technologies have also been driven by the industry and the government, particularly with the installment of over 1,100 phasor measurement units (PMUs) [10]. The PMUs utilize global positioning system (GPS) to provide high-resolution, accurate, and reliable synchronous measurements of inter-connected transmission systems, a key that paves the way for wide-area monitoring, protection, and control (WAMPAC) systems [11].

On the distribution and customer side, the advanced metering infrastructure (AMI) is been developed and deployed. Millions of smart meters are being installed in the AMI to provide two-way, real-time monitoring and communications with an unprecedented spatial-temporal resolution of the grid. Such granularity promises prosperous benefits to the grid, ranging from peak energy reduction (with demand response) to wide-area real-time situation awareness, outage management, and consumer engagements. Furthermore, distributed energy resources (DER) enable customer-side power generation and management with augmented flexibility and reliability, which will reshape the unidirectional power flow into a bidirectional pattern. Moreover, recent progress in energy storage, electrical vehicles, and other emerging technologies are also transforming various stages of electricity delivery in physical power grids.

1.2 Cyber-Physical Security of the Smart Grid

The smart grid encompasses complex cyber-physical energy systems hosted in a heterogeneous network of power, energy, control, sensory, computing, and communication. The emerging smart grid incorporates systems of legacy hardware and software, operates under multiple entities and regulations, faces increasing system stress and uncertainty, and attracts parties of malicious intentions. The reality underscores the challenges to the security and resilience of smart grid that have been on the rise within and across physical and cyber domains [12, 6]. On one hand, the intrinsic complexity and dynamics of bulk power systems have complicated the protection against inherent physical vulnerabilities in the grid. On the other, the cyber-integration also requires substantial efforts on adapted security designs and upgrades against unforeseen exposure and threats to the electrical power grid.

The electrical power grids are complex networked systems vulnerable to internal and external disturbances, including load stress, equipment failure, misoperation, and natural disasters [13]. In smart grid, increasing RES introduces new non-linearity, un-

certainty, time-variance when the grid embraces their sustainability [14]. The DER shapes new, less predictable patterns in power generation, transmission, and distribution with expectable, significant impacts on grid stability [15]. Furthermore, power lines and substations are mostly deployed in the field with limited surveillance or protection, rendering them vulnerable to physical sabotages as reported in the past few years [16, 17, 18].

The cyber-integration inevitably increases the risk of attacks on critical power systems and processes from the cyberspace [12]. Tremendous threats arise from the cyber-attacker's ability to launch a range of anonymous, remote, simultaneous, and coordinated intrusions. From crimes to terrorism and warfare, the fragility of computer and communication networks has been frequently exploited. As inter-networking of devices and services continue to grow, emerging cyber-physical systems raise grand security concerns. Recent incidences, including Stuxnet on nuclear control systems [19], BlackEnergy on power control centers [20], and Botnet on the internet-of-things [21], revealed unforeseen threats that explicitly target the networked physical systems and processes.

Research on the cyber-physical security of the smart grid advances on a multi-disciplinary frontier, converging the physical security of power and energy systems and the cybersecurity of information, control, sensory, and communication systems [22]. The incorporation of knowledge and strengths on physical and cyber security is essential to enhance the security and resilience of smart grid, while neither direction along can secure the critical infrastructure for our modern society.

1.2.1 Physical Security of the Smart Grid

Physical security of power systems focuses on the survivability and reliability of power systems after contingencies. As the core of power system security, the contingency analysis (CA) evaluates the power system stability after credible inadvertent contingencies to minimize interruptions to the delivery of electricity [13]. CA typically runs

on a selection of operating points and covers events including faults, disturbances, and planned outages of inadvertent nature. Security constraints are established by the CA in subsequent modules of the EMS, e.g., optimal power flow, economic dispatch, and unit commitment, to ensure the stable operation of power grids. Under different modeling accuracies and timeframes, steady-state and transient analyses both serve the grid operators to assure the physical security [23, 24]. In practice, the $N-1$ security, i.e., the grid remains in secure operation after the loss of any single components, has been enforced as a standard for major transmission grids across the United States [25].

However, the interconnected power and energy systems have presented challenges to the physical security analysis. Both the complexity and the runtime of CA increase dramatically when the system scales up, rendering it difficult to conduct or implement $N-k$ security in bulk power systems. The heterogeneity and complexity of hardware, software, and operations also limit the accurate and timely evaluation of remote contingencies whose impact could propagate through a long distance in an instant. Without sufficient wide-area situation awareness and coordination, multiple remedial actions determined locally may compete, instead of collaborating, with each other, resulting in degraded conditions and/or cascading failures [26]. Last but not least, while large-scale physical sabotages are rare, they still pose threats to most power facilities and devices not equipped with sufficient surveillance and protection systems [27].

Moreover, the cyber-threats introduces new challenges. Legacy field devices and systems are not designed or equipped with sufficient security features against malignant events from the cyberspace. Concerning about the cyber-exposure of critical information, access, and process, investigations have revealed vulnerabilities, both unknown and zero-day, in the emerging smart grid. The lack of sufficient protection against coordinated cyber-attacks could be catastrophic, as demonstrated by the cyber-attack on a Ukraine regional grid [28]. Meanwhile, intelligent and automated systems, which

have been designed to enhance the system security and reliability, may also be turned into weapons against the smart grid itself. With all these emerging threats, securing the smart grid will require new insights beyond the traditional physical security approaches in power systems.

1.2.2 Cybersecurity of the Smart Grid

Cybersecurity has been widely recognized as a major feature and challenge in the development of smart grid [29]. Utilities have followed the principles of confidentiality, integrity, and availability to install secure public and corporate networks. Firewalls and intrusion detection systems (IDSs) have been deployed to protect control centers and critical field assets against external intrusions. New protocols with security features have also emerged to protect SCADA communications within and among control centers, substations, and user-end devices.

Meanwhile, the smart grid is still far from immunity against cyber-penetrations. Cybersecurity features are often insufficient, obsolete, or absent in legacy power systems, both in control centers as well as field devices. Adoption of existing technologies for the Internet and computer security also needs to proactively accommodate physical properties, requirements, and dependencies of the physical power systems. For instance, multiple log-ins shall not result in denied or delayed access to an operator's account even after a number of failed attempts: attackers may utilize this mechanism to lock operators out of the control system that can result in disastrous consequences. Moreover, anomaly-based and signature-based IDSs also need to adapt to emerging and diversifying patterns in the smart grid to effectively identify traces of malicious behavior from data streams of normal monitoring and control; these real-time data streams will also pose challenges, in terms of both volume and complexity, to the cybersecurity analysis of smart grid. Last but not least, the security mechanisms implemented on physical electronic devices could still suffer from tempering and damages directly, and their dependence on elec-

tricity may also be exploited. As a result, similar to the status of physical security, there is an urgent need to incorporate physical aspects into the cybersecurity of the smart grid.

In short, the security and resilience of the smart grid are contingent upon the effective combination of the strength in both physical and cyber security analysis and against both inadvertent and malignant events. Vulnerabilities and contingencies shall be investigated on a broader spectrum. The causes, processes, and consequences across the cyber-physical spaces shall be comprehensively analyzed with consideration of interdependence and interoperability therein. Operators of the grid should be aware of the risks both externally and internally, while mitigation and restoration efforts need to be guided by adequate security awareness to avoid secondary damages in the post-attack systems.

1.2.3 Threats of Massive Blackouts

Massive blackouts, i.e., the complete interruption of electrical power delivery, are rare but disastrous events in the power grids. Though uncommonly seen, blackouts can affect a large population and area for an extended amount of time and incur significant operational, economic, and social disruptions. Illustrated in Figure 3 [30], the population affected by massive blackouts since 1999 unambiguously demonstrated the catastrophic impacts of blackouts in electrical power grids.

Historically, blackouts are consequences of complex disturbances and dynamics. The cascades often start from a small number of contingencies before propagating to a large area through unexpected protection system failures. Initiating events of blackouts range from software bugs (U.S. Northeast, 2003), extreme load stress (India, 2012), physical sabotage (Pakistan, 2015), to cyber-penetration (Ukraine, 2015). While most of these events were not expected to cause major outages during normal operations, unexpected operating conditions, insufficient situation awareness, or malicious outsider attempts triggered the epidemic process known as the *cascading failures*. Often due to limited coordination and communication between field protective devices, local pro-

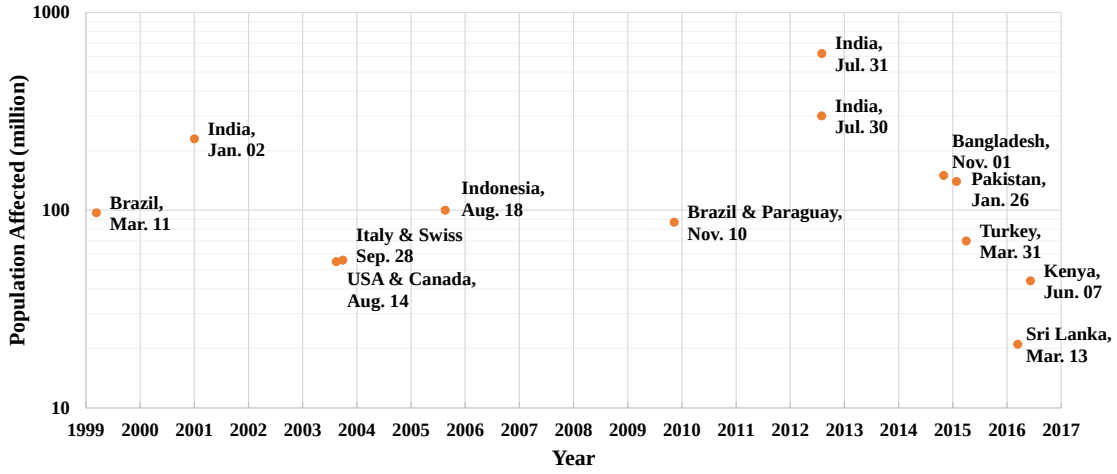


Figure 3. The population affected by major blackouts since 1999.

tection efforts after the initiating events could result in reduced reliability of the entire grid, leading to overloading lines, insufficient generation supply, or instant load loss. For interconnected power grids, although every effort has been made to ensure the grid security, when some situations are not monitored or responded promptly and properly, what could have been a small-scale outage may turn into a massive cascading blackout within minutes, leaving a large population without power for hours or days unexpectedly.

Both the frequency and size of blackouts have been increasing in interconnected power grids of the United States [31]. Aware of the impact of as well as the unpreparedness against potential major blackouts in the future, there have been significant attentions and efforts from the government, industry, and academia to investigate into this challenge. The task force formed by the Institute of Electrical and Electronic Engineers (IEEE) have directed extensive studies to discuss, evaluate, and advise the progress towards a cascade-resilient infrastructure [32, 33, 34]. However, understanding of large-scale cascades are far from mature and our solutions are limited by the complexity of the spatial-temporal system behaviors, the availability of history records and analytic tools, as well as the applicability of effective prevention and mitigation strategies [34].

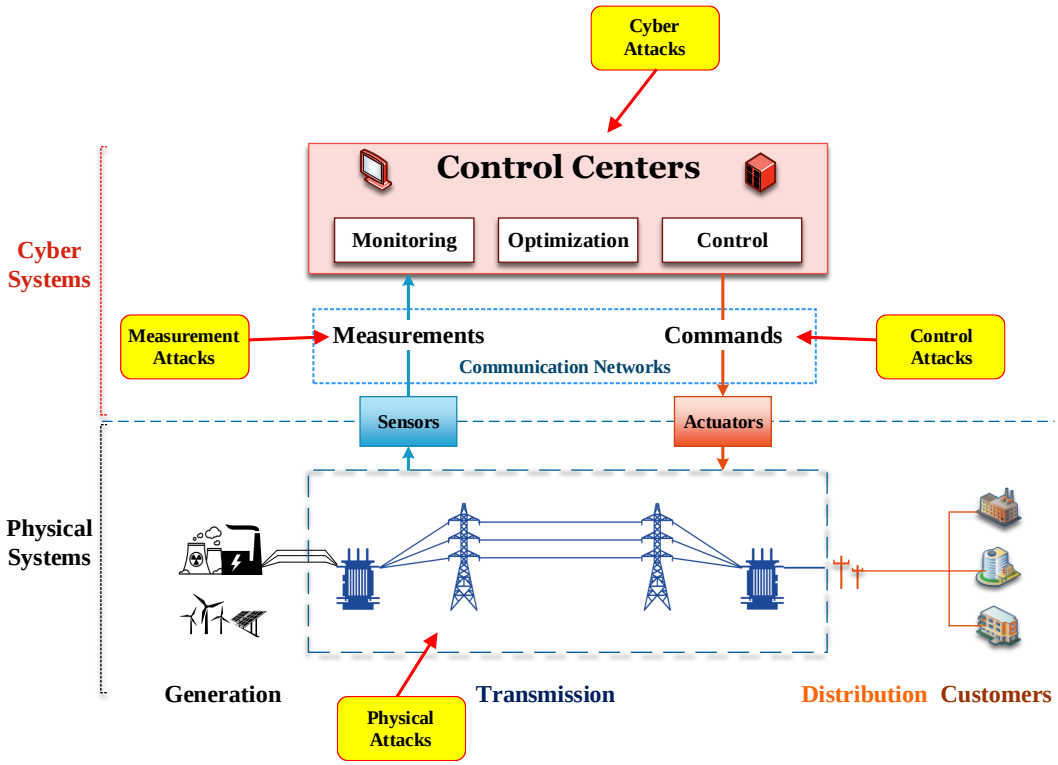


Figure 4. Cyber-physical attacks targeting the transmission grid.

1.3 Significance and Organization

1.3.1 Significance of the Research

Securing the smart grid against massive cascading blackouts requires significant research advancement and end-to-end engineering solutions on both physical and cyber security. Although there have been extensive research efforts that investigated the cyber-physical attack threats and defense strategies in the smart grid, the risk and complexity of cascading blackouts remain a major challenge to securing the smart grid to date [6]. To this end, this dissertation has aimed to systematically assess the grid vulnerability under cascading failures from both complex network and power flow perspectives, efficiently identify the critical cascade-initiating components with machine learning approach, and facilitate the understanding of grid resilience under malicious cyber-physical attacks.

To date, there have been a large number of studies investigating smart grid security

with topological approaches [35], some would date back in the early 2000s [36, 37, 38]. While these approaches provide powerful tools developed in the field of computer and network security, to adopt them in the smart grid requires the further inclusion of power system properties and corresponding models. Such incorporation, while intuitive, is not trivial due to the heterogeneity, complexity, and uncertainty of the cyber-physically integrated smart grid [6]. To this end, this dissertation has investigated and proposed complex network based topological and integrative assessment of cascading failure vulnerability in bulk power grids. The proposed models and metrics effectively identify the system vulnerabilities and critical components in the bulk grids, and the methods have been further extended to both steady-state and transient stability analyses based on more detailed and accurate power flow models [39, 40, 41].

Another challenge to secure the smart grid arises from the scale and dynamics of the interconnected components in the context of cybersecurity. Contingency screening with fast search or heuristic methods have been the effective approaches to identify critical components in a $N - k$ setting [42, 43, 44, 45, 46, 47, 48]. However, they may still fall short to include all credible scenarios for all possible target sets in a wide-area interconnected grid. The grid may fail in cyber or physical space as well as the interface in-between; the failure can occur concurrently or sequentially at distant locations; the impacts can vary significantly due to the combined effect of operating points, failure locations, timing, and order, among others. These factors result in a large search space for the grid operators to create a profile of credible, critical contingencies that require the most attention and emergency plan. To this end, the dissertation resorts to machine learning, particularly unsupervised and reinforcement learning approaches that have been expanding recently, to develop data-driven, self-adaptive methods that can help grid operators to identify the critical component sets more efficiently and accurately. Through adaptive and effective assessment, the proposed research may benefit

the development of advanced real-time monitoring, communication, and control systems for the early detection and prevention of cascading blackouts.

1.3.2 Organization of the Dissertation

The dissertation is organized into 7 chapters with an overall structure illustrated in Figure 5. Following Chapter 1 of introductions, Chapter 2 and Chapter 3 present vulnerability analyses from operational (Chapter 2) and structural perspectives (Chapter 3), respectively. Based on the proposed cascading failure models and metrics in these two chapters, Chapter 4 to 6 investigates cyber-physical attack schemes on control (Chapter 4 and 5) and measurement (Chapter 6) in the smart grid. The conclusions are drawn in Chapter 7 with discussions on future challenges and opportunities.

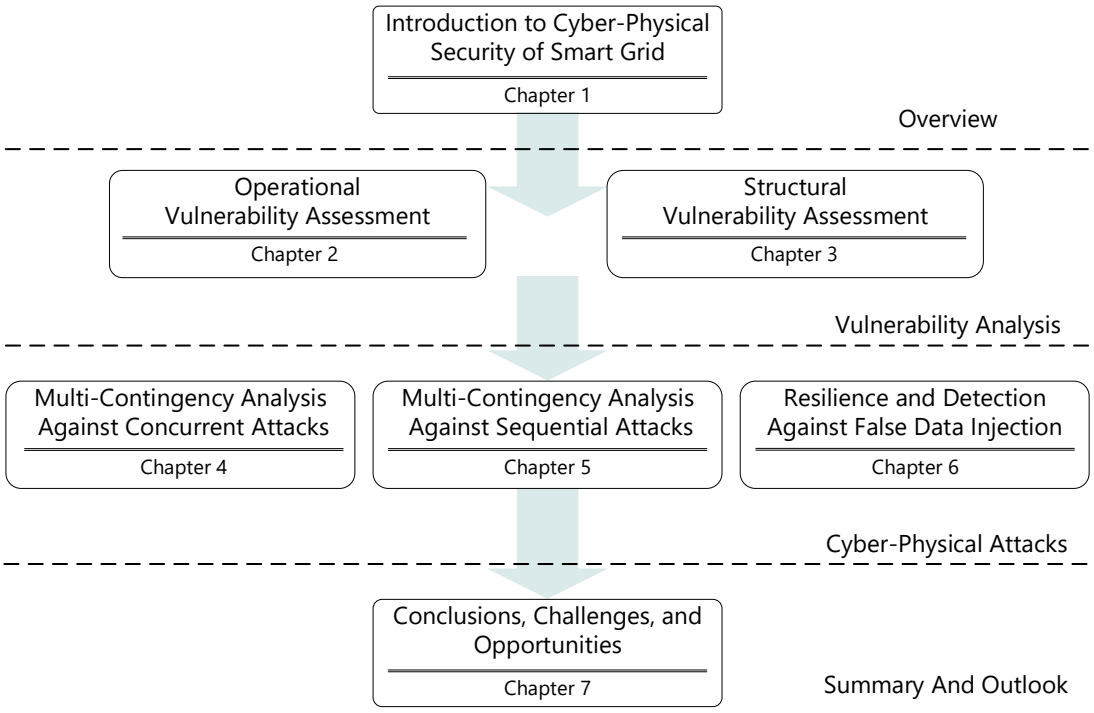


Figure 5. Overall structure of the dissertation.

Among the technical contents, Chapter 2 and 3 proposed complex network and power flow based metrics to identify critical components and processes in the develop-

ment of blackouts. The assessments also develop simulation environments to analyze the impact of potential initiating events, based on which further security analysis can look into the potential attack threats. Chapter 4 and 5 presented coordinated multi-target control attacks launched concurrently (Chapter 4) and sequentially (Chapter 5) utilizing machine learning algorithms. Chapter 6 presented cascading failure-based resilience analysis and supervised learning-based detection methods against well-known false data injection attacks on the measurement inputs of power system state estimators. Each chapter features an overview, detailed description of problem formulation, proposed methodology, simulation results, and respective summaries. The references are provided at the end of all chapters, followed by the bibliography of the dissertation. Collectively, the chapters represent a series of interdependent investigations and publications of the author on the topic of cascading blackouts in the smart grid under malicious attacks.

Specifically, Chapter 2 investigates the effect of overloading and hidden failures in the power grid after the initiating event of relay tripping. A steady-state power flow based model (DC-CFS) is developed to analyze the system behaviors during the cascading process. Based on the model, factors contributing to the massive blackouts will be decomposed and analyzed. A novel metric, the critical moment, is proposed to identify critical consistency and discrepancy between steady-state and transient stability analysis in the cascading blackouts. The investigation will reveal how failures propagate in the grid through due to power flow redistribution and provide insights on how to prevent the failure at its early stage.

Chapter 3 proposed a complex network based model (EB-CFS) to analyze the inherent vulnerability in the structure of power transmission systems. The proposed EB-CFS model, based on the concept of extended betweenness centrality, integrated the topology and property of electrical power grids to effectively identify potential structural

vulnerabilities in the interconnected grid that will lead to a massive blackout. Influence of different loading and overloading situations on cascading failures was also evaluated under different tolerance factors of the system. Simulation results from a standard IEEE 118-bus test system revealed the vulnerability of network components, which was then validated on a DC power flow simulator with comparisons to other topological measurements.

Chapter 4 presents the investigation of cyber-physical attacks launched concurrently on the control commands sent from the control centers to field devices. To address the large search space of potential victims and subsequent computational costs, a self-organizing map based approach was proposed to identify strong attack vectors in the Texas grid with over 5,000 substations. The chapter will introduce how self-organized clusters are formed to identify the combination of vulnerable components in bulk power grids that, when attacked concurrently from the cyberspace, would result in a massive blackout. The proposed approach will assist the grid operator in raising awareness and preparedness against major cyber-intrusions that cause multi-contingencies concurrently in this critical infrastructure.

Chapter 5 presents the investigation into control attacks launched sequentially. Following the preliminary work that identifies this new vulnerability of smart grid, the research proposed a Q-learning based adaptive search strategy to effectively and efficiently identify critical attack sequences that will result in a massive blackout. The Chapter will review the threat of sequential attacks and formulate the search for critical attack sequence as a reinforcement learning problem. Similar to Chapter 4, the proposed scheme addressed the challenge of a large, complex search space in the context of massive blackouts and will provide information to grid operators for better security enhancement in multi-contingency scenarios.

Chapter 6 presents the investigations on cyber-physical attacks on the measure-

ment signals. The chapter will first review the prominent threat posed by the recently revealed false data injection attacks on power system state estimator. The DC-CFS is then utilized to examine the grid resilience against this stealth attack that can bypass the traditional bad data detectors. As the simulation results indicated, the grid demonstrated significant robustness as the false data did not pose a major threat in triggering the blackouts. A supervised learning based approach was proposed to detect the stealth false data, in which three light-weight classifiers effectively identified false data from the normal measurements.

Finally, Chapter 7 summarizes the research and discusses future challenges and opportunities along the direction. The problems, methods, and impacts along each phase of investigation in this research will be reviewed along with the contribution of the work. The remaining challenges to further address potential attack threats with effective defense strategies will be discussed in the closing, with which the author hopes to shed some lights on the future endeavors along the way.

CHAPTER 2

Operational Vulnerability Assessment of Massive Blackouts

2.1 Chapter Overview

Being aware of the critical threat of massive blackouts, researchers from the industry and academia have collectively developed a large number of assessment approaches and tools to comprehensively understand the mechanisms and factors behind a blackout [32, 33]. These efforts provide the foundation to further analyze potential cyber-physical attack threats and impacts practically present in the smart grid. This research also follows this path to first establish a validated simulation platform for the vulnerability assessment and security analysis in the context of cascading blackouts.

Meanwhile, modeling and prediction of massive blackouts still remain a grand challenge due to the complexities and difficulties of diverse grid dynamics, system uncertainties, and attack schemes. To approach a solution to this multi-factor, multi-timescale, and multi-system challenge, investigations often decompose the mechanisms and focus on specific aspects of the blackout with corresponding assumptions and simplifications [34, 49]. While investigations based on different types of models provide respective insights into the cause and process of massive blackouts, they also lead to potential (and frequent) discrepancies, resulting in different precision, conflicting results, as well as distinct requirement of system information and computational resources. However, there are few studies on their discrepancy and consistency in the context of cascading failures. The apparent distinctions in-between can not delineate that to what degree these two methodologies are consistent with each other. While the steady state models are widely used in the cascading failure analysis, this chapter aims at not only investigating the physical process revealed by a specific model, but also providing a reference, through illustrative comparative studies, to help determine a more appropriate model for the analysis of power grid cascading failures from case to case.

Given the considerations above, this chapter will investigate both the operational vulnerability of bulk power grids via a time-efficient steady-state cascading failure simulator (CFS) as well as a comparative study of the steady-state model with the transient stability analysis. For the vulnerability assessment, a DC power flow based CFS will be established based on the state-of-the-art. For the discrepancy comparison, a new metric, the critical moment (CM), will be proposed based on the rotor angle stability and voltage stability principles of power grids to quantitatively analyze the discrepancies. For the dissertation, the validated DC power flow based cascading failure simulator (CFS) will also serve as the platform for topological model validation as well as cyber-physical attack analyses. In addition, this chapter is also expected to narrow the knowledge gap between two well-developed models and to facilitate understanding of cascading failures in power systems.

The rest of this chapter is organized as follows: Section 2.2 describes the power flow based DC-CFS platform for cascading failure analysis. Section 2.3 presents single-contingency assessments of cascading failures simulated with the DC-CFS. Section 2.4 compares the steady-state model with TSA model on two benchmarks, where the new concept critical moment (CM) is proposed to assess the discrepancy between two models as well as the validity of DC-CFS. Finally, Section 2.5 provides a summary of the chapter with some future directions.

2.2 DC-CFS for Cascading Failure Analysis

2.2.1 Cascading Failure Simulators (CFSs)

Simulation models are one of the centerpieces of cascading failure analysis, which aim to integrate physical properties to predict system behaviors and develop corresponding solutions. The IEEE PES CAMS Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failures [34] has reported a variety of simulation models developed for cascading failure analysis. These models focus on certain sets

of assumptions to approximate the real power system, yet a well-accepted model is still absent due to the complexity of interconnected power grids and cascading failure themselves. Meanwhile, there is limited literature comparing the validity of using different power system models to approximate system behavior in cascading failures. This chapter is thus motivated to investigate the discrepancy of two well-established types of cascading failure model, i.e., the DC power flow based steady-state model versus the transient stability model.

The steady-state models have been widely used to approximate power system behaviors for various purposes. For cascading failure analysis, the stochastic ORNL-PSerc-Alaska (OPA) model [50, 51, 52] is among the earliest and most established models for cascading failure analysis. Comprehensive work on self-organized criticality in cascading failures [53, 54, 55] have also been developed using the Manchester model [56, 57] and CASCADE model [58]. In general, the DC power flow based models are powerful for the balance between model complexity and system behavior approximation [34, 59], as they utilize the assumptions of power flow equations [60, 61] for efficient cascading failure simulation and assessment. In this chapter, we have implemented a well-defined CFS [45] with further modifications and analyses that serve as the baseline cascading failure simulator.

In contrast to the steady-state models, transient stability models have also been built on more accurate yet complex equations [24]. Based on the differential algebraic equations (DAE), they have been widely used in power system control design and served as the primary tool for contingency and stability analysis. Although the transient stability analysis (TSA) provides higher precisions to reproduce systems events in reality [62], the time-domain simulations are often cost-prohibitive for the exhaustive screening of all possible situations after contingencies. In practices, only credible contingency sets are chosen to simulate and provide dynamic information alongside the results from steady-

state models.

The steady-state models exhibit significant popularity in smart grid research concerning the cascading failures. There are two typical DC power flow based CFSs distinguished by their time-frame. Some studies [52, 63] focus on long-term effects to evaluate temperature and line-expansion to determine the vulnerability of a branch. Then proper control measures, e.g., vegetation management, can be applied to reduce the risk of blackouts. Meanwhile, other research places a focus on relays [45], because they are critical factors in major blackouts due to the automatic branch tripping mechanism operated by relays [26]. The relay-based CFS usually focuses on short-term effects occurring in seconds or minutes, in contrast to the long-term models that run from less than an hour to a few days. For a fair comparison between the two methodologies, this chapter will compare the relay-based CFS with the transient stability models for cascading failure analysis.

In this chapter, we refer to the original cascading failure simulator in [45] as the CFS, and its modified version in this chapter as the DC-CFS, respectively. In addition, the DC power generation and load are denoted as P_g and P_d, respectively, where g denotes a generation bus and d a load bus; correspondingly, the complete sets of generators and load buses are denoted as G and D, respectively. Similarly, l refers to a branch and B is the set of branches, while the DC branch power flow is denoted by F. The voltage magnitude and angles are denoted as V and θ, respectively.

2.2.2 The DC Power Flow based CFS

The DC-CFS in this chapter is developed based on [45], a steady-state cascading failure simulator for multi-contingency analysis. It belongs to a family of models of cascading failure based on DC power flow assumptions without consideration of reactive power and transmission loss [64, 65, 66]. In this chapter, modifications of modeling and implementation are made to the original CFS for cascading failure analysis and

comparison, and an overview is provided as follows with a flowchart shown in Figure 6:

1. The DC-CFS implemented an additional trigger of bus contingency so that cascading failure of both bus and branch contingencies can be simulated to validate the use of DC-CFS compared to the TSA approach;

2. In the generation and load re-dispatch process of the DC-CFS, we introduced weight vectors to the generation and load buses, which can be determined empirically in advance, or adjusted adaptively according to the feedback of simulated blackout size with proper algorithms;

3. A dedicated module is designed in the DC-CFS to handle the islanding issue so that the simulation can be implemented in parallel and further islanding technique and policy can be incorporated;

4. The system failure criterion of 10% in blackout size in original CFS is canceled in the DC-CFS so that we can explore and compare the full development of a potential cascading failure process in both models. Moreover, we can also justify if this criterion is appropriate in the simulation of cascading failures;

5. Last but not least, more implementation details, including the ramping rate, the ramping period, are provided to further improve this DC-CFS dedicated for cascading failure analysis.

While these modifications are the major contribution of this chapter, the adjustments to the original CFS enable a fair comparison between the DC-CFS and TSA model in cascading failure analysis. The detailed simulation can be divided into four steps below (*Steps A-D*) to elaborate on initial events, dispatch policy, cascading outages, and islanding processing.

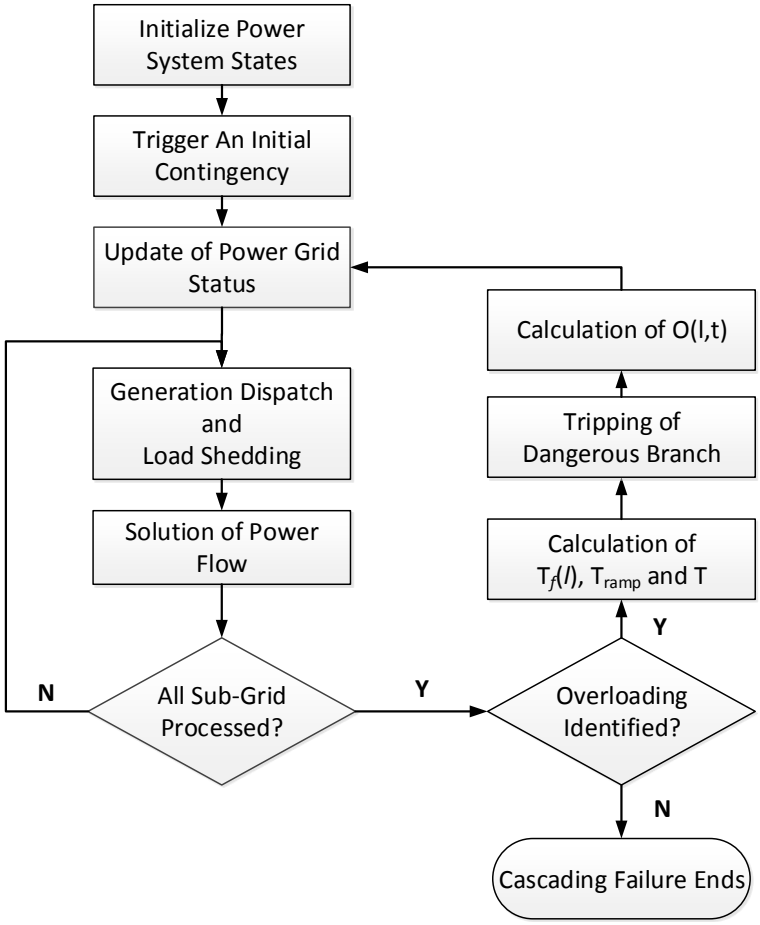


Figure 6. Flowchart of DC-CFS

A. Initial Events

In the DC-CFS we consider potential cascading failures initiated by both branch and bus contingencies in the system. A branch contingency is the tripping of transmission lines typically analyzed in traditional contingency analyses [43, 67, 68]. A bus contingency, similar to the case of a branch, is the tripping of a bus (substation) from the grid, after which no power flow is transmitted through the given bus.

In reality, bus contingencies, e.g., the outage of substations or power plants, occurred less frequently and thus were less studied in contrast to branch contingencies. Nevertheless, a cascading failure can still be triggered by a bus contingency, after which

all branches connecting to the failed bus are tripped [69, 70]. Since at least one branch will be connected to a bus, any single-bus contingency will be at least an $N-1$ event and thus more likely to result in cascading failures or greater damages to the grid, particularly after the violation of $N-1$ security. Therefore, both scenarios will be considered to better understand cascading failures in power systems.

B. Relay-based Overloading Branch Tripping

Branch tripping is one of the most common factors responsible for the cascading failures after the initial event [34]. Therefore, we refer to each tripping as a *cascading failure event (CFE)*, and the whole process of cascading failure is then represented by a series of CFEs. The initial contingency is numbered as CFE 0, while the following CFEs occurred during a cascading failure are numbered by positive integers thereafter. When a CFE occurs, overloading may be found on a branch l whose power flow F_l exceeds its thermal rating of power flow, denoted as C_l. As critical or long-lasting overloading can cause great damage to the power transmission, the relays will respond to these overloadings by tripping dangerously overloading branches from the grid. For an overloaded branch denoted as l', the following accumulative function $O(l',t)$ from [45] determines the severeness of overloading on a branch l at time t:

$$O(l,t) = \int_{t_0}^{t} [F_l(\tau) - C_l] d\tau, \;\; F_l(\tau) > C_l \tag{1}$$

where $F_l(\tau)$ is the branch power flow at time τ. Theoretically, under the steady-state assumption, $O(l,t)$ of a branch l is integrated over the duration when it is overloaded while the system remains in a steady state. As the power flow F_l will be changed by the generation and load re-dispatch after the occurrence of a CFE, t_0 and t in practice will have to be changed accordingly, which will be described later in the next subsection following Eqn. (2). If the accumulation $O(l,t)$ exceeds a dangerous threshold $O_{limit}(l)$ at time $T_f(l)$, the relays will automatically trip off the corresponding branch l. This critical threshold is defined empirically based on referential scenarios as in [45]. Note that

$O(l,t)$ is not the actual heat accumulated on the branch, but an accumulative function of overloading evaluated by the relays to trip dangerous branches accordingly.

C. Generation and Load Redispatch

When a new failure occurs, the power transmission can be disrupted, and the balance of load and generation has to be restored via re-dispatch process [71]. Specifically, between two consecutive cascading failures in a fully-connected grid, the following re-dispatching steps are performed:

C.1 Generation ramping

The generation ramping involves two scenarios:

1. If there is a generation surplus, i.e., $\sum P_g > \sum P_d$, ramp down all generators' output with a given ramping rate r.

2. If there is a generation deficit, i.e., $\sum P_g < \sum P_d$, ramp up all generators' output with the given ramping rate r until ramping is terminated;

The ramping is terminated when any of these two following conditions is met: i) $\sum P_g \geq \sum P_d$; or ii) the output of a given generator reaches its capacity $P_{max}(g)$;

C.2 Generator tripping/load shedding

Similar to the generation dispatch, there are also two corresponding processes to handle the surplus and deficit, respectively:

1. If the surplus still exists after ramping, then the generators with minimal non-zero importance will be instantly tripped one by one in the grid until $\sum P_g \leq \sum P_d$;

2. If the desired balance ($\sum P_g = \sum P_d$) is still not met after a certain amount of time T_{ramp}, the load on the bus with the minimal non-zero importance will be shed one by one until the load-generation balance is established;

C.3 Power flow update

After the ramping and shedding process, the power flow on each branch is instantly recalculated and redistributed to set up a new system operating point.

In this procedure, the ramping in *Step C.1* tries to resolve any imbalance between generation and load caused by cascading failure. In both scenarios, we assumed all generators ramp up or down with a uniformed maximal ramping rate r with respect to their capacity. As this ramping process can be interrupted by a new CFE in the system, the duration of generation ramping period between two CFEs, denoted as T_{ramp}, is determined by the following equation:

$$T_{ramp} = \min_{l \in L}\{T_f(l)\} \tag{2}$$

where $T_f(l)$ corresponds to the dangerous threshold $O_{limit}(l)$ as aforementioned. No failure occurs during this period T_{ramp}, and the power grid is assumed to stay in a steady-state. Therefore, the accumulative overload $O(l,t)$ in Eqn. (1) is integrated from t_0, the moment when a new CFE is observed, to $t_0 + T_{ramp}$, the moment when the next CFE occurs in the system. In this way, if a new CFE occurs in the system, the actual value of t_0 is automatically reset to the time when this CFE occurs, and t is set to $t_0 + T_{ramp}$ when T_{ramp} is calculated by Eqn. (2). This allows the DC-CFS to directly use T_{ramp} as a step time in simulation instead of using small, unit step intervals in classic transient stability models, which can be computationally expensive otherwise.

During the ramping period, a system can resume stable if the generation deficit or surplus is eliminated; however, if the desired balance is not met after ramping, then a generator tripping and/or load shedding is performed in *Step C.2* to ensure the system stability. The importance of a generation bus Y_g is determined by the product of its generation P_g and a weight vector W_g, i.e., $Y_g = W_g \cdot P_g$; similarly, the importance of a load bus is calculated by $Y_d = W_d \cdot P_d$.

Afterward, the system operation point is updated in *Step C.3* to continue the iterative simulation process. This procedure follows the general principle to maximize the

adjustment on the generation side while minimizing the impact on the load/consumer's side as long as the power system remains stable.

D. Islanded Sub-grids Processing

During the process of a cascading failure, an originally fully connected grid can be disintegrated into several islands, which can still maintain independent operation. Each island has independent topology, operating point, and potential cascading failures that continue to propagate therein. Instead of assigning a new CFS for each new island, in this implementation we used an alternative tactic to efficiently simulate cascading failure in islands of a power grid without increasing the implementation complexity.

Specifically, an island emerged when a CFE breaks down the grid is rendered as a new fully-connected sub-grid that carries the most recent system operating point in the corresponding segment. If generation and load are not balanced in an island, the simulator re-dispatches the load and generation and recalculates power flow through *Step C.1* to *Step C.3* to establish a new balanced operating point, and obtains the corresponding value of T_{ramp} in each island if a new CFE occurs.

As islands may be further broken down when failure continues to propagate, it is necessary to synchronize different cascading failure processes in different sub-grids during simulation. Therefore, when the values of T_{ramp} for all current sub-grids are obtained, we will use the minimum of them as a global time step ΔT to advance the simulation:

$$\Delta T = \min_i \{T_{ramp}(i)\} \tag{3}$$

where $i = 1, 2, ..., K$, and K is the number of existing sub-grids. It is notable that two consecutive values of ΔT may be obtained from different islands during the simulation, so the sequence and location of the events are also recorded accordingly. Also, because ΔT is the minimum of T_{ramp} across different islands, by definition every island still remains in steady state with their own operating points.

This sub-grid handling is beneficial because the number of islands emerging during a cascading failure is unknown in advance. This uncertainty causes a high computation overhead for the simulator to process a time-variant number of islands simultaneously. From *Step A* to *Step D*, cascading failures in all existing islands will be simulated recursively until no overloading is further observed.

2.2.3 Assessment Metric

To assess the impact of cascading failures with DC-CFS, we choose the *blackout size* as the assessment metric of a cascading failure. Denoted as ΔP, it is defined as the *percentage* of the overall loss of load (measured in real power) with respect to the original loading:

$$\Delta P = \left[\sum_{d \in D_0} P_{D_0} - \sum_{d \in D'} P'_{D'} \right] / \sum_{d \in D_0} P_{D_0} \tag{4}$$

where D_0 and D' are the sets of load buses in the original grid and the final grid, respectively. P_{D_0} and $P'_{D'}$ are the corresponding load remaining in each grid, respectively. It is also notable that the final load loss, as a result of generation and load re-dispatch in *Step C*, is equivalent to the loss of generation as the system is designed to be balanced after *Step C*.

According to the model described above, we decompose the final blackout size ΔP into three parts. First, if a contingency is initially triggered on a load bus that has a non-zero load, the load on that bus will be instantly lost, which is referred to as the direct loss of real power. Secondly, immediately after the initial contingency, the blackout size is contributed by the system's first re-dispatch and shedding process in *Step C* as an emergent response. Since there is limited time to react to the abrupt contingency, some load will be shed in this emergent response. Third and last, after the re-balance of load and generation, a potential cascading failure triggered by overloading branches will further increase the loss of load.

In addition to the blackout size ΔP, the number of load buses affected during the

cascading failure (ΔN_L) is also assessed as comparative metrics of the cascading failure impact. It is measured as the number of load buses whose load is either completely or partially shed during the cascading. The correlation efficient of ΔN_L and ΔP will be evaluated for comparison in following simulations.

2.3 Vulnerability Assessment with DC-CFS

2.3.1 Simulation Setup

In this chapter, the DC-CFS is implemented in MATLAB and the MATPOWER toolbox [60] is used to calculate DC power flow in the benchmark. The standard IEEE 39-bus system is also chosen from MATPOWER as the benchmark to evaluate the DC-CFS. This system has a total load of 62.54 p.u.; it contains 39 buses (10 of which are generation buses) and 46 branches with specified capacity C_l. The benchmark is an abstract representation of the New England test system, in which a single bus (Bus 39) represents the regional system's interconnection to the rest of US/Canada. As one of the most widely used benchmarks in power system studies, it is a suitable general representation of typical regional power transmission networks.

The ramping rate r of all generateors are set as 5%/min with respect to each generator's capacity. Since we do not have a practical reference of the importance of buses, all generation buses are assigned equal importance ($W_g = 1/N_G$); the same for all load buses ($W_d = 1/N_D$). As a result, Y_g and Y_d are proportional to the generation and load of corresponding types of buses, respectively, and so the simulator trips the generator with minimum non-zero generation and then sheds the non-zero load in the grid when necessary. These values of r, W_g and W_d can be adjusted accordingly when detailed information is obtained in real power system applications. If such information is not available, these weights can also be adjusted heuristically according to the blackout size simulated in the DC-CFS as well as other stability constraints in consideration. This allows better approximation of a real power system to minimize the impact of cascad-

ing. Finally, as mentioned before, we refer to [45] to determine the critical threshold $O_{limit}(l)$ with $T_{ref} = 5s$ and $F_l = 150\% \times C_l$. With all these settings, the DC power flow based simulation results are presented as follows.

2.3.2 Vulnerability Assessment

First, we illustrate the histograms of the final blackout size of both single bus and single branch contingency in Figure 7. As discussed in Section 2.2.2, given the same number of simultaneous contingencies, single-bus contingencies should in general yield greater cascading failure damage than branch contingencies. The distributions in Figure 7 are consistent with this assumption. Roughly 61% of the 39-single bus contingencies and 24% of the 46 single-branch contingencies lead to a blackout size greater than 10% of the overall load in the system. It is also notable that while the majority of the blackout sizes are no greater than 25%, some critical contingencies still result in the loss greater than 40%.

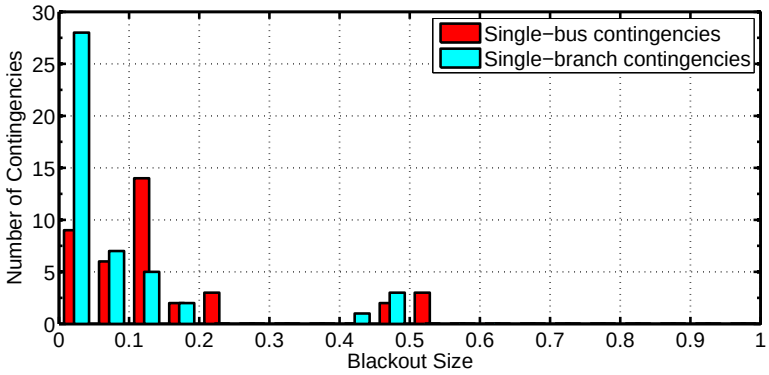
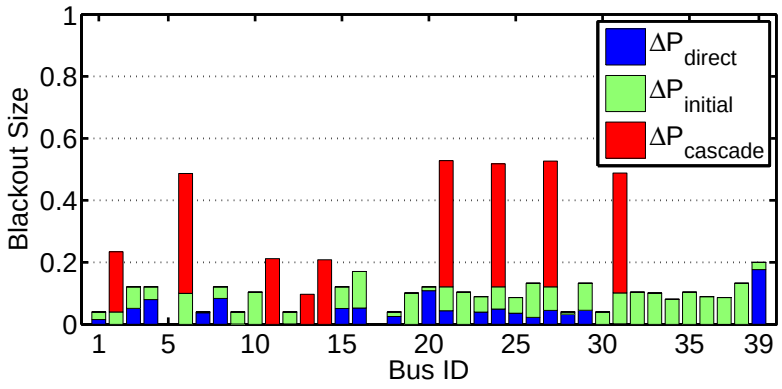


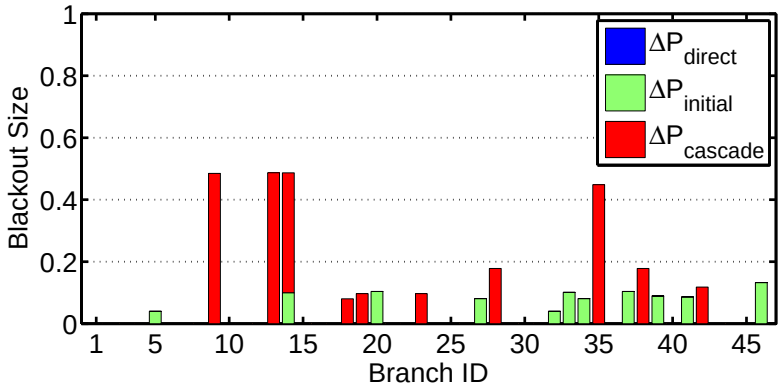
Figure 7. Blackout size distribution in the IEEE 39-bus system.

In addition to the overall blackout size, Figure 8 illustrates the decomposition of overall blackout size in single-bus and single-branch contingencies, respectively, where different components of a blackout size are shown as stacked bars representing different components in final blackout sizes. The first type of bars ΔP_{direct} on the bottom is the direct load loss on the victim buses; the second type of bars $\Delta P_{initial}$ in the middle

represents the load loss after the initial emergent re-dispatch right after the attack; finally, the last type of bars $\Delta P_{cascade}$ on top corresponds to the fraction of blackout sizes contributed by the triggered cascading failures.



(a)



(b)

Figure 8. Decomposition of blackout sizes from single-bus and single-branch contingencies.

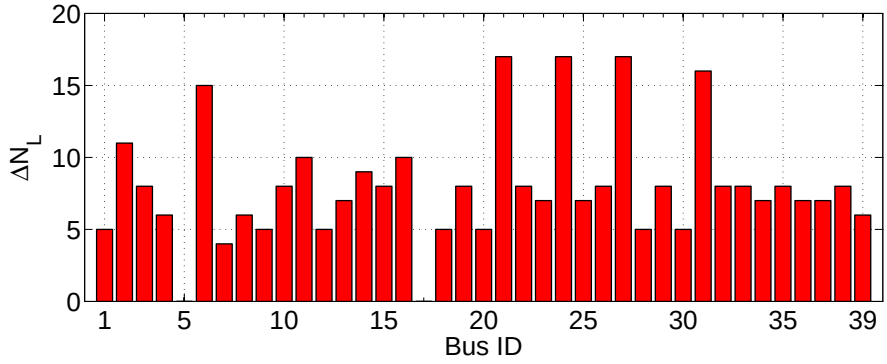
As shown in Figure 8(a), in single-bus contingencies the initial re-dispatch adds a significant amount to the blackout size to the direct loss of load buses, which is observed on most generation buses (Bus 30 to 38) and some load buses (Bus 6, 10, 16, etc). The generation-load combined Bus 39 is the only exception as it carries the largest generation and load simultaneously in the system. As an equivalent bus of interconnection to the rest of US/Canada, Bus 39 in this benchmark provides 15.88% of the generation and

consumes 17.65% of the power in this system, resulting in a significant direct impact on the system when it fails even without a cascading failure. Nonetheless, from Figure 8(a) it is still shown that the cascading failure triggered by less loaded buses is responsible for the most severe single-bus contingencies blackouts. Meanwhile, the type of bus is not closely related to the eventual blackout size, as the most severe single-bus contingencies ($\Delta P > 20\%$) can be found on both load-only buses (Bus 6, 21, 24, 27) and load-generator bus (Bus 31). In fact, because the type of a bus can be defined interchangeably by altering the net injection of the given bus without changing the overall system dynamics, it does not have a definite influence on the eventual blackout size. Instead, the decomposition of ΔP in Figure 8(a) has shown that cascading failure plays a more important role in the final impact.

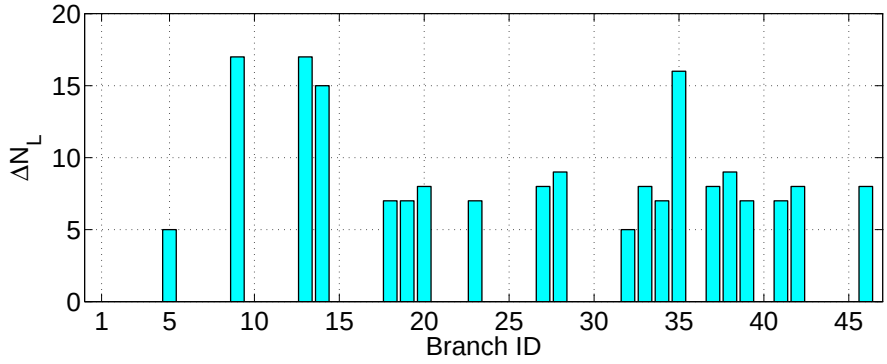
Similar observation can be found in Figure 8(b) for single-branch contingencies. Although for branch contingencies, there is no direct loss of power ΔP_{direct} on branches, the re-dispatch still contributes to some blackout sizes that reach the similar scale as the bus-contingency blackouts without a cascading failure. However, in the most severe cases, the cascading failure is still the major factor in severe blackouts, which raises some ΔP to nearly 50%. For both types of triggers, we have observed that cascading failures contribute significantly in the major blackouts caused by a single-component contingency.

In addition to the blackout size ΔP, we have also evaluated the number of load buses affected in the cascading failures using DC-CFS. The number of load buses affected by a cascading failure(ΔN_L) is shown in Figure 9 with both types of triggers. The correlation coefficients of ΔP and ΔN_L are $\rho_{pl,bus} = +0.9365$ for buses and $\rho_{pl,branch} = +0.9278$ for branches, respectively. The results indicate a relatively high correlation between the blackout size and the number of buses that subject to load shedding during the cascading failures, which is reasonable as the bus with the minimal load

will be directly tripped when generator ramping cannot achieve the load-generation balance.



(a)



(b)

Figure 9. Number of affected load buses after (a) single-bus and (b) single-branch contingencies, respectively.

As a summary of this section, from the simulation results and analysis above, the DC-CFS proves to be a useful tool to understand the vulnerability of a power system against cascading failures. Information on the final impact, cascading failure development as well as contributing factors can be obtained more efficiently with the DC-CFS, which is especially helpful if it is extended to a bulk power system or a detailed regional grid that has a greater number of substations and transmission lines in the system.

2.4 Comparative Studies

While the DC-CFS simulation shown above presented important information on the development and eventual sizes of cascading failures, it is certainly critical to understand how precise these vulnerability assessments are in comparison to some more complex models. As mentioned before, the DC power flow model is a proper representation of high-voltage low-load power grids [59] with a good balance between the computational efficiency and model complexity. It certainly provides important information of power system behavior in cascading failures. However, it does not consider the reactive power and voltage characteristics in a complex power system, and a steady-state assumption can fail to hold in the complex dynamics of a real power system. Therefore, we presented a comparative study between the DC-CFS and Transient Stability Analysis (TSA) to understand the discrepancy and consistency between them for cascading failure analysis. The TSA model is implemented in the Power System Analysis Toolbox (PSAT) software, a popular open source toolbox for the research on both static and dynamic analysis of power systems [72].

In addition to the IEEE 39-bus system shown in Figure 10, we also implemented the IEEE 68-bus system in PSAT shown in Figure 11 as an additional benchmark. The additional system is an extended representation of the New England and the New York power system, with three buses as the equivalent of three external regions connected to these two regional power grids. As an extension to the 39-bus system, the 68-bus system has a significantly larger total load of 176.21 p.u., and variances of both power generation and load consumption are also greater than the 39-bus system. This more complex network can pose a greater challenge to the DC-CFS as discussed below. All parameters used in PSAT can be found in publications for the 39-bus system [73, 74] and the 68-bus system [75], respectively. There is no direct generation dispatch or load shedding in PSAT, and branch tripping is simulated upon each occurrence of CFE iden-

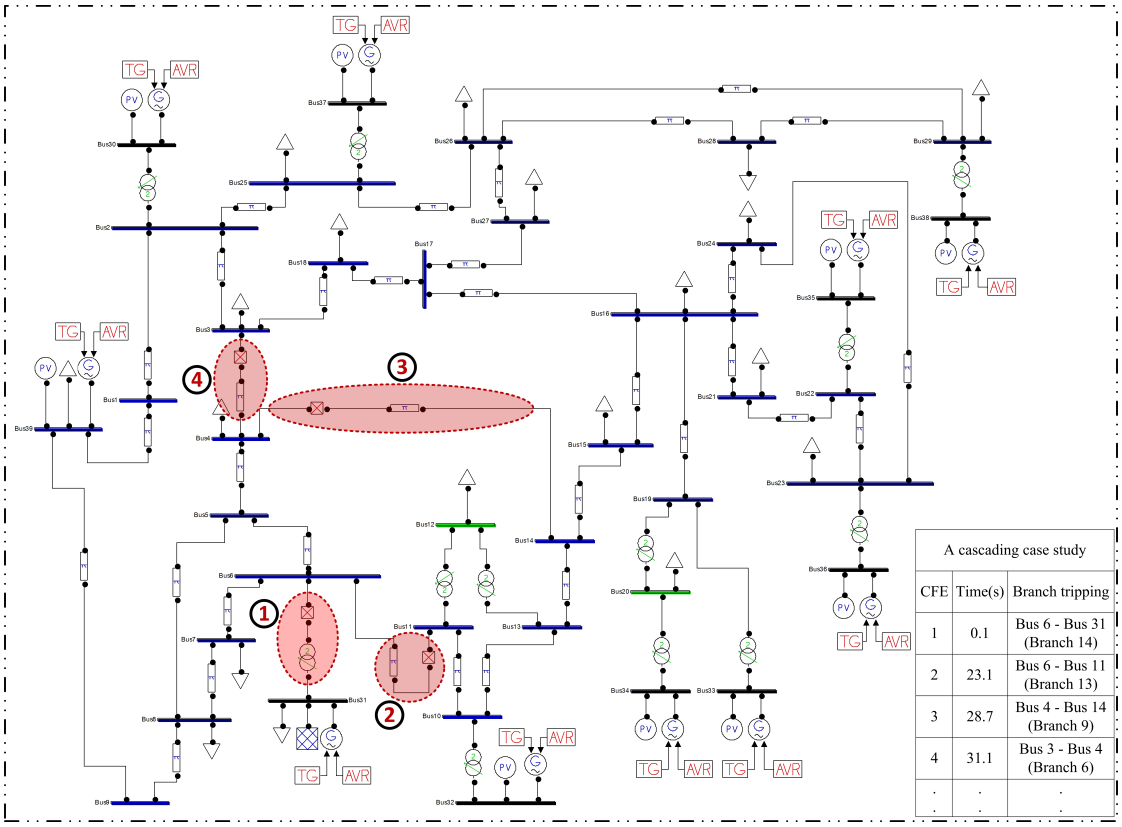


Figure 10. Cascading failures after Branch 13 in the IEEE 39-bus system is tripped. Branches affected in the cascading failure are numbered and highlighted.

tified by the DC-CFS. Numerical comparisons between two models are presented below to reveal their consistency and discrepancy in the simulation of cascading failures.

2.4.1 Case Study

To illustrate the consistency as well as the discrepancy between the DC-CFS and the TSA model, a comparative case study of a single-branch contingency on the IEEE 39-Bus System is first presented as follows. We choose the cascading failure caused by the tripping of Branch 14 (from Bus 6 to Bus 31) as a baseline for the comparative study. This branch failure isolates Generation Bus 31 from the grid, which has been shown previously as a severe cascading failure in the system. According to the DC-CFS simulation result, after the cascading failure has been triggered, subsequent branch tripping has been found on Branch 13, 9, 6, 1, and 23 before the failure terminates. We

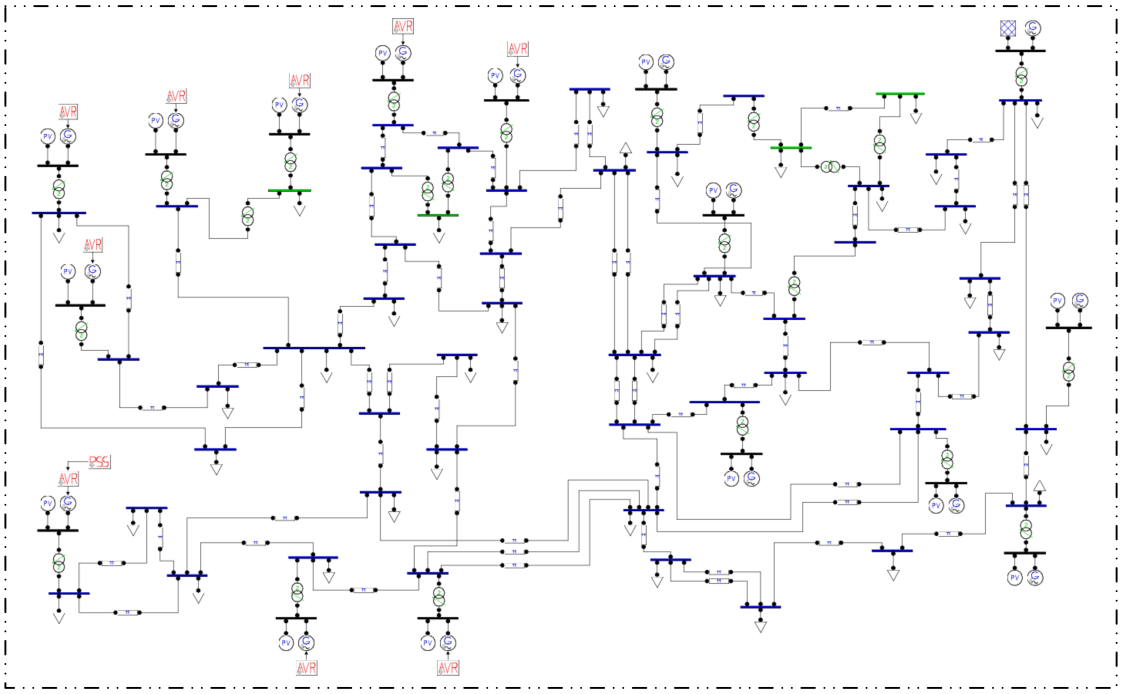
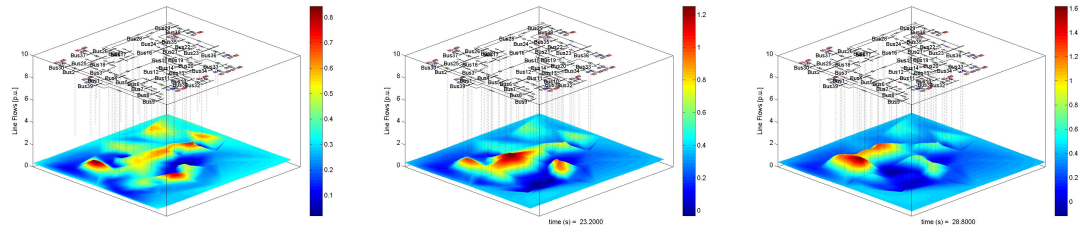


Figure 11. The IEEE 68-bus system in PSAT.

record this sequence of CFEs with the moments of occurrences in DC-CFS, and then set up the simulation of identical branch tripping at the same moments in PSAT. The location and occurrence time of these CFEs are shown in Figure 10. Then we observe whether there is a consistent trend of power re-distribution and branch overloading, and if so, to what extent this consistency holds during the cascading failure.

The corresponding line load rate distribution after each CFE is partially visualized in Figure 12, and the initial system branch flow is shown in Figure 12(a). After the initial CFE on Branch 14 (CFE 1), the active power transmission on Branch 13 increased immediately. This is because Branch 14 is linked to Load Bus 1 with a generator Bus 31, whose failure draws more power to supply Load Bus 7, Load Bus 8 and Load Bus 4 through Branch 13 simultaneously, resulting in a severe overloading condition that forces the relay to trip Branch 13 in CFE 2 after 23.1 seconds. Figure 12(b) shows the subsequent system line load rate change after the tripping of Branch 13, in which the active power transmission on Branch 9 surged immediately. The reason is



(a) (b) (c)

Figure 12. Transmission line load rate distribution (a) before cascading; (b) after Branch 13 is tripped; (c) after Branch 9 is tripped.

that Branch 13 and Branch 9 are two branches connected the load area (left) to the generation area (right). The tripping of Branch 13 significantly increased the Branch 9's transmission burden. As a result, Branch 9 was consequently tripped in CFE 3 at 28.7 seconds after the initial tripping. Until this point, simulation results remain consistent between the two models despite that they are based on different power flow assumptions and that the regulation is only performed in the PSAT simulation.

Upon the next occurrence of CFE, however, the system dynamics begin to change. Although in Figure 12(c), the most severe overloading is still observed on Branch 6 for both DC-CFS and TSA models. However, the system voltage has already started to collapse after CFE 3, making following simulations of two models diverge into different flow distributions. This discrepancy can be observed in the change of rotor angles (Figure 13(a)) and bus voltage magnitudes (Figure 13(b)), respectively. Each curve in Figure 13(a) represents a generator and in Figure 13(b) a bus in the 39-bus system.

As some bus voltages dropped to a relatively low value and some generators start to desynchronize after CFE 3, the system became unstable as the bus voltages began to oscillate till the end of the simulation. In practice, grid operator will trip some generators to prevent further damage to the machines caused by desynchronization. As a result, the branch line load rate distribution in simulation also began to diverge between these two

models from the next CFE. Specifically, the active power transmission on Branch 16 increased dramatically in the TSA model, while the DC-CFS simulation suggested that the next branch to be tripped should be Branch 1. As a summary, for this cascading failure triggered on Branch 14, the steady-state assumption no longer holds after CFE 3 due to the significant change in the power grid dynamics. The importance of CFE 3 in this example leads to the concept of the critical moment (CM) as an index of consistency, which is described as follows.

2.4.2 Critical Moments

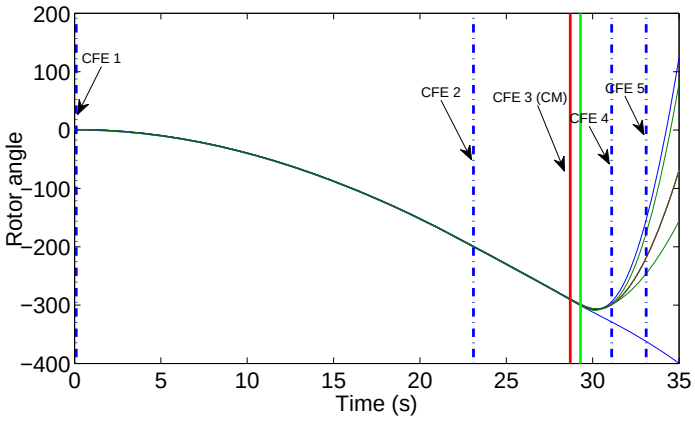
From the case study above, it is desirable to define the CM in a more generic way for comparison between the two models. To define the critical moment (CM) numerically, we refer to two principles of power systems, i.e., the rotor angle stability and voltage stability as the criteria of CM.

Specifically, given the two following numeric criteria:

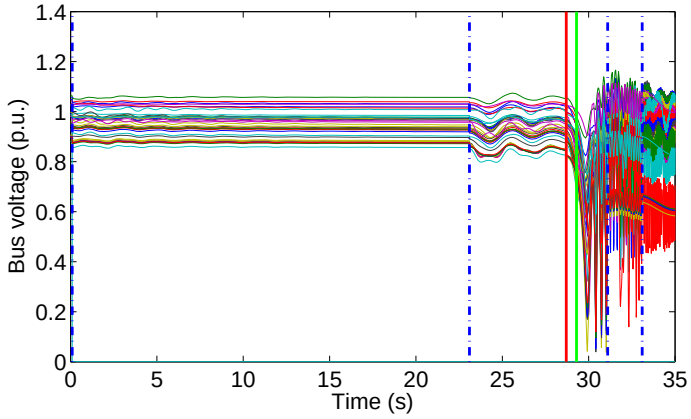
1. The maximal difference between any two rotor angles is greater than 10°;
2. The voltage of any bus deviates from its original voltage in p.u. by 10%.

A critical moment (CM) is defined as the most recent CFE that occurs before the point when either (1) or (2) is met. As an example, if criterion (1) or (2) is satisfied at a moment τ between CFE k and CFE $k+1$ in a cascading failure simulated by the DC-CFS, then CFE k is selected as the CM after which the steady state assumption does not hold for the DC-CFS.

It is notable that for most of the research on transient stability, stability criteria can vary among different benchmarks and different methods, e.g., change of sign of PEBS or an arbitrary value, such as π [76]. In this study, both thresholds are chosen empirically based on the following consideration. For criterion (1), according to [24], the angular difference depends on the power-angle relationship, where it demonstrates a



(a)



(b)

Figure 13. The (a) rotor angles and (b) bus voltages after the initial tripping.

highly nonlinear characteristic. For large-disturbance rotor angle stability (corresponding to small-disturbance or small-signal rotor angle stability), the time frame of interest in transient stability studies is usually 3 to 5 seconds following the disturbance, i.e., the most recent CFE before the divergence. In such a short time frame, it will be reasonable to set "10 degrees" as the criterion to determine the critical moment. For criterion (2), we refer to [23], which states that when the voltage drop below 85% to 90% of its nominal value, more motors may drop out consequently and lead to a cascading effect if

the original cause of voltage drop remains unsolved. Therefore, we choose the moment when the voltage drops to 90% of nominal value, i.e., the 10% deviation, to determine CM with criterion (2). For the case study, the CFEs and CM are marked in Figure 13 as vertical dotted lines and solid lines, respectively.

Although the actual moment τ when one of the criteria is met can also be rendered as a critical point in the simulation, by defining CM as a CFE that corresponds to a failure event in the system instead of a continuous time value, it is more intuitive and convenient to keep track of the CFEs. With the above definition, we have calculated the CMs for the top ten single-component contingencies of both types on IEEE 39-bus and 68-bus system, respectively.

First, for the 39-bus system, the consistency and discrepancy are visualized with a new figure called a Time-domain Difference (T-Diff) plot shown in Figure 14. In this visualization, we selected the top-10 most severe blackouts of single-branch contingencies according to the DC-CFS model and illustrated their normalized duration and CMs in the bar graph. The occurrence time of each CFE in each cascading failure is normalized by their overall duration, respectively. In this way, the horizontal bars represent the series of CFEs for the top-10 cases in the time-domain. The corresponding blackout size ΔP, the total number of CFES (N_{CFE}), the CMs and their actual time of occurrence are listed to the right of the bar graph with the legends shown under it. The superscripts next to CM indicate whether the criterion of rotor angle stability (marked with †) or the criterion of voltage stability (marked with $*$) is met when the corresponding CM is obtained.

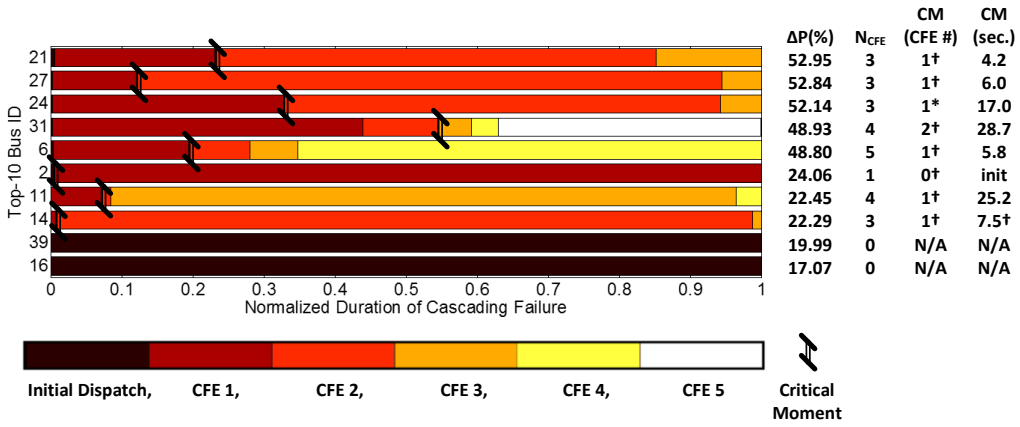
As shown in Figure 14, the CMs of bus-contingencies on average are relatively smaller than those of the single-branch cases. In other words, the duration in which the two models are consistent with each other is relatively longer in single-branch cases. This is reasonable as the tripping of buses usually does not follow the $N-1$ security

standard in cascading failures, and so they may lead to more significant damage to the system stability and results in earlier CM than the branches.

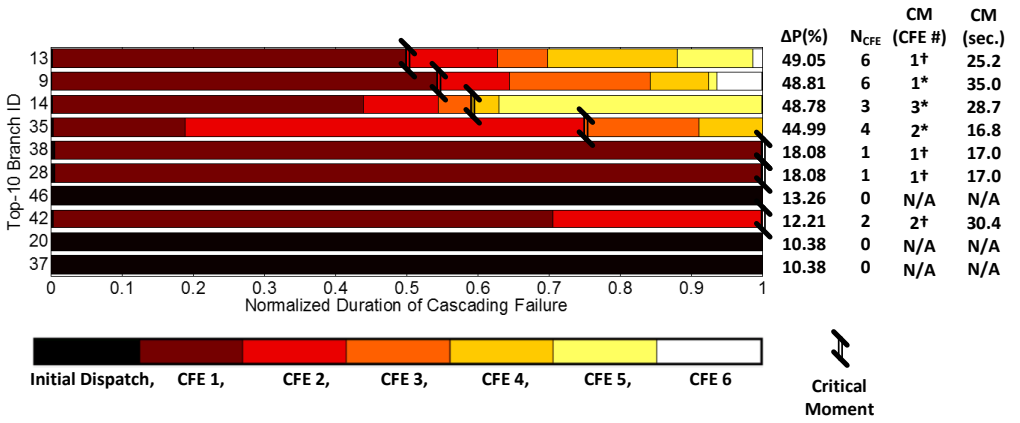
Meanwhile, for some branch contingencies (Branch 28 and 38), consistency between the two models remains throughout the whole cascading failure process. In these cases, the DC-CFS can be utilized for its computational efficiency in cascading failure analysis. For the contingencies that did not result in a cascading failure (indicated by *Init.*), there is no CM between the two models, because the system always stays in a steady state after the initial contingency.

Results of CMs for the 68-bus system can be found in Table 1 with the same notation as in Figure 14. The top-10 severe contingencies all lead to subsequent cascading failures according to the DC-CFS, and corresponding blackout sizes ΔP are comparably larger than that of the 39-bus system. It is also notable that some single-branch contingencies yield identical CMs as the single-bus contingencies in the 68-bus system, as each of these branches is the only branch connecting the corresponding bus to the rest of the power grid.

From Table 1, it is also observed that the CMs in single-bus contingencies are relatively short compared to single-branch contingencies, which is consistent with the 39-bus system. However, although the total number of CFEs becomes greater in the 68-bus system, the CMs of the top-10 single-branch contingencies turn out to be relatively smaller compared to the 39-bus system. The major reason is that some generators (e.g., Bus 12, 13, 14, 15 and 16) are providing at least 10 p.u. of power to the rest of the grid, and the load of buses is also significantly greater (e.g., 4 buses have load greater than 10 p.u., and the maximal load is as large as 60 p.u.). This causes an extremely imbalanced burden on a number of buses in the 68-bus system, while the rest of the grid operates in a state with more redundancy. The contingencies triggered on these transmission lines result in more severe damage to the system, and so the stability is lost



(a)



(b)

Figure 14. Critical moments in the top-10 (a) single-bus and (b) single-branch contingencies in the 39-bus system.

Note: "init." denotes right after the initial dispatch, and "N/A" denotes the moment does not exist. The superscripts next to CM indicate whether the criterion of rotor angle stability (marked with †) or the criterion of voltage stability (marked with $*$) is met when the corresponding CM is obtained.

more easily compared to the 39-bus system where no generator therein has an output greater than 10 p.u. and the maximal load is only 11 p.u.. In other words, as the CM is defined by two stability criteria, it is thereby more likely to observe a smaller CM of a given contingency if the contingency leads to a greater impact on the system's stability.

As a summary, when the oscillation or disturbance is confined within a certain range, the power flow based simulator can well approximate the power system behavior. However, when cascading failures continue to develop, the power flow based CFS can fail in capturing the actual power system behavior as the steady state assumption does not hold anymore. In this case, TSA models are more suitable for the simulation of power system behavior so that proper critical control action can be taken to address severe power grid disturbances. For very large scale benchmarks with thousands of buses, criteria that render a power grid has reached a system failure can also be considered an alternative strategy to evaluate the impact or risk of cascading failures. For instance, in the original CFS [45], the simulation of a cascading failure is terminated when the blackout size reaches 10%, which can help limit the discrepancy caused by the loss of dynamic stability in the system. The CM proposed in this chapter can be further developed and utilized to determine such threshold of blackout size accordingly to take the advantage of the simulation efficiency of DC-CFS for bulk power systems. Meanwhile, as there is still a certain degree of consistency between the DC-CFS and TSA models despite the differences between steady and transient stability models, the DC-CFS model can still be utilized for applications such as early stage intervention and mitigation of cascading failures, if the system has been designed with sufficient stability margin, e.g., greater transmission capacity or fault tolerance, against these severe single-component contingencies.

Table 1. Critical Moments of Top-10 Contingencies in the 68-Bus System.

Rank	**Buses**	ΔP (%)	N_{CFE}	CM (CFE #)	CM (seconds)
1	17	81.84	12	6^*	4.1
2	13	79.84	13	$1^\dagger$	1.7
3	12	70.79	14	$1^\dagger$	1076.5
4	16	62.37	8	1^*	1.6
5	36	61.19	12	1^*	0.8
6	61	49.58	14	$4^\dagger$	8.3
7	15	40.66	9	$2^\dagger$	10.8
8	51	38.11	4	2^*	4.0
9	50	35.28	4	2^*	4.0
10	14	30.85	5	1^*	1.3
Rank	**Branches**	ΔP (%)	N_{CFE}	CM (CFE #)	CM (seconds)
1	74	79.84	13	$1^\dagger$	1.7
2	70	70.79	14	$1^\dagger$	1076.5
3	78	62.37	8	$1^\dagger$	1.6
4	45	51.27	13	$2^\dagger$	2.9
5	71	40.66	9	$2^\dagger$	10.8
6	56	33.82	4	$2^\dagger$	4.6
7	57	33.79	4	$2^\dagger$	6.2
8	72	30.85	7	$1^\dagger$	1.3
9	83	25.12	9	$1^\dagger$	5.1
10	8	19.58	3	$2^\dagger$	9.7

2.5 Chapter Summary

In this chapter, we implemented a modified DC power flow based cascading failure simulator to evaluate its utilization in the contingencies triggered by both bus and branch failures. Simulations on the IEEE 39-bus system were presented to illustrate the utilization of DC-CFS from multiple perspectives. Then simulation results of DC-CFS were compared validated against the TSA approach with two benchmarks (IEEE 39-bus and 68-bus system) implemented in the Power System Analysis Toolbox (PSAT). A new concept, i.e., the critical moment (CM), is proposed and illustrated to measure important consistencies and discrepancies between these two well-established methodologies,

which aims to facilitate a more comprehensive understanding of cascading failures in power systems.

Although built with only DC power flow assumptions, the DC-CFS is able to assess the vulnerability of power grids in the early stage of cascading failures, as discussed in the chapter. Informative details of cascading failure development can be revealed from different perspectives including the size, the contributing factors and the duration of cascading failures. However, as the DC-CFS is utilizing the steady-state assumption to replace the complex transient dynamics of power systems, if the cascading failure violates the power system dynamic stability principle, then the underlying steady-state assumption behind DC-CFS will not hold and the simulator will fail to capture the power system dynamics.

The critical moment (CM) presented in this chapter illustrates the strength and limitation of DC power flow based steady state model in cascading failure analysis. As a model with a number of simplifications of complex power system dynamics, the DC-CFS certainly is able to acquire important information regarding the development and final impact of cascading failures. However, as the discrepancy between these two models emerges in cascading failure simulation when the impact to the system dynamic stability becomes significantly large, the DC power flow based models shall be carefully used to assess the impact of cascading failures after severe system contingencies. It is notable that this definition of CM can be further utilized for comparisons between other power system models, including the long-term stochastic models when proper timing information is provided.

It is notable that the calculation of CM in this chapter still requires simulation of TSA model that will increase the computation overhead. While the major contribution of this chapter is to evaluate the discrepancy and consistency between two models rather than to compete with pure DC-CFS on computation efficiency, it is desirable that CM

can be determined independently for real world applications. This will be the primary focus of our future work. Also, some of the parameters, e.g., the choice of T_{ref} and F_l in the calculation of $O_{limit}(l)$, the ramping rate r in the re-dispatch procedure, and the branch capacity C_l of the benchmark system all have potential influence on the value of CM [77, 69]. This reflects the complex nature of power system and cascading failure itself, which will consist of our focus in the next stage to evaluate the significance of their influence on CM. Furthermore, we will also consider an extension to the AC power flow based cascading failure simulator (AC-CFS) and compare this complex power based model to the TSA approach. Then a hybrid model of the AC-CFS and the TSA model combining the strength of both models with proper visualization [78] can be beneficial to power grid operators, on which the influence of more complex control policies and preventative techniques like early warning signals [79] can be further developed.

CHAPTER 3

Structural Vulnerability Assessment of Massive Blackouts

3.1 Chapter Overview

By its nature, the smart grid is a complex network of cyber and physical systems interacting with each other. The electrical power infrastructure may be exposed to inherent vulnerabilities rooted in its physical properties and topological connections that would critically affect the development of a cascading blackout. Since the interconnections require extensive planning and remain relatively stable after installation, the inherent structural vulnerability in the power grid also has a long-term impact on the risk of massive blackouts, particularly if such vulnerability remain unknown to the operators under normal operating conditions.

Moreover, it is notable that the threat of cascading failures can be intensified by the growing cyber-integration. On one hand, the structural information of the grid could be more easily accessible than the dynamic operating information processed in the control centers; on the other, such structural information can still reveal critical locations and components in the grid that could result in significant damage if exploited by malicious attackers. Studies [80, 81, 22, 82, 6] have revealed that cyber assets and intelligence will raise new challenges to the security of the smart grid. For instance, malicious attackers can take advantage of potential access points at RTUs to plan intrusions with intelligence collected from the intrusions [83, 84, 85]. With further knowledge on the potential of cascading failures, attackers and terrorists can conceive critical attacks that could result in massive blackouts [86]. Therefore, this chapter aims to develop models and methodologies to understand the structural vulnerability with consideration of specific physical properties, which is expected to contribute to both defensive strategies and decision supports to protect the critical infrastructure.

The rest of this chapter is organized as follows. The complex network based ex-

tended betweenness (EB) metric and the proposed EB-based simulator for cascading failure vulnerability assessment are presented in Section 3.2. Simulation results and analyses are provided in Section 3.3. A summary of the chapter will be provided in Section 3.4.

3.2 Structural Vulnerability Assessment Based on Complex Networks

3.2.1 Complex Network Analysis for the Smart Grid

Complex network theories have been one of the most used tools to understand cyber-physical system behaviors in the last decade [87, 35]. By definition, a complex network refers to a network of interacting components with non-trivial properties [88], which have propelled studies in communication networks, social networks, smart grid, and transportation infrastructures, among others. Meanwhile, with increasing interconnection of local networks, growing communication traffic, diversifying demands and services, as well as emerging new technologies, complex networks in the real world are also becoming increasingly sophisticated to operate and coordinate. Such complexity has also lead to cascading failures in complex networks beyond the energy sector [89] and draws growing interest from the research community [36].

Among the efforts to examine the structural vulnerability of power grids with complex network theories, one of the popular approaches is to adopt well-developed concepts, tools, and algorithms from graph theory and topological analysis [90, 91, 92]. In contrast to traditional power system analysis, which requires a very detailed set of power system operating point information and involves a large cost of non-linear calculations, topological approaches utilized justifiable simplifications that require limited knowledge of the structure and reduce the computational overhead without the dynamics.

However, as a complex network with unique physical characteristics, the power grid encompasses unique features that pure topological methods can not generalize [93, 31, 94, 95]. For instance, a key difference lies in the nature of the load. In computer

networks, e.g., the Internet, the load is defined based on the flow of information, which is transmitted along a single path between the source and destination. However, in power grids, the flow of electricity does not follow the geodesic shortest path from generation to load. Instead, electrical power flows along all existing transmission lines throughout the grid before being distributed to the consumers, regardless of the length of paths. In addition, power flows follow the Kirchhoff's Law, a fundamental basis in traditional power system analysis [96, 97] but usually omitted in topological analyses. Considering such trade-off, if complete information is inaccessible or computational cost remains expensive, there is a strong motivation for both the power grid operator as well as the potential malicious attacker to investigate structural vulnerability with integrating both topological and power grid methods.

From the complex network perspective, the power grid can be regarded as a weighted, directed map with two major types of interconnected components, i.e. nodes and edges, referred to as *buses* and *branches* in the context of power grids, respectively. Similar to the previous chapter, both types of contingencies are covered in this chapter. As the failure propagation process is closely related to a system's tolerance of fault, this chapter also investigates the relationship between the final blackout size and the tolerance factor of a system. The goal is to provide an integrative tool with a better balance between accuracy and complexity to identify critical components from a structural perspective based on power system behavior under potential contingencies and/or adversaries.

There have been extensive studies on the complex network security analysis within the context of power grids. For example, R. Fitzmaurice *et al.* use a complex network model to evaluate short-term risk-aversive dispatch policies in power systems [98]. Researchers have also pointed out the relevant possibility that blackouts in a bulk complex network system are first-order phenomena [99]. More recently, Y. Koç *et al.* introduce

the entropy [100] in power system analysis, which has been utilized in other network security studies [101]. Last but not least, spectral method has also been popular in topological analysis of complex networks [102].

On top of the aforementioned efforts to overcome the drawbacks of pure topological measurements for the power grid, a recent study by E. Bompard *et al.* [103, 104, 105, 106] proposed an extended topological power-flow analysis using the Power Transfer Distribution Factor (PTDF). In what follows, l, g and d denote a transmission line, a generation bus and a load bus in the power grid, respectively. Correspondingly, L, G, and D will denote the set of branches, generation buses and load buses, respectively.

3.2.2 Power Transfer Distribution Factor (PTDF)

The PTDF is a matrix of whose elements correspond to the power flow change on a branch l when one unit of real power (1 p.u) is injected at a bus v and withdrawn the slack bus. The matrix will be denoted as F in the rest of the chapter. By definition, the magnitude of each element in F can be interpreted as the sensitivity to nodal power injection of a transmission line, and its sign is the relative direction of the actual flow with respect to the reference direction of the given branch. Based on the assumptions of bus voltage magnitude and angle as well as transmission loss, there are two types of models to calculate the PTDF: the direct current (DC) model assumes lossless transmission and pure real/active power injection in a system, while the alternate current (AC) model considers the transmission loss on branches and the existence of reactive power [60]. The DC models have been widely used thanks to the simplified linear assumptions for fast computation with relatively reliable accuracy [59], while the AC models, in general, have better accuracy at the cost of complexity, as discussed in the operational vulnerability assessment earlier in this dissertation. In this chapter, the DC-PTDF based model is the primary focus in this structural vulnerability assessment, while the AC extension will also be covered in comparison.

3.2.3 Extended Betweenness

Combining the power-flow based PTDF with topological analysis, a new definition of the load in the network can be introduced to analyze the structural vulnerability. The re-defined load on each bus v, proposed by E. Bompard *et al.* and coined the *Extended Betweenness*, involves three major steps:

First, the power flow sensitivity of branch l with respective to the pairwise unit power transmission is calculated by:

$$f_g^d(l) = F_{lg} - F_{ld}, g \in G, d \in D, l \in L \tag{5}$$

where F_{lg} and F_{ld} are the power flow occurred on branch l when a unit power is injected on a generation bus g or a load bus d and withdrawn from a reference slack bus, respectively.

Then, with the definition of power flow sensitivity, we can calculate the capacity of power transmission between a *transmission pair* g and d. Specifically, because of different sensitivities to power flow injection, a more sensitive branch will reach its given power flow limit faster than less sensitive ones given the same capacity. Therefore, the maximal power that could be transferred between any given transmission pair is limited by the most sensitive branch in the whole grid. This assumption can be easily extended to a more realistic case where the branch capacities are different. Assume that each transmission line has a designed limit $P_{max}(l)$ measured in MW, the pairwise power transmission capacity between g and d when the first branch in the grid reaches its thermal rating is defined as:

$$P_g^d = \min_{l \in L}(\frac{P_{max}(l)}{|f_g^d(l)|}), g \in G, d \in D \tag{6}$$

which is calculated for all pairs of generation bus g and load bus d in the system. In other words, P_g^d is a theoretical pairwise power transmission upper-bound between a transmission pair due to the limit of branches.

Last, the extended betweenness of a bus is calculated as the overall power transmission capacity of the given bus v:

$$T(v) = \frac{1}{2} \sum_{g \in G, d \in D, l \in L^v} P_g^d \cdot f_g^d(l),\ g \neq d \neq v \in V \tag{7}$$

where L^v is the set of branches directly connected to a bus v in the set of all buses V. The product $P_g^d \cdot f_g^d(l)$ is the power flow transmitted via branch l when power between a transmission pair g and d is transferred at its pairwise transmission capacity. The discount factor $\frac{1}{2}$ is applied since the total power flowing into a bus is equal to the total power flowing out.

The extended betweenness of a branch is defined similarly. As the branch PTDF F has either a positive or negative sign according to power flow direction, the branch extended betweenness of l is determined as the greater one between the absolute values of total in-flows and out-flows:

$$T(l) = \max_{l_+, l_- \in L} \{ \sum_{g \in G, d \in D} P_g^d \cdot f_g^d(l_+), \sum_{g \in G, d \in D} |P_g^d \cdot f_g^d(l_-)| \} \tag{8}$$

where l_+ and l_- indicate $f_g^d(l)$ with a positive sign and a negative sign, respectively. It is notable that in [104] the extended betweenness is interpreted as a representation of the total power transmitted on a branch l in the grid. However, in the power flow theories, the positive and negative power flow on a branch will cancel each other; in this case, the actual load is measured differently as the sum of both values. As the focus of this chapter is to develop a CFS based on extended betweenness for cascading failure analysis, we adopted the definition of $T(l)$ as it was originally proposed, while further modifications can be implemented to adapt to the power flow assumptions.

We adopt the extended betweenness as the load on each bus and branch because of its strength to incorporate both topological and electrical characteristics of power grids. Although the term *extended betweenness* resembles the concept of betweenness

centrality in graphic theory and complex network studies, it should be noted that there is a distinctive difference between them: the extended betweenness is not based on the geodesic shortest paths. Although it is associated the idea of pairwise transmission flow, the "extended betweenness" implies the overall power transmission capacity according to a power flow based model; consequently, the measurement is closer to the real power systems that purely topological models. In addition, this model utilizes the sensitivity and flow limit on each branch to calculate the structural transmission capacity as an index of load/importance, thereby it provides a better approximation on power transmission than pure topological approaches. In summary, the extended betweenness captures physical characteristics of a real power system that add to its robustness while still retains the strength of security analyses of complex networks.

3.2.4 Extended Betweenness Based CFS (EB-CFS)

On top of the extended betweenness measurement proposed to assess the static structural vulnerability of power grid, we also see the potential of developing a cascading failure simulator (CFS) with the metrics. The motivation is two folds: On one hand, without a complete knowledge of real-time loading information, the extended betweenness can be used as a more power-related approximation of load than pure topological methods, and the overall loss of extended betweenness can be used to approximate the portion of blackout size related to embedded structural vulnerability in power grids. On the other hand, the extended betweenness is still merely a static structural measurement that cannot fully consider the effect of consequent failure propagation in a massive blackout. A further development of a CFS will help us better approximate the consequence of power grid behaviors, including overloading and failure propagation triggered by the initial contingency, so that we can better evaluate and understand the subsequent impact that may cause the collapse of power transmission networks.

Based on the above considerations, we proposed an extended betweenness based

CFS (EB-CFS) for structural vulnerability assessment. The proposed EB-CFS do not depend on the complete real-time generation or load status of a given bulk power grid. This allows power grid operators to assess the inherent structural vulnerability of critical components in cascading failures and can be computationally efficient even in bulk power grids.

In the rest of this section, we will describe the iterative extended betweenness based cascading failure simulator in details. The general procedure of the EB-CFS is shown in the pseudo codes in Table 2, and details of the four major steps are described as follows:

1. Initialization

The first step is to setup initial status of all network components and related parameters. The capacity in the context of extended betweenness is usually calculated as a function of the initial load of a given benchmark, which assumes that branches carrying heavier power transmission load will be designed to have greater capacity[45]. Therefore, we refer to our previous work [107, 69, 70] and assume there is a global *overload tolerance* in a system, denoted as Tol. Numerically, this can be defined as $Tol = Cap(c)/T_0(c)$, where $Cap(c)$ is the capacity and $T_0(c)$ is the initial load (extended betweenness) of a component c in the given system. Note that by definition, the Tol should always be larger than one, and it can also be viewed as the system redundancy between the initial load and its maximal capacity. In reality, the loading of a transmission network is dynamic which varies over time, resulting in different remaining tolerance ratio even with a constant capacity. Therefore, to evaluate different possible tolerances in reality, a numerical analysis on the relationship between tolerance and the cascading impact will be evaluated. By varying the value of Tol used in THE simulation, we can generate different situations of system tolerance to measure the vulnerability of cascading failures for different system states.

To initiate a contingency, we simply screen the buses or branches in the grid and trip

the candidate of interest from the original grid. Then the iterative process of cascading failures below will be started in the EB-CFS.

2. System Update

The structure of a power grid will be changed after the initial contingency or a component failure during the cascades. Consequently, the extended betweenness is re-calculated to reflect the latest transmission capacity of the system. It is notable that updates should be made through computations from the PTDF matrix F to the extended betweenness T, as all intermediate parameters depend on the current network topology. Whenever a new grid topology is set up, we will first recalculate the PTDF depending on whether DC or AC model is chosen. Then, the branch sensitivity $f_g^d(l)$ and the pair-wise power transmission capacity P_g^d will be updated to $f_g'^d(l)$ and $P_g'^d$, respectively. Afterwards, the power flow of branch l generated by a transmission pair g and d will be changed to $P_g'^d \cdot f_g'^d(l)$. The extended betweenness T' at any given moment is calculated with Eqn. (7) and (8). Also, in the cases where the initially fully-connected grid is broken down into disconnected islands, we will set up a new topology for each of the sub-area and re-calculate the extended betweenness T' locally within each sub-area. As a special case, if a new sub-grid contains no generation buses or load buses, by definition the extended betweenness of all components in this isolated sub-grid will be set to zero.

3. Failure Identification

A failure that occurs on either a bus or a branch will affect other components in the grid, but it may or may not result in a fatal overloading. The overloading degree, if exists, becomes a critical index affecting whether an overloading is turning fatal. Hereby we define the overloading ratio of a component c, denoted as $r(c)$, as the extended betweenness over the initial betweenness, i.e. $r(c) = T'(c)/T(c)$. It reflects the impact of the previous failure of each component during the cascading process. As components

Table 2. Extended Betweenness based Cascading Failure Simulator

Initialization: Calculate the initial extended betweenness T as a system's initial load with the corresponding capacity, which is a value set by the system tolerance parameter Tol;
Initial contingency: Initiate a tripping and update the network topology;
while $\exists$ *any tripped or failed component* **do**
Step 1: Re-calculate the PTDF and the extended betweenness to acquire the redistribution of load;
Step 2: Determine if any component is overloaded, and if this overloading is severe enough that it exceeds the capacity, which is referred to as a *fatally overloaded state*;
Step 3: Trip the fatally overloaded component from the grid and update the network topology;
end while
Vulnerability Assessment: Evaluate the total loss ΔEB as the measurement of structural vulnerability after the cascade.

in the system subject to a maximal degree of overloading ratio, they will be shut off and disconnected if the upper-bound is reached. Therefore, we consider a component c is fatally overloaded, or failed, if $r(c) > Tol$; if, however, an overloading occurs but not fatal ($1 < r(c) \leq Tol$), then component c is regarded as deficient but still in operation.

4. Component Tripping

For any failure occurs in the power grid due to the initial contingency or the failure caused by overloading, the network topology will be modified accordingly. In this chapter, the following policy is applied to update the grid topology:

1. If a bus fails, no more power can be transmitted through this nodal connection in the system, and so any branch connecting to it will also lose the transmission ability. Therefore, for any bus failure, the bus itself, as well as all connected branches, are removed from the topology;

2. If a branch fails, as a bus connecting to its end can still be linked to the remaining system by other branches, the EB-CFS will only remove the failed branch from

the network.

3.2.5 Assessment Metrics

In order to identify the most critical component, an assessment metric of structural vulnerability is necessary. In this chapter, we use the loss of total extended betweenness, denoted as ΔEB, to evaluate the vulnerability. The value is defined as the fraction of total extended betweenness lost after the cascading

$$\Delta EB(c) = \frac{\sum T'(c') - \sum T(c)}{\sum T(c)},\ c' \in C' \text{ and } c \in C \tag{9}$$

where C is the initial set of buses (V) or branches (L) according to the type of contingency, and C' is the corresponding set of components in a stabilized power system after a cascading failure. This metric can be more accurate than pure topological measurements or extended betweenness alone, as it covers not only the initial structural vulnerability but also the effect of potential cascading failures. However, it should be noted that due to the combination problem, the feasibility of exhaustive search can be significantly limited in $N-k$ analysis if the order k or the size grid is greatly increased. In this case, other techniques to improve the searching efficiency should be incorporated accordingly.

3.3 Simulations and Results

3.3.1 Simulation Setup

The proposed method requires information on electrical properties of a power grid, and so it will be tested on a modified IEEE 118-bus system [108]. Specifically, dual branches connecting the same pair of buses will be merged as one, and the number of transmission lines is thus reduced to 179. To decide the value of P_{max}, we assign the emergent thermal rating limits to all 179 branches as described in Table 3. These values are obtained from the Appendix of [108] and will be set as constants during the simulation.

Table 3. The capacity of all 179 branches in IEEE 118-bus Benchmark

Branch ID	P_{max} (MW)
7, 9	1250
8	1000
36, 38, 51, 133, 134	750
3, 21, 31, 33, 50, 90, 91, 93, 94, 95, 103, 104, 112, 119, 132, 156, 176	500
All other branches	250

To compare the integrated cascading based metric against pure topological measurements, two topological metrics, i.e., the connectivity loss (δC) and the change of characteristic path length ($\Delta\lambda$) [94] are chosen for comparison.

First, the connectivity loss is defined as the average decrease of the percentage of generation buses no longer connected to any load bus after the cascading failures:

$$\delta C = 1 - \frac{1}{N_D} \sum_{i \in D} \frac{N_G^i(c)}{N_G} \tag{10}$$

where N_G and N_D are the number of generation and load buses in the original grid, respectively. $N_G^i(c)$ is the number of generation bus that can still be reached by bus i after a component c after the imitated cascading failures from the grid.

Secondly, let λ_0 be the characteristic path length of the original grid, i.e. the average length of all pairwise shortest path from generation buses G to load buses D; also, let $\lambda(c)$ be the characteristic path length after a component c is taken down. Then, the change of characteristic path $\Delta\lambda$ is defined as $\Delta\lambda = \lambda(c) - \lambda_0$.

To validate ΔEB as an effective structural vulnerability metric, we utilize the DC power flow based cascading failure simulator (DC-CFS) from the previous chapter. The DC-CFS calculates the total loss of load (in MWs) caused by the failure propagation after tripping of the top-ranking components for each metrics to validate the vulnerability of components.

3.3.2 Pre-cascading Analysis

As aforementioned, the system tolerance Tol is an important factor in the simulation of cascading failures, as it decides to what degree an overloaded component is considered "tolerable" with respect to its initial loading status. To determine a proper range for Tol in simulation, we first consider a system that is designed to avoid any cascading failure after a single contingency. In this case, there shall be a required fault tolerance above which no overloading will be fatal and no cascading failure will occur. This *required tolerance*, denoted as R, is defined as the maximum of overloading ratio r immediately after any single bus/branch removal. Our simulation has shown that in the DC-PTDF model, the maximum and mean values of R are 3.90 and 1.29 for the buses, and 4.26 and 1.38 for the branches, respectively. In the AC-PTDF model, the corresponding values are 2.96 and 1.28 for buses, 4.20 and 1.38 for branches, respectively. These results help us refine the range of Tol to be within 1.0 and 2.0, which will be used in the following simulations of this chapter.

With the refined range, we can also evaluate the number of effective cascades, in which at least one component in the system other than the initial contingency is tripped. Table 4 lists the number of tripping after single-bus and single-branch contingencies for both DC and AC models of PTDF. The table also exhibits how the tolerance parameter can affect the cascading failure simulation. For instance, after single-contingencies under DC-PTDF model, when $Tol = 1.5$, only 23 of all 118 single-bus contingencies and 42 of all 179 single-branch contingencies can lead to a cascading effect. However, if Tol is set to 1.2, the corresponding numbers will rise to 43 and 95, respectively.

3.3.3 Cascading Failure Analysis
Single-Bus Contingencies

For the single-bus contingencies, we perform an exhaustive search over the set of loaded buses D, i.e., buses with non-zero load, to calculate their ΔEB under each

Table 4. Number of cascade-initiating contingencies under different tolerances.

	Single-Bus		Single-Branch	
Tol	DC-PTDF	AC-PTDF	DC-PTDF	AC-PTDF
1.0	91	113	166	178
1.1	68	74	129	140
1.2	43	40	95	95
1.3	35	32	70	70
1.4	26	25	55	52
1.5	23	23	42	41
1.6	18	19	35	36
1.7	16	13	28	25
1.8	9	8	18	17
1.9	7	7	14	13
2.0	7	6	13	12

tolerance. For each value of Tol, we consider the bus with the greatest ΔEB as the most vulnerable. Values of ΔEB of the most vulnerable buses are listed in Table 5 for both DC-PTDF and AC-PTDF model, and trajectories of ΔEB over the chosen Tol range are plotted in Fig.15. These buses, i.e., Bus 30, 38, and 65 in the DC model and Bus 30, 68, 65, 68, 69, and 80 in the AC model, reveal more structural vulnerability than other buses due to their contribution to cascading failures. It is notable that with DC-PTDF, the most vulnerable buses produce ΔEB above 80% only when $Tol \leq 1.8$; meanwhile, with the AC-PTDF model the loss of ΔEB will always stay above 80% for all tested tolerance values. This reflects that the difference in system modeling will also contribute to the eventual vulnerability measurements, a factor that shall be carefully considered when determining the criticality of components.

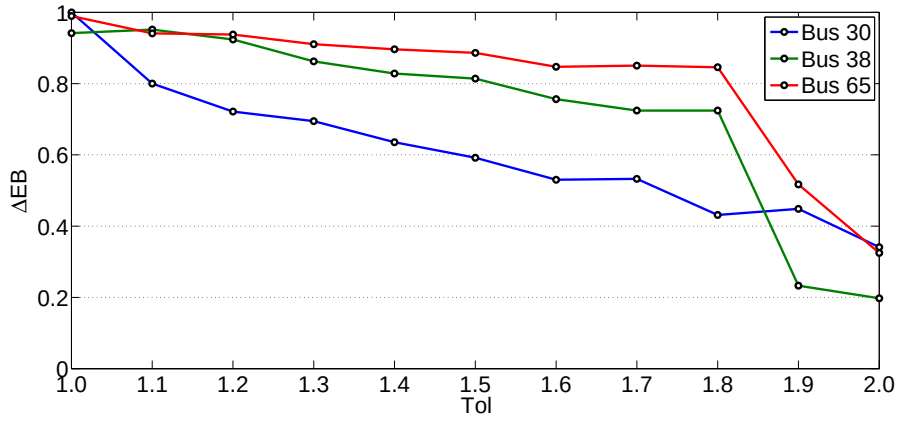
There is another observation regarding the trend of ΔEB when Tol increases. In Fig.15, although ΔEB varies with respect to different Tol, the maximal ΔEB that a single-bus contingency can create is in general non-increasing with the increase of Tol. However, we can also observe that ΔEB for each bus alone may not decrease monotonically, a fact consistent with both PTDF models. Although intuitively, greater toler-

Table 5. The most vulnerable buses in $N-1$ contingencies

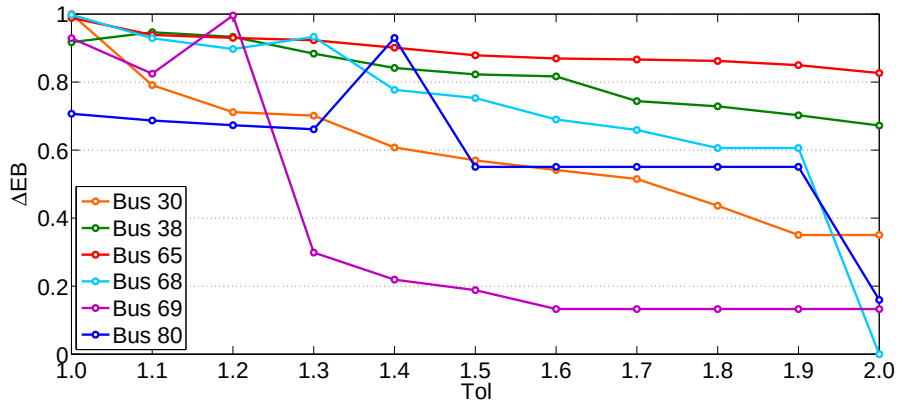
	DC-PTDF				AC-PTDF			
Tol	Bus	ΔEB	Branch	N_{fail}	Bus	ΔEB	Branch	N_{fail}
1.0	30	100.00%	38	108	30	100.00%	38	108
1.1	38	95.16%	38	62	38	94.64%	38	62
1.2	65	93.77%	38	52	69	99.60%	38	55
1.3	65	91.06%	65	41	68	93.28%	65	44
1.4	65	89.61%	65	30	80	92.97%	65	36
1.5	65	88.62%	65	25	65	87.88%	65	28
1.6	65	84.71%	65	20	65	86.93%	65	24
1.7	65	85.05%	65	18	65	86.51%	65	22
1.8	65	84.58%	65	16	65	86.10%	65	21
1.9	65	51.70%	65	13	65	84.86%	65	18
2.0	30	34.10%	65	10	65	82.66%	65	17

ance/redundancy with respect to the initial load should increase the system's resilience and lead to the smaller impact of cascading, this observation is still reasonable due to the complex mechanism behind cascading failure. In some cases, e.g. contingency on Bus 65, a slightly increased tolerance from 1.6 to 1.7 may not be able to reduce the loss of load across the whole grid, as the load will be redistributed elsewhere in another region of the 118-bus system that has less transmission capacity. As a result, this can cause more severe overloading in the new area and result in greater load loss.

Finally, the number of failed components (N_{fail}) after cascading failures is provided for the most vulnerable buses in Table 5. While N_{fail} is correlated to the cascading failure process and thus the value of ΔEB, it is noted that it drops significantly when Tol increases. Meanwhile, ΔEB remains relatively high under most Tol tested. This discrepancy can be interpreted by the varying load on different buses, which will greatly influence the cascading effect but is absent in the measurement of N_{fail}. In practice, even when there is only a small number of failed components in the grid, the power system can fail to maintain stability after the loss of some critical buses.



(a)



(b)

Figure 15. ΔEB of the most critical single-bus contingency in IEEE 118-Bus system according to (a) DC-PTDF and (b) AC-PTDF model.

Single-Branch Contingencies

In this part, we further utilize the EB-CFS for the assessment of $N-1$ branch contingencies. Similar to the single-bus scenario, the most vulnerable branches identified by ΔEB are presented in Table 6. To illustrate the impact of Tol, the values ΔEB of all the branches identified are plotted as bar graphs in Figure 16. The IDs of the most vulnerable branch for each value of Tol are shown on top of the corresponding bar of ΔEB, respectively.

In Figure 16, the maxima of ΔEB in single-branch contingencies generally decreases with an increasing system tolerance; but for specific cases, the cascading failure caused by single-branch contingencies can still yield an increase of ΔEB within the given range of Tol. This is similar to the case of single-bus contingencies, where a greater tolerance re-distribute the load and re-directs the cascade into sub-regions with unexpected overloading. Branches in this new overloaded area will lead to increased loss overall. From Fig.16(a) and Fig.16(b), ΔEB of Branch 93 and 100 in both PTDF models remain comparatively greater than other branches with a larger Tol, demonstrating consistent vulnerabilities across both models. With a further look into the structure, Branch 93 connects Bus 38 to 65 and Branch 100 connects Bus 65 to 68; all these buses have also been consistently identified as the most vulnerable buses in single-bus contingencies previously.

It is notable that for the larger tolerances, the values of ΔEB after single-branch contingencies can be greater than those after single-bus contingencies. For instance, in DC-PTDF model, when $Tol = 1.9$ the maximal branch ΔEB is 65.02% (Branch 93), while the maximal bus ΔEB drops to 51.70% (Bus 65); similar observations are also found with $Tol = 2.0$ in both models. Recall that in the pre-cascading analysis, the mean and maximum of required tolerance R for branches are also greater than the corresponding values of buses. These consistent observations suggest that the loss of some branches can be more critical than the loss of buses even in the presence of a larger tolerance.

Finally, from Table 6, the number of failed branches N_{fail} after losing the most vulnerable branches also decreases drastically when Tol is increased. It is also shown that a small number of critical branch failures in the cascading process can nevertheless result in a severe disturbance or outage in the power grid.

Table 6. The most vulnerable branches in $N-1$ contingencies

	DC-PTDF				AC-PTDF			
Tol	ID	Max ΔEB	ID	Max N_{fail}	ID	Max ΔEB	ID	Max N_{fail}
1.0	36	100.00%	36	170	98	100.00%	54	174
1.1	93	92.05%	93	82	36	96.86%	100	106
1.2	76	90.18%	41	70	51	93.91%	93	64
1.3	135	79.04%	142	48	134	97.81%	21	57
1.4	30	72.43%	36	35	138	87.13%	36	52
1.5	100	68.67%	94	29	26	88.12%	26	58
1.6	100	66.71%	98	29	94	86.15%	94	37
1.7	93	66.33%	94	23	94	78.53%	98	35
1.8	93	68.42%	54	18	100	64.17%	8	17
1.9	93	65.02%	121	15	93	64.89%	121	16
2.0	93	64.18%	121	17	93	89.86%	121	16

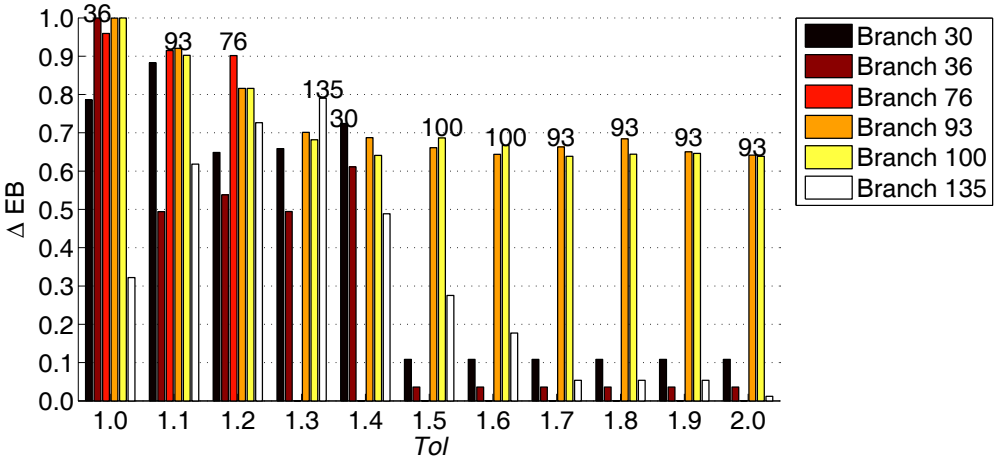
Influence of Tolerance

In previous discussions, a global factor Tol is used as a criterion to determine the system tolerance of fatal overloading in the EB-CFS. This results in overload tolerance proportional to the initial value of extended betweenness for each bus/branch. Meanwhile, for transmission lines in a real power grid, it is common that the actual capacities are designed into a small, finite set of categories according to transmission requirements. Therefore, this part will also discuss another setting where the tolerance are preset independently of the initial EB. In this setting, a constant threshold Tol_U is used to determine the tolerance of EB after redistribution during the cascades. The single-branch contingency with DC-PTDF model will be used as an example to analyze the influence of tolerance.

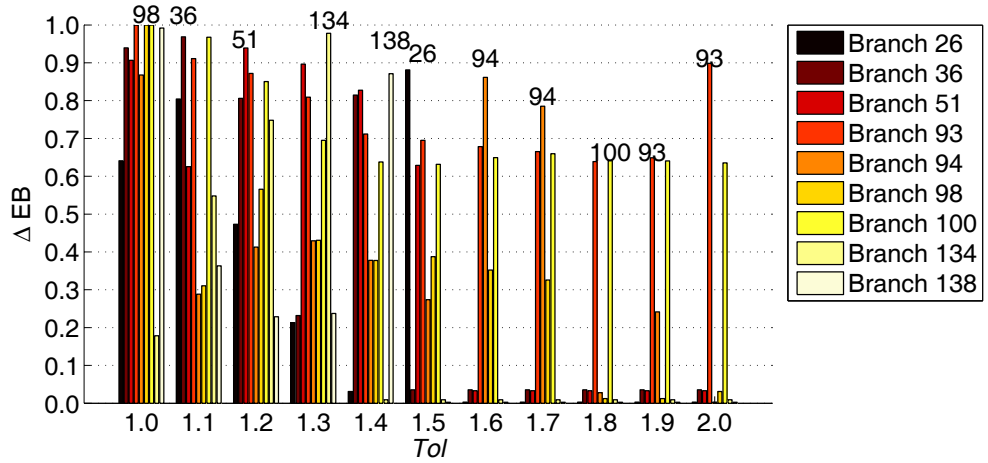
Specifically, the universal tolerance Tol_U is calculated as the product of the maximal T in the initial grid and its corresponding tolerance:

$$Tol_U = \max_l\{T_0(l)\} \times Tol_M \tag{11}$$

where Tol_M is the tolerance factor with respect to the maximal initial extended between-



(a)



(b)

Figure 16. ΔEB of the most vulnerable branches under (a) DC-PTDF and (b) AC-PTDF models, respectively. The most vulnerable branch IDs identified under each Tol are labeled on top of the corresponding bars.

ness that also guarantees no branches are overloaded under Tol_U.

Using Tol_U as a control variable, the most vulnerable branches under different Tol_M become significantly different: for $Tol_M = 1.0$, the most vulnerable branch is Branch 108, and its ΔEB is merely 5.40%. For $\forall Tol_M \geq 1.1$, the most vulnerable branch is always Branch 30, whose $\Delta EB = 10.82\%$. Further investigation into

these two tolerance intervals showed that Branch 108 is the most vulnerable when $Tol_M \leq 1.07$, while it is replaced by Branch 30 when $Tol_M \geq 1.08$. In the latter case, the global capacity Tol_U is sufficiently large, so that there is no cascading failure triggered by single-contingencies in the 118-bus system. As a result, the majority of ΔEB are only contributed by the direct loss in the initial contingency. Meanwhile, both the global constant capacity and the global constant tolerance carry a certain level of simplifications of branch capacity in reality. Since a generally accepted cascading failure model has not been established yet [34], further improvement on the modeling of capacity in EB-CFS can be helpful in understanding the complex power grid security against cascading failure threats.

Run-Time Analysis

The complexity of a CFS poses a constant challenge to cascading failure analysis in practice, and thereby a run-time analysis is provided herein for the proposed EB-CFS. The complexity can be viewed as four-fold from the top down perspective:

1. The number of system tolerance (N_{Tol}) to be evaluated;
2. The number of components in a given grid (N_{grid}) and the number of failures as the initiating events (k).
3. The run-time of a cascade $O(cascade)$, i.e., the overall number of failures (N_f) occurred in a complete cascading process;
4. The run-time to update extended betweenness T for each occurrence of a failure. It can be roughly approximated by $N_G \times N_D \times N_L \times O(T)$, where $O(T)$ is the approximate computational complexity of calculating the extended betweenness for a given component.

Among these four levels of complexity, N_f is the most difficult to obtain analytically as it depends on the structural topology (connectivity and scale), the electrical

property of power systems, and the specific contingency initiated. These dependencies render it infeasible to express N_f in an explicit closed form. Nevertheless, if we only consider single-contingencies ($k = 1$) and assume that the complexity of the worst case to simulate a complete cascading failure is $O(cascade)$, then the overall complexity $O(EB\text{-}CFS)$ can be approximated by $O(EB\text{-}CFS) = N_{Tol} \times N_{grid} \times O(cascade)$.

Although an analytic and explicit form of the complexity of EB-CFS is difficult to obtain, we can still acquire empirical run-time information of the exhaustive search approach in the simulation. Specifically, we implemented the EB-CFS in MATLAB 2010b on a Windows 7 64-bit operating system, with 8 GB DDR5 memory and Intel Xeon W3565 3.20 GHz quad-core processors. The average run-time is obtained from 100 runs of the exhaustive search of single contingencies in the IEEE 118-bus system. The run-time of each complete search, denoted as $RT(Run)$, is recorded along with the average run-time per each given tolerance $RT(Tol)$ and per each contingency $RT(Contingency)$. The results are shown in Table 7 with corresponding types of contingencies and PTDF models. Note that as $RT(Run)$ is obtained from 100 runs while 11 Tol values are tested in each run, $RT(Tol)$ is the average of 1100 samples, and $RT(Contingency)$ is the average of 129,800 samples of single-bus contingencies but the average of 196,900 samples of single-branch contingencies, respectively.

With the information of $RT(Contingency)$, to simulate all the 118 single-bus contingencies in DC-PTDF model with $Tol = 1.0, 1.1, ..., 2.0$, the average run-time of a complete exhaustive search can be approximated by $N_{Tol} \times N_{grid} \times RT(Contingency) = 11 \times 118 \times 0.116 = 150.57$ seconds, which is very close to the actual run-time per search, i.e., 151.22 seconds. Similarly, the estimated overall run-time for single-branch contingencies in the DC-PTDF model is 329.07 seconds, while the actual run-time is also very close as 329.06 seconds.

According to the second row of Table 7, for the grid operator, if the tolerance of

Table 7. Average run-time of EB-CFS for single-contingencies.

Run-Time (sec.)	DC$_{bus}$	AC$_{bus}$	DC$_{branch}$	AC$_{branch}$
RT $(Contingency)$	0.116	1.318	0.167	1.858
RT (Tol)	13.75	155.48	29.92	332.67
RT (Run)	151.22	1,710.26	329.07	3,659.33

the 118-bus system is known beforehand and an initial contingency can be instantly detected, then the EB-CFS can provide a decently fast assessment in less than two seconds, although the AC model takes much longer than the DC model. However, it should be noted that if the tolerance is unknown or a complete evaluation of all possible contingencies is requested in real-time, some fast selection algorithms or parallel computing techniques should be incorporated to improve the computation efficiency of the EB-CFS model. Meanwhile, to perform a fully online screening and evaluation for a bulk energy system, which typically consists of over ten thousand substations and branches, an exhaustive search for all candidates and tolerances will still be cost-prohibitive and advanced techniques shall be developed.

Validation of EB-CFS

This section will validate the ΔEB as a vulnerability measurement, using single-bus contingencies as an example. Specifically, we validated the EB-CFS with the power flow based DC-CFS described in Section 3.3.3 and compared the actual size of blackouts after the most vulnerable buses with the topological metrics.

First, with the two topological metrics δC and $\Delta\lambda$ for comparison, we select the loaded buses with the largest δC and $\Delta\lambda$ as two candidate sets of single-bus contingencies, respectively. A third candidate set is formed by the most vulnerable buses identified by ΔEB. Note that we did not choose zero-loaded Bus 38 as a candidate because it is a transmission bus serving as a transitional transformer connected by only two branches, which can cause no outage without being actually loaded.

Table 8. Validation results of the EB-CFS

Bus ID$_{\Delta EB}$	ΔP	Bus ID$_{\delta C}$	ΔP	Bus ID$_{\Delta\lambda}$	ΔP
80	476.2	8	449.2	65	390.2
65	390.2	100	262.9	69	380.2
69	380.2	110	153.2	30	236.3
68	238.2	12	84.2	49	203.2
30	236.3	85	61.2	70	66.0

With the selected candidate sets, we simulated contingencies on each candidate individually in the DC-CFS and then measured the blackout size ΔP (loss of real power in MWs). The validation results are shown in Table 8, where the subscripts denote the corresponding metric used to select the candidates. The IDs are sorted according to ΔP, respectively. From the results, ΔEB successfully identifies Bus 80, which is the most vulnerable bus in all candidate sets; meanwhile, other candidates chosen by ΔEB also have greater blackout sizes than the buses selected by δC and $\Delta\lambda$. Moreover, among the buses chosen by N_{fail} from Table 5, Bus 65 ranks as the third most vulnerable bus in terms of ΔP, as shown in Table 8.

It is notable that none of these approaches require real-time, dynamic loading, or generation information of the system. The critical components can still be located without real-time information of power system dynamics. From a potential attacker's point of view, the structural information still reveals critical intelligence to design effective attack schemes, which calls for better protection of this information.

In summary, the validation above has shown that the EB-CFS can effectively evaluate the structural vulnerability without the knowledge of dynamic operating points. The proposed approach outperformed the topological measurements in comparison in the task of identifying more vulnerable components, which attributes to its ability in capturing the electrical characteristics in vulnerability assessment.

3.4 Chapter Summary

This chapter proposed an extended topological vulnerability assessment approach for cascading failure analysis. Based on the electrical property of extended betweenness, we proposed an integrated cascading failure simulator to assess the structural vulnerability of both bus and branch contingencies. To consider the complex power transmission and the power loss on transmission lines, we also incorporated an AC model in the cascading failure analysis. Simulations on the IEEE 118-Bus system demonstrated the effectiveness of EB-CFS in revealing structural vulnerability and were validated on the DC-CFS presented in the previous chapter. Discussions regarding the

According to the simulation results, the proposed extended topological approach is able to assess the vulnerability of power grid components in cascading failures with only limited knowledge of dynamic real-time information of a power system. Based on the simulations and discussions, the proposed approach is not only helpful to evaluate the vulnerability of components that pose most threats to the power system; it is also useful to facilitate the understanding defense and protection of a real world complex network systems like power grids by further developing better strategies based on potential and feasible threats.

In this chapter, the tolerance is a global constant across the power grid in the simulation. Some simulation results show that the vulnerability of branches measured at a low system tolerance can vary to a large extent when the tolerance is increased dramatically. This calls for future work to improve this model with less tolerance dependency, and some work has been published [70, 109, 110, 111]. In addition, fast multi-contingency screening methods and intelligent attack strategies can also benefit from the EB-CFS in further security and resilience investigations of the smart grid and other critical infrastructures.

CHAPTER 4

Multi-Contingency Analysis of Concurrent Attacks with Self-Organizing Maps

4.1 Chapter Overview

The smart grid integrates two-way communication into system planning and operations [112], where the control centers rely on the supervisory control and data acquisition (SCADA) systems to monitor and operate the grid. The cyber-physical structure, as illustrated in Figure 17 [113], has been shown vulnerable to cyber-attacks, physical sabotages [12, 80], as well as cyber-physical attacks whose surfaces and targets are across both domains. While the former two malicious actions are intensively investigated by information security and power system security experts, the following three chapters will focus on the cyber-physical attack that targets control commands and measurement data to inflict physical blackouts from the cyberspace.

This chapter focuses on control attacks that manipulate or forge control commands to maliciously trip targeted substations and lines remotely [20, 114]. When tripping commands are issued concurrently, an $N-k$ scenario occurs where N is the total number of substations/lines in the grid and k is the number of victims being tripped. We refer to this as the current attack scheme. As aforementioned, this is usually a worst case scenario but less prepared due to the rarity of such events in the absence of malicious attackers and the cost to screen all possible combinations [115, 116]. However, given the threat of cyber-attacks, we assume this as a "what-if" scenario and will look for effective and efficient methods to identify the potential attack vectors in a large-scale interconnected power grid.

Specifically, this chapter proposes an SOM-based pre-clustering method for multi-contingency analysis of bulk power grid blackouts. The method utilizes a sub-grid approach that outperforms load-based ranking of an entire grid and reduces the complexity of simulation compared to traditional $N-k$ contingency analysis. Simulations are car-

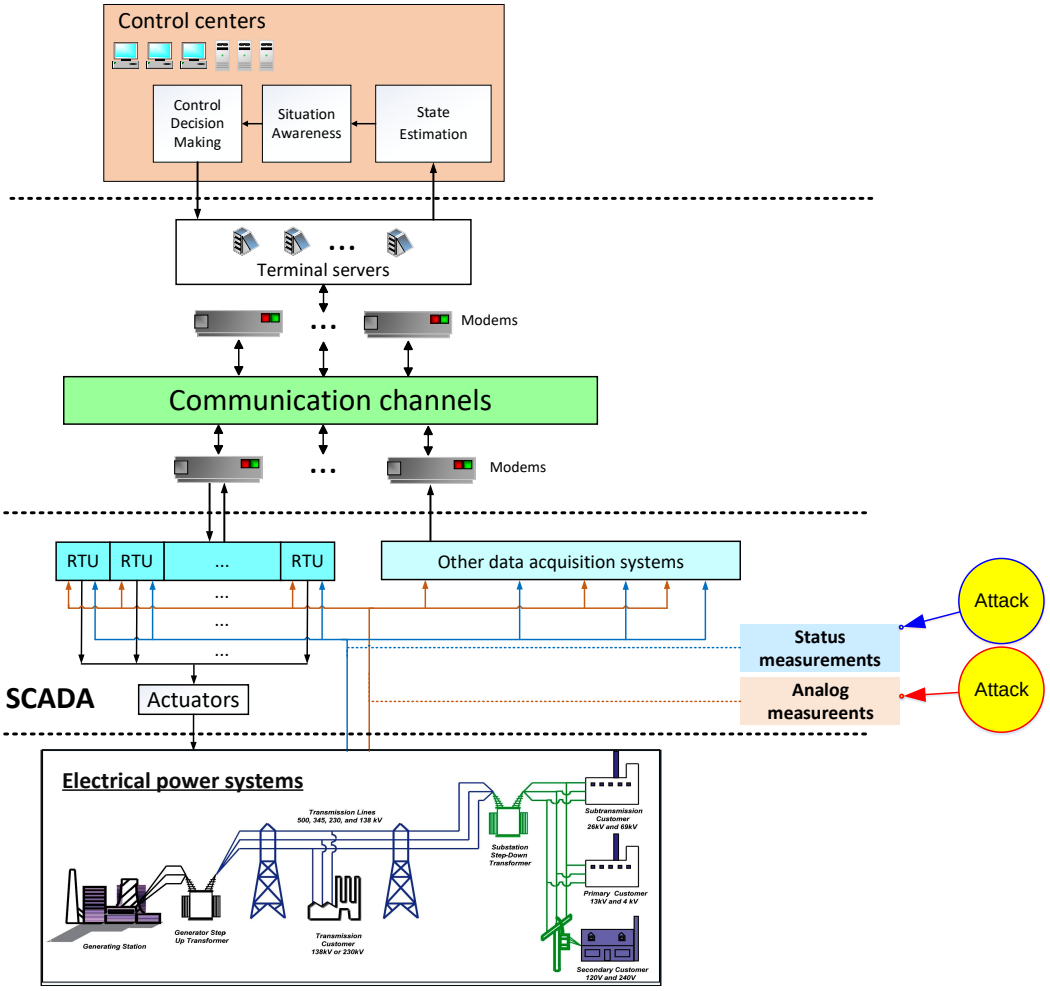


Figure 17. Potential attacks on the status/analog data in the smart grid.

ried out on the Texas grid with over 5,000 substations and the effectiveness will be demonstrated in multiple attack scenarios.

The rest of this chapter is organized as follows: Section 4.2 first reviews the known threat of concurrent attack schemes. Section 4.3 describes the self-organizing map (SOM) algorithm for clustering and the multi-contingency analysis based on the SOM. Section 4.4 describes the simulations set up on Texas benchmark grid with comparisons to both traditional load-ranking based scheme and K-means based clustering scheme; the result shows that the proposed method effectively finds stronger attack vectors. Finally, a chapter summary is provided in Section 4.5.

4.2 Concurrent Attack in Smart Grids

4.2.1 Concurrent Attack Schemes

Attacks in the smart grid are commonly assumed to be launched concurrently in current literature, mostly due to its model simplicity and potential impacts [6]. Such attacks can exploit different aspects of vulnerability in the smart grid: malicious data attacks [84, 117, 118] inject undetectable false data into the state estimation to mislead grid operations. Interdiction analysis [86, 119, 120] extends traditional line contingency into interactive attacker-defender scenarios. Cascaded attacks [37, 121, 122, 123, 124] evaluate the risk of cascading outages triggered by attacking a small set of components. Time synchronization attacks [125, 126, 127] target the critical temporal information and synchronization of measurements for grid operation. These attack scheme studies aided traditional power grid contingency and stability analysis by revealing security concerns that are usually outside the scope of normal operating dynamics, random faults, and major disturbances due to extreme natural events.

4.2.2 Risks of Massive Blackouts under Concurrent Attacks

Attackers of power control systems can create a catastrophic consequence when taking advantage of the cascading blackout vulnerabilities [128]. The targets are not limited to a single component in cyber-attacks, and the compromise of multiple components will trigger a major disturbance that can easily result in cascading blackouts. As the grid are merely protected under $N-1$ security, it is important for both security and forensic experts to understand the $N-k$ vulnerability under intelligent and informed attacks. To date, it remains a complex challenge to thoroughly examine the grid vulnerability under multiple coordinated attacks [6].

Meanwhile, we can recall that in bulk power grids it is increasingly difficult to perform $N-k$ security analysis due to the increase of computational complexity. Researchers have therefore been looking for better approaches to balance between the cost

of precise power grid representation and the efficiency of security analysis. A common practice is to perform heuristic or hierarchical pre-processing [45, 129] to reduce the set of interested targets before conducting the $N - k$ contingency analysis for a limited set of components.

To identify the most critical victims, load ranking has been frequently used as a vulnerability index [107, 129]. As a fundamental electrical characteristic, the load plays one of the most critical roles in the analysis of power grid security [130, 70]. Meanwhile, topological information of the power system can be utilized to support the study of power system security from the perspective of its spatial structure. However, neither the spatial topological feature nor the electric characteristics alone are sufficient to provide a comprehensive evaluation for failure propagation; it is possible to combine the spatial features and the electrical characteristics of the power grid in the design of a cascaded attack. Such attack can be beneficial to the attackers who can only access limited information such as the structure of the power grids, which is important to understand for the grid operators and defenders. In this chapter, we will propose a solution to integrate the load ranking with an effective clustering method that will help refine the range of search and provide a powerful tool for the cascading analysis.

In this chapter, we are interested in bulk power grids, which consist of thousands of substations, power plants, transmission lines and other auxiliary facilities, posing major challenges to traditional screening methods. Performing simulation over these large grids with great topological complexity will cost high in computation and result analysis. For instance, in $N-k$ contingency analysis, an exhaustive search for k most critical substations in a power grid with N substations leads to a problem of combinations, which means for $k = 4$ and $N = 5,000$ it will request simulating the cascading process for approximately 2.6×10^{13} different combinations of substations. Therefore, an effective and efficient modeling of the power system is required to simulate its behavior

when multiple substations are attacked in a large electricity transmission network.

To focus on the effectiveness of the method with lower computational cost, we will model the power grid as a topological network [107], which can effectively represent the high-level power system behaviors with relatively low computation overhead [131]. Thanks to the efforts of numerous researchers, there are many topological network modeling available for the study of power grid security. Petri-net [132, 133], as an example, is a powerful model which can be used to model the coordinated attacks simultaneously happened in both cyber and physical space [134], or be employed to detect and identify the fault or failure in smart grid [135]. However, the application of this method could be limited to relatively small power systems, due to the prohibitive costs of manpower and computation for an accurate model of the bulk power grid infrastructure. Another popular method is to model electrical power systems into a Bayesian network [136, 137, 138], incorporating graph model with probabilistic functions for load prediction and the fault diagnosis in the power grids. Unfortunately, in large power transmission systems, the Bayesian modeling also faces similar difficulties as the Petri-net. The reason is that a bulk power system may contain thousands of substations and transmission lines, and each of them subjects to various generation, relay, thermal, and weather conditions, exposing significant challenges to the computation of conditional probabilities for every component in the power grid. Considering the effectiveness and efficiency in analyzing large scale networks, using simplified topological network models based on complex network analysis [36, 139, 140, 141, 93] can be an appropriate alternative that satisfies our requirements on power system models.

In real world cascading cases, although there may be an area with a cluster of highly condensed grids, e.g. metropolis like Los Angeles, Houston, etc., one can still find that the most critical components are not necessarily neighbors to each other in terms of spatial distance. The cooperative effect of substation failures occurred in distance

can result in a strong impact on the power grid as well. Hence we can pre-cluster the substations into several groups based on their spatial locations and then perform analysis by studying the top-loaded substations in each of the clusters. By using this method, we utilize the spatial features of the power grid to help analyze the electrical system behavior in cascading failure scenarios. This integrated approach is implemented by the utilization of the Self-Organizing Map (SOM), a popular and robust method among the clustering approaches [142]. It is an effective unsupervised approach to cluster and abstract data based on its input features.

4.3 Self-Organizing Map-Based Multi-Contingency Analysis

4.3.1 Self-Organizing Maps (SOM)

The SOM is a classic neural network proposed by T. Kohonen and has been widely applied in clustering, classification, and visualization. It is an unsupervised iterative training approach that projects and visualizes high dimension feature space onto a low dimensional (usually 1-D or 2-D) lattice of weighted neurons [143, 144, 145].

While there are a few SOM-based clustering algorithms developed for other studies, in our work we implement the fundamental non-hierarchical SOM and it turns out to be very effective in finding the vulnerable set of substations in the grid. To make use of the spatial features, we use the spatial location of substations as the input feature of SOM, and a list of cluster IDs will be returned as the output ready for further cascading analysis. Also, the SOM lattice in this chapter is a square lattice which has N neurons in total, and every neuron has two features, i.e. the X and Y coordinates, which carries a 1-by-2 SOM weight vector on each of them. The detailed procedure of SOM initialization and training is described in the following subsections.

Initialization of the SOM

There are many weights initialization approaches for SOM, two of which are tested in our simulation, i.e. the linear initialization approach using greatest eigenvectors, and

the random initialization based on uniformly distributed probability density function.

The first approach is more widely used since it effectively utilizes the information from the input space to initialize the weights of SOM neurons [146]. The weights are selected from the linear subspace spanned by the N largest eigenvectors, i.e., the first N principal components. N is the desired number of neurons on SOM lattice, which is also the number of initial victims in the attack scheme. By using linear initialization we start from the same initial weights in each of experiments, which is beneficial to the cascading analysis comparing to the random initialization approach.

The random initialization is implemented as a comparison to the linear initialization. Though it is also able to identify a victim set which could be more vulnerable than the load-ranking and other clustering method based approach, it introduces another randomness other than the random sampling, which unnecessarily adds to the complexity of our algorithm. Therefore, we only use it to prove the robustness of SOM-based clustering method for failure cascading analyses.

In addition to the initial weights, the total number of iteration T_{itr}, the initial values of the SOM training rate η_0, a neighborhood function $H(\tau)$ with size τ_0 will also be set up during the initialization for the training process. The details are discussed in Section 4.3.1 and Section 4.4.1, respectively.

Training of the SOM

After the initialization, an iterative process will start to train the SOM lattice. The training process can be divided into two stages: a rough training stage with a large initial training rate and a neighborhood radius decreasing radically, followed by a fine tuning stage with both parameters being tuned slowly and smoothly.

In each iteration, a substation will be randomly selected and its coordinates presented as the input of SOM. Then the following process will be performed:

1. Find the best matching unit (BMU) on the lattice. The BMU is the neuron whose

weights yield the smallest distance D in the feature space to the current input;

2. Update the kernel function $H(\sigma)$, where σ is the neighborhood size determining the Euclidean radius of influence of current BMU on the lattice;

3. Gradually decrease the SOM training rate η to refine the speed of weight tuning;

4. Update the weights of neurons *W* according to the latest value of $H(\sigma)$ and η;

Details of these steps are as follows: First, for each sample presented, its distance D to all neurons in the feature space is calculated by:

$$D_{ij} = ||X_S(t) - W_{ij}(t)|| \tag{12}$$

where $X_S(t)$ is the current sample at tth iteration and W_{ij}(t) is the weight vector of the neuron on ith row, jth column on the lattice. The BMU is the neuron corresponding to the minimum of D_{ij}.

Then, the Gaussian function is selected as the kernel or neighborhood function for our model. It is a symmetric function that decreases on both sides away from its center peak:

$$H(\sigma) = e^{-\delta^2/2\sigma^2} \tag{13}$$

where δ is the distance between neurons on the 2-D lattice.

The Gaussian kernel is a mask function to adjust the weights of neurons differently based on their distances to the BMU. Neurons closer to the BMU will be given higher mask value so that when their weights are updated, they will be moved more toward the BMU than more remote neurons on the lattice. During this process, the shape of the lattice will be constantly changing each time a new sample is provided, and the neurons will adjust their locations in the feature space according to the density of input feature distribution. Note that the distance measured on SOM lattice δ is the geometric distance, and the distance in the feature space D is the normalized spatial coordinate distance.

Both τ and η decrease exponentially over training iterations, as in (14), so that the training will slow down over time, changing from a quick and rough beginning stage to a slow and smooth fine tuning stage:

$$\sigma(t) = \sigma_0 e^{-t/\tau_1} \tag{14}$$

$$\eta(t) = \eta_0 e^{-t/\tau_2} \tag{15}$$

where t is the number of current iteration, $\tau_1 = 100/log(\sigma_0)$ is a constant time factor to refine the shrinking rate of σ, and τ_2 is a pre-set number of iterations that divides the stages of rough training and fine tuning.

Once the parameters are updated, the weights of neurons will be adjusted accordingly. The updating value is masked by $H(\tau)$ so that the weights of neurons closer to the current BMU will be modified more:

$$W_{ij}(t+1) = W_{ij}(t) + \Delta W_{ij} \tag{16}$$

$$\Delta W_{ij} = \eta(t) H(\sigma)(X_S(t) - W_{ij}(t)) \tag{17}$$

where $W_{ij}(t)$ and $X_S(t)$ are the same as in equation (12).

When the SOM training ends, the neurons will settle at their own final locations in the feature space, and each of them represents a centroid of the clusters. Then, measured by the Euclidean distance, each substation in the network will be assigned a cluster ID of its nearest neuron. The most loaded one from each cluster will be selected to produce an initial attack vector, which combines the electrical features (load) as well as spatial features (distance) for the following cascading analysis.

4.3.2 Multi-Contingency Analysis with SOM

In this subsection, we will introduce our topological model of the power grid and cascading failure In order to present the power grid as a topological network, there are a few assumptions to be specified.

First, a substation in our power grid cascading model is referred to as a node, regardless of its type as a generator, a load, or simply a transmission substation; a transmission line which connects one substation at each end will be regarded as a branch of the network. Hence the power grid is regarded as a bidirectional unweighted graph [129, 93, 90], a simplification that helps to reduce the computational cost significantly.

Second, we will define the load and fault tolerance of the power system, as the process of failure cascading relies heavily on these two factors. From studies of high-level power grid structure [32, 54, 130], the load of a given node is highly related to the connectivity or centrality of its neighbors, which means that a node connecting to more neighbors, or whose direct neighbors have greater connectivity, will be more likely to carry greater portion of load in the power delivery. In this chapter, we follow [122] to define the load of a node as the product of its degree and the summation of the degree of all its neighbors. Let $Deg(v)$ and $Nbr(v)$ be the degree of a given node v and the set of neighboring nodes of v, respectively, then the load for each node v, denoted as $L(v)$, is calculated as follows:

$$L(v) = Deg(v) \sum Deg(n), n \in Nbr(v) \tag{18}$$

When a victim node is attacked, its load will be proportionally redistributed to its neighbors according to equation (19). The load of each active neighbor of the victim will be updated as follows:

$$L'(n) = \frac{L(n)}{\sum L(n)} L(v), n \in Nbr(v) \tag{19}$$

Affected by the redistribution, surviving nodes in the vicinity of a failed node can be heavily overloaded and fail to operate as before. So, considering a non-recoverable scenario, when a node is overloaded to a certain degree, it will be regarded as fatally overloaded and cut off from the network, and all the branches that directly linked to

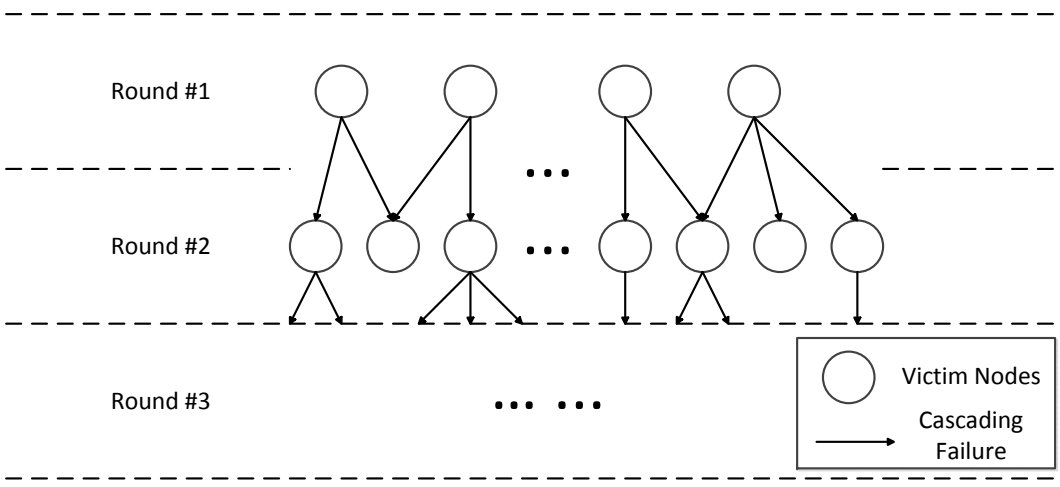


Figure 18. Illustration of a cascading tree following an attack.

it will also be disconnected. The threshold of overloading ratio when a node fails is referred to as the system tolerance, and currently, we only assign a universal system tolerance, denoted as T, for all the nodes in the network. The failure propagation will continue as long as new fatally overloaded nodes emerge in the grid, and eventually, it will lead to a cascading failure across the network. If the initial victims are well-selected, the malicious attacker will be able to create a large scale or fast propagating blackout in the power system.

Finally, when a number of nodes are failed, we use the concept of "round" to help to describe the progress of failure cascading. The definition of a round is illustrated in Figure 18. The very first set of victims forms the nodes failed at first round. Then the nodes failed due to the failure in the first round will be regarded as the victims of the second round, and so forth. In this way, nodes failed at different rounds in a cascading process form a tree-like structure where the "child" nodes are the direct victims of their parent node's failure, and the root nodes are the initial set of victims attacked. A node may have more than one parent if it is affected by multiple nodes failure at the same time, as shown in Figure 18.

One more fact to note is that the load and status of each node are only updated once in each round, and the nodes failed in the same round will not have an instant effect on others. Instead, the failure of all nodes in the last round will simultaneously affect the remaining active nodes in next round.

In summary, the overall cascading process can be generalized in following steps:

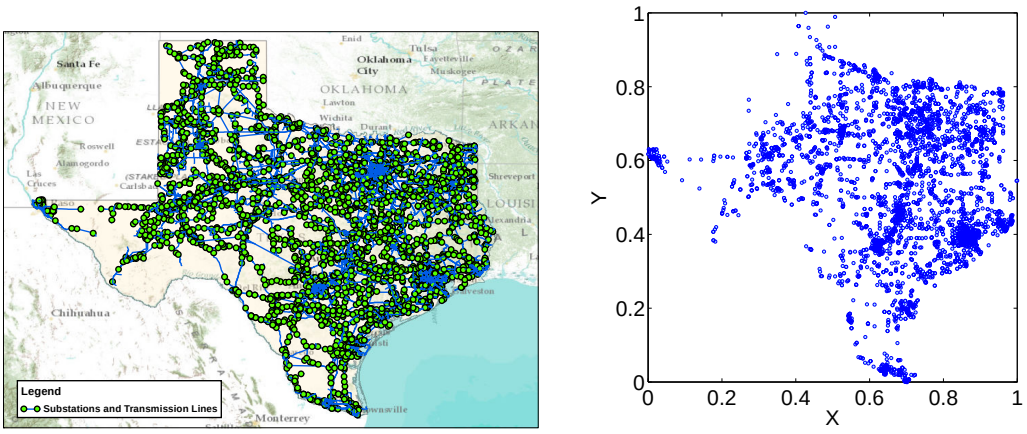
1. Trigger a multi-victim attack by knock down some victims in the grid;
2. Calculate the load redistribution and mark fatally overloaded nodes as failed;
3. Disconnect failed nodes and branches from the grid;
4. Repeat step 2 and 3 until the process reaches a final stabilized stage.

As we want to identify the most critical power grid components from the attacker's perspective, we use the final percentage of failure in the power grid with respect to system tolerance T, denoted as PoF, as the assessment metric:

$$PoF = \frac{N_f}{N} \tag{20}$$

where N_f is the number of failed components and N is the total number of components in a given grid. For each multi-victim attack, we measure the value of PoF after the cascading failure stops at the final, stabilized state.

According the previous definition of round, a cascading tree with more leaves, i.e. PoF, indicates that the attack results in a larger blackout with more component failed consequently; while with fewer rounds it indicates a faster failure propagation with fewer intermediate process and requires a quicker decision to limit its impact at an early stage. The more child nodes a parent node have, the more critical they will be. By using this measurement, we are able to intuitively illustrate the effectiveness of the proposed approach using the cascading failure model described above and highlight the critical components in multi-victim attack scenarios.



(a) (b)

Figure 19. Texas grid shown in (a) ArcMap 10.0 and (b) normalized substation coordinates.

4.4 Simulation and Performance

The benchmark used in our simulation is the Texas power grid, visualized in ArcMap 10.0 using a dedicated demo [78] shown in Figure 19(a). The power grid information is provided in the PLATTS Powermap dataset of North America electrical power infrastructure. The Texas grid managed by the Electric Reliability Council of Texas (ERCOT) is the third largest interconnections in the United States, an ideal representative of a wide-area bulk power grid. The grid presented in this work has 5,390 substations connected by 7,389 transmission lines, and the simulation is performed in the MATLAB 2010b environment.

4.4.1 Simulation Setup

As we assume equal importance to the two input features, i.e. the X and Y coordinates, each of them will be normalized by their respective ranges as follows:

$$z = \frac{z - min(Z)}{max(Z) - min(Z)}, z \in Z \tag{21}$$

where Z is the set of coordinate z, which stands for either x or y coordinate. In this way, neither of them will dominate the clustering result, as shown in Figure 19(b).

In our simulation, the total number of sampling, equally the total number of iteration T_{itr}, is set as 10 times the length of rough training τ_2, as in the literature [145]. For the Texas grid benchmark, τ_2 is set as 25,000, roughly 5 times the number of nodes in the Texas grid. It is not sufficient for a deterministic clustering result; however, it will be able to find out a stronger attack scheme instead. In other words, with τ_2 set to over 10 times the number of nodes, the clustering result with linear initialization and random sampling will be deterministically stabilized to a specific result, given a certain initial neighborhood size σ_0. However, in this case, it is actually unnecessary because the corresponding victim set will not lead to a cascading impact as severe as the sets obtained from a smaller τ_2 just about 4 to 5 times the number of nodes. Therefore, despite that with this parameter setup SOM will produce different clustering results in different experiments, the PoF curve proves that this "insufficient" sampling will be able to identify some more vulnerable victim sets, according to our cascading analysis model.

4.4.2 Attack Performance

First, we will exam the performance of a simple SOM-based attack where the size of SOM neurons is 2×2, namely 4 victim nodes are chosen in the initial attack. Figure 20 shows the 3 most effective SOM-based attack schemes found in our experiments and how they compare to the traditional load-based scheme based on the final percentage of failure PoF at different system tolerances. The system tolerance T ranges in [1.0, 2.5] with a step of 0.05. As shown in the figure, although in each experiment the differences in SOM sampling lead to various clustering results and thus different initial attack victim sets, the PoF curves of the 3 strongest SOM based attack schemes stay stronger than the load based attack scheme as T increases; the PoF curves of these SOM attack victim sets remain around 90% even when the system tolerance is increased to over 2.0.

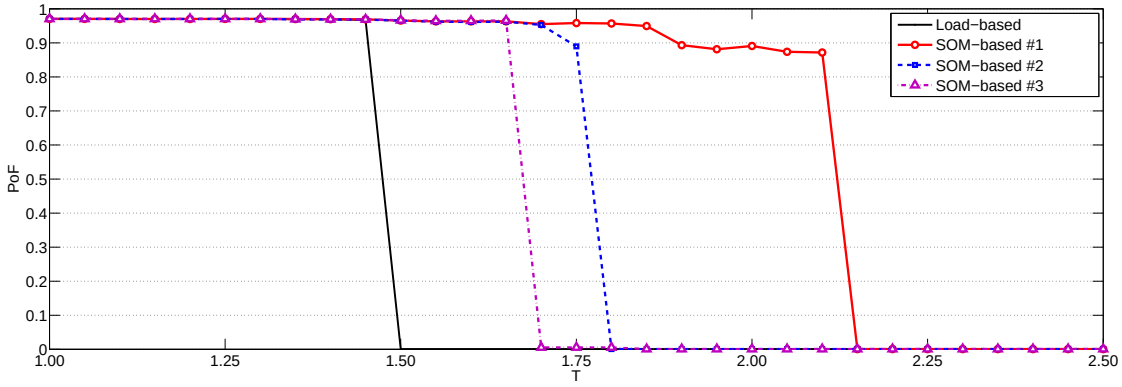


Figure 20. Performance of the most effective SOM-based 4-victim attack schemes

Then we increase the SOM lattice to 3×3 and perform 9 initial victim attacks in our simulation. The value of T has the same setting as above, and the result is shown in Figure 21. Similarly, in this scenario, we also illustrate 3 attack schemes that are found more resistant to large system tolerance T than load-based schemes.

First, take 4-node attack as an example. In Table 9 we compare the three SOM-based initial victim sets in Figure 20 to that of load based scheme. From the table we can find that the SOM-based schemes are able to construct victim sets with nodes carrying significant less load, such as Node 1069 in attack scheme #2, ranked only as the 359th loaded node with a load of 95; similar for the Node 57 in attack scheme #1 with a load of 572.

Similarly, in 9-node attacks (shown in Table 10), we can also find that Node 1460 in attack scheme #2, ranked as low as the 382nd, is included in one of the most critical sets. Therefore, by using SOM-based spatial clustering, we can quickly sort out these complex combinations of nodes that vary significantly in load and assess the impact of their failure to the power grid. Moreover, this not only demonstrates that the load of substations alone is not robust enough in identifying the most vulnerable components, but also reveals that the exhaustive search, even using the load-ranking to facilitate the searching process, is likely to pose a prohibitive cost in identifying a victim set that

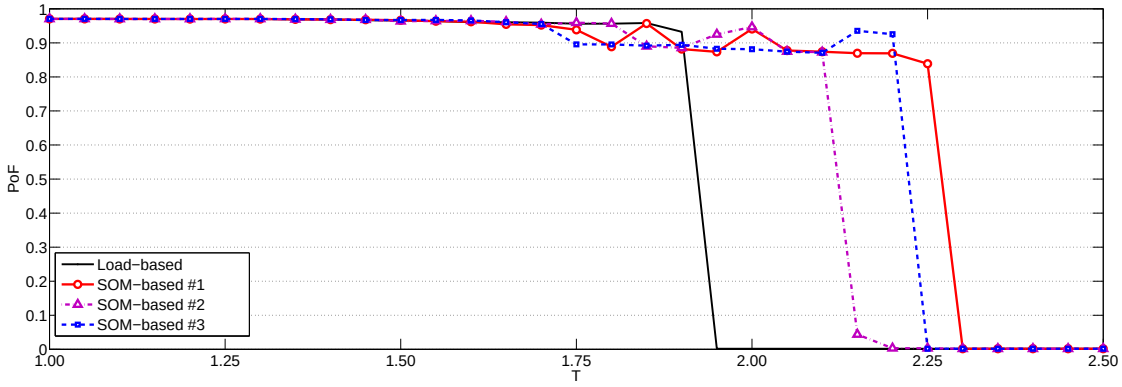


Figure 21. Performance of the most effective SOM-based 9-victim attack schemes

Table 9. Load- and SOM-based 4-bus attack schemes

Load based scheme	Node ID	1892	2747	2063	1046
	Load Rank	1	2	3	4
	Load	1343	1241	1104	1008
SOM based scheme 1	Node ID	1892	1046	17	**57**
	Load Rank	1	4	5	**22**
	Load	1343	1008	975	**57**2
SOM based scheme 2	Node ID	1892	1046	3064	**1069**
	Load Rank	1	4	37	**359**
	Load	1343	1008	410	**95**
SOM based scheme 3	Node ID	1892	2747	1046	2737
	Load Rank	1	2	4	9
	Load	1343	1241	1008	780

includes nodes with much less load than the ones on top. This shows that our SOM-based scheme is capable of searching for the vulnerable components midst the complex mechanisms behind cascading failures.

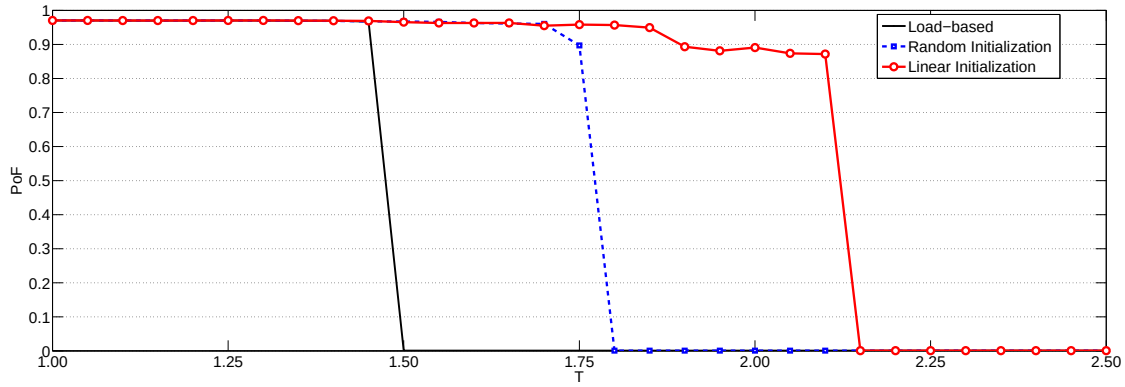
4.4.3 Comparative Studies

In the following part, we will first compare two different approaches for the initialization of the SOM weights. For both linear and random initialization, 100 independent experiments are performed to compare the strongest attack schemes found in each type. As shown in Figure 22, the random initialization approach can indeed find out some

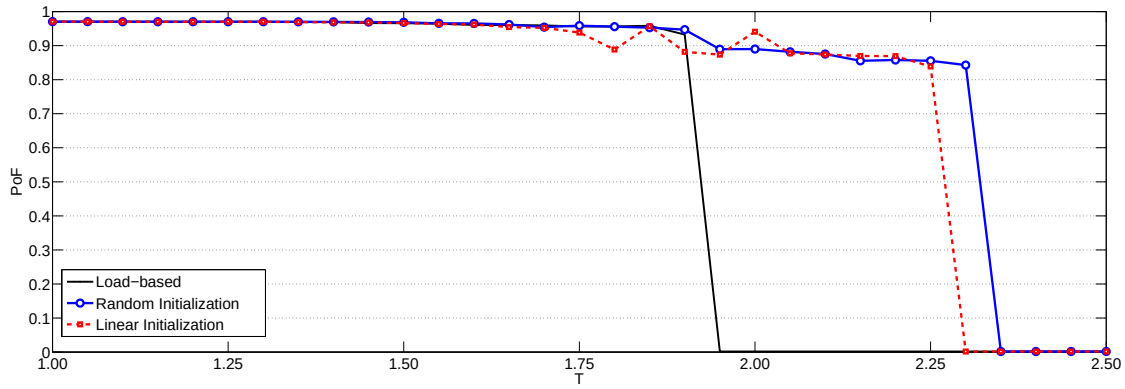
most vulnerable sets in the Texas grid; however, as discussed previously, the random initialization will add another independent randomness in SOM clustering and introduce more uncertainty in the search for most vulnerable sets. Therefore its reliability is reduced when applied to other power systems and the computational cost of simulation will increase as well.

In addition to the comparison between load-ranking and SOM based schemes, another scheme based on K-means clustering is also tested to assess the effectiveness of SOM clustering in our model. K-means is also a widely used classic clustering method which partitions the input space into K clusters. However, it may converge to a local minimum and can not handle the situation well where clusters are not of equivalent size or samples are evenly distributed [147]. These drawbacks also limit the use of K-means in our model, as shown below in the simulation results.

To compare with the SOM-based scheme, in K-means the original input features are also normalized according to their ranges of distribution, respectively. The input space will be divided into K clusters whose boundaries are decided by the distance to the nearest cluster centroid. The initial value of K centroid is generated from a random uniform distribution within the range of $[0, 1]$. In each iteration, a random node is sampled and given the cluster ID of its nearest centroid. Then, clusters centroids will be updated to the new means of in-cluster nodes. An empty cluster after all sampling is finished will be dropped and then only $K - 1$ clusters will become the output. This iterative process will continue until a pre-defined maximal number of iteration is reached. The K-means approach is essentially a special case of SOM clustering, where the neighborhood size σ is fixed to zero and only the weight of BMU will be updated. Similar to the post-processing of SOM-based scheme, the top loaded nodes from each cluster will be chosen to perform a cascading analysis. In our simulation, 100 experiments are conducted for both approaches, and the most effective attack from both are selected for



(a)

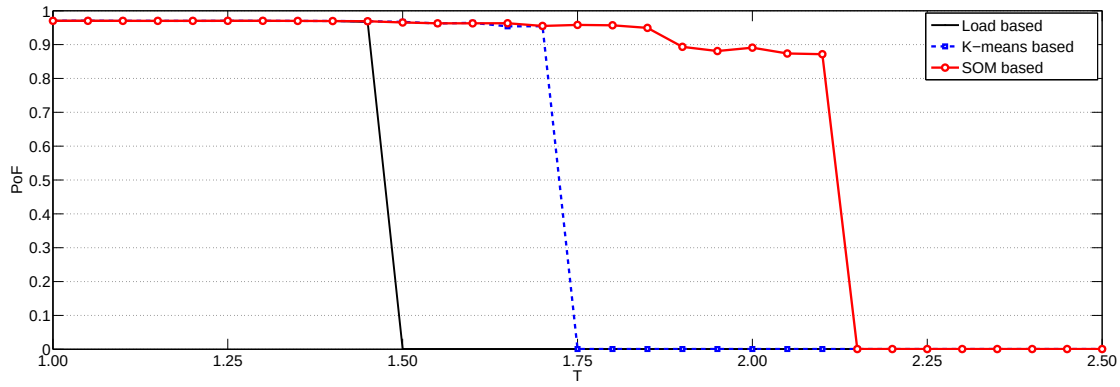


(b)

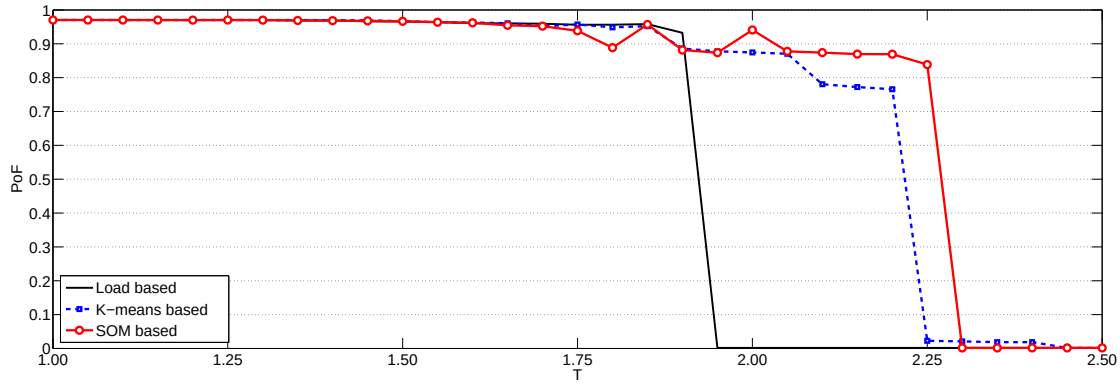
Figure 22. Comparing the most vulnerable set with two initialization methods: (a) 4-victim attack and (b) 9-victim attack.

comparison. As shown in Figure 23(a) and Figure 23(b), in both cases the SOM based schemes outperformed the K-means at finding the stronger attacks.

Finally, the clustering results corresponding to the 4-node attack in Figure 23(a) are illustrated in Figure 24, where different clusters are marked by different colors and shapes. As shown in the figures, the SOM clustering result differs from the K-means clustering as the former produces some sharp angle borders, resulting in irregular shapes of clusters, e.g., Cluster 2 (marked in red) with a triangle-like outline; meanwhile, the K-means clusters are more radial, which generates less effective attack in the cascading



(a)



(b)

Figure 23. Comparing SOM and K-means: the most vulnerable set in (a) 4-node attack and (b) 9-node attack.

failure analysis. From the observations and comparisons above, we can safely conclude that the integrated SOM-based clustering method exhibits both effectiveness and robustness for cascading failure and power grid security analysis.

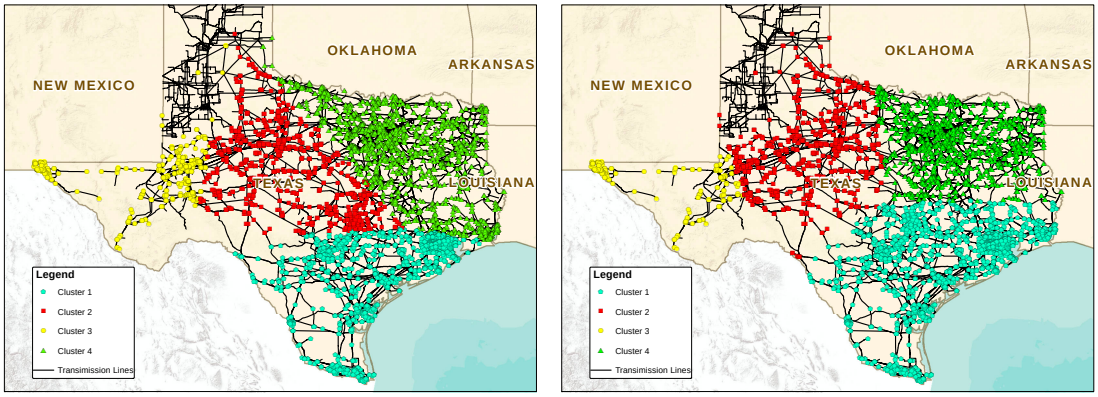
4.4.4 Discussions

There are a few failure behaviors discovered in our simulations. First, as shown in both 4-nodes and 9-nodes attacks, both PoF curves yield a shape of "step-down" function, which indicates that there is a threshold of tolerance T that prevents the failure of some critical components which contribute to a significant impact on the power

Table 10. Load- and SOM-based 9-bus attack schemes

Load scheme	ID	1892	2747	2063	1046	17	2782	1286	1476	2737
	Rank	1	2	3	4	5	6	7	8	9
	Load	1343	1241	1104	1008	975	960	795	784	780
SOM scheme # 1	ID	1892	2747	1046	3064	907	1277	4526	1030	2598
	Rank	1	2	4	37	46	78	111	158	205
	Load	1343	1241	1008	410	384	279	240	186	150
SOM scheme # 2	ID	1892	1046	17	1286	2415	1467	3064	2598	**1460**
	Rank	1	4	5	7	17	18	37	205	**382**
	Load	1343	1008	975	795	660	658	410	150	**88**
SOM scheme # 3	ID	1892	1046	17	1286	401	1467	3064	2405	2725
	Rank	1	4	5	7	16	18	37	101	123
	Load	1343	1008	975	795	696	658	410	256	217

grid failure. For different sets of victims, the threshold values are different, as these nodes contribute to different procedures of failure cascading. However, if the system has a relatively low tolerance, in either 4 or 9 initial victims case, attacking the victim nodes simultaneously is still strong enough to break down almost the entire regional grid without the presence of proper defense response. And when we increase the number of initial targets from 4 to 9, it is expected that the strongest of latter should be more influential than that of the former over the same range of tolerance, which is verified comparing Figure 20 and Figure 21. For the tolerance interval from 1.5 to 2, we could see that in the 9-victim attack, the percentage of failure PoF from the same attack set remains greater than 4-victim attack to a larger tolerance. However, when the universal tolerance is increased high enough, both PoF curves still show a quick step-down with oscillation in some cases. Also, according to the victim sets of 4-node and 9-node attack schemes in Table 9 and 10, we can find that some initial victims in 4-node attack are not necessarily included in the most effective 9-node attack sets, which means that in cascading analysis, to extend most vulnerable set with more victims is more complicated than the simple extension or combination of smaller victim sets.



(a) (b)

Figure 24. Clusters of (a) SOM and (b) K-means approach corresponding to the most vulnerable set in 4-node attack.

Secondly, it is noticed that for some attack sets, their PoF curves do not fall monotonically with increased tolerance, and this can be observed below and above their corresponding step-down thresholds of T; for some curves, it may not even be possible to identify a threshold. The observation is against the intuitive assumption that greater tolerance will always contribute to the reduction of failure cascading scale in power grids. However, it matches the reality instead, as a slightly increased tolerance is not guaranteed to restrict the cascading effect globally; it may only be able to protect some victims of a parent node's failure, which can re-direct the failure propagation elsewhere and the overloading in this new area can lead to a larger number of node failure as a result. Nevertheless, if we keep increasing T, the value ofPoF will step down ultimately.

Another factor that affects the result is that, in this work, we only assign a universal system tolerance for all the substations in the grid. For a more comprehensive model, in reality, the tolerance of substations can vary from each other and may be changing during the cascading procedure due to dynamic status and protective mechanisms. In this case, the curve may show some changes compared to a universal tolerance model; however, it is still expected that similar oscillation of PoF over T will be observed since

the major factor discussed above still exists.

There are some other approaches for multi-contingency cascading analysis related to our simulation presented above. As mentioned in the review [34], there is a number of different tools for the risk assessment of cascading failures in bulk power system, and these methods all have their relative strength and weaknesses in specific applications. For example, in traditional power system $N-k$ contingency analysis and attack strategies studies, it is a common practice to simulate and validate the algorithms on a relatively small benchmark, such as the IEEE 5, 30, 39, 54 or 118-Bus systems. This allows less computation overhead as well as more flexibility and accuracy for the parameter tuning. But this can also raise concerns about the scalability of these approaches, and the utility of some approaches may remain in question for bulk power systems, e.g. the Texas grid in our simulation, which consists of a more gigantic, complex structure and dynamics, requesting not only more intensive computations but also additional policies and revisions to address these issues.

However, it is notable that the complete information on most bulk power systems to such detailed level is unlikely to be accessible for most malicious attackers; it may not even be available to the research community and utility providers. For the attackers, collecting all these operational information in reality (such as power generation of all generators and consumption at all substations) from the power system control centers could be too risky and challenging; and the collected information can be easily outdated or stained with noisy data, resulting in inaccurate or even unnecessary collection from the attackers' perspective. Therefore, it is expected that most attackers will try to put their efforts to maximize the impact of their attacks based on the incomplete electrical information; and the topological information, which is more accessible through many GIS databases, can be a potential source of intelligence that they will rely on. This geographic information will remain constant or subject to little influence from the dynamic

load consumption and power supply, which is a powerful auxiliary source for the smart grid security analysis.

In summary, the challenges of multi-contingency analysis for smart grid attacks can be concluded in the following perspective:

1. The restricted scalability of many $N-k$ contingency analyses which are validated mostly on relatively small power system benchmarks;

2. The limited knowledge of attackers on the complex dynamics in real-time power systems, in contrast to the power system managers, that restricts their strength in modeling the power system and the estimation of the impact of their attacks;

3. The difficulties in solving both linear and non-linear equations in bulk power systems with incomplete information and intensive computational burden.

Therefore, the proposed SOM based multi-contingency cascading failure analysis, as the simulation results have illustrated above, reveals its merit in the multi-contingency analysis for bulk power system cascading failure studies. Meanwhile, it is expected that with increasing electrical grid data collected, more tools for comprehensive multi-contingency analysis will be developed to respond to the call for an efficient evaluation of the risk and to explore the underlying mechanism of cascading failure from the security perspective.

4.5 Chapter Summary

This chapter proposes a topological method to analyze the vulnerability of substations in power transmission grids based on SOM clustering. While the physical characteristics are considered as the basis for the evaluation of power grid security, associating cascading analysis with spatial feature based clustering shows that the combined approach is able to locate the more critical components in a large scale power grid than

traditional methods. This is expected to provide an efficient tool for the $N-k$ contingency analysis in both inadvertent and adversarial scenarios. In our approach, the potential victims are processed by the robust SOM clustering so that the candidates of a search are refined to a limited range, which significantly reduces the computational cost while keeping the capability to identify some of the most vulnerable sets or attack schemes in the grid. This approach shows better performance for cascading analysis in comparison to the traditional load ranking based and the K-means based clustering method, and the result will provide insightful information for decision support and power grid protective mechanism.

There are several important future research directions along this topic. First, in the corresponding 2013 publication of this chapter, we consider the power grid security and attacks from a topological analysis point of view. While this assumption has been widely adopted in many existing literature [122, 129, 148, 121, 36, 139], the power grid is a unique complex system with no less than a complicated topological structure; more importantly, it has the fundamental circuit theory (i.e. Kirchhoff's law) governing the electricity generation, transmission, and distribution. Therefore, it will be critical to advance beyond the topological analysis and consider the physical laws of the power systems. One possible extension was to integrate our approach with the extended topological model [77] to analyze how our proposed method will perform with the consideration of several key features in power flow analysis. Secondly, we can improve our cascading model by introducing overcurrent relays and generation ramping to approximate power system failure behaviors. Finally, critical temporal features during the procedure of cascading can also be analyzed [69], so that we can simulate different strategies with limited strength and resource to optimize defense mechanism against smart grid attacks.

CHAPTER 5

Multi-Contingency Analysis of Sequential Attacks with Q-Learning

5.1 Chapter Overview

The current multi-contingency analysis in power systems has mostly focused on contingencies occurred concurrently [42, 45, 67]. Attacks launched this way are expected to be more impactful yet also easier to model and analyze without involving the timing and ordering of multiple attempts. Meanwhile, recent studies on the sequential attack have revealed another vulnerability in the smart grid [149, 110, 123]. In sequential attacks, attackers can compromise critical components consecutively, which is similar to the $N-1-1$ contingency and its further extensions. The number, target, and timing of attacks could be determined by the attackers to could lead to a maximal damage. The preliminary study [149] has shown that sequential attacks with the same strength can cause comparable damages as the concurrent attacks; nonetheless, sequential attacks require fewer resources to coordinate, and the vulnerability of the same targets in such attacks can differ significantly: line outages, if triggered back-to-back at critical locations, can still lead to much severe system blackouts than when they occur at the same time.

To identify most critical sequences that can lead to large-scale system failures, existing sequential attack and contingency studies rely either on heuristic graph methods [110], exhaustive search [123], or engineering expertise [150]. A more systematic and effective method can be helpful when bulk power systems are considered. Instead, this chapter focuses on impacts of sequential topology attacks with consideration of physical system behaviors when the attack has bypassed the detection, as it is equally important to investigate the attack schemes based on its impacts on the physical system to fully understand its threat.

The development of machine learning algorithms provides promising tools to han-

dle the challenge from a cost-prohibitive stochastic search space. The patterns underlying in the system dynamics and cascading failures can be revealed adaptively by computational intelligence algorithms, as demonstrated in applications like AlphaGo [151, 152] and other complex problems [153, 154, 155]. The adaptability, i.e, the ability to self-tune based on previous experiences can also aid the vulnerability analysis of a complex networked system like the smart grid. This chapter introduces a novel Q-learning based approach to adaptively identify the more vulnerable attack sequence that can cause critical system failure from sequential topology attacks. In what follows, the term "sequential attack" (SA) exclusively refers to the sequential line-switching interdiction on the power transmission grids.

The major contributions of this chapter are as follows:

1. The chapter proposed a reinforcement learning based approach for vulnerability analysis of sequential attacks in power transmission grids. The approach evaluates the blackout damage resulting from line-switching interdiction with consideration of overloading-related cascading outages and hidden line failures. It formulates the problem under the reinforcement learning framework and identifies critical sequences in sequential attacks with the Q-learning algorithm;

2. The proposed method, utilizing the Q-learning algorithm and Monte Carlo simulation, effectively identified grid vulnerability under sequential attacks causing complex system outages. Simulation-based case studies showed that critical attack sequences that lead to large blackouts have been identified. Results with different systems and loading levels have shown the effectiveness of the proposed method as it discovers more vulnerable target sequence in sequential attacks;

3. Only topological information has been used to identify the critical attack sequences with the Q-learning approach; this echoes the vulnerability observed in

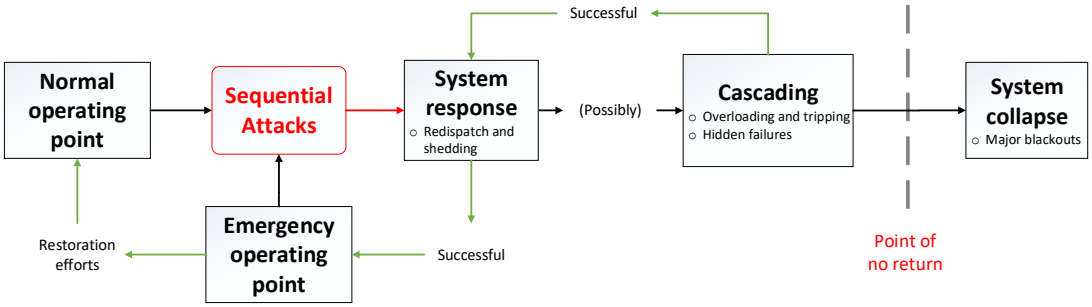


Figure 25. The intermediate states in cascading blackouts of electrical power grid.

[148] as complete information of system dynamics is not required to identify critical sequences in the power grid.

The rest of the chapter is organized as follows: Section 5.2 introduces the threats of sequential line-switching attacks and describes the proposed Q-learning based approach to identify critical attack sequences. Section 5.3 demonstrates the simulation results on three benchmark systems of different scales and under different loading. Finally, Section 5.4 provides a summary of the chapter and some future directions.

5.2 Sequential Attack Analysis with Q-Learning

5.2.1 Sequential Attacks in Smart Grid

A sequential attack is considered in this chapter as a series of coordinated interdiction on the power transmission grid. Specifically, this chapter considers an interdiction as a line-switching attack, i.e., the malicious operation that trips a transmission line out-of-service. Each line-switching directly changes the topology of a transmission grid [156, 157]; in practice, these attacks can be launched from manipulated control commands, false line status data, or physical sabotages. They can also be disguised as irrelevant disturbances or contingencies that are harder to defend [150]. Following the stages of blackout identified in [158], Figure 25 illustrates the state transitions of power systems where a sequential attack may interfere to trigger a cascading blackout.

Mathematically, a sequential attack scheme can be formulated as a sequence S of

ordered and timed 2-tuples [110, 123, 113]:

$$S = \{(a_1, t_1), (a_2, t_2), ..., (a_k, t_k)\}, k \leq N \tag{22}$$

where (a_i, t_i) describes the i-th line-switching attack launched on target line a_i at time t_i; k is the number of attacks in the sequence and N is the number of active lines in the power grid. By definition, the time-domain sequence $T = \{t_1, t_2, ..., t_k\}$ is non-negative and monotonically non-decreasing for any attack sequence $A = \{a_1, a_2, ..., a_k\}$ [123].

The inclusion of selection, ordering, and timing in (22) obstructs the analysis of sequential attack schemes [123]. The target selection needs to be made from a total of $\binom{N}{k}$ combinations; ordering of the combinations expands the problem to a search space with $\frac{N!}{(N-k)!}$ possible permutations; in addition, the timing introduces a continuous variable in time domain, where there is little research that provides a ground truth or a systematic approach to the best knowledge of the authors. Particularly, attacks launched with arbitrary timing during fast transient states will lead to complicated and nondeterministic system responses. Therefore, this chapter focuses on the analysis of the first two aspects for different sequential attack sequences A with the help of a steady-state assumption; the investigation on timing T will remain a future work of this dissertation.

Given this consideration, three assumptions are made in this chapter to further refine the definition of sequential attacks:

Assumption 1: Attackers can access and manipulate the topological information of power systems. The topological information refers to the connectivity of substations and transmission lines, recorded in the status data and changeable by circuit breaker operations or malicious manipulations (as shown in Figure 17).

Assumption 2: Each line-switching attack $a_i \in A$ is launched during a steady-state of the system, which includes both normal and emergency operating points in Figure 25. This assumption decomposes a sequential topology attack into a series of k consecutive

individual line-switching attacks on a power grid, allowing this study to focus on the identification of critical attack sequence A.

Assumption 3: Without loss of generality, the cost to attack any line is considered equal in this chapter.

With the assumptions above, the attack objective is to identify a minimal attack sequence that causes a critical system failure through cascading outages. The critical system failure occurs when the number of line outages exceeds a critical threshold N_θ that leads to a system collapse and/or major blackouts, shown as the point of no return in Figure 25.

5.2.2 The Q-learning Algorithm

Q-learning belongs to a category of semi-supervised learning algorithms [159] known as the reinforcement learning (RL). In general, RL seeks an action sequence that produces the maximal cumulative rewards via a trial-and-error manner. A typical framework of reinforcement learning is shown in Figure 26 [159]. An *agent* takes a sequence of actions at a series of states before it reaches an ultimate goal. The quality of each action is assessed by an evaluative feedback from an *environment*, known as the "reward". By adaptively adjust its actions, the agent has an ultimate objective to learn an optimal policy from the cumulative rewards to maximize the expected total rewards it will receive from the environment.

In general, the expected total rewards Q is computed by a discounted cumulative function of the reward r_t observed upon the action a_t taken at state s_t:

$$Q = \sum_{t=1}^{n} \gamma^{t-1} r_t(s_t, a_t) \tag{23}$$

where γ is a discounted factor. Setting $\gamma = 1$ weights every immediate reward equally in the sequence of actions. In practice, γ is commonly set slightly smaller than 1.0 to facilitate the convergence of Q value during the learning process [159].

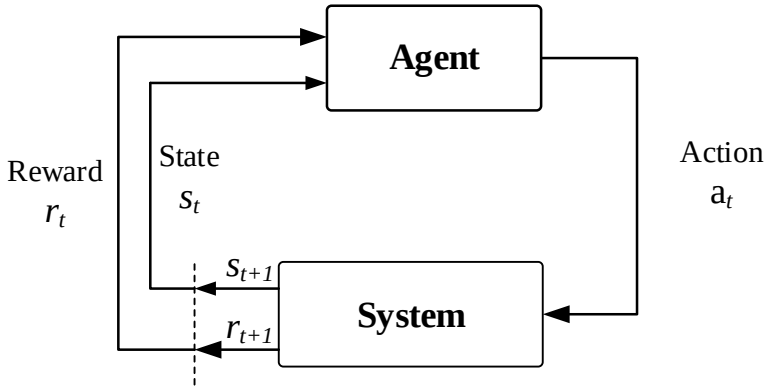


Figure 26. Flowchart of reinforcement learning process.

Although the true optimal value of Q^* is usually unknown in practice, it can be approximated by the Q-learning algorithm iteratively. The Q-learning is an off-policy, temporal difference reinforcement learning algorithm that approximates the optimal Q value with Monte Carlo simulation [160]. The general procedure of the algorithm is described below:

In Q-learning, a Q value is assigned to each state-action pair (s, a). Each triplet of Q, s and a creates an entry in a Q-table. Initially, all the Q values are set to zero.

Then, when a state s_t is observed at time t, the agent first searches for a set of available actions A_t. The optimal action a_t^* at s_t is determined by:

$$a_t^* = arg \max_{a_j \in A_t} Q(s_t, a_j) \tag{24}$$

where A_t is the set of available actions at s_t. If multiple a_t^* exists, a random tie-breaker will be chosen as the a_t^*. Note that (24) favors the maximum of total rewards Q instead of an immediate reward r_t to achieve the long-term optimality.

In search for the policy towards the optimal total rewards, random experiments are run repeatedly to update the Q value, during which the quality of the action sequence is

improved towards the optimum:

$$Q(s_t, a_t) \leftarrow (1-\alpha)Q(s_t, a_t) + \alpha\{r_{t+1}(s_t, a_t) + \gamma \max_a Q(s_{t+1}, a)\} \tag{25}$$

where α is the *learning rate* that controls the aggressiveness of learning. Empirically[159], setting $\alpha = 1$ will make the agent extremely aggressive, focusing on the immediate reward r_{t+1} received and the estimated approximate total future rewards $\max_a Q(s_{t+1}, a)$. This can lose the knowledge learned from previous experiments and cause unnecessary oscillations. On the contrary, setting $\alpha = 0$ will make the agent extremely conservative, as it sticks to its initial estimate and learns nothing from its actions. In practice, the value is often chosen as a trade-off between aggressiveness and conservativeness.

The updated Q value for the given state-action pair is saved in the Q-table for the future decision-making process. It is possible that the agent makes non-optimal actions at the beginning of training when it tries to learn from the feedback of rewards. Eventually, the algorithm will converge to the optimal action sequence that collects the maximal total rewards [160].

Exploitation vs. Exploration: It is notable that Q-learning could be sensitive to deteriorate initialization and local optima problems. This can cost more learning time in practice. Therefore, *exploration* is commonly used in reinforcement learning. This chapter utilizes the optimistic initial guess and the ϵ-greedy method for the exploration purpose.

The optimistic initial guess overcomes deteriorate initialization of Q-learning. It initializes the Q values of all valid actions of any state s_0 encountered for the first time to be a positive constant, e.g., $+1$, so that the agent is first encouraged to explore different actions and later adjust the Q value estimates towards the actual long term rewards.

The ϵ-greedy method is used to address the local optima problem during the learning process. Specifically, when the agent queries an action a_t from the Q table for the

current state s_t, the ϵ-greedy method forces the agent to take a non-optimal valid action, i.e., any action other than a^* in Eqn. (24), with a small probability ϵ. Numerically, this means that the probability that the agent takes the optimal action is given by:

$$P(a_t = a_t^* \mid s_t) = 1 - \epsilon \tag{26}$$

where a_t^* is the optimal action at s_t according to (24). A proper choice of ϵ can balance the trade-off between exploitation and exploration so that the algorithm converges to the optimal policy in an effective and efficient manner. To avoid excessive exploration after the agent has learned much from the trials, the exploration parameter ϵ can starts from a larger initial value ϵ_0 then linearly decreases with a certain step distance $\delta\epsilon$ to a near-zero value ϵ_f, after which it remains constant. This allows the agent to sufficiently explore the searching space and then fine-tunes the Q value in a timely manner during the learning process.

5.2.3 Q-Learning for Sequential Attack Vectors

The paradigm of Q-learning applies well to the security analysis of sequential attacks in the smart grid, as shown in Figure 27. An attacker, who seeks to identify the more vulnerable components in the power grid in sequential attacks, is considered as the agent in Q-learning. The electrical power grid can be viewed as an independently operating environment that responds to the malicious actions of attackers. With these two interactive roles, the action of the attacker is the malicious line-switching while the states can be defined by parameters of the system. The attack objective is to create a critical system failure where a fatal fraction of lines are out of service. The learning objective of the attacker is to find the optimal policy that reaches this goal with the least number of lines attacked. The pseudo code of the vulnerability analysis is shown in Table 11, and the design of the state s_t, the action a_t, and the reward r_t are given as follows.

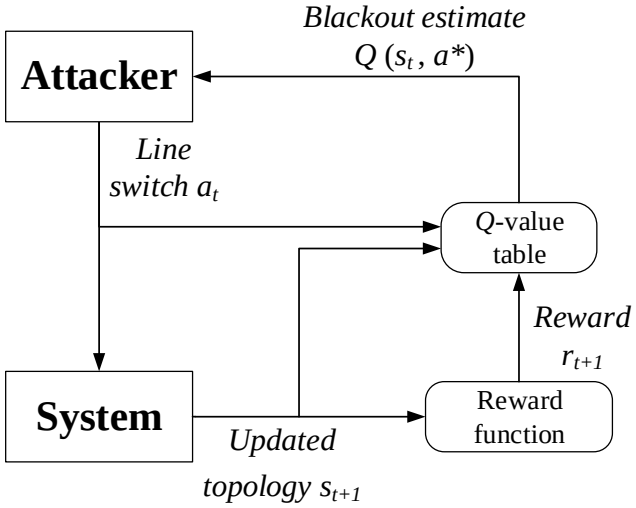


Figure 27. The flowchart of Q-learning based vulnerability analysis for sequential attacks.

According to Assumption 1, the *state* is exclusively defined by the system topology available to a potential attacker. According to Assumption 2, the state also exclusively refers to the steady-state prior to sequential attacks. The initial state is $s = \mathbf{1}$; the intermediate states s_t are post-attack steady states after any cascading outages triggered by the previous attacks. A complete system failure occurs when $s = \mathbf{0}$ and a critical failure occurs when the number of surviving lines (non-zero elements in s) is dangerously low. It is notable that a number of transitional states could exist between two consecutive attacks if there is a series of cascading outages. To evaluate the quality of sequential attack action, the transitional states are not considered as individual states during the Q-learning but only as intermediate transitions between s_t and s_{t+1}.

The topological system state s_t is defined as a vector of line status $s_t = \{s_t(1), s_t(2), ..., s_t(N)\}$, where:

$$s_t(l) = \begin{cases} 0, & \text{if line } l \text{ is in-service at time } t \\ 1, & \text{if line } l \text{ is out-of-service at time } t \end{cases} \tag{27}$$

The action is defined as the line-switching attack as in (22). An attack a_i on line l

Table 11. Pseudo Code of Q-learning Based Multi-Contingency Analysis

Initialization: Initialize the Q-table and the benchmark system
for $current\ number\ of\ trials \leq maximal\ trials$ **do**
  Reset: $N_o = 0$, $s_0 = \mathbf{1}$;

  while $N_o \leq N_\theta$ **do**
    1. Acquire attack candidates:
    Obtain all valid line targets A_t from the current steady state s_t;
    2. Initiate an attack:
    Choose a line l from A_t and set its status $s_t(l) = 0$. Set $a_t = l$;
    3. Simulate cascading outages:
    With the attack updated in s_t, run the CFS until a new post-attack steady-state s_{t+1};
    4. Obtain evaluative feedback:
    Obtain N_o from s_{t+1} and generate the reward r_{t+1} according to (28);
    5. Learning from trial:
    Update the value of $Q(s_t, a_t)$ according to (25).
  end while
end for

switches the status of l from in-service to out-of-service. The corresponding value in s_t is set to zero.

The evaluative feedback or reward r is a critical parameter in reinforcement learning. Given the aforementioned attack objective to create a critical system failure, this chapter proposes the following reward function:

$$r_{t+1}(s_t, a_t) = \begin{cases} +1, & \text{if } N_o \geq N_\theta \text{ and } k < N_\theta \\ -1, & \text{if } N_o \geq N_\theta \text{ and } k \geq N_\theta \\ 0, & \text{otherwise} \end{cases} \tag{28}$$

where N_o is the total number of lines outages used to define the *blackout size*. N_θ is the critical threshold at the point-of-no-return (the attack objective), and k is the number of attacks launched sequentially. A sequential attack scheme is successful ($r = +1$) if it achieves the objective by triggering a cascade, i.e., the entire scheme causes N_θ or more line outages with less than N_θ actions. Otherwise, it is either unsuccessful ($r = -1$) if

it takes $k = N_\theta$ attacks to achieve the objective blackout size or neutral ($r = 0$) if the number of attacks and line outages are both still under N_θ. In the last case, the sequential attack will continue until the objective blackout size is reached.

5.3 Simulations and Results

5.3.1 Simulation Setup

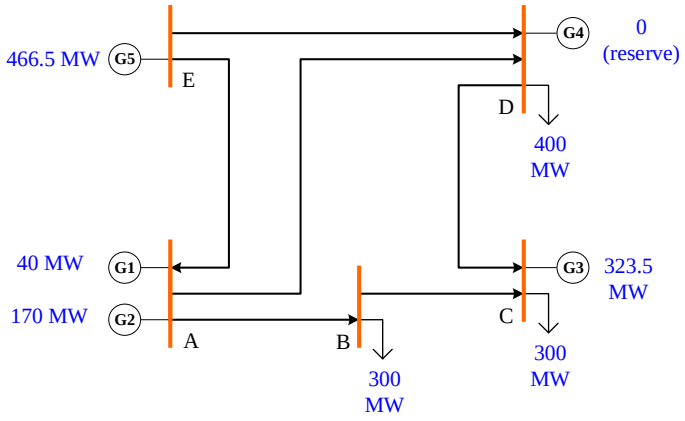
The simulation platform is an extension of the DC-CFS developed in previous chapters, with an additional consideration of hidden failure in cascading outages [161]. The hidden failures consider random outages of exposed lines next to the tripped lines and are integrated into the simulator.

Specifically, after the tripping of a fatally overloaded line, exposed line will be tripped with certain hidden failure probability. We consider the degree and duration of persisting line overloading and the hidden failure probability is defined as a function of the overloading risk $O(l)$ and critical overloading threshold O_T. Mathematically, the hidden failure probability is defined as:

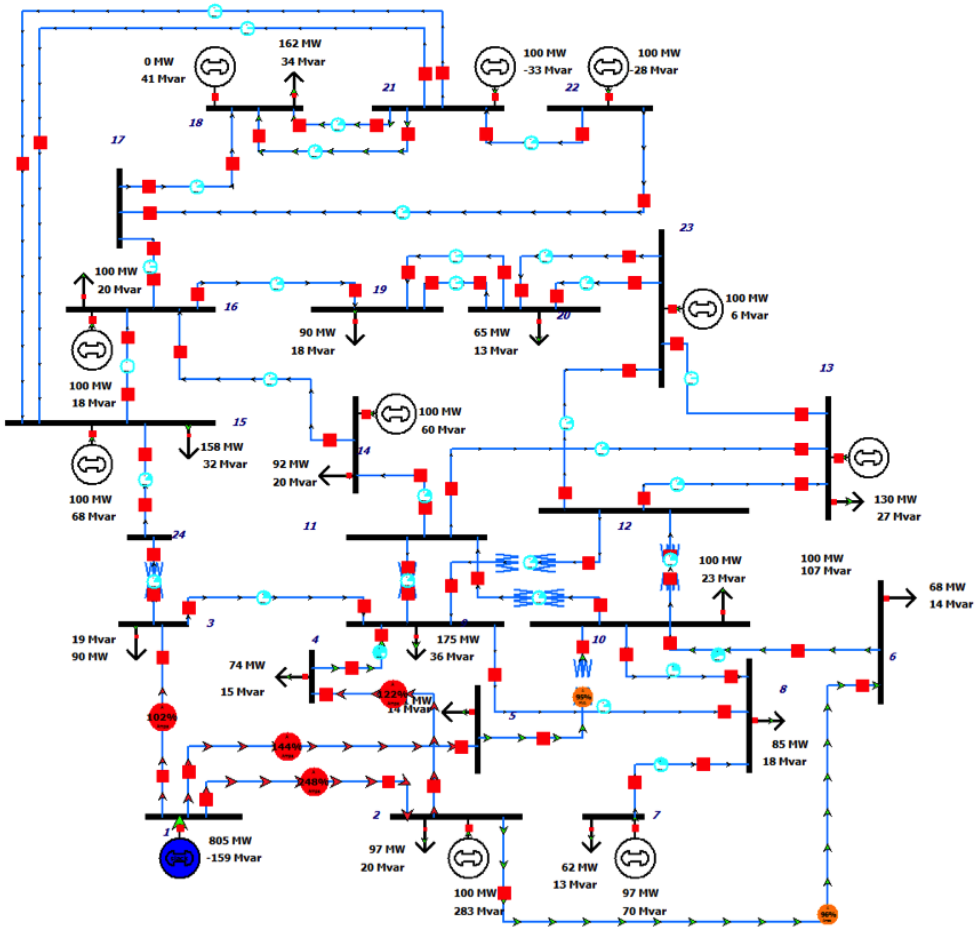
$$p(l) = \begin{cases} O(l)/O_T, & \text{if } O(l) > 0 \\ 0, & \text{otherwise} \end{cases} \tag{29}$$

The performance of the proposed Q-learning based vulnerability analysis is tested on three benchmarks: a small-size IEEE 5-bus test system [162], a mid-sized IEEE 24-bus reliability test system (RTS-79)[163], and a large-scale IEEE 300-bus system [60]. Parameters of the three test systems are provided in Table 12 and the one-line diagrams for the 5-bus and RTS-79 are shown in Figure 28.

Different systems will have different critical levels at which cascading outages can lead to a system collapse. In this chapter, we defined the blackout size as the combined number of line outages caused by the direct line-switching attack and the cascading failures triggered by the sequential attacks. For the smaller IEEE 5-bus benchmark, we consider the attack objective to be a complete system failure, i.e., $\theta = 100\%$ and $N_\theta = 6$;



(a)



(b)

Figure 28. (a) IEEE 5-bus test system and (b) IEEE RTS-79 test system.

Table 12. Benchmark system information

Benchmark	N_{bus}	N_{line}	Load (MW)	Capacity (MW)
IEEE 5-bus	5	6	1,000.0	1,530.0
IEEE RTS-79	24	38	2,850.0	3,405.0
IEEE 300-bus	300	411	23,525.8	32,678.4

for the IEEE RTS-79 system and the larger IEEE 300-bus system, we consider a critical system failure as the attack objective, where the system will lose its functionality after a fatal number of lines are down. Subsequently, we consider $\theta = 20\%$ ($N_\theta = 8$) for the RTS-79 system and $\theta = 2.5\%$ ($N_\theta = 11$) for the 300-bus system.

In the experiments, Monte Carlo simulations are used to address the randomness from the stochastic hidden line failures [161]. As a common practice for validation, repeated simulations on typical operating points will verify the effectiveness of the method in stochastic scenarios. A set of 100 independent simulations is first performed on each of the three benchmark systems. Every experiment consists of up to 1,000 trials during which the Q-learning agent searches for attack sequences that will reach the attack objective N_θ. At the beginning of the first trial in each experiment, the initial Q values are set to $+1.0$ and the same for any new state-action pairs onward, which is an "optimistic" estimate to encourage exploration during the early stages. In each subsequent trials, the system is reset to the attack-free initial state with no line outages, while the Q values learned from previous trials are retained.

We start each experiment with a relatively large exploration probability of $\epsilon_0 = 0.3$ and decrease it to a small final value of $\epsilon_f = 0.005$, with a step-down by $\Delta\epsilon = -0.005$ after each trial. Meanwhile, following the common practice of Q-learning, we choose $\alpha = 0.1$ for a less aggressive learning process and $\gamma = 0.9$ to weight slightly more on the recent reinforcements [159].

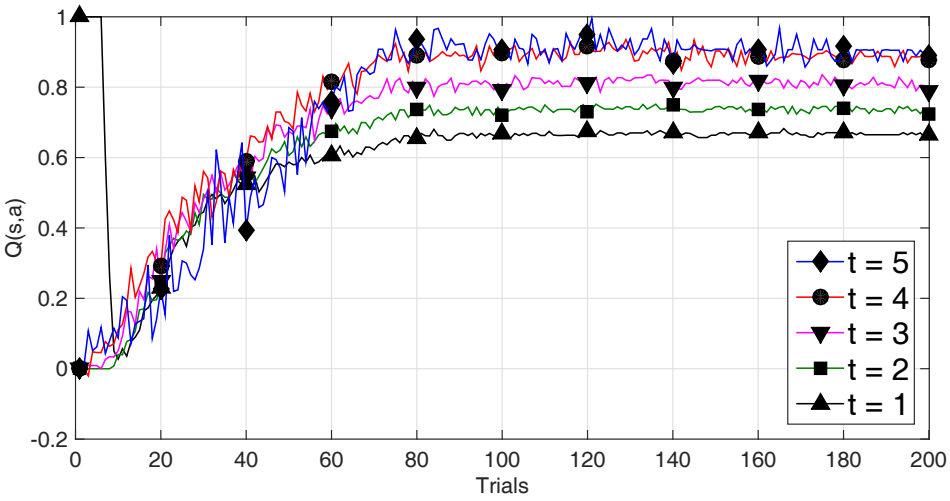
Table 13. Number of Line Outages from Sequential Attacks on the IEEE 5-bus System Increased by Q-learning

Order of attack	Initial	Eventual	Best of random attack
$t = 2$	2.37	**3.23**	2.62
$t = 3$	3.54	**4.34**	3.70
$t = 4$	4.54	**5.34**	4.77
$t = 5$	5.48	**5.94**	5.73

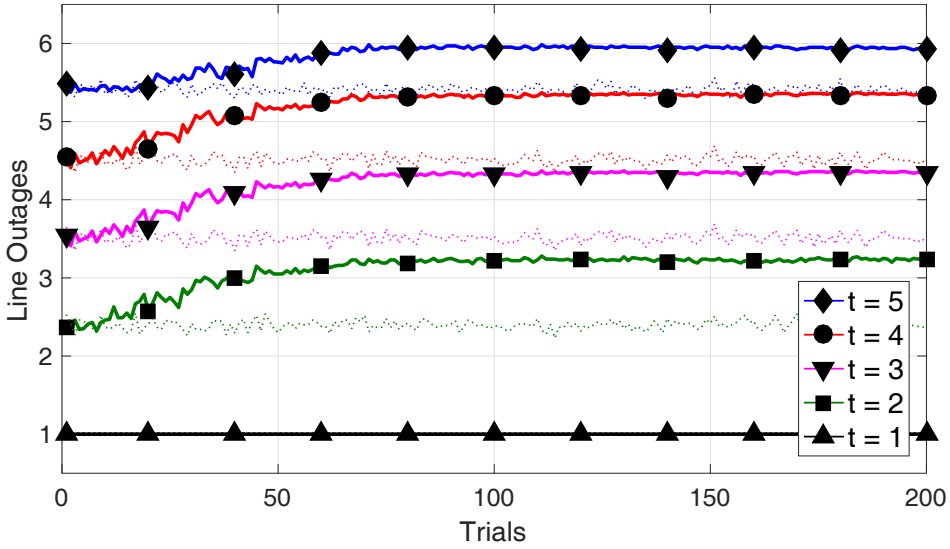
5.3.2 Attack Performance

We first evaluate the proposed method on the IEEE 5-bus test system, for which the attack performance saturated after about 200 trials. Figure 29 shows the Q values of the action in each attack and the number of line outages afterward. In Figure 29(a), we first observed that the initialized Q value for $t = 1$ quickly decreased from $+1.0$ to near-zero after 10 trials, showing that these early trials were mostly unsuccessful. After the initial trails, the Q-learning started to explore successful attack sequences and update the Q values quickly, reflecting the expected total reward learned from its trials. After about 100 trials, the Q values were stably increased to different ranges of expected total rewards for different rounds of attack in the sequence.

In addition to the Q values, the number of line outages is shown in Figure 29(b). As a comparison, the number of line outages caused by random attacks has also been plotted as unmarked dash-lines with different colors for corresponding values of t. Except for the first attack ($t = 1$), the average blackout size after each attack in the sequence was increased during the Q-learning process as shown in Table 13. The improvement was most significant for the second attack ($t = 2$), with an increase of 0.86 additional line outages. The additional line outages from Q-learning for the fifth attack ($t = 5$) was 0.46, and the eventual blackout size on average (5.94) was close to a complete system failure. Note that the system is $N - 1$ secured so that there is only one line outage after the first attack. In comparison, the random attacks did not utilize any knowledge



(a)



(b)

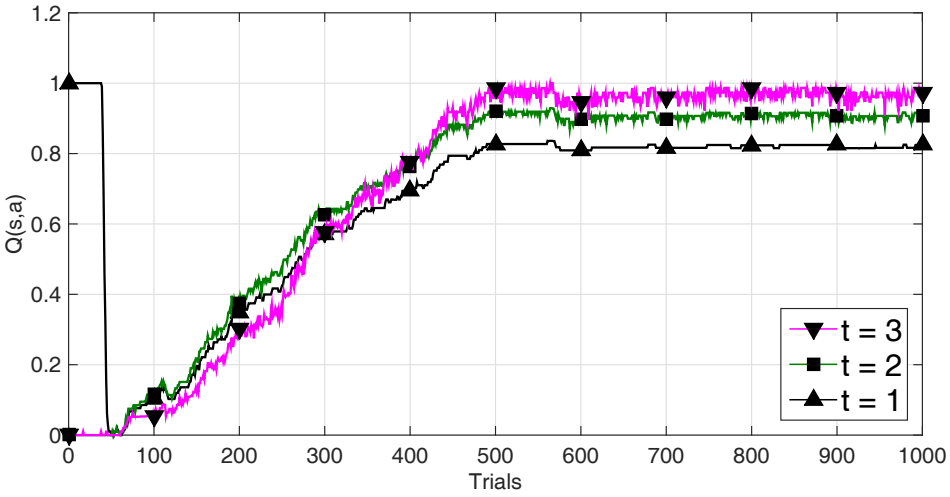
Figure 29. Results from the IEEE 5-bus system: (a) the $Q(s, a)$ values of actions taken in each attack; (b) the number of line outages after each attack.

from previous trials and thus failed to identify more vulnerable sequences over time. These results on the 5-bus system have exhibited the effectiveness of the Q-learning based vulnerability analysis, learning from trials to reach the objective blackout size with purely topological information.

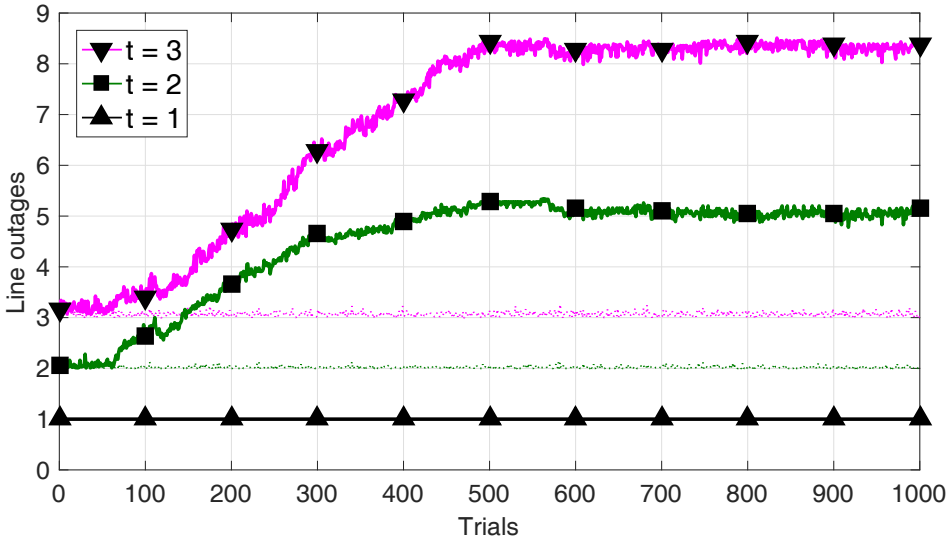
Figure 30 shows the attack performance on the IEEE RTS-79 system. Similar to the 5-bus system, we also observed similar changes of Q value for the sequential attacks in Figure 30(a), with respective expected total rewards from the attack. Meanwhile, as shown in Figure 30(b), with Q-learning the blackout size was improved from 2.06 to 5.15 after the second attack ($t = 2$) and from 3.15 to 8.39 after the third attack ($t = 3$), respectively. Although the RTS-79 system is $N - 1$ secured, with an attack objective $N_\theta = 8$, it only took three sequential attacks to cause a critical 8-line blackout after 500 trials with Q-learning. With the same level of topological information, the proposed Q-learning based scheme was more effective in finding critical attack sequence on the RTS-79 system.

The proposed approach is further validated on a large-scale benchmark, the IEEE 300-bus system. The results are shown in Figure 31. Similarly, the Q values converged through the learning process (Figure 31(a)) and the reinforcements improved the blackout sizes after the second attacks towards the attack objective, an 11-line outage, after 598 trials (Figure 31(b)) on average. Some oscillations persisted after 700 trials, as the final blackout size differed slightly due to cascading outages and hidden failures when the objective was achieved. The results validated that the proposed approach is scalable to bulk power systems.

The cost of attack can also be evaluated by the average number of attacks required to achieve the objective blackout size, which is shown in Figure 32. The dashed lines indicate the respective objective blackout sizes, which are the unsuccessful (worst) case for the attackers as they would need to attack as many lines as possible to achieve the attack objective. According to Figure 32, the initial number of attacks required to reach the objective blackout sizes are 5.48, 7.29, and 10.14 for the 5-bus, the RTS-79, and the 300-bus systems, respectively. These numbers were reduced to 4.67 for the 5-bus system after 100 trials, 2.82 for the RTS-79 system after 500 trials, and 3.16 for the



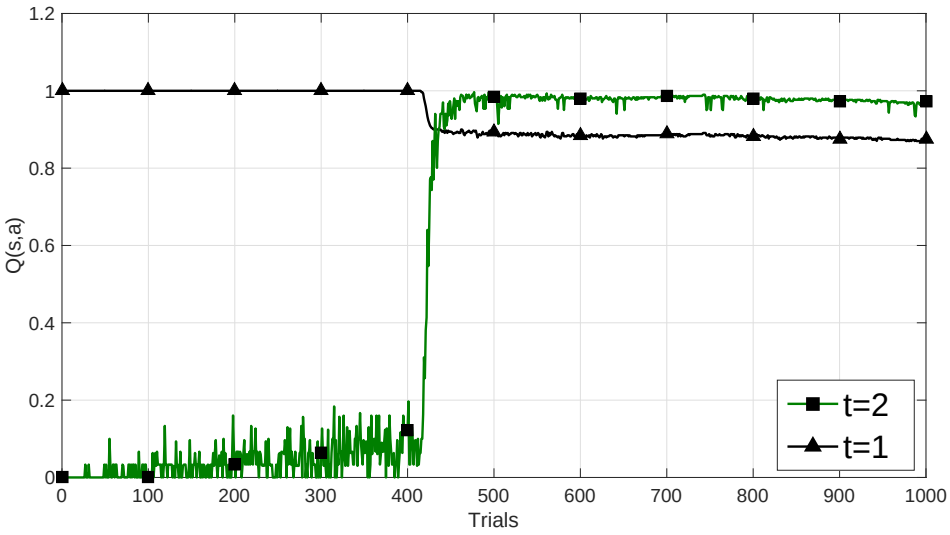
(a)



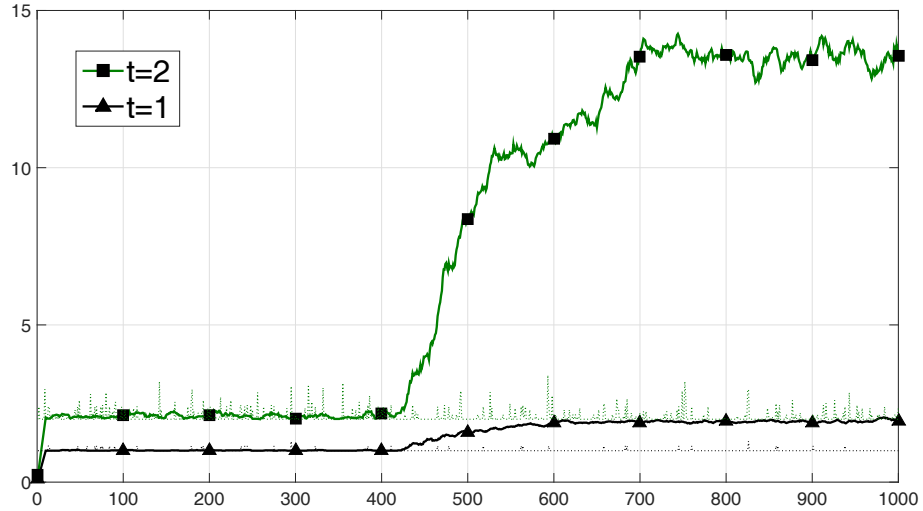
(b)

Figure 30. Results of the IEEE RTS-79 system: (a) the $Q(s, a)$ values of the chosen action for each attack in the sequence and (b) the number of line outages after each attack.

300-bus system after 700 trials, respectively. Afterward, their values remained in stable ranges, respectively. The eventual numbers of sequential attacks launched to reach the attack objectives were 4.60, 2.85, and 3.09, respectively, for the three systems. From



(a)



(b)

Figure 31. Results from the IEEE 300-bus system: (a) the $Q(s, a)$ values of the chosen action for each attack in the sequence and (b) the number of line outages after each attack.

these simulations, the Q-learning based scheme also effectively reduced the number of attacks through the learning process.

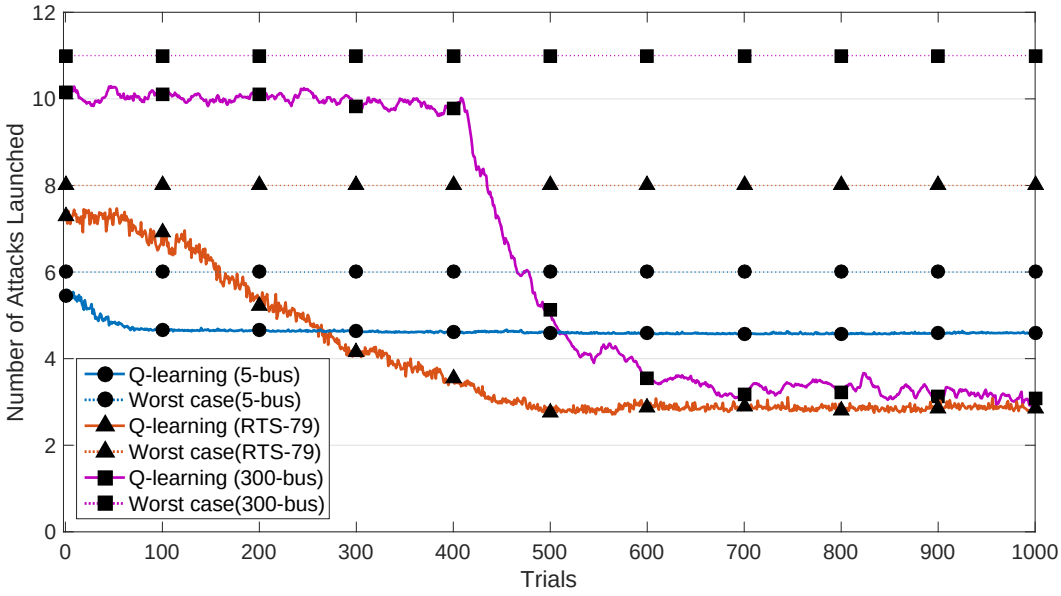


Figure 32. The number of attacks taken to achieve the objective blackout size (dashed line) for the IEEE 5-bus, RTS-79, and 300-bus systems. The numbers reduced by the Q-learning exhibited the effectiveness of Q-learning in identifying more vulnerable attack sequences.

5.3.3 Disucssions

As the load of power systems fluctuates with time, the robustness of the proposed approach shall be tested under different operating points (OP). Assuming a benchmark system's total default load is 100%, we solved the optimal power flow to obtain an OP with a peak load at 120% and another with a reduced load at 80% for the benchmarks. Simulations were repeated on the three benchmark systems and the eventual blackout size when the attack objectives were achieved are shown in Table 14 with different loading settings.

From the simulation, the proposed Q-learning based approach has successfully identified critical sequential topology attacks with respective objectives on all three benchmarks with different loading levels. In general, lowering loading levels reduce the system stress and make them more resilient to cascading outages and sequential attacks. In contrast, the peak loads turn $N-1$ secured systems (under default loading)

more stressed and vulnerable. The blackout sizes in Table 14 are consistent with these discussions. As load increases, sequential attacks caused more line outages with the same number of attacks and attack objective were achieved faster.

Table 14. Influence of Load Variation on the Eventual Blackout Sizes

IEEE 5-bus	Default Load	Peak Load	Reduced Load
$t = 1$	1.00	1.99	1.00
$t = 2$	3.39	4.02	3.29
$t = 3$	4.44	5.02	4.36
$t = 4$	5.44	5.98	5.38
$t = 5$	5.98	**6.00**	5.62
$t = 6$	**6.00**	-	**6.00**
IEEE RTS-79	Default Load	Peak Load	Reduced Load
$t = 1$	1.00	1.81	1.00
$t = 2$	5.15	5.85	2.03
$t = 3$	**8.38**	**8.40**	3.45
$t = 4$	-	-	4.35
$t = 5$	-	-	5.10
$t = 6$	-	-	6.05
$t = 7$	-	-	7.11
$t = 8$	-	-	**8.19**
IEEE 300-bus	Default Load	Peak Load	Reduced Load
$t = 1$	1.84	1.92	1.02
$t = 2$	**13.91**	**14.72**	3.08
$t = 3$	-	-	5.59
$t = 4$	-	-	9.73
$t = 5$	-	-	**13.10**

Note: A '-' indicates that the attack objective has already been achieved.

5.4 Chapter Summary

This chapter presented a novel Q-learning based vulnerability analysis of electrical power grid in the sequential topological attacks. By monitoring topology change in the system, the Q-learning based sequential scheme was able to find out vulnerable sequences that led to critical blackouts in the system. Not only did the scheme increase

the number of line outages through the learning process, but it also reduced the number of attacks launched by excluding unpromising attack sequences that could not take advantage of the cascading vulnerability. Simulation results on three IEEE systems of different scales have demonstrated the learning ability and the effectiveness of the proposed approach. From the perspective of a grid defender/operator, the Q-learning based vulnerability analysis can serve as a tool to identify critical components in a potential sequential attack scheme. It also gives a warning sign that topological status information of the system could be utilized to conceive disastrous attack schemes. These insights are expected to help improve situation awareness of the smart grid against cyber-attacks.

The future work will focus on the development of detection and mitigation strategies against sequential attacks. While the proposed approach utilizes reinforcement learning to screen potentially vulnerable sequences of topological line-switching, it is not limited to the DC power flow or hidden failure models; adaptions can be made to consider other factors such as voltage and frequency for vulnerability analysis. Meanwhile, it is valuable to explore other potential information, sources, and parameters to identify if they may result in more catastrophic attack impacts on the critical power infrastructure. Finally, the online learning ability will also be a valuable feature to be added for real-world applications.

CHAPTER 6

Resilience And Detection Against False Measurement Attacks

6.1 Chapter Overview

While control commands in the smart grid are ideal targets of cyber-attackers who aim to inflict direct disruption to the power system, the measurements are also potential victims of cyber-attacks for various purposes. Although compromised measurements may not directly cause system damages as the commands, they can leverage misinformation that leads to inadequate situation awareness and/or incorrect control actions. Many research ahs revealed that such manipulation poses multiple threats to system operations and could be exploited to induce large-scale blackouts [6]. Meanwhile, this chapter will look at the problem more from the perspective of a grid operator, for whom the emphasis will be placed on the assessment of grid resilience as well as the detection of false data in the system.

Specifically, this chapter will first provide a preliminary resilience analysis of FDI attack regarding its potential to create cascading blackouts [164]. Specifically, an AC version of the CFS will be developed to report voltage violations, line outage, and load shed resulting from injected false data in state estimation. A comparison is made with different attack strengths in terms of magnitude and severeness. This part tries to bridge current studies on FDI attacks with power system blackout analysis to better understand the practical threat of FDI attacks on the smart grid.

In addition, this chapter will also investigate the supervised learning based approaches to detection FDI attacks. In [165], M. Ozay, *et al.,* first proposed the use of supervised machine learning based classifiers to detect false data using the distance between attacked and normal measurements. However, the attack vectors were built in the measurement space rather than the state space, which might not fully exploit the stealthiness proposed in [84]. In addition, the performance was only tested against the

attack sparsity, i.e., number of compromised meters, while the magnitude of injected false data was not considered. Lastly, the possible imbalance between attacked and normal data samples should also be considered as a challenge in practical applications.

The rest of this chapter is organized as follows: Section 6.2 introduces the basic concepts of FDI attacks, including the power system state estimation, the residual based bad data detection, and the false data injection attack schemes. Section 6.3 introduces the analytic framework based on the previously developed cascading failure model to analyze the grid response and resilience in the presence of false data. Section 6.4 describes the formulation of the FDI detection as a classification problem and introduces the classifiers for detection with discussions on two influence factors. Section 6.5 presents the resilience analysis and detection performance based on simulation. Section 6.6 summarizes the chapter and discusses some future works.

6.2 False Data Injection Attacks

In 2009, Y. Liu, *et al.* have revealed that measurements collected from supervisory control and data acquisition (SCADA) systems are exposed to the threat of malicious false data injection (FDI) attacks [84]. Given the critical role of accurate and trustworthy power system state estimation (PSSE) in power system control and operation, numerous attack and defense studies have been conducted to understand the threat of FDI attacks ever since [118].

The attack studies focus on stealth schemes that utilize the knowledge of the topological Jacobian matrix to bypass the residual-based bad data detectors in the system. Attack schemes can thus be built based on minimum energy leakage [166], system topology [167], or the sparsity of the Jacobian matrix [168]. Moreover, when full knowledge of the Jacobian matrix is not available to the attackers, stealth FDI attacks can still be constructed with incomplete [169, 170, 171] or local topology information [172, 173]. Worse still, the ICA-based attack can infer the stealth attack vector without the knowl-

edge of the Jacobian matrix [174, 175]. The attacks can also be coordinated [176, 177] or cast into bi-level or tri-level optimization problems that can counter the presence of a grid defender [178, 179].

The defense studies focus on both the detection of FDI attacks and the protection of measurements. Detectors utilizing the low rank and sparsity of the Jacobian matrix has been proposed in [180, 181]. An adaptive online CUSUM detectors have been proposed [182]. Spatial and temporal based detection schemes have also been proposed in [183], while an online detection scheme has been proposed in [184]. In the meantime, secure communication channels and protocols have been established [185]. Greedy, game theoretic, and other methods have been used for optimizing the placement of PMUs for more secure measurements [186, 187, 188], significantly reducing attacker's ability to launch FDI attacks.

6.2.1 Power System State Estimation

Electrical power systems depend on reliable state variables for control and dispatch of the generation, transmission and distribution of electricity. In PSSE, the relationship between the known measurement variable $\mathbf{z}$ and the unknown state variable $\mathbf{x}$ can be written as [189]:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{n} \tag{30}$$

where $\mathbf{h}(\mathbf{x})$ is a non-linear function determined by the power grid topology and $\mathbf{n}$ is the random measurement noise. $\mathbf{n}$ is commonly assumed to be a zero-mean Gaussian variable with known covariance $cov(\mathbf{n}) = \mathbf{R}$.

In practice, the nonlinear function $\mathbf{h}(\mathbf{x})$ is approximated by a linear function based on the following direct current (DC) assumptions [60]:

1. The magnitudes of all bus voltages V are close enough to be equal to 1 p.u.;

2. The active power transmission on all branches is lossless;

3. The angular difference $\delta\theta$ between any two bus voltages are small enough so that $\sin(\delta\theta) \approx \delta\theta$.

With the above DC assumption, (30) can be replaced by:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n} \tag{31}$$

where $\mathbf{H}$ is the *Jacobian* matrix of power grid topology. Let M be the number of measurements and N the number of states, $\mathbf{H}$ is a $M \times N$ matrix with $M \gg N$, so that redundant measurements can recover the accurate state variable $\mathbf{x}$ from $\mathbf{z}$. In practice, the linear approximation can also be achieved if sufficient phasor measurement units have been installed [189].

To solve the linear equation in (31), the weighted least square (WLS) estimation is commonly used. WLS minimizes the following cost function $\mathbf{J}(\mathbf{x})$:

$$\mathbf{J}(\mathbf{x}) = (\mathbf{z} - \mathbf{H}\hat{\mathbf{x}})^{\mathbf{T}}\mathbf{R}^{-\mathbf{1}}(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}) \tag{32}$$

and the estimated state variable $\hat{\mathbf{x}}$ is given by:

$$\hat{\mathbf{x}} = (\mathbf{H}^{\mathbf{T}}\mathbf{R}^{-\mathbf{1}}\mathbf{H})^{-\mathbf{1}}\mathbf{H}^{\mathbf{T}}\mathbf{R}^{-\mathbf{1}}\mathbf{z} \tag{33}$$

6.2.2 Bad Data Detection

In PSSE, meter and sensor faults can result in deteriorated state estimation results. To improve estimation accuracy, bad data detection (BDD) that identifies and removes these bad measurements are commonly employed. The following is a brief introduction to the widely used residual-based BDD from [189], where further details can found therein.

Let $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$ be the measurement residual, the normalized L_2-norm of $\mathbf{r}$ is:

$$L(\mathbf{r}) = \mathbf{r}^{\mathbf{T}}\mathbf{R}^{-\mathbf{1}}\mathbf{r} \tag{34}$$

$L(\mathbf{r})$ follows the χ^2_{M-N} distribution with at most $M-N$ degree of freedom. Therefore, the χ^2-test is used to determine a threshold τ with a given confidence p. The null hypothesis H_0 of the residual-based bad data test is:

$$H_0 : \mathbf{r^T R^{-1} r} \leq \tau \tag{35}$$

If H_0 is accepted, then no bad data exist in the SE solutions with a confidence of p; if H_0 is rejected, then bad data exist and they are subsequently eliminated by the largest normalized residual (LNR) test with another threshold γ:

$$\mathbf{r}_i^N = \frac{\mathbf{r}_i}{\sqrt{diag(\mathbf{S})diag(\mathbf{R})}} > \gamma \tag{36}$$

where $\mathbf{r}_i$ is the i-th residual in $\mathbf{r}$, $i = 1, 2, ..., M$, $\mathbf{S} = \mathbf{I} - \mathbf{K}$ is the residual sensitivity matrix, $\mathbf{I}$ is the $M \times M$ identity matrix, $\mathbf{K} = (\mathbf{H^T R^{-1} H})^{-1}\mathbf{H^T R^{-1}}$, and $diag(\cdot)$ is the diagonal elements of a given matrix. After $\mathbf{r}_i^N$ has been calculated for every measurement in $\mathbf{z}$, the measurement $\mathbf{z}_j$ producing the largest normalized residual that satisfies (36), i.e., $j = \text{argmax}_i\{\mathbf{r}_i^N | \mathbf{r}_i^N > \gamma\}$, is considered as a bad measurement and will be eliminated from $\mathbf{z}$. $\mathbf{r}_i^N$ is repeatedly calculated for bad data removal until no residual satisfies (36) or a maximal number of bad data have been removed. In practice, the BDD and PSSE are iteratively executed until no normalized measurement residual $\mathbf{r}_j^N$ satisfies (36) or the maximal allowed number of bad data has been reached.

6.2.3 False Data Injection Attack

In general, false data injection (FDI) is written in the following form:

$$\mathbf{z_a} = \mathbf{z} + \mathbf{a} = \mathbf{Hx} + \mathbf{a} + \mathbf{n} \tag{37}$$

where $\mathbf{a}$ is the injected false measurement data.

If $\mathbf{a}$ is directly generated and injected into the measurements without the knowledge of $\mathbf{H}$, $L(\mathbf{r})$ does not necessarily follow the χ^2_{M-N} distribution. The residual-based BDD can only detect the false data if $\mathbf{a}$ increases the residual statistic in (34)-(36).

If $\mathbf{H}$ is available to the attacker, however, a completely unobservable FDI for the above BDD can be constructed. Specifically, the stealth false measurement data $\mathbf{a}$ in (37) can be generated in the following form:

$$\mathbf{a} = \mathbf{Hc} \tag{38}$$

where $\mathbf{c}$ is the false state data. Then the compromised measurement $\mathbf{z_a}$ becomes:

$$\begin{aligned} \mathbf{z_a} &= \mathbf{Hx} + \mathbf{Hc} + \mathbf{n} \\ &= \mathbf{H}(\mathbf{x} + \mathbf{c}) + \mathbf{n} \\ &= \mathbf{Hx_a} + \mathbf{n} \end{aligned} \tag{39}$$

which is in the same form of $\mathbf{z}$ in (31). Meanwhile, the residual also remains the same to (35):

$$\begin{aligned} \mathbf{r_a} = \mathbf{z_a} - \mathbf{H}\hat{\mathbf{x}}_\mathbf{a} &= \mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c}) \\ &= \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{Hc}) \\ &= \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \end{aligned} \tag{40}$$

Therefore, residual-based BDD is not able to identify the false data $\mathbf{a}$ if the original attack-free data $\mathbf{z}$ can pass the residual-test in (35). The LNR test in (36) is also not capable of eliminating the attacked measurements, although false data can possibly be rejected by a lucky hit if the original measurement $\mathbf{z}$ itself is rejected as bad data.

Let κ be the number of compromised measurements, it has been proved in [84] that if the following condition is satisfied, it is guaranteed that there exists an FDI attack unobservable by the residual based BDD:

$$\kappa > M - N + 1 \tag{41}$$

Mathematically, κ is equivalent to the sparsity, i.e., the L-0 norm of the attack vector $\mathbf{a}$.

Among the current studies of FDI attacks, this chapter chose two typical FDI schemes in comparison: the direct FDI with the random false measurement and the stealth FDI with the random false state:

1. **Direct FDI Attack**

   In the first scheme, we consider the attacker has no knowledge of $\mathbf{H}$ when injecting false data into the measurements. A random attack vector $\mathbf{a} \sim N(0, \sigma_{\mathbf{a}}^2)$ is generated with a given false measurement variance $\sigma_{\mathbf{a}}^2$, similar to [165]. The false data $\mathbf{a}$ is then injected directly into the measurements $\mathbf{z}$ by (37).

2. **Stealth FDI Attack**

   In the second scheme, we assume the attacker has the full knowledge of $\mathbf{H}$ and thereby can construct a stealth FDI attack as in [84]. In this case, a targeted false state $\mathbf{x_a}$ is generated by $\mathbf{x_a} = \mathbf{x} + \mathbf{c}$. We assume that $\mathbf{c} \sim N(0, \sigma_{\mathbf{c}}^2)$, where $\sigma_{\mathbf{c}}^2$ is the variance.

6.3 Grid Resilience under FDI Attacks

Manipulated measurements from FDI attack can mislead system operation to increase the risk of cascading blackouts. For instance, when energy management system (EMS) re-dispatches power to manipulated measurements, the powers system can run in degenerated state with potential overloading, voltage violation, or other stability issues. Considering the extreme case with a fully knowledgeable attack, line outages and cascading blackouts may also be triggered by contingencies after the injection of targeted attack vectors. However, such risk can be low compared to control attacks as the power system is designed to be resilient against faults and disturbances by nature. It merits careful examination to determine if an FDI attack can actually result in feasible damage to the system to the level of cascading blackouts.

The resilience analysis in this chapter will examine the ability of the grid to with-

stand the FDI by retaining an operational transmission without major failures such as a local blackout, voltage collapse, or any cascading outages. The resilience is evaluated on two factors that quantify the strength of an FDI attack, i.e., the magnitude and the severeness.

1. The *magnitude* of FDI attack, denoted as α, is a scale factor of $\mathbf{a}$ that describes the extent of manipulation for each measurement. Assume that original state is 1.0 p.u. and the nominal upper/lower limits are 0.9 and 1.1 p.u., respectively. $\alpha = 0.1$ indicates the false states in $\mathbf{c}$ are up to 0.01 p.u. or 10% of the maximal deviation allowed by the state limits; $\alpha = 1.0$ indicates the false states can reach a maximal deviation of 0.1 p.u..

2. The *severeness* of FDI attack, denoted as ρ, refers to the fraction of measurements subject to manipulation. If $\rho = 0.1$, 10% of measurements are manipulated; if $\rho = 1.0$, all measurements are manipulated. In this chapter, the location of attacked measurements is randomly selected and tested with different severeness.

With the two factors introduced, the false data $\mathbf{a}$ becomes:

$$\mathbf{a} = \alpha \mathbf{\Delta H c} \tag{42}$$

where $\mathbf{\Delta} = diag(\delta)$, and δ is an $m \times 1$ index vector with $\rho \times m$ (rounded) randomly selected elements equal to one and the rest equal to zero.

Blackouts are often results of complex system responses, unstable operations, and protection failures. While it is challenging to properly consider all factors in a single simulator, this chapter considers short-term blackout risks contributed by the following mechanisms:

Line Overloads and Outages

This chapter considers the over-current-relay triggered cascading line outages as the first system response. An AC power flow based cascading model was built from

a DC power flow cascading outage simulator [190]. The DC simulator implements re-dispatch, islanding and active power flow overload response to simulate cascading outages from over-current relay actions. Details of the DC simulator can be found in Chapter 2 of this dissertation.

On top of these features, the AC simulator in this chapter removes the DC assumptions and considers reactive power limits, transmission loss and steady-state voltage stability in cascading blackouts. Lines with persisting overloading beyond a critical threshold will be subsequently tripped and simulation will continue until no more overloading is observed. The number of lines tripped and the load shed due to emergent re-dispatch are reported to analyze system resilience.

Voltage Violations

Voltage stability plays an critical role in blackouts as voltage collapse or power swings cause severe damages in the system [158]. THe previous study [190] has shown that the steady-state model remains consistent with more detailed transient stability model if the voltages are within the magnitude and angle constraints. With the voltage computed from steady state AC power flow solutions, any voltage violations emerging either after the FDI or from the cascading line outages can be reported if either of the following conditions is not satisfied:

$$\theta_{min} \leq \theta \leq \theta_{max} \tag{43}$$

$$V_{min} \leq V \leq V_{max} \tag{44}$$

where $V_{min} = 0.9\ p.u.$, $V_{max} = 1.1\ p.u.$, $\theta_{min} = -10°$, and $\theta_{max} = +10°$, according to the critical moment defined in [190]. Note that a violation does not warrant a voltage collapse or pole flip; it is rather a warning of the voltage instability caused by FDI.

6.4 Detecting FDI Attacks with Supervised Learning

From the perspective of machine learning, the aforementioned FDI detection problem can be conceived as a binary classification problem. Let $\mathbf{s}$ be the measurement data samples with M features from either $\mathbf{z}$ (negative class) or $\mathbf{z_a}$ (positive class). The corresponding class labels y is defined as:

$$y = \begin{cases} +1, & \text{if } \mathbf{a} \neq \mathbf{0} \\ -1, & \text{if } \mathbf{a} = \mathbf{0} \end{cases} \tag{45}$$

Without loss of generality, the distance between two arbitrary samples $\mathbf{s}_i$ and $\mathbf{s}_j$ is given by:

$$\|\mathbf{s}_i - \mathbf{s}_j\|_2 = \begin{cases} \|\mathbf{z}_i - \mathbf{z}_j + \mathbf{a}_i - \mathbf{a}_j\|_2, & \text{if } \mathbf{a}_i, \mathbf{a}_j \neq \mathbf{0} \\ \|\mathbf{z}_i - \mathbf{z}_j + \mathbf{a}_i\|_2, & \text{if } \mathbf{a}_i \neq \mathbf{0}, \mathbf{a}_j = \mathbf{0} \\ \|\mathbf{z}_i - \mathbf{z}_j\|_2, & \text{if } \mathbf{a}_i, \mathbf{a}_j = \mathbf{0} \end{cases} \tag{46}$$

Note that the right side expressions are different from that of [165].

According to (46), the presence of false data can be determined by the vector distance. Consider the following two assumptions: 1) $\mathbf{a}_i$ is sufficiently greater than the noise $\mathbf{n}$; 2) the mean of $\mathbf{a}_i$ is sufficiently greater than its variance. In general, both assumptions will hold for attackers who aim at creating disturbances in the smart grid via the injection false data. Consequently, the two classes can be classified by proper learning methods to detect the FDI attacks.

6.4.1 Classifiers for FDI Detection

There are numerous machine learning methods available for the binary classification problem described above. A practical concern is that complex algorithms are often expensive in real-time implementations despite their superior performance in difficult classification problems. On the other hand, it remains unknown if false data constructed

by the above schemes are separable by the simple algorithms. This chapter considers the following learning algorithms that are widely used in practice:

Support Vector Machine

Support vector machine (SVM) is a binary classifier to find the maximum-margin hyperplane that separates the two classes. Given the definition of y_i and $\mathbf{s}$ in (45), if the data is linearly separable, the decision boundaries can be expressed as two parallel hyperplanes:

$$\begin{cases} \mathbf{w^T s}_i + b = +1, \text{if } y_i = +1 \\ \mathbf{w^T s}_i + b = -1, \text{if } y_i = -1 \end{cases} \tag{47}$$

Data samples satisfying either equations in (47) are called the support vectors. The region that lies between the parallel boundaries are called the margin, and the distance between this two hyperplane, i.e., the width of the margin, is $D = 2/\mathbf{w^T w}$. For binary classification, the data samples from different classes should lie on corresponding side of the margin, and the maximal margin should yield the maximal D, i.e., the minimum of $\mathbf{w^T w}$. Combining the formulation above, the linear SVM solves the following optimization problem:

$$\min_{\mathbf{w}} \ \frac{1}{2}\mathbf{w^T w} \tag{48}$$

$$\text{s.t. } y_i(\mathbf{w^T s}_i + b) \geq 1, \ i = 1, 2, ..., m \tag{49}$$

This is a quadratic programming problem and the solutions of $\mathbf{w}$ and b can be obtained using the following the Lagrangian of the optimization:

$$L(\mathbf{w}, b, \alpha) = \frac{1}{2}\mathbf{w^T w} - \sum_{i=1}^{m} \alpha_i [y_i(\mathbf{w^T s}_i - b) - 1] \tag{50}$$

where α is the Lagrange multiplier. The problem satisfies the Karush-Kuhn-Tucker

(KKT) conditions, and it can be solved by the Lagrange dual of this problem:

$$\text{maximize } L(\alpha) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{m} y_i y_j \alpha_i \alpha_j \mathbf{s}_i^{\mathbf{T}} \mathbf{s}_j \tag{51}$$

$$\text{s.t. } \sum_{i=1}^{m} \alpha_i y_i = 0 \tag{52}$$

If the samples are not linearly separable, then a kernel function $K(\mathbf{s}_i, \mathbf{s}_j)$ is used to replace the inner product $\mathbf{s}_i^T \mathbf{s}_j$ in (51), if $K(\mathbf{s}_i, \mathbf{s}_j)$ has the following property:

$$K(\mathbf{s}_i, \mathbf{s}_j) = \phi(\mathbf{s}_i)^{\mathbf{T}} \phi(\mathbf{s}_j) \tag{53}$$

where $\phi(\mathbf{s})$ is a mapping function of $\mathbf{s}$ into a higher dimension.

In this chapter, the Gaussian radial basis function is used as the kernel in the SVM classifier:

$$K(\mathbf{s}_i, \mathbf{s}_j) = e^{-\lambda \|\mathbf{s}_i - \mathbf{s}_j\|^2}, \ \lambda > 0 \tag{54}$$

k-Nearest Neighbor (kNN)

kNN is a simple and widely-used effect classifier that assign the samples to the class of its nearest neighbors. The Euclidean distance is used to determine the closeness between the current unlabeled sample $\mathbf{s}_i$ and all the labeled samples S:

$$d_{ij} = \|\mathbf{s}_i - \mathbf{s}_j\|, \mathbf{s}_j \in S \tag{55}$$

For $k = 1$, the predicted class label y_i is given by the labeled sample closest to y_i:

$$y_i = arg \min_{y_j} \{d_{ij}\} \tag{56}$$

For $k > 1$, the majority voting is used to determine the eventual label from k nearest neighbors of $\mathbf{s}_i$. In this chapter, the number of nearest neighbor is chosen according to cross-validation performance. In this chapter, the number of nearest neighbors is chosen from $k = \{1, 3, 5, 7\}$ according to the best cross-validation performances.

Extended Nearest Neighbor (ENN)

The ENN is a variation of kNN that improves the latter's performance [191]. Traditional kNN is sensitive to the distribution of predefined classes, mostly because the nearest neighbors of data sample with a low density tend to be dominated by the other class with a higher density [192]. To address the "two types of errors" [193] in kNN method, we propose an extended nearest neighbors (ENN) method which takes advantage of learning the global distribution of class and local neighbors to make a classification prediction.

Let S_1 and S_2 be the set of samples that belong to $y = -1$ (class 1) and $y = +1$ (class 2), respectively. A generalized class-wise statistic T_i is calculated to measure the distribution of each class:

$$\begin{aligned} T_i &= \frac{1}{n_i} \sum_{\mathbf{s} \in S_i} \frac{1}{k} \sum_{r=1}^{k} I_r\left(\mathbf{s}, S\right) \\ &= \frac{1}{n_i} \sum_{\mathbf{s} \in S_i} t_k(\mathbf{s}),\ i = 1, 2 \end{aligned} \tag{57}$$

where $\mathbf{s}$ is a sample with known class label in $S = S_1 \cup S_2$. $I_r\left(\mathbf{s}, S\right)$ is a binary function that indicates whether $\mathbf{s}$ and its r-th nearest neighbor belong to the same class:

$$I_r\left(\mathbf{s}, S\right) = \begin{cases} 1, & \text{if } \mathbf{s} \in S_i \text{ and } \mathrm{NN}_r\left(\mathbf{s}, S\right) \in S_i \\ 0, & \text{otherwise} \end{cases} \tag{58}$$

where $\mathrm{NN}_r\left(\mathbf{s}, S\right)$ is the r-th nearest neighbor of x by the Euclidean distance, given the currently known sample set S.

In (57), $t_k(\mathbf{s})$ is a point-wise statistic of sample $\mathbf{s}$ evaluating the number of its k nearest neighbors that are from the same class. The generalized class-wise statistic T_i measures the ratio of the nearest neighbors belonging to the same class over the number of samples n_i and nearest neighbors k in a given class. It can be perceived as a coherence measurement for each class, indicating whether the nearest neighbors of samples from one class are dominated by the samples from other class. A larger T_i indicates that the

samples in S_i are more condensed and their nearest neighbors are mostly from the same class, whereas a smaller T_i indicates that more nearest neighbors of the samples in one class belong to another.

Given a new sample $\mathbf{z}$ to be classified, we compute the expected total gains of T_i when $\mathbf{z}$ is assigned to class $y = -1$ (class 1) and class $y = +1$ (class 2), respectively. As higher T_i implies a more densely distributed class i, $\mathbf{z}$ will be assigned to the class that yields the maximal total gain. The gain for each respective class is described as follows:

First, assuming that $\mathbf{z}$ is from class 1, we calculate the following class-wise statistics T_1^1 and T_2^1 by:

$$\begin{aligned} T_1^1 &= \frac{1}{(n_1+1)k} \sum_{\mathbf{s}\in S_1\cup\{\mathbf{z}\}} \sum_{r=1}^{k} I_r\left(\mathbf{s}, S'\right) \\ T_2^1 &= \frac{1}{n_2 k} \sum_{\mathbf{s}\in S_2} \sum_{r=1}^{k} I_r\left(\mathbf{s}, S'\right) \end{aligned} \tag{59}$$

where T_i^j is the statistic of class i when the new sample $\mathbf{z}$ is assigned to class j and $S' = S_1 \cup S_2 \cup \{\mathbf{z}\}$ is the updated set of samples.

Then, assuming that $\mathbf{z}$ is from class 2, we also calculate the corresponding class-wise statistics T_1^2 and T_2^2 by:

$$\begin{aligned} T_1^2 &= \frac{1}{n_1 k} \sum_{\mathbf{s}\in S_1} \sum_{r=1}^{k} I_r\left(\mathbf{s}, S'\right) \\ T_2^2 &= \frac{1}{(n_2+1)k} \sum_{\mathbf{s}\in S_2\cup\{\mathbf{z}\}} \sum_{r=1}^{k} I_r\left(\mathbf{s}, S'\right) \end{aligned} \tag{60}$$

Instead of using the k nearest neighbors for a majority voting, we calculate the total gains for each class:

$$G^k = \sum_{i=1}^{2} (T_i^k - T_i),\ k = 1, 2 \tag{61}$$

The new sample $\mathbf{z}$ is assigned to class 1 if $G^1 > G^2$ and class 2 if $G^1 < G^2$. Similar to the kNN method, the number of nearest neighbors in consideration is also chosen from $k = \{1, 3, 5, 7\}$ according to the best cross-validation performances.

6.4.2 Attack Strength in FDI Detection

The sample distance in (46) depends on the characteristics of $\mathbf{a}$. Therefore, the sparsity and variance of $\mathbf{a}$ are two key factors to be considered. The sparsity measures the number of compromised measurements in the FDI attack, and the variance indicates the magnitude of disturbances brought by the false data. They both reflect the attack strength of an FDI and the detection performance will be sensitive to these two factors and need to be examined in this chapter.

The first factor, i.e., the number of false measurement data injected into the system, is defined previously as the variable κ in (41). The fraction of compromised measurements, i.e., $\rho = \kappa/M$ is used to analyze the attack detection performance.

Secondly, the variance of false measurement data injected to the system determines the deviation from normal measurements. Although the value of $\mathbf{a}$ does not change the residual in (40), it affects the sample distance in (46) that will results in different detection performance. Specifically, we defined this factor α as a scale factor of the false data variances defined above, i.e., $\sigma_{\mathbf{a}}^2$ in the direct FDI attack or $\sigma_{\mathbf{c}}^2$ in the stealth FDI attack.

6.4.3 Performance Metrics

Let $\hat{y}_i$ and y_i be the predicted and actual class of a measurement sample $\mathbf{s}_i$, respectively. Let TP, TN, FP, FN be the true positive, true negative, false positive and false negative of the detection. If the data samples are balanced, i.e., there are equal number of positive and negative samples in the training data, the performance is evaluated by the detection accuracy Acc:

$$Acc = \frac{|TP| + |TN|}{|TP| + |TN| + |FP| + |FN|} \tag{62}$$

If the data samples are imbalanced, e.g., the number of negative samples is significantly greater or less than the number of positive samples, then the F_1 score is used to

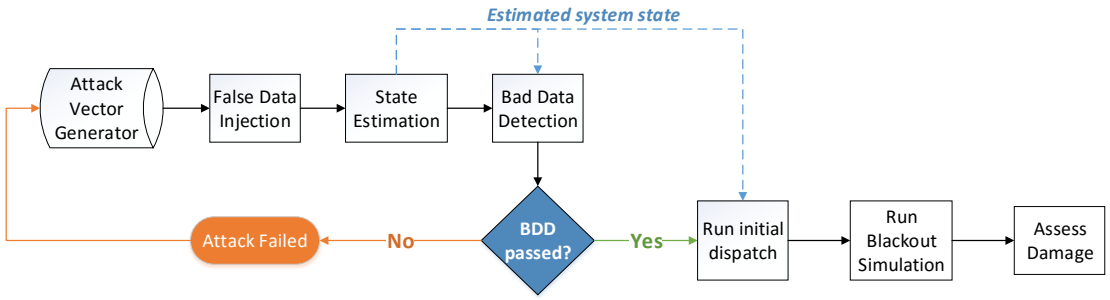


Figure 33. Flowchart of false data injection assessment. The dashed line indicates data flow.

evaluate the detection performance:

$$F_1 = \frac{2|TP|}{2|TP| + |FP| + |FN|} \tag{63}$$

The detection performance will be evaluated against different values of A and P to test the robustness under various attack strength in practice.

6.5 Simulations

6.5.1 Simulation Setup

Simulation Setup for Resilience Analysis

Figure 33 shows the flowchart of the simulation procedure. The IEEE 300-bus system with $n = 600$ states is used as the benchmark. Excluding measurements on generation and zero-injection buses, there are $m = 2,184$ measurements subject to FDI. The benchmark is configured to be $N - 1$ secured with no voltage violations nor overloading from any single line outage. The total load demand is fixed as a short-term consideration. For each α and ρ , $1,000$ random false state attack vectors $\mathbf{c}$ are generated from uniform distributions $U(a, b)$, where the boundaries (a, b) are $(-10°, +10°)$ for angles and $(-0.1\ p.u., +0.1\ p.u.)$ for magnitudes, respectively.

The false data in (42) are injected at $t = 0$ and cleared after a typical SCADA sampling interval, at $t = 15s$. α and ρ are evaluated with 50 values in the logarithmic interval $[10^{-4}, 1]$ and 40 values in the linear interval $[0.1, 1]$, respectively. The state estimation and bad data detection are both simulated in the MATPOWER toolbox [60].

The maximal number of Newton iterations and bad data are 10 and 50, respectively. The simulation starts with responses to the manipulated measurements and reports results at the end of blackout simulation.

Simulation Setup for Learning-Based Detectors

We choose the IEEE 30-bus test system as the benchmark [194]. There are 30 buses and 41 branches with a total load demand of 189.2 MW. A total of $M = 284$ measurements are used to estimate $N = 60$ state variables. A one-line diagram of this system is shown in Figure 34. The measurements include four sets of measurements: the bus voltages angles and magnitudes, the bus injected active and reactive power, the branch active and reactive power injection at the from-end, and the branch active and reactive power withdrawal at the to-end. The AC system states to be estimated are the bus voltages angles and magnitudes.

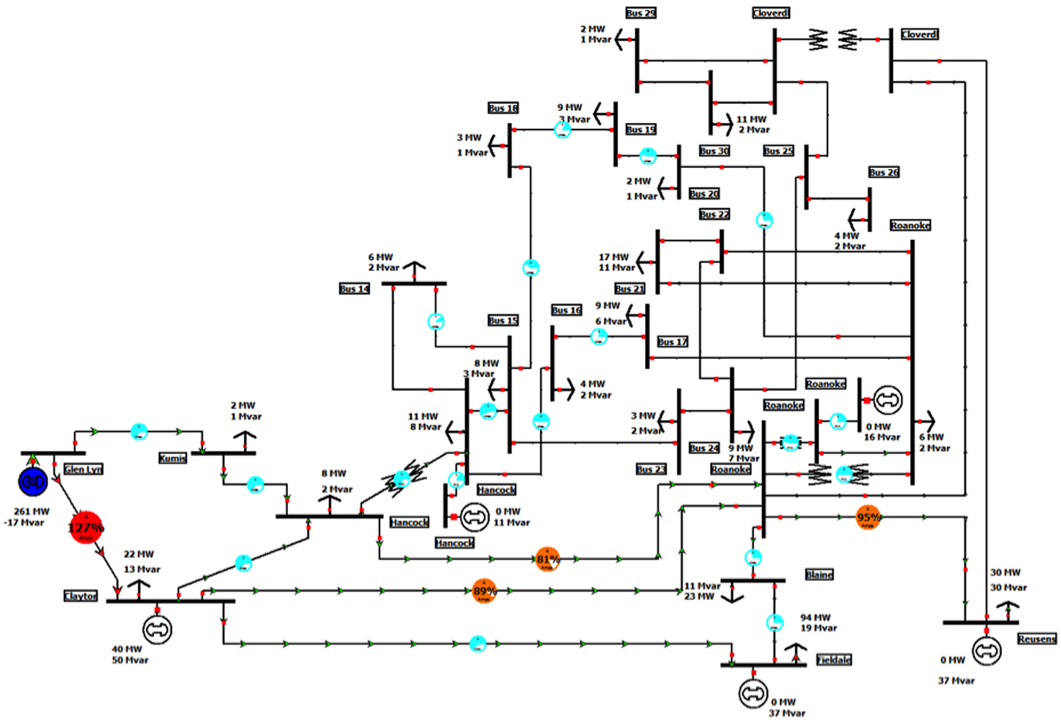


Figure 34. The IEEE 30-bus test system.

For the simulation, $1,000$ steady-state operating points (OP) are first sampled from the 30-bus system. Each OP refers to a configuration of power grid topology with corresponding generation output and load demand. We consider the topology as a control variable and the 30-bus system is fully-connected in the investigation. The load demand may dynamically change; to keep the system balanced, the generation will also vary accordingly, thus each balanced configuration, combining generations and load demands at all buses with the given grid topology, forms a new OP. To consider the load demand variation, for each OP the total load demand are firstly randomly sampled from the range between 95% and 105% of the original benchmark. The corresponding bus generations and power flows are then obtained from AC optimal power flow (AC-OPF) solutions subjecting to minimal generation cost. Afterward, the measurements of each OP are collected with random measurement noise $\mathbf{n}$ added using the covariance $\mathbf{R}$ from the MATPOWER Toolbox [60]. The states are calculated by the AC state estimator, also provided in MATPOWER. These 1000 OP measurements are labeled as the normal (negative) samples with $y = -1$.

For the attack schemes, $1,000$ attacked (positive) samples labeled with $y = +1$ are also obtained. With each given value of P and A, each attack vector $\mathbf{a}$ is generated and added to the corresponding measurement $\mathbf{z}$. The false data variance for the direct and stealth FDI are given by $\sigma_{\mathbf{a}}^2 = 0.05$ and $\sigma_{\mathbf{c}}^2 = 0.05$, respectively. We consider three levels of A: $A = 0.1$ (small), $A = 1.0$ (medium), and $A = 10.0$ (large). The values of P is chosen between 0.05 to 1.00 with a step distance of 0.05.

To test the detection performance, we consider both balanced and imbalanced cases, where the number of normal data is either equal to (balanced) or much smaller than (imbalanced) the number of attacked data, respectively. In balanced case, all the 1000 attacked samples are used; for the imbalanced case, only 100 attacked samples are randomly picked. In either balanced or imbalanced scenario, half of the positive samples

and half of the negative samples are randomly chosen to form the training set detectors, while the other half are kept as the testing set. The reported detection performances below are obtained from the average of 100 independent experiments.

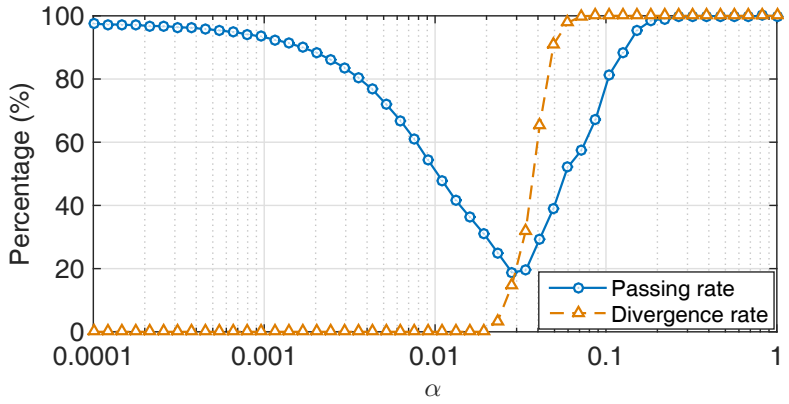
6.5.2 Resilience Analysis

The effectiveness of FDI attacks is first evaluated by the passing rate and divergence rate of FDI attacks. The passing rate is the percentage of FDI attack vectors that can pass the BDD and be accepted as part of trusted measurements. The divergence rate is the percentage of FDI attacks that will cause a diverged SE solution, indicating that the estimation has failed to converge after excessive removal of bad data, which renders the system unobservable [195]. To effectively analyze FDI stealthiness, the passing rate is measured only for FDI with a converged SE solution. Values of both rates are illustrated in Figure 35.

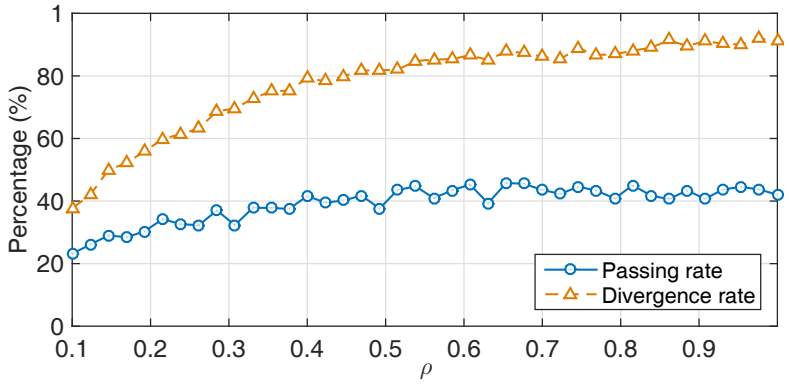
In Figure 35(a), both rates showed some patterns with the change of α. High passing rate and zero divergence rate were observed when $\alpha < 0.001$; high passing rate and high divergence rate were observed when $\alpha > 0.1$. For α between 0.001 and 0.1, the passing rate plunged below 20% at $\alpha \approx 0.03$ before returning to 100% after $\alpha > 0.2$; the divergence rate remains at zero when $\alpha \leq 0.01$ but surged to 100% after $\alpha \geq 0.05$. Without a converged SE solution, the manipulated measurements that passed BDD still would not cause any misinformed system response directly. The passing rate p was not 100% under small α because some attacked measurements would have been identified as bad data in an FDI-free case due to large measurement noise, and these measurements are rejected "accidentally".

Meanwhile, Figure 35(b) shows a different pattern for ρ, the percentage of measurements manipulated, with $\alpha = 0.05$ fixed. Both rates fluctuated with the increase of ρ. The passing rate increased from 23% to around 40%; more significantly, the divergence rate increased from 40 % to above 85%. Figure 35(b) suggested that manipulating

most measurements are not ideal if only random false data are injected. An effective FDI would be built with a proper choice of magnitude and severeness to achieve either high passing rate (stealthiness) or high divergence rate (damage).



(a)



(b)

Figure 35. Effectiveness of FDI attacks with (a) fixed $\rho = 1.0$ and (b) fixed $\alpha = 0.05$.

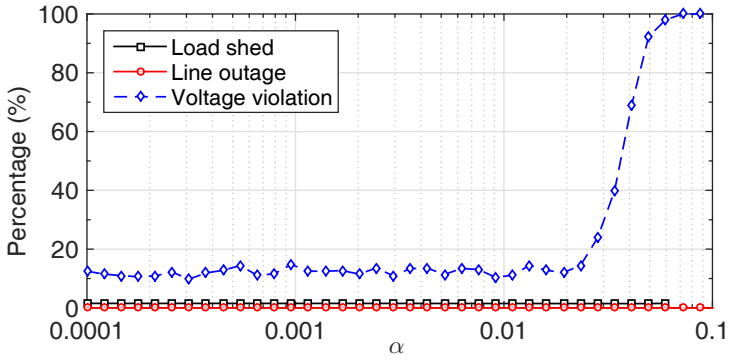
The grid resilience against both FDI attacks is shown in Figure 36. Figure 36(a) reports the percentage of load shedding, line outage, and voltage violation due to FDI attacks with a fixed severeness $\rho = 1.0$ but different magnitudes α. When $\alpha < 0.01$, the load shed (black) and line outage (red) fluctuated with little variances; their mean values were 1.5% and 0.02%, respectively. The voltage violation (blue) was in a higher

range, between 10% to 15%, partially because was assumed that attackers have no exact knowledge of bus voltages, leading to higher chance of voltage violations even under small attack magnitudes. However, as divergence rate surged to 100% when $\alpha > 0.05$ (see Figure 35(a)), the estimation could not return a valid state; voltage violations were observed for every FDI attack thereon. Further simulation thus requires the transient stability model and the steady-state simulator stopped reporting load shed or line outages thereafter. The maximal amount of re-dispatched generation active power, in response to any initial FDI, was less than 7 MWs. It was relatively small compared to the total generation capacity of 32,678.4 MWs. No major blackout was reported with greater than 10% load shed in the simulation. These observations suggested that the benchmark power grid yields resiliency against overloading, islanding and line tripping that are tied to blackouts under different magnitudes of FDI attacks. However, voltage stability is exposed to more risks when the attack magnitude is beyond a certain level.

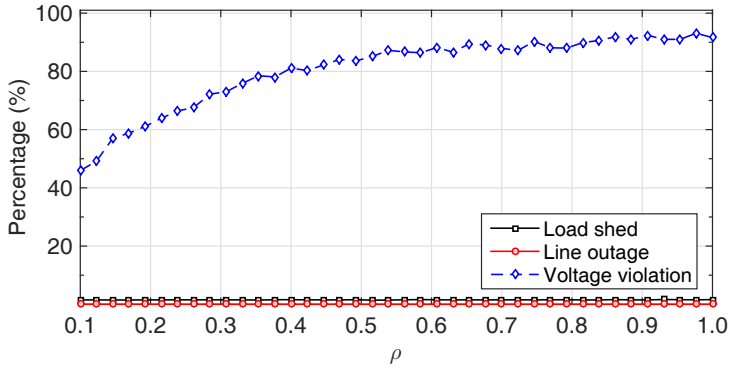
Figure 36(b) shows grid resilience with different values of ρ with fixed magnitude $\alpha = 0.05$. Both percentages of load shed and line outages were in a range similar to that in Figure 36(a); but voltage violation steadily increased from below 50% to 90% as ρ increased, consistent to the divergence rate in Figure 35(b). No major blackouts were reported. These observations suggested that although the passing and divergence rate both increased with ρ, the grid remained resilient to load shed and line outages; meanwhile, severe false data injections with increasing number of compromised measurements still posed threats to the voltage stability of the system.

6.5.3 Detection Performance

The detection accuracy of direct and stealth FDI attacks on balanced data are shown in Figure 37, under different values of A and P. The training performance are testing performance are shown in dashed and solid lines, respectively. From both figures, all three detectors yield over 80% accuracy for direct FDI attacks and over 85% accuracy



(a)



(b)

Figure 36. Grid resilience with different (a) magnitudes of FDI at $\rho = 1.0$, and (b) severeness of FDI at $\alpha = 0.05$.

for stealth FDI attacks.

For the direct FDI attack in Figure 37(a)–37(c), the detection accuracy increased with the attack strength for all three detectors. When A or P was increased, the SVM based detector achieved 100 % accuracy faster than the ENN and kNN based method. The kNN based detector outperformed ENN based detector when $A = 0.1$ or P was small, but the performance of the latter quickly improved as A was increased before both achieved 100% accuracy when P is sufficiently large. The detectors will be capable of identifying FDI attacks that are more likely to cause severe disturbances to the system.

For the stealth FDI attack in Figure 37(d)–37(f), the SVM-based detector showed

better accuracy with small attack strength A and P and was the only detector to achieve 100 % accuracy. The ENN based detector outperformed kNN based detector in most cases, though both failed to achieve 100 % accuracy under the direct FDI attack.

Particularly, it is notable that for $A = 0.10$, a critical range of P was observed during which the accuracy improved significantly with the increase of P: in Figure 37(a), the SVM testing accuracy increases from 91% to 100% when $0.3 \leq P \leq 0.5$; similar patterns are observed for kNN and ENN testing accuracy when $0.5 \leq P \leq 0.8$. Such pattern is also found for $0.05 \leq P \leq 0.2$ in Figure 37(d). The improved accuracy with a greater attack strength P is caused by more distinguishable samples due to the increase of distance d_{ij}.

The detection performance (F_1 score) with imbalanced data are shown in Figure 38 of the stealth FDI, respectively. The SVM-based detector still exhibited superior overall performance, and all detectors achieved optimal performance when A and P are sufficiently large. Meanwhile, a similar pattern of performance change in the critical range of P has also been observed. Sensitivity analysis on how the individual factors in the performance metrics, i.e., $|TP|$, $|TN|$, $|FP|$, and $|FN|$, were affected by the attack schemes will be featured in the future work for improvement of the proposed supervised learning based detectors.

6.6 Chapter Summary

This chapter presented a two-part study consisting of a resilience analysis of false data injection attacks on the power grid and a comparative study on the supervised learning-based detection against FDI threats. The resilience analysis provided a preliminary result to evaluate power grid resilience against FDI attacks considering the impact of the magnitudes and number of attacked measurements. With a dedicated AC power flow based simulator, the system responses considering the potential development of cascading blackouts have been simulated and investigated. From the simulation

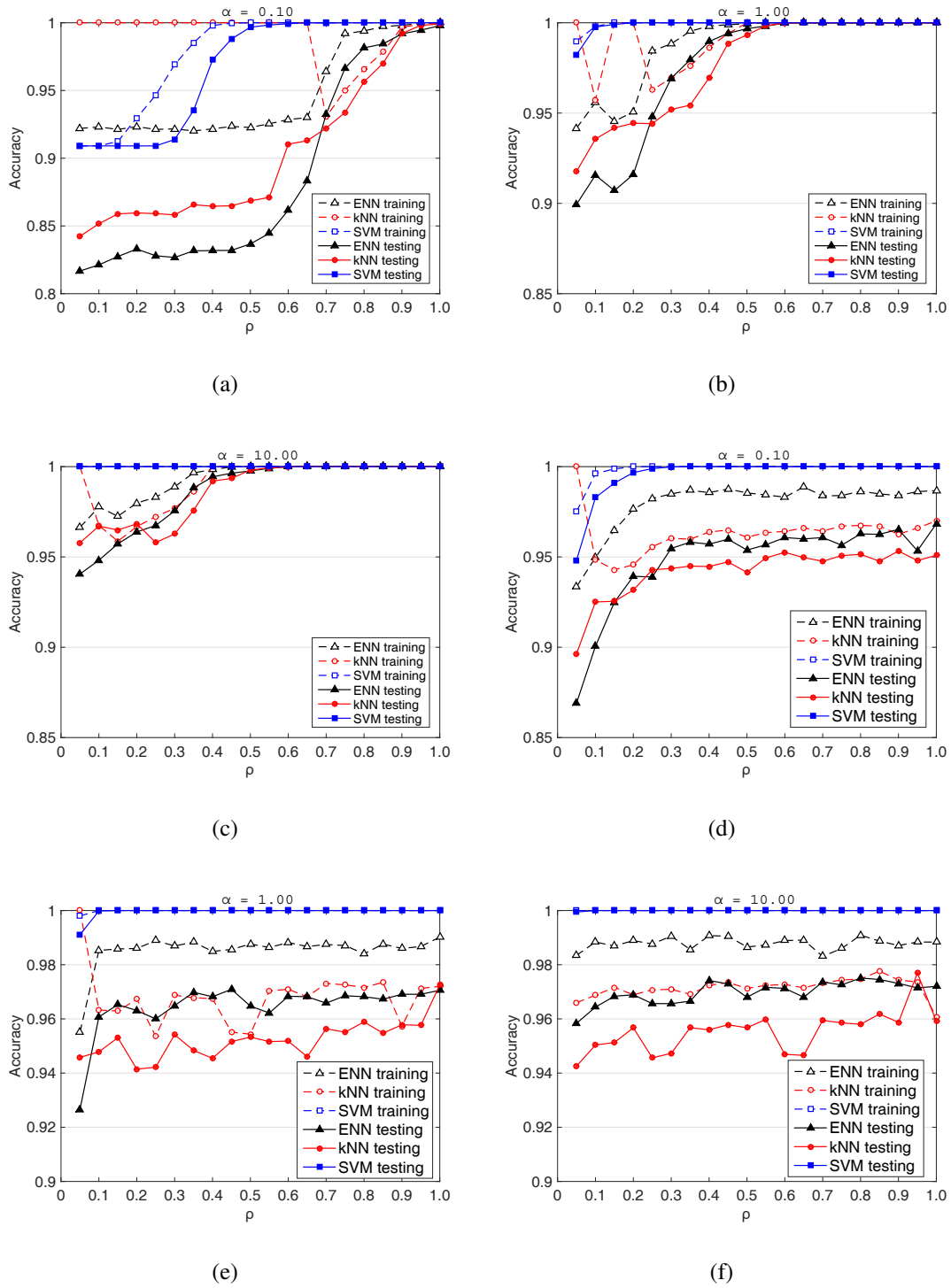


Figure 37. Detection accuracy on balanced data: (a) $\alpha = 0.1$, (b) $\alpha = 1.0$, and (c) $\alpha = 10.0$ in direct FDI attacks; (d) $\alpha = 0.1$, (e) $\alpha = 1.0$, and (f) $\alpha = 10.0$ in stealth FDI attacks.

results, the FDI attack showed less threat in creating line overloading or outages to trigger massive blackouts through cascading failures. However, voltage violations can be frequently triggered even with a moderate magnitude or severeness of false data. The resilience analysis is expected to facilitate a better understanding of FDI attack impacts in the context of cascading blackouts.

The comparative study investigated supervised learning based classifiers in the detection of false data injection in the smart grid. Following the conversion of false data detection to binary classification, the learning based detectors exhibited satisfactory performance, which is promising for the stealth false data injection that can bypass traditional residual-based bad data detection. The three detector designs of choice achieved optimal detection performance against attacks that would cause major disturbances with large amount or magnitude of false measurements.

In practice, the learning based false data classifiers can be implemented as an effective secondary or auxiliary detector to the residual based bad data detectors, identifying false data after the bad data have been removed by LNR test. However, for each measurement, the potential number of bad data is not a constant, which will leave missing features in the data samples. Robust classifiers that can handle such missing features can significantly improve the practical value of learning base false detectors. In practice, it is also beneficial to combine the bad data and false data detectors as a single integrated system. In addition, the learning based detectors can be improved to not only detect the presence of false data but also locate each individual false data in the measurements. Lastly, the run-time performance and cost analysis of these learning based detectors should also be further investigated for real-world implementations.

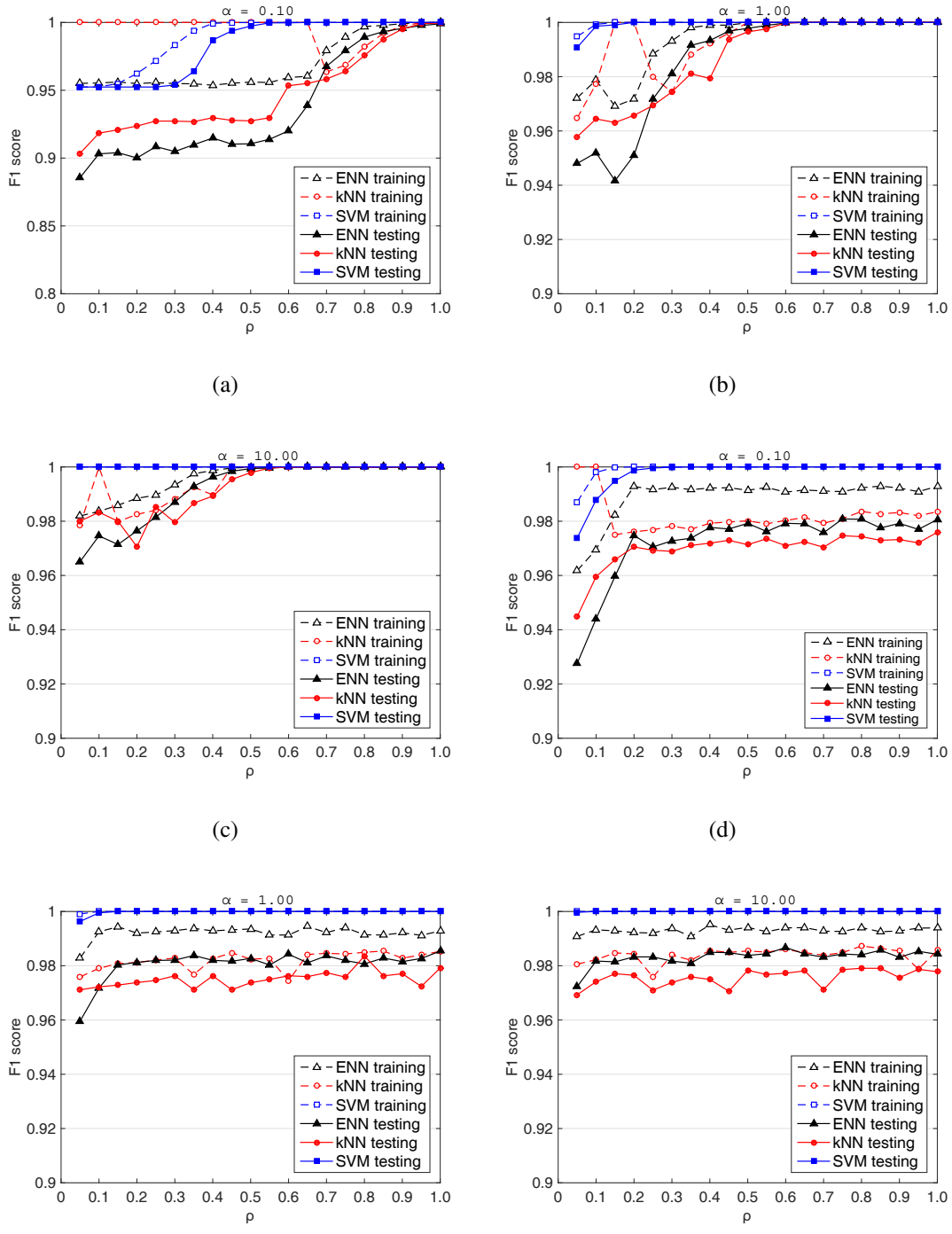


Figure 38. F_1 score on imbalanced data: (a) $\alpha = 0.1$, (b) $\alpha = 1.0$, and (c) $\alpha = 10.0$ in direct FDI attacks; (d) $\alpha = 0.1$, (e) $\alpha = 1.0$, and (f) $\alpha = 10.0$ in stealth FDI attacks.

CHAPTER 7

Conclusions

7.1 Summary of the Dissertation

The smart grid is a vital upgrade of the electrical power infrastructure. Despite variations of systems and techniques adopted around the globe, the key feature of the smart grid, i.e., cyber-physical integration of physical systems and processes with information and communication technologies, brings both promises as well as perils to the power and energy infrastructure. It is of paramount importance to secure the grid in both physical and cyber space for the delivery of electricity that supports our modern society.

The research presented in this dissertation systematically investigated the cyber-physical security of smart grid on the topic of massive cascading blackouts. The research is composed of the vulnerability analysis of cascading blackouts and the identification of critical components and processes that could be exploited by informed attackers. The goal of this research is to advance the understanding of smart grid security and resilience against major blackouts with the increasing cyber-physical integration, with which critical risks can be better identified and critical assets better protected. The contribution of the research is twofold:

First, the vulnerability analysis of cascading blackouts models the spatial-temporal cascading process from operational and structural perspectives. Investigations focused on the major factors that contribute to the propagation of failures due to the dynamic power flows and the static grid topology and established simulation platforms to evaluate the vulnerability under different scenarios.

In the operational vulnerability analysis, the research examined the power flow based cascading in power transmission systems after an initial contingency that trips substations or lines in the grid. A power flow based cascading failure model was established to simulate and evaluate steady-state system responses and failure mechanisms

that contribute to a massive cascade of failures. The investigation analyzed the influence of direct tripping, emergency response, and cascading failures as three major factors in the development of blackouts, and the cascades from overloading and hidden failures play a major role in the creation of major blackouts. Based on further comparison with detailed transient stability analysis, the concept of critical moments was proposed to assess the consistency between steady-state and transient stability analyses in approximating the system behavior during cascading blackouts. The investigations are expected to help grid operators establish an efficient warning system at the early stage of a cascade. The cascading failure model will also serve as a simulation platform to validate further structural vulnerability analysis and the impact of potential cascade-initiating attacks.

In the structural vulnerability analysis, we focused on how the power grid topology and electrical properties could reveal information of inherent vulnerabilities in the structure of interconnected power systems. A complex network model based on betweenness centrality that incorporated the power flow distribution factor (PTDF) was established to analyze the critical components in the structure of the grid. The research proposed the use of the total loss of the extended betweenness as the index of vulnerability and compared the metric against classic topology-based metrics. The simulation results revealed that the structural information, combining the topology of grid interconnection and the electrical property of power flows, can be used to identify the critical substations and transmission line in the grid. Such vulnerability is determined by the grid topology, the line flow sensitivity, and the rated capacity that are independent of the real-time system dynamics and operation. The results demonstrated that the structural information from the extended betweenness better revealed the information of critical components in the grid, which can assist the resilience enhancement in the planning and upgrade of transmission systems. In addition, the results also highlighted the potential risks even when

attackers have only limited structural information of the grid.

Second, the research identifies and analyzes potential attack schemes that can target the critical components to initiate a cascading blackout. The investigations focused on how the system information can be exploited by attacks on control and measurement signals in the transmission system and utilized advanced machine learning techniques to identify the critical targets efficiently and adaptively.

For attacks on control signals, the investigation analyzed two coordinated schemes on transmission substations and lines: the concurrent attack and the sequential attack. For the concurrent attack, the research proposed a self-organizing map based strategy that was able to identify low-ranking but high-risk components unknown to traditional contingency ranking. Simulation results demonstrated that the most vulnerable components from the self-organized clusters produce critical attack vectors that may bring down bulk grids like the Texas grid. For the sequential attack, the research proposed a Q-learning based strategy to adaptively identify critical attack sequences that exploit consecutive tripping to initiate cascades and maximize blackouts. The proposed Q-learning strategy was able to effectively identify critical sequences that lead to critical system failures across simulations on multiple benchmarks. The investigations on the concurrent and sequential attack schemes aim to develop advanced adaptive tools for penetration tests while raising operator's awareness against prominent cyber-attack threats on the industrial control systems.

For attacks on the measurements, the research evaluated the grid resilience against the false data injection attacks targeting the state estimators and developed supervised learning-based detection against the prominent attack threats. By evaluating the potential size of blackouts, the number of line outages and the violations of bus voltages, the resilience analysis revealed the system tolerance against the false data undetectable by residual-based bad data detectors. The results indicated that the grid might be able to

remain robust against the false data in terms of the size of load loss and the number of line outages that the attack may trigger. However, the number of false voltage violation alarms raised by the false data injection can still pose a threat to reliable system operation. To provide an early detection of the false data, the research developed supervised learning based approaches that utilized support vector machines and nearest neighborhood-based binary classifiers for light-weight detection under both balanced and imbalanced cases. Simulations revealed that the learning-based detectors effectively superior performance against the strong false data injection attacks.

In conclusion, the dissertation investigated the smart grid vulnerability in cascading blackouts through operational and structural analyses and identified schemes that could generate critical attack vectors on both controls and measurements to initiate a cascading blackout. The simulation results demonstrated the impacts of malicious cyber-physical attacks on the grid and the challenges that infrastructure would face during the cyber-physical integration, and the work hopes to improve our awareness, preparedness, and responses against catastrophic consequence against the catastrophic events.

7.2 Challenges and Opportunities

There are significant research directions and opportunities following the work presented in this dissertation. First, the power systems are increasingly complicated and advanced modeling of the grid structures and behaviors are under growing need. Hardware-in-the-loop co-simulation of cyber-physical systems in the grid can provide abundant detailed and accurate information for vulnerability assessment, attack analysis, and defense response. In addition, the inclusion of communication and computation modules in the security analysis will be critical: it will not only help identify feasible and impactful schemes that would pose practical threats to the system but also advise on effective resource allocation and emergency responses against the high-risk threats. Considerations of industrial devices, protocols, and policies in-use will contribute to

the establishment of early, accurate defense against the major threats at the stages of evaluation, prevention, detection, mitigation, and restoration.

Among the major challenges and opportunities along this prominent direction, this dissertation would like to highlight three critical topics pertinent to the future work following this dissertation:

7.2.1 Infrastructure Interdependence

Interdependence plays an increasing yet critical role in smart grid security, whose influences reach not only across the cyber and physical layers but also beyond the energy sector. Between the cyber and physical systems, not only will the physical operations rely on trustworthy computation and communication; the cyber operations are also contingent upon reliable electricity supply from the physical grid. Also, between the energy and other sectors, we should be vigilant that the availability of electrical power relies on proactive mining, transportation, and coordination, while the availability itself has a far-reaching impact on other sectors including food, water, transportation, communication, and healthcare, among others.

In the first regard, cyber-physical attack analysis shall extend beyond traditional cyber attacks on physical systems [6]. Physical sabotages targeting cyber systems and security have been less investigated, yet the threats can be nevertheless devastating when the dependence of electricity is exploited. Most cyber systems and security mechanisms have assumed the availability and reliability of electrical power to operate designated electronic devices. Under physical attacks, these devices can be damaged or disabled by intentional surges and outages of electricity. Such vulnerabilities should also be integrated into the investigation of the cyber-physical security in the smart grid. In addition, it should also be noted that the cyber-physical interdependence may be exploited recurrently and interactively by complex intrigue schemes. Assuming an attacker had successfully triggered a power outage: during this outage, the security mechanism on

some critical field devices can be compromised, following which parameters and data stored therein may be manipulated. Once the power has been restored, the attacker can either utilize the compromised device to access more information from the cyberspace or induce further damages into the physical system. To date, there are still limited investigations into interactive schemes like this, which repeatedly exploit the vulnerability of the cyber-physical interdependence.

In addition, the smart grid itself is a heterogeneous network of interdependent and interoperating systems, where numerous CPSs are being developed and deployed for the future. The vulnerability of the entire grid, meanwhile, will be determined by the weak components among them. Various subsystems, includeing wind farms [196], energy storages [197, 198], electric vehicles [199], renewable energy systems [200], microgrids [201, 202], distributed energy systems [203], PMUs [124], AMI [204], among others, require careful scrutinization of cyber-physical security when integrated and operated in the smart grid.

Moreover, the interdependence also exists beyond the smart grid. Through both cyber and physical interconnections, the smart grid can be vulnerable to attacks on its dependent infrastructures as well as casting vulnerability onto these infrastructures. A large number of critical infrastructures are also vulnerable to cyber-physical attacks on the smart grid, as illustrated in Figure 39. While some early work has looked into the problem [205, 206, 207] and agencies like the U.S. National Science Foundation (NSF) has established programs such as the Critical Resilient Interdependent Infrastructure Systems and Processes (CRISP), investigations on cross-infrastructure interdependence have largely remained to be conducted.

7.2.2 Imperfect Attacks

Investigations of cyber-physical attack threats are often conducted in the worst case scenario to fully understand their impacts. Assumptions of the worst case usually in-

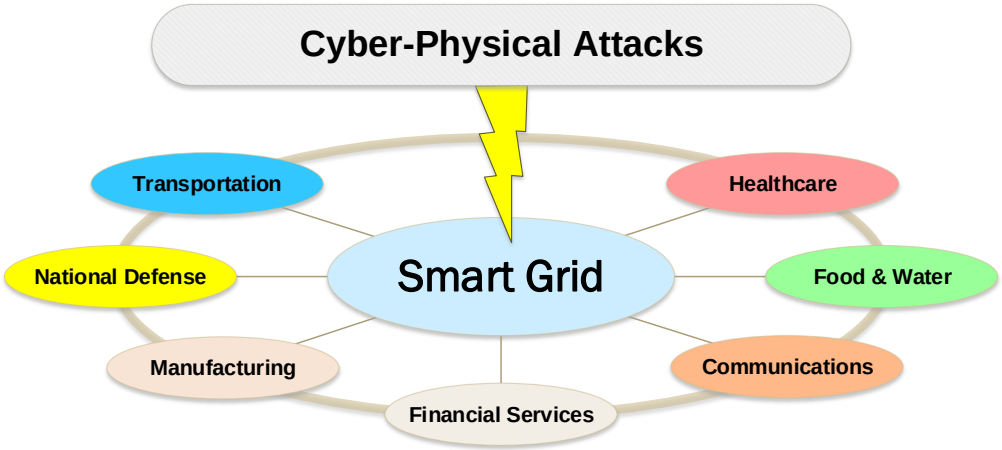


Figure 39. Example of interdependent sectors vulnerable to cyber-physical attacks on the smart grid.

clude the full access of resource, knowledge, and/or control of the system as well as a well-defined intention of the attack objective. These "perfect attacks" are crucial to reveal the maximal damages an attacker may induce in the system.

Meanwhile, for practical and usable security, it is also an essential task to investigate the imperfect attacks, which will include scenarios where attackers have limited information, resource, or time-window to perform a sophisticated attack. Along this direction, the information of the power system can be better categorized and classified to accurately assess the level of risks and impacts based on the type and level of information accessed by the attacker. The resources of an attack should also be identified, which may include the computational power, the communication channels, as well as the domain expertise that would lead to a feasible and impactful attack. This will enable better monitoring and protection of critical assets. The time-window, including both the time to penetrate a system, the timing of an attack, as well as the duration that attack signals are present will also have significant impacts on the actual risks. These factors will warrant further investigation to understand the attack threats on a full spectrum, allowing grid operators to react promptly and properly to feasible threats in real-world

scenarios.

Furthermore, as the cyber-physical integration continues, the exposure and vulnerability of critical systems and processes will also reveal new zero-day threats in the grid. It is therefore important to roll out penetration tests at all levels to identify new vulnerabilities that even an ill-informed attacker could exploit. Due to the complexity of cyber-physical interdependence and interactions in the smart grid, it is becoming increasingly challenging to enumerate and evaluate attack surface, path, and schemes. However, thanks to the development of machine intelligence, it is possible to combine human expertise and intelligent algorithms to develop adaptive and automatic pen-tests that can self-screen and identify threats unforeseen or unnoticed in complex systems in the grid.

7.2.3 Attack-Resilience

In the real world, it is hardly possible to enumerate or eliminate all potential attack threats for a perfectly secured smart grid [208]. Therefore, attack-resilience should be integrated against the permanent presence and evolution of threats, for both blackouts and beyond. On one hand, additional security features and mechanisms against the most significant attack threats should be established as a core for the measurement and control of cyber-physical power and energy systems. Meanwhile, the costs of attack-resilient designs should be balanced with the risks of feasible attacks, so that a proper trade-off between economic concerns and security impacts can be achieved. Meanwhile, we should be aware that the development and deployment of advanced and distributed intelligence are double-edged: the intelligent systems will become both targets of cyber-physical attacks as well as tools to defend against them. Overall, security analysis should integrate the impacts of the latest development in generation [209], transmission [112], and distribution systems [210, 211] of the smart grid, enhance their resilience against potential attacks, and utilize their potentials to assure the delivery of electricity in the

21st century.

Beyond the technical considerations, the smart grid is a critical infrastructure that involves organizations and individuals in both private and public sectors. From high-level regulations and policies to individual awareness and practice, human factors should be inclusive throughout the design, implementation, and restoration of a secure and smart grid. While the grid is becoming more and more automatic and intelligent, there should always be sufficient "room" left for manual supervision, intervention, and optimization. Across security stages of prevention, evaluation, detection, mitigation, and restoration, security designs shall keep human in the loop to enhance both attack awareness and attack resilience of the smart grid.

LIST OF REFERENCES

[1] T. Overbye and J. Weber, "Visualizing the electric grid," *IEEE Spectrum*, vol. 38, no. 2, pp. 52–58, 2001.

[2] National Institute of Standards and Technologies (NIST), "Framework and roadmap for smart grid interoperability standards - release v3.0," National Institute of Standards and Technologies (NIST), Tech. Rep., 2014, accessed on May 1, 2017. [Online]. Available: http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf

[3] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, 2011.

[4] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid – the new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[5] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 5–20, 2013.

[6] H. He and J. Yan, "Cyber-physicalhysical attacks and defences in the smart grid: A survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, pp. 13–27, December 2016.

[7] U.S. Energy Information Administration. U.S. Department of Energy. "Electric power monthly." Accessed on February 28, 2017. February 2017. [Online]. Available: https://www.eia.gov/electricity/monthly/

[8] U.S. Energy Information Administration. U.S. Department of Energy. "Short-term energy outlook." Accessed on March 7, 2017. March 2017. [Online]. Available: https://www.eia.gov/outlooks/steo/report/

[9] Edison Electric Institute. "Transmission projects: At a glance." Accessed on April 13, 2017. December 2016. [Online]. Available: http://www.eei.org/issuesandpolicy/transmission/Documents/Trans_Project_lowres_bookmarked.pdf

[10] J. E. Dagle, "The north american synchrophasor initiative (NASPI)," in *IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2010, pp. 1–3.

[11] J. Bertsch, C. Carnal, D. Karlson, J. McDaniel, and K. Vu, "Wide-area protection and power system utilization," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 997–1003, May 2005.

[12] M. Govindarasu, A. Hann, and P. Sauer, "Cyber-physical systems security for smart grid," Power Systems Engineering Research Center, Tech. Rep., Feb. 2012, accessed on March 27, 2017.

[13] K. Morison, L. Wang, and P. Kundur, "Power system security assessment," *IEEE Power and Energy Magazine*, vol. 2, no. 5, pp. 30–39, Sept 2004.

[14] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57–64, June 2010.

[15] H. Jiayi, J. Chuanwen, and X. Rong, "A review on distributed energy resources and microgrid," *Renewable and Sustainable Energy Reviews*, vol. 12, no. 9, pp. 2472 – 2483, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032107001025

[16] W. Pentland. Forbes. "FBI, joint terrorism task force arrest suspect in arkansas power grid attacks." Accessed on March 27, 2017. October 14 2013. [Online]. Available: http://www.forbes.com/sites/williampentland/2013/10/14/fbi-joint-terrorism-task-force-arrest-suspect-in-arkansas-power-grid-attacks/

[17] R. Smith. "Assault on california power station raises alarm on potential for terrorism." Accessed on May 1, 2017. February 5 2014. [Online]. Available: http://www.wsj.com/news/articles/SB10001424052702304851104579359141941621778

[18] S. Masood. NY Times. "Rebels tied to blackout across most of pakistan." Accessed on May 7, 2015. January 25, 2015. [Online]. Available: http://www.nytimes.com/2015/01/26/world/asia/widespread-blackout-in-pakistan-deals-another-blow-to-government.html

[19] T. M. Chen, "Stuxnet, the real start of cyber warfare? [editor's note]," *IEEE Network*, vol. 24, no. 6, pp. 2–3, 2010.

[20] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–1, 2016.

[21] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb 2017.

[22] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[23] P. Kundur, N. J. Balu, and M. G. Lauby, *Power System Stability and Control*. McGraw-hill New York, 1994, vol. 7.

[24] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and classification of power system stability IEEE/cigre joint task force on stability terms and definitions," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, August 2004.

[25] North American Electric Reliability Corporation. North American Electric Reliability Corporation. "Reliability assessment guidebook." Accessed on April 10, 2017. December 2012. [Online]. Available: http://www.nerc.com/comm/PC/Reliability%20Assessment%20Subcommittee%20RAS%20DL/Reliability%20Assessment%20Guidebook/Reliability%20Assessment%20Guidebook%203%201%20Final.pdf

[26] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Tech. Rep., 2004, accessed on April 20, 2017. [Online]. Available: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

[27] P. K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "Network vulnerability to single, multiple, and probabilistic physical attacks," in *Military Communications Conference*, San Jose, CA, USA, Oct. 2010.

[28] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). "Cyber-attack against ukrainian critical infrastructure." Accessed on April 3, 2017. February 25 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[29] National Institute of Standards and Technologies (NIST), "Guidelines for smart grid cybersecurity," Tech. Rep., 2014, accessed on May 3, 2017. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.7628r1

[30] Wikipedia. "List of major power outages." Accessed on March 21, 2017. [Online]. Available: https://en.wikipedia.org/wiki/List_of_major_power_outages

[31] P. Hines, J. Apt, and S. Talukdar, "Large blackouts in North America: Historical trends and policy implications," *Energy Policy*, vol. 37, no. 12, pp. 5249–5259, 2009.

[32] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Part I - overview of methodologies," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2011, pp. 1–10.

[33] M. Papic, K. Bell, Y. Chen, I. Dobson, L. Fonte, E. Haq, P. Hines, D. Kirschen, X. Luo, S. Miller, N. Samaan, M. Vaiman, M. Varghese, and P. Zhang, "Survey of tools for risk assessment of cascading outages," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2011, pp. 1–9.

[34] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[35] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. W. Geem, "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, no. 9, pp. 9211–9265, 2015.

[36] R. Albert, H. Jeong, and A. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[37] Y.-C. Lai, A. Motter, and T. Nishikawa, "Attacks and cascades in complex networks," in *Complex Networks*, ser. Lecture Notes in Physics, E. Ben-Naim, H. Frauenfelder, and Z. Toroczkai, Eds. Springer Berlin Heidelberg, 2004, vol. 650, pp. 299–310.

[38] P. Crucitti, V. Latora, and M. Mar.iori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, p. 045104, Apr. 2004.

[39] S. Poudel, Z. Ni, and W. Sun, "Electrical distance approach for searching vulnerable branches during contingencies," *IEEE Transactions on Smart Grid*, 2017, in press.

[40] S. Poudel, Z. Ni, X. Zhong, and H. He, "Comparative studies of power grid security with network connectivity and power flow information using unsupervised learning," in *International Joint Conference on Neural Networks (IJCNN)*, July 2016, pp. 2730–2737.

[41] S. Poudel, Z. Ni, T. M. Hansen, and R. Tonkoski, "Cascading failures and transient stability experiment analysis in power grid security," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, September 2016, pp. 1–5.

[42] C. Davis and T. Overbye, "Multiple element contingency screening," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1294–1301, Aug. 2011.

[43] Q. Chen and J. McCalley, "Identifying high risk n-k contingencies for online security assessment," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 823–834, May 2005.

[44] C. Rocco, J. Ramirez-Marquez, D. Salazar, and C. Yajure, "Assessing the vulnerability of a power system through a multiple objective contingency screening approach," *IEEE Transactions on Reliability*, vol. 60, no. 2, pp. 394–403, 2011.

[45] M. J. Eppstein and P. D. Hines, "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698–1705, 2012.

[46] P. Rezaei, P. Hines, and M. Eppstein, "Estimating cascading failure risk with random chemistry," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2726–2735, September 2015.

[47] C. Long, D. You, J. Hu, G. Wang, and M. Dong, "Quick and effective multiple contingency screening algorithm based on long-tailed distribution," *IET Generation, Transmission & Distribution*, vol. 10, pp. 257–262(5), January 2016.

[48] P. Kaplunovich and K. Turitsyn, "Fast and reliable screening of n-2 contingencies," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4243–4252, Nov 2016.

[49] H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9 – 22, 2017.

[50] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "An initial model for complex dynamics in electric power system blackouts," in *Hawaii International Conference on System Sciences (HICSS)*, Jan 2001, pp. 710–718.

[51] S. Mei, F. He, X. Zhang, S. Wu, and G. Wang, "An improved opa model and blackout risk assessment," *IEEE Transactions on Power Systems*, vol. 24, no. 2, pp. 814–823, 2009.

[52] J. Qi and S. Mei, "Blackout model considering slow process and SOC analysis," in *IEEE Power and Energy Society General Meeting (PESGM)*, 2012, pp. 1–6.

[53] B. Carreras, D. Newman, I. Dobson, and A. Poole, "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Transactions on Circuits and Systems I: Regular Papers,*, vol. 51, no. 9, pp. 1733–1740, 2004.

[54] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 2, p. 026103, 2007.

[55] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, "Critical points and transitions in an electric power transmission model for cascading failure blackouts," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 12, no. 4, pp. 985–994, 2002.

[56] M. A. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, "Value of security: modeling time-dependent phenomena and weather conditions," *IEEE Transactions on Power Systems*, vol. 17, no. 3, pp. 543–548, Aug 2002.

[57] D. Kirschen, D. Jayaweera, D. Nedic, and R. Allan, "A probabilistic indicator of system stress," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1650–1657, 2004.

[58] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 01, pp. 15–32, 2005.

[59] B. Stott, J. Jardim, and O. Alsac, "DC power flow revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, 2009.

[60] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[61] R. Baldick, "Variation of distribution factors with loading," *IEEE Transactions on Power Systems*, vol. 18, no. 4, pp. 1316–1323, Nov 2003.

[62] D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt, "Model validation for the August 10, 1996 WSCC system outage," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 967–979, 1999.

[63] H. Ren, I. Dobson, and B. Carreras, "Long-term effect of the n-1 criterion on cascading line outages in an evolving power transmission grid," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 1217–1225, Aug. 2008.

[64] D. Bienstock, "Optimal adaptive control of cascading power grid failures," *ArXiv e-prints*, Dec. 2010.

[65] K. Turitsyn and P. Kaplunovich, "Fast algorithm for N-2 Contingency problem," in *Hawaii International Conference on System Sciences (HICSS)*, 2013, pp. 2161–2166.

[66] P. Kaplunovich and K. Turitsyn, "Statistical properties and classification of n-2 Contingencies in large scale power grids," in *Hawaii International Conference on System Sciences (HICSS)*, Jan. 2014, pp. 2517–2526.

[67] V. Donde, V. López, B. Lesieutre, A. Pinar, C. Yang, and J. Meza, "Severe multiple contingency screening in electric power systems," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 406–417, 2008.

[68] X. Wang, Y. Song, and M. Irving, *Modern Power Systems Analysis*. Springer, 2008.

[69] J. Yan, Y. Zhu, H. He, and Y. Sun, "Revealing temporal features of attacks against smart grid," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, Feb. 2013, pp. 1–6.

[70] Y. Zhu, J. Yan, Y. Sun, and H. He, "Risk-aware vulnerability analysis of electric grids from attacker's perspective," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, Feb. 2013, pp. 1–6.

[71] J. Arroyo and A. Conejo, "Modeling of start-up and shut-down power trajectories of thermal units," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1562–1568, 2004.

[72] F. Milano, "An open source power system analysis toolbox," *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1199–1206, 2005.

[73] M. Pai, *Energy Function Analysis for Power System Stability*. Springer, 1989.

[74] a. Karami and S. Esmaili, "Transient stability assessment of power systems described with detailed models using neural networks," *International Journal of Electrical Power & Energy Systems*, vol. 45, no. 1, pp. 279–292, 2013.

[75] B. Pal and B. Chaudhuri, *Robust Control in Power Systems*. Springer, 2005.

[76] R. Zarate-Minano, T. Van Cutsem, F. Milano, and A. Conejo, "Securing transient stability using time-domain simulations within an optimal power flow," *IEEE Transactions on Power Systems*, vol. 25, no. 1, pp. 243–253, Feb. 2010.

[77] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, Mar. 2014.

[78] J. Yan, Y. Yang, W. Wang, H. He, and Y. Sun, "An integrated visualization approach for smart grid attacks," in *Intelligent Control and Information Processing (ICICIP), 2012 Third International Conference on*, July 2012, pp. 277–283.

[79] H. Ren, X. Fan, D. Watts, and X. Lv, "Early warning mechanism for power system large cascading failures," in *IEEE International Conference on Power System Technology (POWERCON)*, 2012, pp. 1–6.

[80] M. Amin, "Energy infrastructure defense systems," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 861–875, 2005.

[81] Y. Mo, T.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[82] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," *Electronics*, vol. 5, no. 3, p. 40, 2016. [Online]. Available: http://www.mdpi.com/2079-9292/5/3/40

[83] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[84] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[85] M. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2013, pp. 1–5.

[86] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 905–912, May 2004.

[87] G. A. Pagani and M. Aiello, "The power grid as a complex network: A survey," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 11, pp. 2688–2700, 2013.

[88] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, no. 4, pp. 175–308, 2006.

[89] Y. Moreno, R. Pastor-Satorras, and A. Vespignani, "Epidemic outbreaks in complex heterogeneous networks," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 26, no. 4, pp. 521–529, 2002.

[90] S. Jonnavithula and R. Billinton, "Topological analysis in bulk power system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 12, no. 1, pp. 456–463, Feb. 1997.

[91] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E*, vol. 69, p. 025103, Feb. 2004.

[92] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, "Robustness of the European power grids under intentional attack," *Physical Review E*, vol. 77, no. 2, p. 026102, 2008.

[93] E. Cotilla-Sanchez, P. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the North American electric power infrastructure," *IEEE Systems Journal*, vol. PP, no. 99, p. 1, May 2012.

[94] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 20, no. 3, 2010.

[95] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Topological models and critical slowing down: Two approaches to power system blackout risk analysis," in *Hawaii International Conference on System Sciences (HICSS)*, 2011, pp. 1–10.

[96] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Generation, Transmission & Distribution*, vol. 4, no. 2, pp. 178–190, 2010.

[97] N. Fan, H. Xu, F. Pan, and P. Pardalos, "Economic analysis of the N-k power grid contingency selection and evaluation by graph algorithms and interdiction methods," *Energy Systems*, vol. 2, no. 3-4, pp. 313–324, 2011.

[98] R. Fitzmaurice, A. Keane, and M. O'Malley, "Effect of short-term risk-aversive dispatch on a complex system model for power systems," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 460–469, 2011.

[99] A. Scala, S. Pahwa, and C. Scoglio, "Cascade failures from distributed generation in power grids," *arXiv preprint arXiv:1209.3733*, 2012.

[100] Y. Koç, M. Warnier, R. E. Kooij, and F. M. Brazier, "An entropy-based metric to quantify the robustness of power grids against cascading failures," *Safety Science*, vol. 59, pp. 126–134, 2013.

[101] Z. Chen and C. Ji, "An information-theoretic view of network-aware malware attacks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 530–541, Sept. 2009.

[102] V. Fioriti, M. Sforna, and G. D'Agostino, "Spectral analysis of a real power network," *International Journal of Critical Infrastructures*, vol. 8, no. 4, pp. 354–367, 2012.

[103] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, pp. 481–487, 2012.

[104] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.

[105] E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks," *IET Generation, Transmission & Distribution*, vol. 4, no. 6, pp. 716–724, 2010.

[106] E. Bompard, M. Masera, R. Napoli, and F. Xue, "Assessment of structural vulnerability for power grids by network performance based on complex networks," *Critical Information Infrastructure Security*, pp. 144–154, 2009.

[107] W. Wang, Y. Sun, and H. He, "Topological analysis of cascading failures in bay area power grid," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2012, pp. 1–9.

[108] S. Blumsack, "Network topologies and transmission investment under electric-industry restructuring," Ph.D. dissertation, Carnegie Mellon University, 2006.

[109] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3274–3284, Dec 2014.

[110] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340–2354, Dec 2014.

[111] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Joint substation-transmission line vulnerability assessment against the smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1010–1024, 2015.

[112] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, "Smart transmission grid: Vision and framework," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 168–177, Sept 2010.

[113] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 200–210, Jan 2017.

[114] S. Sayyadipour, G. R. Yousefi, and M. A. Latify, "Mid-term vulnerability analysis of power systems under intentional attacks," *IET Generation, Transmission Distribution*, vol. 10, no. 15, pp. 3745–3755, 2016.

[115] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, 2017, in press.

[116] Y. Chen, J. Hong, and C. C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Transactions on Smart Grid*, 2017, in press.

[117] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[118] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, 2017, in press.

[119] J. Salmeron, K. Wood, and R. Baldick, "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Transactions on Power Systems*, vol. 24, no. 1, pp. 96–104, Feb 2009.

[120] A. Delgadillo, J. M. Arroyo, and N. Alguacil, "Analysis of electric grid interdiction with line switching," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 633–641, May 2010.

[121] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, p. 065102, 2002.

[122] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[123] J. Yan, Y. Tang, Y. Zhu, H. He, and Y. L. Sun, "Smart grid vulnerability under cascade-based sequential line-switching attacks," in *IEEE Global Communications Conference: Selected Areas in Communications: Smart Grid Communications (GC' 15 - SAC - Smart Grid Communications)*, San Diego, USA, Dec. 2015.

[124] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov 2015.

[125] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

[126] Z. Zhang, M. Trinkle, A. Dimitrovski, and H. Li, "Combating time synchronization attack: A cross layer defense mechanism," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, Apr. 2013, pp. 141–149.

[127] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1952–1973, September 2016.

[128] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *International Journal of Electrical Power and Energy Systems*, vol. 28, no. 9, pp. 627–633, 2006.

[129] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in u.s. power grid," in *IEEE Global Communications Conference (GLOBECOM)*, Dec. 2011, pp. 1–6.

[130] D. Newman, B. Carreras, V. Lynch, and I. Dobson, "Exploring complex systems aspects of blackout risk and mitigation," *IEEE Transactions on Reliability*, vol. 60, no. 1, pp. 134–143, Mar. 2011.

[131] Z. Wang, A. Scaglione, and R. Thomas, "The node degree distribution in power grid and its topology robustness under random and selective node removals," in *IEEE International Conference on Communications Workshops (ICC)*, 2010, pp. 1–5.

[132] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, 1989.

[133] R. Zurawski and M. Zhou, "Petri nets and industrial applications: A tutorial," *IEEE Transactions on Industrial Electronics*, vol. 41, no. 6, pp. 567–583, 1994.

[134] T. Chen, J. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec. 2011.

[135] V. Calderaro, C. Hadjicostis, A. Piccolo, and P. Siano, "Failure identification in smart grids based on petri net modeling," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 10, pp. 4613–4623, 2011.

[136] W. B. Knox and O. Mengshoel, "Diagnosis and reconfiguration using Bayesian networks: An electrical power system case study," in *IJCAI 2009 Workshop on Self-* and Autonomous Systems*, 2009.

[137] L. He, "Application of Bayesian network in power grid fault diagnosis," in *Natural Computation (ICNC), 2008 Fourth International Conference on*, vol. 1, Oct. 2008, pp. 61–64.

[138] Q. Shi, S. Liang, W. Fei, Y. Shi, and R. Shi, "Study on Bayesian network parameters learning of power system component fault diagnosis based on particle swarm optimization," *Intelnational Journal of Smart Grid and Clean Energy*, vol. 2, no. 1, pp. 132–137, 2013.

[139] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[140] M. Celenk, T. Conley, J. Willis, and J. Graham, "Predictive network anomaly detection and visualization," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 288–299, June 2010.

[141] X. Guan, T. Qin, W. Li, and P. Wang, "Dynamic feature analysis and measurement for large-scale network traffic monitoring," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 905–919, Dec. 2010.

[142] J. Vesanto and E. Alhoniemi, "Clustering of the self-organizing map," *IEEE Transactions on Neural Networks*, vol. 11, no. 3, pp. 586–600, May 2000.

[143] T. Kohonen, "The self-organizing map," *Proceedings of the IEEE*, vol. 78, no. 9, pp. 1464–1480, Sept. 1990.

[144] T. Kohonen, M. R. Schroeder, and T. S. Huang, *Self-Organizing Maps*, 3rd ed. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2001.

[145] S. Haykin, *Neural Networks: A Comprehensive Foundation*, 2nd ed. Prentice Hall, 1998.

[146] J. Vesanto. "SOM implementation in SOM toolbox." Accessed on May 1, 2017. [Online]. Available: http://www.cis.hut.fi/somtoolbox/documentation/somalg.shtml

[147] F. Bao, V. Lobo, and M. Painho, "Self-organizing maps as substitutes for k-means clustering," in *International Conference on Computational Science - Volume Part Iii*, ser. ICCS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 476–483.

[148] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 2013.

[149] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "The sequential attack against power grid networks," in *IEEE International Conference on Communications (ICC)*, June 2014, pp. 616–621.

[150] N. Fan, R. Chen, and J. P. Watson, "N-1-1 contingency-constrained optimal power flow by interdiction methods," in *IEEE Power and Energy Society General Meeting (PSEGM)*, July 2012, pp. 1–6.

[151] D. Silver, R. S. Sutton, and M. Müller, "Temporal-difference search in computer go," *Machine learning*, vol. 87, no. 2, pp. 183–219, 2012.

[152] D. Silver, A. Huang, C. J. Maddison, A. Guez, L. Sifre, G. Van Den Driessche, J. Schrittwieser, I. Antonoglou, V. Panneershelvam, M. Lanctot, *et al.*, "Mastering the game of go with deep neural networks and tree search," *Nature*, vol. 529, no. 7587, p. 484, 2016.

[153] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, and M. Riedmiller, "Playing atari with deep reinforcement learning," *arXiv preprint arXiv:1312.5602*, 2013.

[154] X. Guo, S. Singh, H. Lee, R. L. Lewis, and X. Wang, "Deep learning for real-time atari game play using offline monte-carlo tree search planning," in *Advances in neural information processing systems*, 2014, pp. 3338–3346.

[155] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski, *et al.*, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, p. 529, 2015.

[156] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[157] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.

[158] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The anatomy of a power grid blackout - root causes and dynamics of recent major blackouts," *IEEE Power and Energy Magazine*, vol. 4, no. 5, pp. 22–29, Sept 2006.

[159] R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction*. MIT press Cambridge, 1998, vol. 1, no. 1.

[160] C. J. C. H. Watkins, "Learning from delayed rewards," Ph.D. dissertation, King's College, Cambridge, 1989.

[161] J. Chen, J. S. Thorp, and I. Dobson, "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *International Journal of Electrical Power and Energy Systems*, vol. 27, no. 4, pp. 318–326, 2005.

[162] F. Li and R. Bo, "Small test systems for power system economic studies," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2010, pp. 1–4.

[163] Illinois Center for a Smarter Electric Grid (ICSEG). Information Trust Institute, University of Illinois at Urbana-Champaign. "IEEE 24-bus system." Accessed on May 1, 2017. [Online]. Available: http://publish.illinois.edu/smartergrid/ieee-24-bus-system/

[164] J. Yan, Y. Tang, B. Tang, H. He, and Y. Sun, "Power grid resilience against false data injection attacks," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[165] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, Aug 2016.

[166] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2010, pp. 220–225.

[167] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 7, pp. 1294–1305, July 2013.

[168] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306–1318, 2013.

[169] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 3153–3158.

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

[171] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information," *IEEE Transactions on Smart Grid*, 2017, in press.

[172] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, July 2014.

[173] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Transactions on Smart Grid*, 2017, in press.

[174] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2011, pp. 244–248.

[175] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," *IEEE Systems Journal*, pp. 1–11, 2017, in press.

[176] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2487–2497, 2015.

[177] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1592–1602, July 2016.

[178] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sept 2016.

[179] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 720–729, March 2017.

[180] L. Liu, M. Esmalifalak, and Z. Han, "Detection of false data injection in power grid exploiting low rank and sparsity," in *IEEE International Conference on Communications (ICC)*, June 2013, pp. 4461–4465.

[181] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, March 2014.

[182] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis," *IEEE Systems Journal*, vol. 10, no. 2, pp. 532–543, June 2016.

[183] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2014.

[184] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, 2017, in press.

[185] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010, pp. 327–332.

[186] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[187] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Transactions on Smart Grid*, 2017, in press.

[188] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, Feb 2017.

[189] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. CRC press, 2004.

[190] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, January 2015.

[191] B. Tang and H. He, "ENN: Extended nearest neighbor method for pattern recognition [research frontier]," *IEEE Computational Intelligence Magazine*, vol. 10, no. 3, pp. 52–60, 2015.

[192] J. H. Friedman, S. Steppel, and J. Tukey, *A nonparametric procedure for comparing multivariate point sets*. Stanford Linear Accelerator Center Computation Research Group Technical Memo, 1973, no. 153.

[193] P. Indyk and R. Motwani, "Approximate nearest neighbors: Towards removing the curse of dimensionality," in *ACM Symposium on Theory of Computing*. ACM, 1998, pp. 604–613.

[194] Illinois Center for a Smarter Electric Grid (ICSEG). Information Trust Institute, University of Illinois at Urbana-Champaign. "IEEE 30-bus system." Accessed on May 1, 2017. [Online]. Available: http://publish.illinois.edu/smartergrid/ieee-30-bus-system/

[195] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[196] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Transactions on Smart Grid*, pp. 1–15, 2017, in press.

[197] A. K. Farraj and D. Kundur, "On using energy storage systems in switching attacks that destabilize smart grid systems," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*. IEEE, 2015, pp. 1–5.

[198] C. P. Nguyen and A. J. Flueck, "Agent based restoration with distributed energy storage support in smart grids," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 1029–1038, 2012.

[199] Y. Tang, J. Yang, J. Yan, Z. Zeng, and H. He, "Frequency control using on-line learning method for island smart grid with EVs and PVs," in *International Joint Conference on Neural Networks (IJCNN)*, July 2014, pp. 1440–1446.

[200] M. Almassalkhi and I. Hiskens, "Model-predictive cascade mitigation in electric power systems with storage and renewables - part I: Theory and implementation," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 67–77, Jan. 2015.

[201] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, "Towards a cyber resilient and secure microgrid using software-defined networking," *IEEE Transactions on Smart Grid*, 2017, in press.

[202] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, Feb 2015, pp. 1–5.

[203] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proceedings of the IEEE*, pp. 1–22, 2017, in press.

[204] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 10, pp. 4746–4756, Oct 2013.

[205] S. Wang, L. Hong, X. Chen, J. Zhang, and Y. Yan, "Review of interdependent infrastructure systems vulnerability analysis," in *Intelligent Control and Information Processing (ICICIP), 2011 2nd International Conference on*, vol. 1. IEEE, 2011, pp. 446–451.

[206] S. Wang, L. Hong, and X. Chen, "Vulnerability analysis of interdependent infrastructure systems: A methodological framework," *Physica A: Statistical Mechanics and its applications*, vol. 391, no. 11, pp. 3323–3335, 2012.

[207] S. S. Shah and R. F. Babiceanu, "Resilience modeling and analysis of interdependent infrastructure systems," in *Systems and Information Engineering Design Symposium (SIEDS), 2015*. IEEE, 2015, pp. 154–158.

[208] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, pp. 1–19, 2017, in press.

[209] D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle, "Smart generation and transmission with coherent, real-time data," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 928–951, June 2011.

[210] R. H. Lasseter, "Smart distribution: Coupled microgrids," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1074–1082, 2011.

[211] R. F. Arritt and R. C. Dugan, "Distribution system analysis and the future smart grid," *IEEE Transactions on Industry Applications*, vol. 47, no. 6, pp. 2343–2350, 2011.

BIBLIOGRAPHY

Abur, A. and Exposito, A. G., *Power System State Estimation: Theory and Implementation*. CRC press, 2004.

Agarwal, P. K., Efrat, A., Ganjugunte, S., Hay, D., Sankararaman, S., and Zussman, G., "Network vulnerability to single, multiple, and probabilistic physical attacks," in *Military Communications Conference*, San Jose, CA, USA, Oct. 2010.

Albert, R., Jeong, H., and Barabási, A., "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

Albert, R., Albert, I., and Nakarado, G. L., "Structural vulnerability of the North American power grid," *Physical Review E*, vol. 69, p. 025103, Feb. 2004.

Almassalkhi, M. and Hiskens, I., "Model-predictive cascade mitigation in electric power systems with storage and renewables - part I: Theory and implementation," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 67–77, Jan. 2015.

Amin, M., "Energy infrastructure defense systems," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 861–875, 2005.

Arritt, R. F. and Dugan, R. C., "Distribution system analysis and the future smart grid," *IEEE Transactions on Industry Applications*, vol. 47, no. 6, pp. 2343–2350, 2011.

Arroyo, J. and Conejo, A., "Modeling of start-up and shut-down power trajectories of thermal units," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1562–1568, 2004.

Arroyo, J. M., "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Generation, Transmission & Distribution*, vol. 4, no. 2, pp. 178–190, 2010.

Ashok, A., Govindarasu, M., and Ajjarapu, V., "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, 2017, in press.

Ashok, A., Govindarasu, M., and Wang, J., "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, pp. 1–19, 2017, in press.

Bakken, D. E., Bose, A., Hauser, C. H., Whitehead, D. E., and Zweigle, G. C., "Smart generation and transmission with coherent, real-time data," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 928–951, June 2011.

Baldick, R., "Variation of distribution factors with loading," *IEEE Transactions on Power Systems*, vol. 18, no. 4, pp. 1316–1323, Nov 2003.

Bao, F., Lobo, V., and Painho, M., "Self-organizing maps as substitutes for k-means clustering," in *International Conference on Computational Science - Volume Part Iii*, ser. ICCS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 476–483.

Bertino, E. and Islam, N., "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb 2017.

Bertsch, J., Carnal, C., Karlson, D., McDaniel, J., and Vu, K., "Wide-area protection and power system utilization," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 997–1003, May 2005.

Bienstock, D., "Optimal adaptive control of cascading power grid failures," *ArXiv e-prints*, Dec. 2010.

Blumsack, S., "Network topologies and transmission investment under electric-industry restructuring," Ph.D. dissertation, Carnegie Mellon University, 2006.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwang, D.-U., "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, no. 4, pp. 175–308, 2006.

Bompard, E., Masera, M., Napoli, R., and Xue, F., "Assessment of structural vulnerability for power grids by network performance based on complex networks," *Critical Information Infrastructure Security*, pp. 144–154, 2009.

Bompard, E., Napoli, R., and Xue, F., "Extended topological approach for the assessment of structural vulnerability in transmission networks," *IET Generation, Transmission & Distribution*, vol. 4, no. 6, pp. 716–724, 2010.

Bompard, E., Pons, E., and Wu, D., "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, pp. 481–487, 2012.

Bompard, E., Wu, D., and Xue, F., "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., and Havlin, S., "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

Calderaro, V., Hadjicostis, C., Piccolo, A., and Siano, P., "Failure identification in smart grids based on petri net modeling," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 10, pp. 4613–4623, 2011.

Carreras, B. A., Lynch, V. E., Dobson, I., and Newman, D. E., "Critical points and transitions in an electric power transmission model for cascading failure blackouts," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 12, no. 4, pp. 985–994, 2002.

Carreras, B., Newman, D., Dobson, I., and Poole, A., "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Transactions on Circuits and Systems I: Regular Papers,*, vol. 51, no. 9, pp. 1733–1740, 2004.

Celenk, M., Conley, T., Willis, J., and Graham, J., "Predictive network anomaly detection and visualization," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 288–299, June 2010.

Chakhchoukh, Y. and Ishii, H., "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2487–2497, 2015.

Chen, J., Thorp, J. S., and Dobson, I., "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *International Journal of Electrical Power and Energy Systems*, vol. 27, no. 4, pp. 318–326, 2005.

Chen, Q. and McCalley, J., "Identifying high risk n-k contingencies for online security assessment," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 823–834, May 2005.

Chen, T. M., "Stuxnet, the real start of cyber warfare? [editor's note]," *IEEE Network*, vol. 24, no. 6, pp. 2–3, 2010.

Chen, T., Sanchez-Aarnoutse, J., and Buford, J., "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec. 2011.

Chen, Y., Hong, J., and Liu, C. C., "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Transactions on Smart Grid*, 2017, in press.

Chen, Z. and Ji, C., "An information-theoretic view of network-aware malware attacks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 530–541, Sept. 2009.

Cotilla-Sanchez, E., Hines, P., Barrows, C., and Blumsack, S., "Comparing the topological and electrical structure of the North American electric power infrastructure," *IEEE Systems Journal*, vol. PP, no. 99, p. 1, May 2012.

Crucitti, P., Latora, V., and Mar.iori, M., "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, p. 045104, Apr. 2004.

Cuadra, L., Salcedo-Sanz, S., Del Ser, J., Jiménez-Fernández, S., and Geem, Z. W., "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, no. 9, pp. 9211–9265, 2015.

Dagle, J. E., "The north american synchrophasor initiative (NASPI)," in *IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2010, pp. 1–3.

Davis, C. and Overbye, T., "Multiple element contingency screening," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1294–1301, Aug. 2011.

Delgadillo, A., Arroyo, J. M., and Alguacil, N., "Analysis of electric grid interdiction with line switching," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 633–641, May 2010.

Deng, R., Xiao, G., and Lu, R., "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, Feb 2017.

Dobson, I., Carreras, B. A., Lynch, V. E., and Newman, D. E., "An initial model for complex dynamics in electric power system blackouts," in *Hawaii International Conference on System Sciences (HICSS)*, Jan 2001, pp. 710–718.

Dobson, I., Carreras, B. A., Lynch, V. E., and Newman, D. E., "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 2, p. 026103, 2007.

Dobson, I., Carreras, B. A., and Newman, D. E., "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 01, pp. 15–32, 2005.

Donde, V., López, V., Lesieutre, B., Pinar, A., Yang, C., and Meza, J., "Severe multiple contingency screening in electric power systems," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 406–417, 2008.

Edison Electric Institute. "Transmission projects: At a glance." Accessed on April 13, 2017. December 2016. [Online]. Available: http://www.eei.org/issuesandpolicy/transmission/Documents/Trans_Project_lowres_bookmarked.pdf

Eppstein, M. J. and Hines, P. D., "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698–1705, 2012.

Esmalifalak, M., Nguyen, H., Zheng, R., Xie, L., Song, L., and Han, Z., "A stealthy attack against electricity market using independent component analysis," *IEEE Systems Journal*, pp. 1–11, 2017, in press.

Esmalifalak, M., Nguyen, H., Zheng, R., and Han, Z., "Stealth false data injection using independent component analysis in smart grid," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2011, pp. 244–248.

Fan, N., Chen, R., and Watson, J. P., "N-1-1 contingency-constrained optimal power flow by interdiction methods," in *IEEE Power and Energy Society General Meeting (PSEGM)*, July 2012, pp. 1–6.

Fan, N., Xu, H., Pan, F., and Pardalos, P., "Economic analysis of the N-k power grid contingency selection and evaluation by graph algorithms and interdiction methods," *Energy Systems*, vol. 2, no. 3-4, pp. 313–324, 2011.

Fan, Y., Zhang, Z., Trinkle, M., Dimitrovski, A. D., Song, J. B., and Li, H., "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov 2015.

Fang, X., Misra, S., Xue, G., and Yang, D., "Smart grid – the new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

Farraj, A. K. and Kundur, D., "On using energy storage systems in switching attacks that destabilize smart grid systems," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*. IEEE, 2015, pp. 1–5.

Fioriti, V., Sforna, M., and D'Agostino, G., "Spectral analysis of a real power network," *International Journal of Critical Infrastructures*, vol. 8, no. 4, pp. 354–367, 2012.

Fitzmaurice, R., Keane, A., and O'Malley, M., "Effect of short-term risk-aversive dispatch on a complex system model for power systems," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 460–469, 2011.

Friedman, J. H., Steppel, S., and Tukey, J., *A nonparametric procedure for comparing multivariate point sets*. Stanford Linear Accelerator Center Computation Research Group Technical Memo, 1973, no. 153.

Govindarasu, M., Hann, A., and Sauer, P., "Cyber-physical systems security for smart grid," Power Systems Engineering Research Center, Tech. Rep., Feb. 2012, accessed on March 27, 2017.

Guan, X., Qin, T., Li, W., and Wang, P., "Dynamic feature analysis and measurement for large-scale network traffic monitoring," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 905–919, Dec. 2010.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. P., "Smart grid technologies: Communication technologies and standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, 2011.

Guo, H., Zheng, C., Iu, H. H.-C., and Fernando, T., "A critical review of cascading failure analysis and modeling of power system," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9 – 22, 2017.

Guo, X., Singh, S., Lee, H., Lewis, R. L., and Wang, X., "Deep learning for real-time atari game play using offline monte-carlo tree search planning," in *Advances in neural information processing systems*, 2014, pp. 3338–3346.

Haykin, S., *Neural Networks: A Comprehensive Foundation*, 2nd ed. Prentice Hall, 1998.

He, H. and Yan, J., "Cyber-physicalhysical attacks and defences in the smart grid: A survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, pp. 13–27, December 2016.

He, L., "Application of Bayesian network in power grid fault diagnosis," in *Natural Computation (ICNC), 2008 Fourth International Conference on*, vol. 1, Oct. 2008, pp. 61–64.

Hines, P., Cotilla-Sanchez, E., and Blumsack, S., "Topological models and critical slowing down: Two approaches to power system blackout risk analysis," in *Hawaii International Conference on System Sciences (HICSS)*, 2011, pp. 1–10.

Hines, P., Apt, J., and Talukdar, S., "Large blackouts in North America: Historical trends and policy implications," *Energy Policy*, vol. 37, no. 12, pp. 5249–5259, 2009.

Hines, P., Cotilla-Sanchez, E., and Blumsack, S., "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 20, no. 3, 2010.

Huang, Y., Tang, J., Cheng, Y., Li, H., Campbell, K. A., and Han, Z., "Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis," *IEEE Systems Journal*, vol. 10, no. 2, pp. 532–543, June 2016.

Hug, G. and Giampapa, J. A., "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

Illinois Center for a Smarter Electric Grid (ICSEG). Information Trust Institute, University of Illinois at Urbana-Champaign. "IEEE 24-bus system." Accessed on May 1, 2017. [Online]. Available: http://publish.illinois.edu/smartergrid/ieee-24-bus-system/

Illinois Center for a Smarter Electric Grid (ICSEG). Information Trust Institute, University of Illinois at Urbana-Champaign. "IEEE 30-bus system." Accessed on May 1, 2017. [Online]. Available: http://publish.illinois.edu/smartergrid/ieee-30-bus-system/

Indyk, P. and Motwani, R., "Approximate nearest neighbors: Towards removing the curse of dimensionality," in *ACM Symposium on Theory of Computing*. ACM, 1998, pp. 604–613.

Jiayi, H., Chuanwen, J., and Rong, X., "A review on distributed energy resources and microgrid," *Renewable and Sustainable Energy Reviews*, vol. 12, no. 9, pp. 2472 – 2483, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032107001025

Jin, D., Li, Z., Hannon, C., Chen, C., Wang, J., Shahidehpour, M., and Lee, C. W., "Towards a cyber resilient and secure microgrid using software-defined networking," *IEEE Transactions on Smart Grid*, 2017, in press.

Jonnavithula, S. and Billinton, R., "Topological analysis in bulk power system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 12, no. 1, pp. 456–463, Feb. 1997.

Kaplunovich, P. and Turitsyn, K., "Fast and reliable screening of n-2 contingencies," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4243–4252, Nov 2016.

Kaplunovich, P. and Turitsyn, K., "Statistical properties and classification of n-2 Contingencies in large scale power grids," in *Hawaii International Conference on System Sciences (HICSS)*, Jan. 2014, pp. 2517–2526.

Karami, a. and Esmaili, S., "Transient stability assessment of power systems described with detailed models using neural networks," *International Journal of Electrical Power & Energy Systems*, vol. 45, no. 1, pp. 279–292, 2013.

Kim, J. and Tong, L., "On topology attack of a smart grid: Undetectable attacks and countermeasures," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 7, pp. 1294–1305, July 2013.

Kim, T. T. and Poor, H. V., "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

Kirschen, D., Jayaweera, D., Nedic, D., and Allan, R., "A probabilistic indicator of system stress," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1650–1657, 2004.

Knox, W. B. and Mengshoel, O., "Diagnosis and reconfiguration using Bayesian networks: An electrical power system case study," in *IJCAI 2009 Workshop on Self-* and Autonomous Systems*, 2009.

Koç, Y., Warnier, M., Kooij, R. E., and Brazier, F. M., "An entropy-based metric to quantify the robustness of power grids against cascading failures," *Safety Science*, vol. 59, pp. 126–134, 2013.

Kohonen, T., "The self-organizing map," *Proceedings of the IEEE*, vol. 78, no. 9, pp. 1464–1480, Sept. 1990.

Kohonen, T., Schroeder, M. R., and Huang, T. S., *Self-Organizing Maps*, 3rd ed. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2001.

Kosterev, D. N., Taylor, C. W., and Mittelstadt, W. A., "Model validation for the August 10, 1996 WSCC system outage," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 967–979, 1999.

Kosut, O., Jia, L., Thomas, R., and Tong, L., "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

Kosut, O., Jia, L., Thomas, R. J., and Tong, L., "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2010, pp. 220–225.

Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., Van Cutsem, T., and Vittal, V., "Definition and classification of power system stability IEEE/cigre joint task force on stability terms and definitions," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, August 2004.

Kundur, P., Balu, N. J., and Lauby, M. G., *Power System Stability and Control*. McGraw-hill New York, 1994, vol. 7.

Lai, Y.-C., Motter, A., and Nishikawa, T., "Attacks and cascades in complex networks," in *Complex Networks*, ser. Lecture Notes in Physics, Ben-Naim, E., Frauenfelder, H., and Toroczkai, Z., Eds. Springer Berlin Heidelberg, 2004, vol. 650, pp. 299–310.

Lasseter, R. H., "Smart distribution: Coupled microgrids," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1074–1082, 2011.

Li, F., Qiao, W., Sun, H., Wan, H., Wang, J., Xia, Y., Xu, Z., and Zhang, P., "Smart transmission grid: Vision and framework," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 168–177, Sept 2010.

Li, F. and Bo, R., "Small test systems for power system economic studies," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2010, pp. 1–4.

Li, F., Luo, B., and Liu, P., "Secure information aggregation for smart grids using homomorphic encryption," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010, pp. 327–332.

Li, Z., Shahidehpour, M., Alabdulwahab, A., and Abusorrah, A., "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sept 2016.

Li, Z., Shahidehpour, M., and Aminifar, F., "Cybersecurity in distributed power systems," *Proceedings of the IEEE*, pp. 1–22, 2017, in press.

Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y., "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–1, 2016.

Liang, G., Zhao, J., Luo, F., Weller, S., and Dong, Z. Y., "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, 2017, in press.

Lin, H., Slagell, A., Kalbarczyk, Z., Sauer, P., and Iyer, R., "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, 2017, in press.

Liu, L., Esmalifalak, M., Ding, Q., Emesih, V. A., and Han, Z., "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, March 2014.

Liu, L., Esmalifalak, M., and Han, Z., "Detection of false data injection in power grid exploiting low rank and sparsity," in *IEEE International Conference on Communications (ICC)*, June 2013, pp. 4461–4465.

Liu, N., Chen, J., Zhu, L., Zhang, J., and He, Y., "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 10, pp. 4746–4756, Oct 2013.

Liu, S., Chen, B., Zourntos, T., Kundur, D., and Butler-Purry, K., "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.

Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., and Butler-Purry, K., "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

Liu, X. and Li, Z., "False data attacks against ac state estimation with incomplete network information," *IEEE Transactions on Smart Grid*, 2017, in press.

Liu, X. and Li, Z., "Local topology attacks in smart grids," *IEEE Transactions on Smart Grid*, 2017, in press.

Liu, X. and Li, Z., "Trilevel modeling of cyber attacks on transmission lines," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 720–729, March 2017.

Liu, X., Li, Z., and Li, Z., "Optimal protection strategy against false data injection attacks in power systems," *IEEE Transactions on Smart Grid*, 2017, in press.

Liu, X., Li, Z., Liu, X., and Li, Z., "Masking transmission line outages via false data injection attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1592–1602, July 2016.

Liu, X. and Li, Z., "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, July 2014.

Liu, Y., Ning, P., and Reiter, M. K., "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

Long, C., You, D., Hu, J., Wang, G., and Dong, M., "Quick and effective multiple contingency screening algorithm based on long-tailed distribution," *IET Generation, Transmission & Distribution*, vol. 10, pp. 257–262(5), January 2016.

Masood, S. NY Times. "Rebels tied to blackout across most of pakistan." Accessed on May 7, 2015. January 25, 2015. [Online]. Available: http://www.nytimes.com/2015/01/26/world/asia/widespread-blackout-in-pakistan-deals-another-blow-to-government.html

Mei, S., He, F., Zhang, X., Wu, S., and Wang, G., "An improved opa model and blackout risk assessment," *IEEE Transactions on Power Systems*, vol. 24, no. 2, pp. 814–823, 2009.

Milano, F., "An open source power system analysis toolbox," *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1199–1206, 2005.

Mnih, V., Kavukcuoglu, K., Silver, D., Graves, A., Antonoglou, I., Wierstra, D., and Riedmiller, M., "Playing atari with deep reinforcement learning," *arXiv preprint arXiv:1312.5602*, 2013.

Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., Graves, A., Riedmiller, M., Fidjeland, A. K., Ostrovski, G., *et al.*, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, p. 529, 2015.

Mo, Y., Kim, T.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., and Sinopoli, B., "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

Mohsenian-Rad, A.-H. and Leon-Garcia, A., "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

Moreno, Y., Pastor-Satorras, R., and Vespignani, A., "Epidemic outbreaks in complex heterogeneous networks," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 26, no. 4, pp. 521–529, 2002.

Morison, K., Wang, L., and Kundur, P., "Power system security assessment," *IEEE Power and Energy Magazine*, vol. 2, no. 5, pp. 30–39, Sept 2004.

Moslehi, K. and Kumar, R., "A reliability perspective of the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57–64, June 2010.

Motter, A. E. and Lai, Y.-C., "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, p. 065102, 2002.

Moussa, B., Debbabi, M., and Assi, C., "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1952–1973, September 2016.

Murata, T., "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, 1989.

National Institute of Standards and Technologies (NIST), "Framework and roadmap for smart grid interoperability standards - release v3.0," National Institute of Standards and Technologies (NIST), Tech. Rep., 2014, accessed on May 1, 2017. [Online]. Available: http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf

National Institute of Standards and Technologies (NIST), "Guidelines for smart grid cybersecurity," Tech. Rep., 2014, accessed on May 3, 2017. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.7628r1

Nedic, D. P., Dobson, I., Kirschen, D. S., Carreras, B. A., and Lynch, V. E., "Criticality in a cascading failure blackout model," *International Journal of Electrical Power and Energy Systems*, vol. 28, no. 9, pp. 627–633, 2006.

Newman, D., Carreras, B., Lynch, V., and Dobson, I., "Exploring complex systems aspects of blackout risk and mitigation," *IEEE Transactions on Reliability*, vol. 60, no. 1, pp. 134–143, Mar. 2011.

Nguyen, C. P. and Flueck, A. J., "Agent based restoration with distributed energy storage support in smart grids," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 1029–1038, 2012.

North American Electric Reliability Corporation. North American Electric Reliability Corporation. "Reliability assessment guidebook." Accessed on April 10, 2017. December 2012. [Online]. Available: http://www.nerc.com/comm/PC/Reliability%20Assessment%20Subcommittee%20RAS%20DL/Reliability%20Assessment%20Guidebook/Reliability%20Assessment%20Guidebook%203%201%20Final.pdf

Overbye, T. and Weber, J., "Visualizing the electric grid," *IEEE Spectrum*, vol. 38, no. 2, pp. 52–58, 2001.

Ozay, M., Esnaola, I., Vural, F. T. Y., Kulkarni, S. R., and Poor, H. V., "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, Aug 2016.

Ozay, M., Esnaola, I., Vural, F. T. Y., Kulkarni, S. R., and Poor, H. V., "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306–1318, 2013.

Pagani, G. A. and Aiello, M., "The power grid as a complex network: A survey," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 11, pp. 2688–2700, 2013.

Pai, M., *Energy Function Analysis for Power System Stability*. Springer, 1989.

Pal, B. and Chaudhuri, B., *Robust Control in Power Systems*. Springer, 2005.

Papic, M., Bell, K., Chen, Y., Dobson, I., Fonte, L., Haq, E., Hines, P., Kirschen, D., Luo, X., Miller, S., Samaan, N., Vaiman, M., Varghese, M., and Zhang, P., "Survey of tools for risk assessment of cascading outages," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2011, pp. 1–9.

Pentland, W. Forbes. "FBI, joint terrorism task force arrest suspect in arkansas power grid attacks." Accessed on March 27, 2017. October 14 2013. [Online]. Available: http://www.forbes.com/sites/williampentland/2013/10/14/fbi-joint-terrorism-task-force-arrest-suspect-in-arkansas-power-grid-attacks/

Poudel, S., Ni, Z., and Sun, W., "Electrical distance approach for searching vulnerable branches during contingencies," *IEEE Transactions on Smart Grid*, 2017, in press.

Poudel, S., Ni, Z., Zhong, X., and He, H., "Comparative studies of power grid security with network connectivity and power flow information using unsupervised learning," in *International Joint Conference on Neural Networks (IJCNN)*, July 2016, pp. 2730–2737.

Poudel, S., Ni, Z., Hansen, T. M., and Tonkoski, R., "Cascading failures and transient stability experiment analysis in power grid security," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, September 2016, pp. 1–5.

Pourbeik, P., Kundur, P. S., and Taylor, C. W., "The anatomy of a power grid blackout - root causes and dynamics of recent major blackouts," *IEEE Power and Energy Magazine*, vol. 4, no. 5, pp. 22–29, Sept 2006.

Qi, J. and Mei, S., "Blackout model considering slow process and SOC analysis," in *IEEE Power and Energy Society General Meeting (PESGM)*, 2012, pp. 1–6.

Rahman, M. and Mohsenian-Rad, H., "False data injection attacks against nonlinear state estimation in smart power grids," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2013, pp. 1–5.

Rahman, M. A. and Mohsenian-Rad, H., "False data injection attacks with incomplete information against smart power grids," in *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 3153–3158.

Ren, H., Dobson, I., and Carreras, B., "Long-term effect of the n-1 criterion on cascading line outages in an evolving power transmission grid," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 1217–1225, Aug. 2008.

Ren, H., Fan, X., Watts, D., and Lv, X., "Early warning mechanism for power system large cascading failures," in *IEEE International Conference on Power System Technology (POWERCON)*, 2012, pp. 1–6.

Rezaei, P., Hines, P., and Eppstein, M., "Estimating cascading failure risk with random chemistry," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2726–2735, September 2015.

Rios, M. A., Kirschen, D. S., Jayaweera, D., Nedic, D. P., and Allan, R. N., "Value of security: modeling time-dependent phenomena and weather conditions," *IEEE Transactions on Power Systems*, vol. 17, no. 3, pp. 543–548, Aug 2002.

Rocco, C., Ramirez-Marquez, J., Salazar, D., and Yajure, C., "Assessing the vulnerability of a power system through a multiple objective contingency screening approach," *IEEE Transactions on Reliability*, vol. 60, no. 2, pp. 394–403, 2011.

Salmeron, J., Wood, K., and Baldick, R., "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 905–912, May 2004.

Salmeron, J., Wood, K., and Baldick, R., "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Transactions on Power Systems*, vol. 24, no. 1, pp. 96–104, Feb 2009.

Sayyadipour, S., Yousefi, G. R., and Latify, M. A., "Mid-term vulnerability analysis of power systems under intentional attacks," *IET Generation, Transmission Distribution*, vol. 10, no. 15, pp. 3745–3755, 2016.

Scala, A., Pahwa, S., and Scoglio, C., "Cascade failures from distributed generation in power grids," *arXiv preprint arXiv:1209.3733*, 2012.

Shah, S. S. and Babiceanu, R. F., "Resilience modeling and analysis of interdependent infrastructure systems," in *Systems and Information Engineering Design Symposium (SIEDS), 2015*. IEEE, 2015, pp. 154–158.

Shi, Q., Liang, S., Fei, W., Shi, Y., and Shi, R., "Study on Bayesian network parameters learning of power system component fault diagnosis based on particle swarm optimization," *Intelnational Journal of Smart Grid and Clean Energy*, vol. 2, no. 1, pp. 132–137, 2013.

Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., Schrittwieser, J., Antonoglou, I., Panneershelvam, V., Lanctot, M., *et al.*, "Mastering the game of go with deep neural networks and tree search," *Nature*, vol. 529, no. 7587, p. 484, 2016.

Silver, D., Sutton, R. S., and Müller, M., "Temporal-difference search in computer go," *Machine learning*, vol. 87, no. 2, pp. 183–219, 2012.

Smith, R. "Assault on california power station raises alarm on potential for terrorism." Accessed on May 1, 2017. February 5 2014. [Online]. Available: http://www.wsj.com/news/articles/SB10001424052702304851104579359141941621778

Solé, R. V., Rosas-Casals, M., Corominas-Murtra, B., and Valverde, S., "Robustness of the European power grids under intentional attack," *Physical Review E*, vol. 77, no. 2, p. 026102, 2008.

Sridhar, S., Hahn, A., and Govindarasu, M., "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

Srikantha, P. and Kundur, D., "Denial of service attacks and mitigation for stability in cyber-enabled power grid," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, Feb 2015, pp. 1–5.

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

Stott, B., Jardim, J., and Alsac, O., "DC power flow revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, 2009.

Sun, C.-C., Liu, C.-C., and Xie, J., "Cyber-physical system security of a power grid: State-of-the-art," *Electronics*, vol. 5, no. 3, p. 40, 2016. [Online]. Available: http://www.mdpi.com/2079-9292/5/3/40

Sutton, R. S. and Barto, A. G., *Reinforcement learning: An introduction*. MIT press Cambridge, 1998, vol. 1, no. 1.

Tang, B. and He, H., "ENN: Extended nearest neighbor method for pattern recognition [research frontier]," *IEEE Computational Intelligence Magazine*, vol. 10, no. 3, pp. 52–60, 2015.

Tang, Y., Yang, J., Yan, J., Zeng, Z., and He, H., "Frequency control using on-line learning method for island smart grid with EVs and PVs," in *International Joint Conference on Neural Networks (IJCNN)*, July 2014, pp. 1440–1446.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). "Cyber-attack against ukrainian critical infrastructure." Accessed on April 3, 2017. February 25 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Turitsyn, K. and Kaplunovich, P., "Fast algorithm for N-2 Contingency problem," in *Hawaii International Conference on System Sciences (HICSS)*, 2013, pp. 2161–2166.

U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Tech. Rep., 2004, accessed on April 20, 2017. [Online]. Available: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

U.S. Energy Information Administration. U.S. Department of Energy. "Electric power monthly." Accessed on February 28, 2017. February 2017. [Online]. Available: https://www.eia.gov/electricity/monthly/

U.S. Energy Information Administration. U.S. Department of Energy. "Short-term energy outlook." Accessed on March 7, 2017. March 2017. [Online]. Available: https://www.eia.gov/outlooks/steo/report/

Vaiman, M., Bell, K., Chen, Y., Chowdhury, B., Dobson, I., Hines, P., Papic, M., Miller, S., and Zhang, P., "Risk assessment of cascading outages: Part I - overview of methodologies," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2011, pp. 1–10.

Vaiman, M., Bell, K., Chen, Y., Chowdhury, B., Dobson, I., Hines, P., Papic, M., Miller, S., and Zhang, P., "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

Vesanto, J. and Alhoniemi, E., "Clustering of the self-organizing map," *IEEE Transactions on Neural Networks*, vol. 11, no. 3, pp. 586–600, May 2000.

Vesanto, J. "SOM implementation in SOM toolbox." Accessed on May 1, 2017. [Online]. Available: http://www.cis.hut.fi/somtoolbox/documentation/somalg.shtml

Wang, J.-W. and Rong, L.-L., "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, 2009.

Wang, S., Hong, L., and Chen, X., "Vulnerability analysis of interdependent infrastructure systems: A methodological framework," *Physica A: Statistical Mechanics and its applications*, vol. 391, no. 11, pp. 3323–3335, 2012.

Wang, S., Hong, L., Chen, X., Zhang, J., and Yan, Y., "Review of interdependent infrastructure systems vulnerability analysis," in *Intelligent Control and Information Processing (ICICIP), 2011 2nd International Conference on*, vol. 1. IEEE, 2011, pp. 446–451.

Wang, W., Cai, Q., Sun, Y., and He, H., "Risk-aware attacks and catastrophic cascading failures in u.s. power grid," in *IEEE Global Communications Conference (GLOBECOM)*, Dec. 2011, pp. 1–6.

Wang, W., Sun, Y., and He, H., "Topological analysis of cascading failures in bay area power grid," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2012, pp. 1–9.

Wang, X., Song, Y., and Irving, M., *Modern Power Systems Analysis*. Springer, 2008.

Wang, Z., Scaglione, A., and Thomas, R., "The node degree distribution in power grid and its topology robustness under random and selective node removals," in *IEEE International Conference on Communications Workshops (ICC)*, 2010, pp. 1–5.

Watkins, C. J. C. H., "Learning from delayed rewards," Ph.D. dissertation, King's College, Cambridge, 1989.

Wikipedia. "List of major power outages." Accessed on March 21, 2017. [Online]. Available: https://en.wikipedia.org/wiki/List_of_major_power_outages

Yan, J., He, H., Zhong, X., and Tang, Y., "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 200–210, Jan 2017.

Yan, J., Tang, Y., Tang, B., He, H., and Sun, Y., "Power grid resilience against false data injection attacks," in *IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

Yan, J., He, H., and Sun, Y., "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, Mar. 2014.

Yan, J., Tang, Y., He, H., and Sun, Y., "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, January 2015.

Yan, J., Tang, Y., Zhu, Y., He, H., and Sun, Y. L., "Smart grid vulnerability under cascade-based sequential line-switching attacks," in *IEEE Global Communications Conference: Selected Areas in Communications: Smart Grid Communications (GC' 15 - SAC - Smart Grid Communications)*, San Diego, USA, Dec. 2015.

Yan, J., Yang, Y., Wang, W., He, H., and Sun, Y., "An integrated visualization approach for smart grid attacks," in *Intelligent Control and Information Processing (ICICIP), 2012 Third International Conference on*, July 2012, pp. 277–283.

Yan, J., Zhu, Y., He, H., and Sun, Y., "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 2013.

Yan, J., Zhu, Y., He, H., and Sun, Y., "Revealing temporal features of attacks against smart grid," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, Feb. 2013, pp. 1–6.

Yan, Y., Qian, Y., Sharif, H., and Tipper, D., "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 5–20, 2013.

Yang, Q., Yang, J., Yu, W., An, D., Zhang, N., and Zhao, W., "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2014.

Zarate-Minano, R., Van Cutsem, T., Milano, F., and Conejo, A., "Securing transient stability using time-domain simulations within an optimal power flow," *IEEE Transactions on Power Systems*, vol. 25, no. 1, pp. 243–253, Feb. 2010.

Zhang, Y., Xiang, Y., and Wang, L., "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Transactions on Smart Grid*, pp. 1–15, 2017, in press.

Zhang, Z., Gong, S., Dimitrovski, A., and Li, H., "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

Zhang, Z., Trinkle, M., Dimitrovski, A., and Li, H., "Combating time synchronization attack: A cross layer defense mechanism," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, Apr. 2013, pp. 141–149.

Zhu, Y., Yan, J., Sun, Y., and He, H., "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3274–3284, Dec 2014.

Zhu, Y., Yan, J., Tang, Y., Sun, Y., and He, H., "The sequential attack against power grid networks," in *IEEE International Conference on Communications (ICC)*, June 2014, pp. 616–621.

Zhu, Y., Yan, J., Tang, Y., Sun, Y. L., and He, H., "Resilience analysis of power grids under the sequential attack," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340–2354, Dec 2014.

Zhu, Y., Yan, J., Sun, Y., and He, H., "Risk-aware vulnerability analysis of electric grids from attacker's perspective," in *IEEE PES Conference on Innovative Smart Grid Technologies (ISGT)*, Feb. 2013, pp. 1–6.

Zhu, Y., Yan, J., Tang, Y., Sun, Y. L., and He, H., "Joint substation-transmission line vulnerability assessment against the smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1010–1024, 2015.

Zimmerman, R., Murillo-Sanchez, C., and Thomas, R., "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

Zurawski, R. and Zhou, M., "Petri nets and industrial applications: A tutorial," *IEEE Transactions on Industrial Electronics*, vol. 41, no. 6, pp. 567–583, 1994.