University of Rhode Island

DigitalCommons@URI

Open Access Master's Theses

2013

Modelling and Analysis on Smart Grid Against Smart Attacks

Jun Yan

University of Rhode Island, jun_yan@my.uri.edu

Follow this and additional works at: <https://digitalcommons.uri.edu/theses>

Recommended Citation

Yan, Jun, "Modelling and Analysis on Smart Grid Against Smart Attacks" (2013). *Open Access Master's Theses*. Paper 16.

<https://digitalcommons.uri.edu/theses/16>

This Thesis is brought to you for free and open access by DigitalCommons@URI. It has been accepted for inclusion in Open Access Master's Theses by an authorized administrator of DigitalCommons@URI. For more information, please contact digitalcommons-group@uri.edu.

MODELLING AND ANALYSIS ON SMART GRID AGAINST SMART
ATTACKS

BY
JUN YAN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
ELECTRICAL ENGINEERING

UNIVERSITY OF RHODE ISLAND

2013

MASTER OF SCIENCE THESIS
OF
JUN YAN

APPROVED:

Thesis Committee:

Major Professor

Haibo He

Lisa DiPippo

Yan Sun

Nasser H. Zawia

DEAN OF THE GRADUATE SCHOOL

UNIVERSITY OF RHODE ISLAND

2013

ABSTRACT

Modern power systems worldwide are facing a rising appeal for the upgrade to a highly intelligent generation of electricity networks commonly known as the Smart Grid. Advanced monitoring and control systems like Supervisory Control And Data Acquisition (SCADA) and Advanced Metering Infrastructure (AMI) systems have been widely deployed and management based on them provides more flexible and achievable optimal control of power generation, transmission and distribution. However, the growing integration of power system with communication networks also brings increasing challenges to the security of the modern power grid, from both cyber and physical space. Malicious attackers can take advantage of the increased access to the monitoring and control of the system and exploit some of the inherent structural vulnerability of power grids. Motivated by these security challenges, the goal of this thesis is to facilitate the understanding of power grid outages and blackouts triggered by these attacks, to analyze the cascading process that leads to the impactful events, and to support the decision making in defense and protection for a reliable and secure Smart Grid around the corner. Simulation results from real-world power system benchmarks have been analytically discussed from both the spatial and temporal perspectives and important decision-support information have been revealed through several chapters of the thesis. This research is part of an ongoing National Science Foundation (NSF) funded Smart Grid security project led by Dr. Haibo He, Dr. Yan (Lindsay) Sun from the Electrical Engineering Department and Dr. Peter August from the Natural Resources Science Department, all at the University of Rhode Island.

ACKNOWLEDGMENTS

I would like to express special gratitude of the following people and programs.

The research of the thesis would not be possible without the invaluable advisory and support from my major professor, Prof. Haibo He from Dept. of Electrical, Computer and Biomedical Engineering. Prof. Yan (Lindsay) Sun from the same department with whom I have worked on the Smart Grid security project has also given numerous precious comments and suggestions on many aspects that are greatly appreciated. Prof. Peter August from the Department of Natural Resources Science provides numerous support and suggestions on the GIS part for the spatial analysis. I also thank Prof. Lisa DiPippo from the Computer Science Department for her support in the preparation of my proposal, thesis and defense.

I would also like to thank the Department of Electrical, Computer and Biomedical Engineering for the wonderful hardware facilities as well as the courses that prepared me for this research, and the URI International Engineering Program (IEP) as well as its director Dr. Sigrid Berka for the precious chance to start the author's Master's study at URI. This work is also financially supported by the National Science Foundation (NSF) under Grant # CNS 1117314.

I am grateful to my former teammate, Yida Yang who also contributes a lot to the demo, and my fellow labmates at Computational Intelligence and Self-Adaptive Systems (CISA) Laboratory: Zhen Ni, Yufei Tang, Jing Wang, Bo Tang and Xiangnan Zhong, as well as the visiting labmate Xiao Fang for all the hours of fun and hard working that we have shared.

I owe many thanks to my friends for their company and encouragements. I love my parents, Haoning Yan and Weihua Song, whose love and support I can't never thank enough.

TABLE OF CONTENTS

ABSTRACT	ii
ACKNOWLEDGMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vii
LIST OF FIGURES	viii
CHAPTER	
1 Introduction	1
1.1 The Smart Grid and Its Security Challenges	1
1.2 The General Methodology	4
1.2.1 The Focus of the Study	4
1.2.2 The Basic Assumptions	6
1.2.3 The Benchmark Power System	7
1.2.4 The Structure of the Thesis	8
2 Literature Review	9
2.1 Smart Grid Reliability/Stability Analysis	9
2.1.1 State Estimation	10
2.1.2 Contingency Analysis	11
2.1.3 Dynamic/Transient Stability Analysis	12
2.1.4 Cascading Failure Analysis	13
2.2 Smart Grid Security Analysis	15

	Page
2.2.1 Smart Grid Security Issues	15
2.2.2 Categories of Smart Grid Attacks	16
2.2.3 Smart Grid Security Tools	18
2.3 Summary of the Literature Review	19
3 Power Grid Modelling	20
3.1 Topological Model	20
3.2 Assessment Metric	25
4 Visualizing Cascading Failure for Spatial Pattern Analysis . .	27
4.1 Spatial Analysis for Cascading Failure in Power Grids	27
4.2 Visualize the Cascading Attack	28
4.2.1 The Cascading Simulator	28
4.2.2 Interface Between MATLAB and ArcGIS	30
4.2.3 Visualization in ArcGIS	34
4.3 Simulation Result	37
4.4 Discussion	41
5 Revealing Temporal Features in the Cascading Failure Process	50
5.1 Temporal Features in Power Grid Cascading Failure	50
5.1.1 Model Specification for the Temporal Analysis	51
5.1.2 Temporal Features of Cascading Failure	53
5.2 Simulation Setup	56
5.3 Temporal Feature Revealed	57
5.4 Discussions	61
5.4.1 Time-Delay Relay	61

	Page
5.4.2 Spatial Connectivity	63
5.4.3 System Tolerance	63
5.5 Summary	64
6 Conclusion and Future Work	66
6.1 Conclusion	66
6.2 Future Work	67
LIST OF REFERENCES	69
BIBLIOGRAPHY	78

LIST OF TABLES

Table		Page
1	Summary of connectivity and PoF distribution	46
2	General information on the most loaded nodes in temporal analysis	58

LIST OF FIGURES

Figure	Page
1	The power grid of the upper Bay area, displayed in ArcMap 10.0. 8
2	Illustration of the load redistribution policy 22
3	Illustration of “rounds” as a cascading tree. 24
4	Diagram of the compact ArcGIS-MATLAB visualization platform 29
5	The detailed flowchart of the integrated visualization platform 36
6	The upper Bay Area grid under normal operation 39
7	The first victim failed at the first round 39
8	Final stabilized cascading failure 40
9	Cascading effect of the first attack 41
10	Sequential attack: (a) launching the 2nd (b) end of the 2nd 42
11	Sequential attack: (a) launching the 3rd (b) end of the 3rd 43
12	An example of cascading migration (a) before critical moment (b) after critical moment 45
13	A victim near the edge (a) being attacked and (b) its cascading impact 47
14	A hub victim that yields no cascading effect 48
15	The flowchart of cascading failure model with time-delay 54
16	The upper Bay Area power grid with 510 nodes 57
17	The cascading failure caused by attacks for $T = 1.1$ 59
18	The change of failure percentage at each round for Node 57. 61
19	The influence of system tolerance 64

CHAPTER 1

Introduction

1.1 The Smart Grid and Its Security Challenges

Since its birth over a century ago, the power system in the United States has been evolved into one of the largest complex networks ever witnessed in human history. With the increasing consumption demand, the modern electrical power grids are now growing into a mammoth system with numerous interconnected regional grids, owned and operated by power corporations at all levels and scales. However, complex interests, operations and managements among different power companies often complicate cross-region transmission tasks and sometimes result in an inefficient or poorly-coordinated power delivery. And the traditional power grids in modern times are facing some rising challenges. As the need and variety of consumption increases, more and more latest technologies have been incorporated into the power system, such as the distributed renewable energy generation, the electric vehicle (EV) charging system, smart meters, etc., which all contribute to the complexity of modern power delivery. The ever increasing reliance on electricity and request of power quality have been constantly calling for better power delivery, more flexible pricing, faster power restoration, among others.

The challenges above have motivated the industry and society for a new generation of power system with more informative, intelligent and automatic operations [1]. This new generation of power grid, commonly referred to as the Smart Grid, will modernize the traditional power grid and improve its reliability, flexibility and efficiency. The Smart Grid is expected to have more distributed controls and consumer-based interactions, and some key applications of this upgrade includes:

1. Installing advanced metering infrastructure (AMI) and other intelligent devices to reduce extra unnecessary demand, as well as the operation and maintenance cost [2,3];
2. Implementing distributed automation to enhance the reliability of power system [4];
3. Utilizing automated controls for better and flexible power management [5].

The most significant feature of the Smart Grid, in contrast to the traditional power system, is the large scale of implementation of a two-way communication network connecting both the power plants, the transmission network sensors and the consumers. This enhanced and interactive system will optimize the power delivery quality, efficiency and stability at a lower cost via the computer-based automation. With the incorporation of communication and computer networks in assistance to the traditional power delivery, the Smart Grid is already an emerging gigantic intelligent network system in which power flows are flexibly directed by highly automatic systems like the Supervisory Control and Data Acquisition (SCADA) system.

However, the Smart Grid yields not only a boost of economic benefits but also a growing number of potential threats from the cyberspace [6]. While the distributed control can reduce the criticality of some control center and thus weaken the impact of attacks targeted on them, the distributed access from the system-on-a-chip (SoC) electrical devices can possibly allow malicious attackers penetrating into the power systems with increased difficulties to detect and track them. Meanwhile, with the huge volume of data flowing along the power transmission network, they are becoming more vulnerable to data or command interception and unauthorized modification, which can be utilized to either cheat the meters for an unfair price or disrupt power system operations. More seriously, knowledge of the power

grid can be learned and the information or intelligence could be used to hack into the distributed control units that may be less protected than the centralized operation and management hubs, resulting in unpredictable security risks. Hence, it becomes crucial to realize and react to the vulnerability of Smart Grid in the new forms of potential attacks. These “smart” attacks, if deliberately designed and launched successfully on some critical components, can cast a disastrous impact on the power grid transmission and significantly jeopardize the interest of both the public, the industry as well as the economics.

One of the vulnerabilities of Smart Grid that could be taken advantage of by the attackers are the possibility of cascading failure events in power systems, in which a few failed components can trigger the collapse of normal power transmission and consequently results in blackouts in the distribution networks on the users’ side. There are many examples of power grid failures with severe consequences; i.e. the 2003 blackout in northeast U.S., the 2011 blackout in California, Arizona and Mexico, and the most recent 2012 massive blackout in India have all left millions of people in darkness. They have shown that major power blackouts caused by cascading failure, though rare as they are, cast significant impact to both society and industry [7, 8]. Therefore, the government, the engineering community and power industry are paying growing attention to the power grid cascading analysis and many significant results have been published [9–12].

However, while a number of power grid stability and security issues have been resolved, it is noticed that the complexity of smart grid security has nevertheless been diluted, and the understanding of it is still far from comprehensive [13, 14]. For instance, how the cascading effect triggered by different failures propagates in different systems is not yet predictable or precisely approximated by any model [9] [12]. More questions, for instance how attackers, aiming at maximizing impact

to the grid at the lowest cost by just taking down only a few components, could utilize the structural vulnerability and the potential access to key components in the grid, and how the smart grid and its operators should respond correspondingly to these attacks, still remain unclear to both the industry as well as the research community. Therefore, the complexity of cascading failure and the computational cost to simulate these events still call for more effective and efficient modeling, simulating and analyzing tools. They will be critical to provide a comprehensive and robust assessment for decision support and defense strategy improvement to protect the Smart Grid against the smart attacks [15] [16].

Given these considerations, the goal in the study of this thesis is to shed some light on the problem of how to secure the Smart Grid against major blackouts caused by intelligent attacks. Specifically, in this work the focus will be first to reveal what are the impacts of potential attacks, how to identify the critical components, and what are the system failure behavior in the attack scenarios. Based on the work and preliminary results, more works on how to respond to these failures via proper counter-measurements (either manual or automatic) can be conducted to enhance the security of the future Smart Grid.

1.2 The General Methodology

As the last part of the introduction, the general methodology employed to study the problem of Smart Grid Security will be discussed in detail to provide the readers a clear and general idea of the work included in this thesis.

1.2.1 The Focus of the Study

In this thesis, three major objectives for the research have been specified:

1. Understanding cascading process: Intuitively, we are interested in revealing how the cascading failures propagate across the region, and how it develop

over time.

2. Identifying most vulnerable components: For this purpose, we want to properly measure the impact of the failure of victim under attack, and then effectively and efficiently locate the most vulnerable components that will cause the greatest impact if they are attacked;
3. Discussing corresponding defenses responses: This will become the practical meaning of the work to provide spatial and temporal information and knowledge for the defenders to respond to potential attacks.

In the study of cascading failure, simulations and analysis will be the key methodology, since it will be very difficult and expensive to set up a test in real power system. This is also the major approach through which the malicious attackers can build up an informative attack based on the power grid status. Particularly, in this study three objectives of simulation can be defined to analyze the power system behavior in a cascading even:

1. Electrical measurements: This is the most traditional and well-developed indicators of power system which evaluate the load shedding/yield, the number of outage lines and substations, or the population under blackout, among others. These are all the technical indices directly assessing the power system stability and security from the operation and engineering point of view.
2. Spatial patterns: As cascading failures often yield a large scale regional impact, their geographic information can not only exhibit some spatial patterns but also reveal the potential cost of mitigation and restoration. With the help of GIS systems, the spatial information can be displayed more intuitively through a properly designed visual platform. Hence, with the help

of the author’s colleagues working in the same project, it is helpful to employ a GIS demo and then analyze the spatial pattern and characteristics of cascading failures in a power system.

3. Temporal features: While time-domain dynamic/transient stability analysis has been popular in the power and energy society for many years, it is not yet a well-developed area in the power system cascading analysis. Although it is helpful to evaluate consecutive cascading events that finally lead to a regional blackout, to track the causal relationship between them and to record all the events and factors that have possibly affected the cascading failure process, the complexity is usually intimidating. However, using some proper assumptions and simplifications, a well-designed model with proper indices can reveal critical features in the cascading process and provide information for a better timing decision to respond to the failure, which is especially useful when in reality only restricted resource and limited time are given.

1.2.2 The Basic Assumptions

Due to the inherit complexity of the dynamics and failure behaviors of power system, to set up a valid model of power grid attacks, it will be necessary to introduce a few essential assumptions and limit the scope of problem to investigate within a certain range. The major assumptions involve the topological representation of the power system. With resourceful researches from the computer science and communication society on the topological vulnerability of complex networks under attacks (e.g. [17] and [18]), the investigation of smart grid security will start from available topological methods and models with necessary modifications.

Specifically, this means the research in the thesis will first take the assumption that the smart grid can be modeled as a complex network, to which current topological vulnerability metrics from complex network studies can be applied. Power

flow models are also widely used in traditional power grid stability and contingency analysis. However, it is known that an accurate replication of a large scale power grid with thousands of components and detailed operation status and control management is indeed prohibitive and unnecessary. In this proposed project, the goal model will try to avoid and simplify some complex realtime dynamics like three-phase ac voltage, disturbance of power quality and consumer-side distribution.

1.2.3 The Benchmark Power System

The subject, as the focus of proposed research, will be the power transmission network. It is a cluster of power delivery networks that are usually regarded as a single interconnected or regional grid, which transmits power from a number of generation power plants to numerous distribution substations via a set of facilities like transformers and relays. The transmission involves two major types of power grid component, i.e. the substations and transmission lines. An illustration of a metropolitan power grid around the Bay area is shown in Fig.1, where substations are marked in green and transmission lines in blue. The data are extracted from the POWERmap GIS dataset provided by PLATTS, a McGill company. From the figure we can intuitively see that our refined focus considers less types of components than a complete monumental power grid that will also include generation networks and distribution networks alike. Therefore, it better matches the assumption of smart grid as an interconnected complex networks and serves the purpose of both effective and efficient modeling of power transmission networks. Meanwhile, it still holds substantial importance in the study of smart grid security from two aspects: First, the transmission networks are more vulnerable to cyber-attacks than power plants and control centers guarded and protected in the assess-restricted generation networks. Second, their failures (causing most blackouts) contribute to more significant impact and damage to the society and industry than the distribution

Figure 1. The power grid of the upper Bay area, displayed in ArcMap 10.0.

networks, whose failures (usually referred to as disturbances) are mostly local and constrained to only a small area.

1.2.4 The Structure of the Thesis

The rest of this thesis is organized as follows: In Chapter 2, a literature survey of the state-of-the-art in Smart Grid security studies will be presented. A detailed model used for the simulation in this work will be described in Chapter 3. In Chapter 4 to 5, implementation details, simulations and discussions will be first provided from the attacker's point of view, each followed with some discussions from the defender's perspective. Specifically, chapter 4 will explore the spatial patterns of cascading failures, while Chapter 5 will reveal temporal features of the post-attack system failure events identified from our simulations. The conclusion and future work are with Chapter 6.

CHAPTER 2

Literature Review

This chapter will briefly review some of the up-to-date researches related to Smart Grid security issues in multiple fields. As the following discussion indicates, while a significant amount of work has been done and numerous issues satisfactorily resolved, there are still many emerging challenges in the applications of Smart Grid that slow down the effort of its installation and replacement of traditional power grids. The first section of this chapter will introduce the reliability and stability analysis from the perspective of power system operation, which lies the theoretical foundation for vulnerability assessment and security analysis. The second section will introduce the modern network security approaches that deal with the specific applications in the application of Smart Grid.

2.1 Smart Grid Reliability/Stability Analysis

Reliability or stability analysis of Smart Grid is the extension of traditional power system analysis for the emerging new generation. In general, a Smart Grid can be represented though a set of conceptual models [19]. From the intuitive and interactive illustrations shown in [19], it is inevitable that the introduction of renewable resources, storage and intelligent demand response will bring unforeseen patterns and variances in the power generation, transmission and distribution [20]. For example, the output of generation power from wind farms as well as the fast-changing demand of electrical vehicle charging are highly unpredictable and uncontrollable, both of which pose great challenges to the traditional power grid that runs on a strictly constrained operating point of voltage, phase, frequency and power level. Similar upgrades in Smart Grid require the conversion of traditional power system stability analysis into the modern approaches, especially with the

utilization of powerful tools from the developments of intelligent algorithms and computing resources. Specifically, in this section four aspects, i.e. state estimation, contingency analysis, transient stability analysis, and cascading failure analysis for the reliability and stability of Smart Grid will be discussed.

2.1.1 State Estimation

State estimation (SE) is a classic approach to generate proper control policy for various system states [21]. It is derived on classic control theory and combined with the power system characteristics to determine the actual system state that cannot be directly observed from a collection of redundant measurements. This is critical in power grids as the operators relies greatly on the precise information of system states, to properly adjust the operation points and maintain the stable delivery of electricity to various power consumers. As the upgrade of transmission capacity usually falls behind the increase of generation and demand, and the measurements are always mixed with certain amount of noise, the system operators and managers need to accurately estimate the true power system states and carefully balance between the operation constraints and the cost. As a result, intense research efforts have been focused in the field of state estimation to ensure the stability of power systems and industrial large scale state estimation system have been widely applied in the power grid control centers [22, 23].

In Smart Grid, the state estimation faces a lot of challenges from both efficiency and security perspective. With the increased complexity in the modern Smart Grid, which is embedded with a vast online sensor network generating a gigantic flow of data, together with increased number of states that can yield even more irregular variances, the system state estimator needs to be efficient and accurate as much as possible. Moreover, as the data collected from the now less-protected sensors could be hijacked or forged, the study of state estimation also

needs to come up with modern detection approaches that can effectively handle the false data injected to the estimator so that accurate control policy for the operation of power systems can be provided. Numerous works on the state estimation application in Smart Grid have been published to handle the reliability issues for state estimation [24–26]. However, as the part in a system operator mostly related to the communication networks in Smart Grid, state estimation is still exposed to most cyber security threats than other aspects.

2.1.2 Contingency Analysis

Contingency analysis (CA) is a traditional static approach that simulates the outage for a given set of power grid components or elements under a given model and evaluates the consequent events following the outage [27–29]. CA methods usually assesses the redundancy and robustness of power grids in the outages of some of the components, and concludes if a grid is $N - k$ secure if it is able to remain within an operation domain when k components are put in an outage situation. In most cases a power system is only guaranteed to be $N - 1$ secure due to the cost of maintaining a large redundancy above its operation points and the computational complexity in evaluating multi-contingency events for a large power system.

However, due to the reports of large scale blackouts and the growing threats from cyberspace that malignant attackers are obtaining more computing resource to knock down multiple components at the same time, recent works in the field of CA focus on the development of fast, adaptive search algorithm to efficiently eliminate sets of guaranteed $N - k$ secured contingencies and refine the candidates to a decent level. Many have works have applied artificial neural networks [30] or radial basis function network [31] for contingency analysis. Others have focused on efficient monitoring and detection methods [32, 33] for CA purpose.

2.1.3 Dynamic/Transient Stability Analysis

Dynamic stability analysis (DSA), or transient stability analysis (TSA) [34] deals with the synchronization of generators relating to the electromagnetic behaviors. This analysis focus on the control of specific power system state, or operating points, including rotor angle, active and reactive power flow, generator voltage, in the presence of a given disturbance (e.g. a single or three-phase one-end grounded fault) [27]. Using optimization and control theories, DSA/TSA solves coupled differential equations of detailed system state measurements and observes each transient power system state in the time domain. The observed states can be directly used to evaluate the ability of each power generator to remain operationally stable against the given fault or disturbance, and different control regulators or policies can be applied to stabilize the system at an equilibrium point while trying meet the load demand in a grid with the given fault.

DSA/TSA methods are usually validated on a small power system benchmarks, yet the complexity in time-domain simulation (simulating power system behavior for a few seconds with a step length of 1ms or less) leads to studies on the computing methods for stability analysis [35–38]. Some researches focus on secure and robust TSA algorithms [39, 40]; meanwhile, many adaptive control policies based on machine learning algorithms [41] like Artificial Neural Network (ANN) [42], Support Vector Machine (SVM) [43, 44], Heuristic Dynamic Programming (HDP) [45] or Particle Swarm Optimization [46] have been proposed to adaptively control the power system states. In addition, modern DSA/TSA often employ benchmarks like doubly fed induction generator (DFIG) for wind farms or static synchronous compensator (STATCOM) for voltage stability, reflecting the latest trend of the installation of renewable energy in the Smart Grid. Although the computational cost of DSA/TSA on a large scale system remains prohibitive,

related analysis on a small benchmark can usually provide good indication and validation for large power transmission networks in real world.

2.1.4 Cascading Failure Analysis

As mentioned previously, cascading failure is the main reason that some small system faults resulting in major blackouts. As reported in [7], in August 2003, a defect operator failed to perform a critical redistribution of power for an overloaded transmission line, resulting in the major blackout that affected more than 55 million people in the Northeast American region. Similarly, in the recent India blackout in 2012, with the power system approaching its peak limit during the extreme heat in the summer, a tripped transmission line left more than 300 million people in a blackout on July 30, while on the following day a failed relay in the partially restored system made over 600 million people out of power in another blackout [8]. In both events, all industry, public transportation, health service and consumer use were interrupted, and many of the affected population, without individual backup generators of their own, struggled in the blackout chaos.

In many cascading failures, the automatic protective relays deployed across the power transmission network is the most common reason that turns an single or small scale outage into a blackout. When they cut off failure-affected components to maintain the stability of power system, some failed or improper attempts will result in more subsequent disconnections of power grid components, triggering an avalanche effect across the whole network.

Due to the highly interconnected nature of power grid, when a victim in the grid is take down, the influence of its failure is not likely to be constrained within the initial victims. It could possibly propagate along the grid and cause an overloading issue across the network [9–11]. For a well-designed system with proper control policy or an less-effective attack, the failure can be tolerated to some

extent, causing only some disturbances in power transfer quality without further propagation [47]. However, if the attacker has a good understanding of the power grid and initiates the attack from more vulnerable components in the power grid, the failure of these victims may lead to some fatal overloading and cause cascading in a large area.

Many systematic models for cascading analysis have been developed in great depth [9–11] to address these challenges in analyzing the power grid cascading failure. Among them, ac power flow model has its strength in accuracy as it carries the reactive power in calculation, which better approximate power grid in reality at the cost of greater computational complexity [12] [9]. Dc power flow models are very popular with a tradeoff between the precision of power grids approximation and the computational cost of simulation [48], but they require detailed physical parameters of the power grid that are hard to obtain in reality. High-level statistic approaches use historic data to analyze the power grid failure from a general perspective [49] [50]. Topological models are also frequently used in the security analysis of power system as they provide powerful tools from complex system and computer science fields [51] [52] and work with most GIS databases of electric utilities in industry. In addition to the modelling work [53], there are also studies on system dynamics and operation points, evaluating the self-organized criticality in power system cascading failures, which also plays an important role in cascading analysis [15, 16, 54]. Finally, some researches also works on large scale power systems, like the Western Electricity Coordinating Council [55] [56] or Polish Grid in winter [12], and the mathematical software [57] to solve power system dynamics effectively and efficiently.

Unfortunately, the cascading effect of power system is not well understood and many of the works did not provide comprehensive models [9] to represent

how the failure propagates through the grid, or how to constrain the cascading effect at some critical moments before it leads to a blackout. Therefore in this thesis, we are mostly interested in evaluating these fatal cascading failures caused by malicious cyber-attacks, where the victims are selected based on both the attackers' knowledge of the power grid topology and the predicted behavior of failure cascading.

2.2 Smart Grid Security Analysis

While the blooming Smart Grid technologies, the security issues are also becoming more challenging with the mass computer based monitoring, control and metering, and numerous researches have proposed their general frameworks or platforms from their perspective for the comprehensive understanding of smart grid security [58–61]. In these section, we will discuss the general security issues and the major types of Smart Grid attacks, with some powerful tools developed to assess and address these issues.

2.2.1 Smart Grid Security Issues

Smart Grid, as an integration of power transmission networks and communication networks, can be vulnerable in both physical and cyber space [13, 14, 62]. These include challenges in accurate measurement and monitoring of power system states, power transmission reliability against disruptive events, control of access and authentication, detection and defence against malicious attacks, as well as the protection of user privacy [63]. Coordinated attacks can take place in both networks and it can be difficult to identify these attacks and distinguish them from usual disturbances, especially when millions of users data are also recorded by smart meters all across the country, while there are only a few control centers to ensure the stability of the whole interconnected systems. In this thesis, we are

specifically interested in the attacks on power system directly, which usually bring the most catastrophic effects if proper counter-measures are not called in time. However, in reality attacks on different levels can be launched simultaneously, so we will first briefly explore the major types of Smart Grid attacks to better explain the related fields for this study.

2.2.2 Categories of Smart Grid Attacks

Generally, to refine the scope of the thesis we can roughly divide attacks in the Smart Grid into three categories based on the definition in [13, 14], which are the consumer-end attacks, the data attacks, and the direct attacks, and the subject of this study will be the last type that can lead to the most severe impact to the power system.

Consumer-end Attacks

The consumer-end attacks are the attacks happening at the consumer end [63–65], e.g. smart meters or distribution network controllers. Many of these attacks are the personal attempts to treat the meters with some software or Trojan scripts for unfair electricity price, or to steal user consumption profile for private information. Although they do not carry the purpose to jeopardize power system stability or security which appears less fatal or impactful, consumer-end attacks is not trivial as the user-end devices have feedback access all the way up to control centers. If attackers aim at creating social chaos, they can still try to forge suspicious or erroneous requests and send them to the control center, resulting in a denial of power delivery service for the “corrupted user demand”. This denial may either shut down the switch of normal residential buildings or interrupt the quality of power delivered to critical social infrastructures like hospitals, transportation. In other cases, user data can also be stolen from the smart meters, giving off private

information that can pose other threats to individual users.

To address issues raised by this type of attack, researchers have been focused on the development of a secure interaction between the smart meter and the users [66–68]. These include better encryption [66] and authentication [69, 70], as well as advanced meter reading and communication techniques [67]. In addition, privacy issues have also been studied from both hardware and software aspects [68, 71, 72].

Data Attacks

By its name, data attacks are the type of Smart Grid attacks targeting at the data flow that are transmitted along the communication network [13, 73]. Many researches suggest that the data attacks are mostly related to the state estimation of power systems [14, 74]. Attacks of this type include insertion, alteration, or deletion of data or control commands [75–77]. The application of these attacks can overlap with the consumer-end attacks in the deception of metering devices, but usually in data attacks they are targeted at power system instead of a single user-end device and organized in a more specialized way.

As some studies have revealed, the detection on the false data injection [78] or load alteration attacks [79] can be very difficult if the attackers have sufficient knowledge about the topological information of the power grids. In these worst cases, the attackers do not have to know about the operating point or the exact states of the system, yet they can nevertheless forge fake data without showing anomaly and successfully walk around the traditional detection methods. Because of the data protection can be extremely hard due to the vast amount of data collected and generated through a gigantic network, there are still many ongoing researches to optimize the chance of detection and lower the risk of disastrous consequences from data attacks.

Direct Attacks

The most severe attacks in the power grids is the cyber-physical ones directly aimed at the disruption of critical power transmission network components like power plants, substations or transmission lines [80–82]. By creating outage and tripping of these components which were in normal operation, the attackers can turn an interconnected power system into an instable state, which usually ends up in massive blackouts as a consequence of cascading failures mentioned Sect. 2.1.4 in this chapter.

In reality, direct attacks can be done by via data attacks, for instance forging fake messages of system state, outage, instability or tripping and sending them to the control centers, resulting in mistaken actions and regulations that causes cascading effects. These attacks can also be coordinated in a cyber-physical space by tools like Petri-nets [83], which will significantly increase their chance of success and the severity of the attack. Studies have shown that by exploiting the vulnerability of power systems, direct attacks can be studied as contingencies of outage since they have similar effects, yet the consequence of these malicious attacks can be much more catastrophic with the well-chosen victims selected by the intelligence information [55, 84].

2.2.3 Smart Grid Security Tools

To address thee security issues, many traditional approaches from the network security studies, including intelligent and efficient trust control, advanced encryption, bad data detection, etc. have been introduced. In addition, to better approximate and understand the interaction between attackers and defenders in securing the Smart Grid, theorems and techniques from game theory, petri-net, clustering/partitioning, data mining have been introduced. Researches based on game theory can effective display the optimal choice for both attackers and defend-

ers based on their own cost in the scenarios [85,86]. Petri-nets are very powerful in identifying and handling multiple events happened cyber-physically [83,87]. Clustering and partitioning techniques reveal critical and effective measures to refine the influence of attacks with a small area so that the protection and restoration will cost significantly less [61,88,89]. Data mining algorithms can take great advantage of the growing volume of data collected throughout the Smart Grid network sensors and extract important information on the healthiness and anomaly of the operation power grids [90]. Still, many of these tools are facing difficulties in application due to their scalability, computational efficiency or real-time capabilities [91].

2.3 Summary of the Literature Review

In this chapter we briefly introduced the emerging reliability and security issues and related researches in Smart Grid. It should be noticed that many of the researches in reliability and security analysis overlap with each other. In many cases it is impossible to investigate security issues without evaluating the stability and reliability of power systems, while it is also crucial to evaluate the cyber-physical safety and protection of power systems when they are greatly integrated with online communication networks. As a result, this thesis will set aside the differences of reliability and security studies while focus on the specific vulnerability assessment of direct attacks in Smart Grid that challenges its reliability and security.

CHAPTER 3

Power Grid Modelling

In this chapter, we will describe the model of power grid and cascading failure adopted in this study, which provides the simulation model for the purpose of cascading failure analysis.

3.1 Topological Model

As mentioned previously in Chapter 2, among the power system models available for cascading analysis, in this work the topology-based model will be chosen to provide the preliminary result and insight for further investigation. Most of the topological information on the structure of a power grid can be obtained in the form of geospatial dataset. It has been standardized thanks to the effort of power and energy industry, geographic information system (GIS) industry, as well as government supported academic institutes like the Power Systems Engineering Research Center (PSERC) and the National Institute of Standards and Technology (NIST). In contrast to the wide area dynamic operational states and parameters stored and protected in the control centers, these topological data are more accessible from commercial companies or academic institutes. They provide the time-invariant information that does not subject to the transient state of power systems, which makes it a useful source of knowledge in the vulnerability assessment of power grids.

In order to represent the power grid as a topological network, there are a few assumptions to be specified:

First, as part of a transmission network, 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 pass-through transmission substation; also, a transmission line which

connects one substation at each end will be regarded as a branch in the network. Hence the power grid is regarded as a bidirectional unweighted graph [51,52,92,93], a simplification that helps to reduce the computational cost significantly.

Second, we will define the load, on which the process of failure cascading relies heavily. From studies of high-level power grid structure [9, 15, 52, 54], it is shown that the load of a given node is highly related to the connectivity or centrality of its neighbors. It means that a node, either connecting to more neighbors or whose direct neighbors have greater connectivity, will be more likely to take greater portion of load in the power delivery. Therefore, in this work we define the load of a node as the product of its degree and the summation of the degree of all its neighbors, as in [92,94]. Let $Deg(v)$ be the degree of a given node v and $Nbr(v)$ the set of neighboring nodes of v , respectively, then the load for each node v , denoted as $L(v)$, is calculated as follows:

$$L(v) = Deg(v) \sum_{n \in Nbr(v)} Deg(n) \quad (1)$$

Thirdly, we will describe the redistribution policy in the topological model. When a victim node (say Node v) is attacked by intruders or cut off by cascading failure, its load will be proportionally redistributed to its neighbors $u \in Nbr(v)$ and the load of each active neighbor n of the victim will be updated according to Equation (2):

$$\Delta L(n) = \frac{L(n)}{\sum_{u \in Nbr(v)} L(u)} L(v) \quad (2)$$

A numeric example for Equation (2) can be shown: supposing two neighboring nodes A and B both carry a load of 100, and the total load of all of Node A's neighbors is 1000, then when Node A first fails during the cascading failure, Node B will carry an extra load of 10 since its original load contributes to 10% of the total neighboring load of Node A. Another illustrative and intuitive example is

Figure 2. Illustration of the load redistribution policy

shown in Fig.2, where the total load of all neighbors of victim node O is 100. The numbers next to each node in black is the original load, and the numbers in red is the extra load that will be added on each node if the hub node O is failed either by direct attacks or by the effects of cascading process. The redistribution policy is displayed clearly in this scenario.

Once a node fails, it will be disconnected from the power grid, which means it will be removed from the neighborhood sets of all nodes in current power grid topology, and any branches connecting to this failed node will be tripped as no more power could be delivered through it. Note that an isolated node is also regarded as failed since all branches connecting to it have been tripped. If no failure occurs after a certain amount of time, the power grid is considered as stabilized, which

marks the end of a cascading failure.

The redistribution can cause overloading on some of surviving neighbors of victim v in the grid and can lead to subsequent cascading failures. 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 with all the branches that directly linked to it. The threshold of overloading ratio, above which a node is considered failed, is then referred to as the system tolerance, and currently we 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, leading to a cascading failure across the network. If the initial victims are well-selected, the malicious attacker will be able to create a remarkable blackout in its scale or speed of propagation in the power system. Note that there is no ground-truth for the practical value of T , and so in the simulation different values of T will be tested for this important factor, which will also affect the cascading process significantly.

Finally, when a number of nodes are failed, we use the concept of “round” to help describing the progress of failure cascading. The definition of a round is illustrated in Fig.3. The very first set of failed nodes consists of the victims in the initial attack. Then the nodes knocked down by the cascading failure of initial victims will be regarded as the victims of second round, so on and so forth. In this way, failed nodes at different rounds of 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 multi-victims set of attacks. In this structure a node may have more than one parent if it is affected by multiple nodes failure at the same time, which represents the overlapping of multi-victim cascading, as shown in Fig.3.

Figure 3. Illustration of “rounds” as a cascading tree.

As the failure propagates through the surviving networked nodes, the load of the remaining system will be shed due to the impaired transmission capacity. At a certain moment, the load will be likely to drop to an extent low enough that the load carried by each branch will all stay below the fatal overloading threshold and thus the cascading process will come to a final stabilized state. The simulator will then stop the simulation and return all the data recorded during the cascading process for further analysis.

One more fact to notice is that the load and status of each node is only updated once at each round, which means the nodes failed in the same round will not have instant effect on others. Instead, the failure of all nodes of last round will simultaneously affect the remaining active nodes in next round. In this sense, our cascading model better matches a simultaneous failure process.

In spite of the assumptions and simplifications above, this topological model still is important for cascading analysis in the following aspects:

1. First, it works extremely efficient in simulating the cascading process with less computation overhead compared to power flow models. As an example, the topology-based simulation for Bay area with about 500 nodes cost similar

amount of time as a DC power flow model for IEEE 39 bus system with 39 nodes only;

2. In addition, in searching a set of multiple victims in a simultaneous attack scheme, topology based models usually provide more information and less computation overhead in refining the set of candidate victims;
3. Last but not least, it yields satisfactory approximation precision and the topographic information is not subject to dynamic variance, providing good evaluation accuracy in the structural vulnerability of power grids.

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

1. Trigger a multi-node cascading failure 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 state.

3.2 Assessment Metric

As we want to identify the most critical power grid components from the failure cascading perspective, we use the final percentage/fraction of failure in the power grid with respect to system tolerance T , denoted as PoF , as the assessment metric:

$$PoF = \frac{N_f}{N} \quad (3)$$

where N_f is the number of failed components and N the total number of components in a given grid. For each attack simulated, we measured the value of PoF

after the cascading failure stops at the final stabilized state. The physical meaning of $PoFe$ is related to the size of blackout as well as the cost of restoration, as each component brought down during the cascading failure process requires some time, ranging from hours to days, before the power transmission can be fully recovered.

According the previous definition of “round”, a cascading “tree” with more “leaves”, i.e. PoF at the final round, indicates that the initial victims have resulted in a larger blackout with more component failed consequently after the initial attack; while with less rounds it indicates a faster failure propagation with fewer intermediate process and requires a quicker decision to limit its impact at an early stage. In addition, the more “child” nodes a parent node has, the more critical it will be. By using this measurement, we are able to intuitively illustrate the effectiveness of the proposed approach using the simulation model described above and highlight the critical components in the power grid in any direct attack scenarios.

CHAPTER 4

Visualizing Cascading Failure for Spatial Pattern Analysis

As discussion in Chapter 1 and 2, for this chapter we will first focus on the spatial patterns of cascading failures in power system. To illustrate the cascading process in the space, a demo in ArcGIS is first developed with my colleague and then the spatial patterns are visualized through examples accompanied by discussions.

4.1 Spatial Analysis for Cascading Failure in Power Grids

In most researches, the information on the power systems are usually represented with the digitalized measurement, for instance generator voltage, load, phase angle, active and reactive power, among others. They are recorded as numerical values and tables, which is convenient for quantitative studies. Although many of them are accompanied by some visualization tools, it is noted that most of them did not take it as a formal form of security analysis. In many cases, the power transmission network is only represented as an abstract grid which only emphasizes the information on the substation type (generation, transmission and distribution) and the existing transmission lines connecting them. Their exact locations and lengths are usually not considered since acquiring and maintaining such information with their detailed status are either difficult (with remote locations) or expensive (to install meters and keep track of the huge amount of data generated) [29].

However, with the development of geographic information system (GIS), more and more up-to-date power grid data become available with improved accuracy. As a result, a growing number of GIS based analyses that have become popular among the study of smart grid security [29, 55, 95].

The GIS information of power grids can also be a potential intelligence resource for the attackers. These data are usually more accessible than the internal data guarded within the power control centers; yet they provide some informative details like the power grid topology and connectivity, the voltage categories, the power plants and their ownership, the length of transmission lines that could be used to approximate the admittance and resistance to solve power flows and simulate effectiveness of potential attacks. Therefore, we are interested in visualizing the power grids in the space and assessing their structural vulnerability through the spatial patterns.

Specifically, in this chapter the geospatial location and connectivity of power grid substations will be visualized for cascading analysis. The implementation of the GIS platform will be elaborated, and interesting yet important spatial information on power system cascading failure behavior will be illustrated and discussed, which has been part of the work published in [96].

4.2 Visualize the Cascading Attack

4.2.1 The Cascading Simulator

In this research, the single-victim attack algorithm proposed in [92] and introduced in Chapter 3 of this thesis is adopted as the simulation model to acquire the simulation results of cascading failure of substations and transmission lines. MATLAB is chosen as the simulation platform and the simulator will record both the stabilized grid after cascading as well as every intermediate process during the failure propagation. The failure sequence of nodes (in forms of substation IDs) will be forwarded to a MATLAB interface, which searches the victim nodes and branches in GIS database and updates the database with a new attribute as an identifier. A VBA script will be run in ArcGIS to keep track of the database and visualize the status of one interested group of objects in the ArcGIS map in the

Figure 4. Diagram of the compact ArcGIS-MATLAB visualization platform

form of layers, which could be overlapped to provide customized visualization for analysis. In our platform, we deploy 2 layers to represent the transmission network of a Smart Grid: substations and transmission lines. The flowchart of our platform is demonstrated in Fig.4. Note that the GIS databases are stored in the “shapefile” format in our experiments.

In the cascading model, as described in Chapter 4, we assume that when a node (substation) is down, its load is redistributed to its neighbors. Also, we assume that there is only one transmission line (branch) between two nodes, and multiple branches between two nodes will be treated as one.

Under these assumptions, we start the attack by picking a single victim node in the power grid. Once a node is knocked down, all the branches connected to it will also be considered as failed at the same time. Using a constant tolerance for the grid, the algorithm recalculates the load distribution iteratively and a cascading

procedure will be generated throughout the grid until the grid reaches a final stabilized status. A cascading failure is assessed by the fraction of failed nodes, denoted by PoF at each round. Here one 'round', as described previously in Chapter 4, is defined as a period of time in which a number of nodes are knocked down simultaneously by the cascading failure. In other words, in every new round a set of new victim nodes emerges. Victims in each round could be updated to the visualization interface, which is called an online model; or their information could be stored in a data sequence until the cascading process finalized, and then the failures of all rounds could be exported as a whole.

In general, the process of this attack simulation and visualization could be described as below:

1. Build up the topology for a power grid;
2. Calculate the metrics value of each node to choose the most vulnerable node to be the first victim node;
3. Recalculate the distribution of load and find out new victims at each round, store the victim substation IDs;
4. Communicate the results from MATLAB to GIS database, and update the visual information in the ArcGIS;
5. Repeat the process until no more failure nodes can be identified, i.e., the end of the cascading failure process.

4.2.2 Interface Between MATLAB and ArcGIS

In ArcGIS, our GIS database is stored in a format called "shapefiles", defined by Environmental Systems Research Institute (ESRI) as a popular geospatial data format for GIS systems. A dataset usually consists of three shapefiles for each

single layer: a .shp file containing primary geographic reference data, a .dbf file storing all the attribute values, and a .shx file saving the shape index table. It may also contain a projection file (.prj) or a spatial index file (.sbn), which are not used in our current experiments [97]. The database format is ideal for visualization as it can be imported into two sets of fields in MATLAB, one fixed set containing the geometry information such as the coordinates and types of object (e.g., point, link or polygon), and another set of attributes includes all other specific information of the object. For entries like power plants and substations, the attribute set stores information including information of location, load, owner, voltage category, generator/fuel type, etc. For branches (transmission lines) the attribute set could provide voltage category, length in mile or kilometers, IDs and names of nodes connected, among others. These set attributes could be easily customized and updated, which is ideal for real-time monitoring and management through a visualization platform.

The shapefile database can be imported to MATLAB as structure arrays by using MATLAB mapping toolbox. The mapping toolbox is a set of tools and utilities to process geographic data analysis and map displaying. It was first introduced in MATLAB 6.0 and is updated with every following release of MATLAB. An interface in MATLAB is also developed to update the cascading information into shapefiles, which can be described as four steps, the data pre-loading, the initialization, the search and update of victims, and the export.

Pre-load Data

At the first step, MATLAB loads a sequence of a cascading failure generated by the attack algorithm. The failure sequence is an M-by-N matrix of which all element values are initialized to zero, where M is the number of rounds of cascading and N is the number of final victim nodes. For each row in the matrix, the j th

row in failure sequence contains the IDs of all victim nodes that have already been knocked down at the j th round.

In addition, MATLAB also loads the shapefiles from both databases of substations and transmission lines, matching up the victim nodes information with the failure sequence. The import is done by a function called `shaperead` from MATLAB's mapping toolbox, which reads geo-information stored in shapefile format and arrange them into an array of geo-structures. The compact geo-structure array is MATLAB-friendly and easy to customize, providing fast calculation as well as good compatibility.

After this step, we store three arrays in MATLAB: an M-by-N failure sequence called *Fail_seq*, a K-by-1 structure array of nodes called `NODE` and an L-by-1 structure array of branches called `LINK`, where K and L are the numbers of substations and transmission lines in our database, respectively. In our case, $K = 553$ and $L = 726$.

Initialization

At the second step, our interface customizes the database by introducing a new field `FAIL` to each element of both structure arrays `NODE` and `LINK`, which would be exported as one attribute for each database. In our current development, this attribute will simply record the round number when the current object is taken down by the failure cascading. A zero value of `FAIL` means the current object (node or link) has not been affected by the cascading, while a positive value k indicates that the current object is already taken down in the k th round. In this way, our VBA script could effectively read the `FAIL` attribute and visualize its value in ArcGIS.

Search and Update Victim Nodes

In the shapefile dataset, the substations' IDs are stored in an attribute named SUBID, which would be imported as one field of the structure array in MATLAB. Also, the IDs of the two nodes connected by a given transmission line are stored in our transmission line database and would be imported as two fields named SUB1ID and SUB2ID in the structure array of LINK. In this step, the interface first searches the SUBID field of structure array NODE with each of the failed nodes' IDs, and updates the field of FAIL of the corresponding node with the round that it fails, i.e. the number of the first row that contains the ID in the fail sequence. Then our interface does the same thing for the transmission lines, compares the IDs of *Fail_seq* with the sequences of SUB1ID and SUB2ID to identify which branches are connected to the given failed nodes, and updates the FAIL value for each transmission line with the round number in which it fails.

In order to provide better performance, we also sort the database according to the most important information. In this interface, both structure arrays NODE and LINK are sorted on the FAIL value before written back to the database. To be specific, entries of nodes or branches will be stored in an order such that the node failed at the earliest round will stay on top of the array while the node failed in the final round will stay at the bottom. In this way, the VBA script in ArcGIS can read the FAIL value sequentially and highlight this key information more efficiently.

Export to Shapefiles

The export of geo-structure array in MATLAB is as convenient as the import process. The mapping toolbox provides a function called shapewrite to export geo-structure arrays to shapefiles. Since we only add one field in the structure array which will be converted to an attribute in the database, we simply call shapewrite with the name and directory of the two databases and the updated information

is saved into shapefiles for the ArcGIS. One practical fact to note is that when exporting geo-structure to a shapefile format using the *shapewrite* function, a number writing error may appear in earlier version (before R2007b) of mapping toolbox. A numeric value longer than 10 digits will cause a mismatch in shapefiles while the bug was not informed in MATLAB. In R2007b, an error will occur, warning that matrix dimensions do not match. The best solution is to update MATLAB to the latest version in which the bug has been fixed.

While we are processing a GIS database which stores information of substations and transmission lines separately, we should keep aware that there could be some data inconsistency across the shapefiles for each layer. The limited size of our snapshot could lead to incomplete information on connectivity of power grid. In some cases, the value of SUB1ID or SUB2ID in the structure array LINK for the branches could be zero. The reason is that the corresponding branch may connect a pure power plant to a substation, while we do not have an SUBID for this node of power plant. And there are also other cases that a node itself is both a power plant and substation, assigned to distinct IDs. As a result, in the upper Bay Area power grid studied in this chapter, there are 41 out of 726 branches yielding some form of data inconsistency, while 13 of the ID-mismatch nodes in the branch layer are actually isolated from the main grid in the Bay Area, which possibly means that they could be part of another power grid not fully covered in this regional snapshot.

4.2.3 Visualization in ArcGIS

The credit of this subsection is given to Yida Yang, who worked with the author together in the same project, with the corresponding script and text written by him. To keep the integrity of this chapter, this subsection (Sect. 4.2.3) is included as in the original published conference paper [96]. The objective of the

visualization is to acquire the GIS database containing data for substation and transmission line failure and then display the results in ArcGIS in an animated way, so that the cascading failure effects are effectively displayed and the critical nodes can be quickly identified. In addition, the interface should allow user interaction, meaning that users can manually select attack victim on the platform and see the cascading effect due to the failure of such nodes. Therefore, users can compare and contrast the vulnerability of nodes visually and identify the nodes that are most critical.

The objective is achieved by Visual Basic for Applications (VBA) programming in ArcGIS Desktop, which is one of the application components of ArcGIS. It consists of ArcObjects, a set of platform-independent software components written in C++, which provides services to support GIS applications on the desktop in the form of thick and thin clients and on the server. The results of the visualization program are displayed in ArcMap, the main component of ArcGIS Desktop, together with geographical basemap. The flowchart for visualization is shown in Fig.5 and the corresponding script was developed by my co-worker Yida Yang as a co-author in the published conference paper [96].

The VBA script has 4 major steps:

1. Retrieve selected attack victim node from user and pass the node information to MATLAB;
2. Read shapefiles to obtain the node and link information after Matlab finishes calculation and returns the result;
3. Draw all categories for both substation and transmission line data according to the value in the FAIL attribute;
4. Apply color for better visualization.

Figure 5. The detailed flowchart of the integrated visualization platform

Step 2 and step 3 can be accomplished by using ArcObjects member functions and methods. In step 2, a workspace has been opened to load the feature classes in shapefile. The IMap.DeleteLayer and IMap.AddLayer functions are used to clean previous data and add new data, respectively. Two sets of data have been added into the workspace, one for substations, and the other for transmission lines.

In step 3, the iRender object is used to add categories according to the FAIL value. The iRender.Addvalue function was called twice to apply to both substations and transmission lines. The categories added for both data sets match the round in which they were knocked down.

Step 4 has been the most challenging part. In this part, the program displays the substations and transmission line failure in an order in which they have been knocked down. Due to the possibility of a node (substation) fails after all the transmission lines affiliating to it have already failed, a mismatch between the FAIL value in substation and transmission line in the same loop cycle may occur. The issue was resolved by comparing the FAIL value for substation and transmission line and making the “painting” function for transmission line wait for one or multiple loop cycles until the FAIL value for both are equal. In addition, three colors, red and blue and black are used to distinguish substations and transmission lines that are knocked down in the current round, knocked down in previous rounds or in normal operation, respectively. The nodes, which are more critical and may cause more devastating effect if failed, can be identified. Furthermore, the time interval between failure rounds can be controlled by the “Wait” function.

4.3 Simulation Result

The visualization platform has been developed with MATLAB R2010b and ArcGIS 10.0. The data are a snapshot extracted from the POWERmap GIS dataset provided by PLATTS, including 726 transmission lines and 553 substations to

represent the major power grid of upper Bay area in San Francisco, California, as shown in Fig.. Each link and node contains attributes that could be imported into MATLAB in forms of structure arrays.

Several experiments have been performed using this real database. Fig.7 to Fig.8 show some map snapshots of the results. A node or a link in normal condition is shown in black. All the new victims at the current round are highlighted in red, while the previous victims have been marked as blue for clear visualization. In the all these experiments, the network tolerance factor (see [92]) is set to be 1.2, an empirical value also suggested in [55]. Fig.7 displays the moment when the first victim node is under attack. When it fails, all the branches associated with it also fails. Fig.8 shows the finalized cascading failure where all possible substations and transmission lines fail according to the cascading failure simulator. These results clearly demonstrate that by carefully selecting the attack victim nodes at the very beginning, it is possible to break down the entire Bay area power grid.

In addition, we are also able to visualize the effects of *sequential attacks* of the grid via using this platform. Here, the sequential attack means that more than one attacks can be launched sequentially in different rounds. In the sequential attack model tested in our experiment, it is assumed that the cascading effect of the previous attack had already come to a stop due to some system protection mechanisms, but the failure area has not been restored before the launch of another attack. So the previous cascading will only black out part of the grid and the new attack will continued to cause failure propagation in the remaining power grid.

The results of sequential attack are shown in Fig.9 to Fig.11b. In Fig.9 we show the result of first attack (launched at the identical victim as in Fig.7) right before the cascading failure is stopped thanks to some type of rescue effort. Then Fig.10a shows the beginning of another attack, which starts afterwards and affects

Figure 6. The upper Bay Area grid under normal operation

Figure 7. The first victim failed at the first round

Figure 8. Final stabilized cascading failure

a distinct region from the first attack chosen by the attacker. At this moment, as we can see, the result of the first attack still remains unrestored. Then Fig.10b shows the cascading effect at the end of the second attack when it comes to a natural stop. Finally in Fig.11a, the third and last attack starts in a region closer to the second one, while Fig.11b shows the final cascading result of all three attacks. Note that the failure propagation of the first attack has separated the grid into several disconnected regions or “islands” when it was stopped by rescue effort. Therefore, the cascading effect of the following attacks, which takes place in the separated islands, will not propagate to the other islands of the grid. This example illustrates not only how failure can propagate in different sub-grids, but also that the remaining grid can be the potential target of a series of attacks.

Figure 9. Cascading effect of the first attack

4.4 Discussion

From our simulation results, some interesting initial observations have been made. As shown in Fig.12a and Fig.12b, there are some critical moments during the cascading procedure, in which failure of certain nodes can cause a long distance migration of subsequent cascading failure into a remote part of the power grid in a very short time. These nodes should also be considered as critical as the victims that yield a large size of final cascading failure, for the reason that they play important roles in the prevention of a small area failure turning into a cross-region disaster. At the beginning stage, the new failures only emerge in neighbors of most recently failed nodes, and the spatial distance between them is relatively small. This shows a typical behavior of a transmission cluster, in which interdependent nodes are closely connected by branches. However, after several rounds, the edge nodes of cascading become more spatially scattered: new victim nodes could be widely separated in distance, and the cascading may happen in remote regions that

(a)

(b)

Figure 10. Sequential attack: (a) launching the 2nd (b) end of the 2nd

(a)

(b)

Figure 11. Sequential attack: (a) launching the 3rd (b) end of the 3rd

are not around the edge of most recent cascading failure areas. We refer to the *critical moment* as the round when new victim nodes become disconnected in a remote region in comparison to the existing victim nodes, a phenomenon that poses more challenges to the protection of power grids and requires more inter-regional cooperation among different power companies and operators. Our experiments show the existence of such critical moments of failure migration, which are also observed and described in [55] in a power grid structured in a theoretical rather than practical way, whose observation was that “the consecutive cascading failure can occur at an arbitrary long distance”.

In addition, our simulation results also reveal that the connectivity of components does not necessarily determine the severity of subsequent cascading failure when they are the initial victims, even though connectivity itself, as in the definition of load, is highly associated with the load. For example, in Fig.6 to 8, the attack on an edge node connecting only a leaf node to the main grid, can also result in a severe cascading failure; however, another example shown in Fig.13a and 13b reveals that a node with almost the same connectivity in the grid, i.e. a transitional node connecting a leaf node to the main grid, will only result in a much smaller impact in the power system.

More interestingly, in simulation we can find some hub nodes that yield a large connectivity and serve as a regional connecting point; and while most attacks on them can lead to significant impact on the security of the benchmark system (Table 1), in some specific cases, the failure of a hub node (a node serves as a regional connecting point) may merely lead to no or little cascading impact as shown in Fig.14.

These observations have been summarized in Table 1, which shows the degree (the number of immediate neighbors), the number of nodes with the corresponding

(a)

(b)

Figure 12. An example of cascading migration (a) before critical moment (b) after critical moment

Table 1. Summary of connectivity and PoF distribution

Node Degree	Number of Nodes	Number of $PoF > 10\%$	Node Degree	Number of Nodes	Number of $PoF > 10\%$
1	163	7	10	1	1
2	127	24	12	1	1
3	150	44	14	1	1
4	31	10	15	3	2
5	9	3	16	3	3
6	9	4	22	1	1
7	4	1	27	1	1
8	3	1	32	1	1
9	2	1			

the degree, and among these nodes how many single-victim attacks can lead reach a PoF above 10% in the upper Bay area. As we can see, although for nodes with a larger degree, the discrepancy between the corresponding number of nodes and the number of more vulnerable victims narrows down, it is still observed that for nodes with any connectivity, even with very small values, they can still trigger large area cascading failures as well. In other words, the degree of a node itself is not a good indicator to predict the final impact of an initial attack. The reason behind can be interpreted by the influence of the neighboring nodes. As an example, the edge victim node in Fig.6 has a neighbor with higher connectivity to the main regional transmission network than the other victim node in Fig.13a. This difference in neighborhood nodes results in the different load and thus distinct cascading impact once they've been attacked and their load redistributed. Therefore, due to the network resilience and redistribution policy, the spatial vulnerability of power system could be more complex than a simple topological issue which requests further in-depth investigation.

In summary, these observations above have shown that some crucial information could be obtained from the visualization of the cascading failure in the geo-space. Also, since most simulation of the attack and the entire cascading pro-

(a)

(b)

Figure 13. A victim near the edge (a) being attacked and (b) its cascading impact

Figure 14. A hub victim that yields no cascading effect

cess cost less than 2 seconds using the GIS maps, it is very efficient to simulate Smart Grid attacks and locate the most vulnerable nodes of a given transmission network in this intuitive and illustrative way. With this information at hand, it becomes more convenient for designers to refine topology of the electric grid under operation constraints, increase fault tolerance, and redistribute the power flow properly, which would help improve the security and reliability of the smart grid. In addition, some of the important simulation results (e.g. most fatal attack and their corresponding victims) could be stored as an intelligence database, so that if a cascade failure is inevitable in real world scenario, power engineers can quickly identify the source of failure or blackout, find out the most emergent nodes to protect or restore at the current round, such that it will be possible to efficiently recover the Smart Grid from black-outs and significantly reduce the time that consumers have to suffer from power outages.

Other preliminary results, following similar direction from both the author

of the thesis [98] as well as from other researchers [29, 55] have also shown other approaches that we can explore the structural vulnerability of the power system via geospatial information or geographic correlation. However, this will not be covered in the proposed scope of the thesis, and interested readers can refer to these reference papers for more information.

CHAPTER 5

Revealing Temporal Features in the Cascading Failure Process

In addition to the spatial information of cascading failure discussed in previous chapter, in this chapter, as part of a published work [99], the author will discuss the exploration of temporal features of cascading process.

5.1 Temporal Features in Power Grid Cascading Failure

Compared to traditional power system security analysis, there is another less-developed topic on cascading failure, i.e. the assessment of temporal features or patterns for the intermediate events and stages of cascading failure, which can become a new perspective to the cascading analysis. In reality, a cascading failure rarely propagates across the whole power transmission network and blacks out large scale areas without being detected, mitigated or stopped by automatic-protective mechanism and rescue efforts. In order to reduce the risk and impact of major blackouts, the knowledge of temporal features and patterns is critical for responding to cascading failures with timely and sufficient defense strength at an early stage. To be specific, there are three major reasons to further investigate the cascading failure from the time domain:

1. While various selections of victims can lead to similar scale of cascading failures in a power grid, the procedure of each varies from one another by features like the scale, rate, duration of failure propagation at certain critical moments and stages;
2. The resources available to defend cascading failure are usually limited and require different amount of time to be activated, so timing is critical to properly deploy the defense power to optimize the effect of rescuing efforts;

3. Though well-design power systems with larger fault tolerance can be more resilient to cascading failures and Smart Grid attacks, the required cost of hardware and maintenance can be intimidating. Thus comprehensive studies on temporal features, which add a “temporal” factor to the power system resilience, can maximize the effectiveness and efficiency of defense with relatively lower requirements of system tolerance. This is critical for smaller, distributed infrastructures and facilities that are widely integrated in the Smart Grid.

In this chapter, another factor in cascading failure, i.e. the overcurrent relays in power systems, will be incorporated into the study. As mentioned in Chapter 2, power system relays play a critical role in many cascading events. The relays, which can automatically cut off risky components to maintain the stability of the current power network, can also adversely trigger a large scale outage due to the insufficient generation units connected to the grid to meet the demand when the relays disconnect them.

From the security perspective, relays hacked or controlled by malignant attackers can pose a great threat to the power system stability. Using this hijacked relays, attackers can trip branches, isolates substations and islands grids, among others. Therefore, it is important to consider and simulate the role and influence of these relays in cascading failure events. Based on the simple model described in Chapter 4 and employed in Chapter 5, some modifications have been made to better approximate the system behavior with the presence of power system relays.

5.1.1 Model Specification for the Temporal Analysis

The simulation model for the temporal analysis in this chapter is based on the one that was used previously. However, it has an important modification to represent a critical temporal factor that will affect the failure propagation, i.e. power

system relays that cut overloaded components after the accumulated overload exceeds a certain amount. This means instead of instantly tripping (or removing) the heavily overloaded node or branch, to better approximate the temporal process of failure propagation, in this modified model the overloaded components will maintain less efficient but yet effective operation for a certain amount of time until the thermal overload has been accumulated over a given threshold. From the defensive view, this period represents a transitional window embedded in the power system that allows proper reactions before the overloading situation worsens.

Therefore, we apply a time-delay overcurrent relay in our model which monitors and modifies the status of overloading nodes. To be specific, a timer will be triggered whenever a node starts to overload, and its output is taken into an accumulative function of both overloading ratio and time. In each round, we test the overloading status of nodes, increase the value of the timer and update cascading node failures accordingly. It may take several rounds for a node turns from overloading to failure, and once it fails the corresponding load redistribution and topology updating will be performed for the iterative simulation in the next round.

With the assumptions above, the accumulative time-delay function is defined as

$$d(n) = \sum_{k=0}^n L_k - TL_0 \quad (4)$$

where n is the number of rounds that a node has been through in overloading status, T is the tolerance of a given system, and L_k is the current load of a given node at round k . The timer is triggered when L_k is larger than its capacity TL_0 and accumulates over the duration of overloading. Similar to the continuous realtime relay in [12], an empirical threshold of $d(n)$ is set so that any node carrying an extra load of 50% of its capacity for D rounds will be regarded as failed, and the relay will instantly disconnect the failed nodes from the power grid. In other

words, D is the maximal time-delay before the relay considers the overloading of a given node is fatal enough to be cut off from the power grid.

According to Equation (4), the overloading timer of a node launches when its load goes above its capacity, otherwise it will be reset to zero. In other words, the relay will not affect the status of a node that has already failed, not yet reached a fatally overloaded ratio, or already recovered from the dangerous state. From Equation (4) it is shown that for nodes which yield lower overloading ratio or less overloading rounds, they will remain in operation longer. Also, since in reality some policies will be automatically applied to the overloaded component to mitigate its overloading, we consider a maximal duration of overloading, beyond with the overloading will not be fatal anymore. Specifically, in the following simulation it is assumed that a cascading failure ends when no subsequent failure emerges in $3D$ rounds.

In general, the overall procedure of cascading failure is illustrated in Fig.15. This simulation model builds up the platform for our temporal feature analysis.

5.1.2 Temporal Features of Cascading Failure

To reveal the temporal features of cascading failure initiated by attacks, the percentage of failed nodes (PoF) at a given round will be measured, whose definition is the same as in previous chapters. Intuitively, the value of PoF will increase nonlinearly over time, and at some moments its raise will suddenly boost within a short period, which means the cascading failure is accelerating during this period. For each cascading failure initiated from different victims, there are three aspects to look into this temporal feature:

Figure 15. The flowchart of cascading failure model with time-delay

Leaps

A “leap” is the sudden dramatic rises of PoF within a small number of rounds, whose duration and magnitude differentiate various process of cascading failure from each other and provides key information on the optimal timing for response action. With similar final PoF , the duration of a cascading failure can tell how quickly the leap can shock the power grid and the magnitude can illustrate how strong the impact is. Specifically, a leap of the failure percentage occurs between round n and $n + \Delta n$ if the following criterion is satisfied for all rounds between n and $n + \Delta n$

$$PoF(n + \Delta n) - PoF(n) \geq P_1 \quad (5)$$

where $P_1 = 0.015$, so we will consider an increase of PoF as a leap if its magnitude is no less than 1.5% for at least one round, and its duration is an upper bound N such that any $\Delta n \leq N$ satisfies the condition in Equation (5). Note that P_1

is related to the strength of the initial attack, and for some large power grids P_1 should be decreased accordingly as even the same powerful attacks in those grids are not likely to result in the same actual number of failure, or the magnitude of leaps.

First response moment

In the early stage of failure propagation, the period before the first leap occurs or the overall failure percentage reaches a certain degree is often the “golden time” to take actions to minimize the impact of cascading failure. Hence a first response moment n_0 is defined as

$$n_0 = \min\{n_1, n_2\} \quad (6)$$

where

$$n_1 = \underset{n}{\operatorname{argmin}}\{PoF(n+1) - PoF(n) \geq P_1\} \quad (7)$$

$$n_2 = \underset{n}{\operatorname{argmin}}\{PoF(n) \geq P_2\} \quad (8)$$

In the equations above, we use $P_1 = 0.015$ as in Equation (5), and choose $P_2 = 0.1$ to mark the threshold for a failure that exhibits significant damage to the power grid. Therefore Equation (6) identifies the very first round in which either the *first leap* appears or the failure percentage *PoF first reaches 10%*.

Number of leaps and buffer period

In each cascading procedure, there could be multiple leaps, and the number of leaps in a single cascading procedure reflects how radical the increase of *PoF* is. Given a fixed final failure percentage *PoF*, a number of leaps indicates that the cascading failure will go through several stages, between which the rate propagation will slow down for certain amount of time, then it will accelerate again when some other critical component failures occur due to their fatal overloading. Hence, the

intervals between leaps of a *PoF* curve, if exist, can provide useful information on the buffer periods during which actions can be taken to effectively mitigate the cascading failure before next dramatic rise of failure percentage.

The knowledge of this feature reveals more importance when the defense strength of power grids are limited to cope with small scale cascading failures. In many cases, there could be a few small leaps and buffer periods, and each of them represents a temporal window that allows power grid managers to reallocate power demands, activate backup resources, and restore normal power delivery; whereas in other cases cascading failure with consecutive big leaps merely allows limited time to response immediately at an early stage.

For all the temporal features discussed above, one fact to notice in our model is that the system parameters such as maximal time-delay D , system tolerance T and even the spatial connection can substantially affect the cascading procedure in different power grids. Therefore in the simulation we will also evaluate how these factors can impact the cascading failure.

5.2 Simulation Setup

In the following simulations, we will reveal temporal features of cascading failure by testing various maximal delays D , victims v_0 and system tolerances T . The test power grid in our simulation is the Bay Area grid extracted from the POWERmap GIS dataset provided by PLATTS. This snapshot is the latest update in July 2012 with 510 nodes in the lower Bay area, which is slightly different from the one used in previous chapter. It represents a typical regional power grid of a metropolitan area which will easily draw the attention of potential malignant attackers, and its topology and geometry is shown in Fig.16. Note that a leap in this power grid by previous definition involves the failure of more than 12 nodes within one round, which can be a serious enough failure in the power system.

Figure 16. The upper Bay Area power grid with 510 nodes

We consider the power grid has a possible system tolerance T ranging from 1.0 to 2.0. Assume that attackers can only obtain limited information of the power grid such as the topology and the top loaded nodes, but they have no further knowledge of the status of power grid generation, operation or management. Intuitively they are likely to choose the nodes with the greatest load if there is no other cost of attack considered. Therefore we perform the simulation on the nodes with the greatest initial load to explore the temporal features in cascading failure and how they are affected by different system parameters.

5.3 Temporal Feature Revealed

First, by setting system tolerance $T = 1.1$, we select the top 9 nodes with the largest load as the candidate of victim for a single victim attack, and then simulate the cascading process for various values of D under a given tolerance. The general

Table 2. General information on the most loaded nodes in temporal analysis

Rank	Node ID	Load	PoF_f
1	15	2496	92.94%
2	14	2112	92.94%
3	38	1380	92.75%
4	53	1131	92.94%
5	29	825	92.75%
6	77	781	92.75%
7	76	741	92.94%
8	57	702	92.94%
9	55	689	92.94%

information of victim load and blackout size is shown in Table 2, where PoF_f is the final failure percentage after each attack under the condition that $T = 1.1$ and $D = 0$. Each cascading failure starts from distinct attacked victim that has the greatest load in Bay Area. As we can see from Table 2, the final percentage of failure PoF_f is similar to each other in most cases under the given low system tolerance $T = 1.1$, providing little information to compare between these attack schemes. Although this appears to indicate that all these attacks are impactful, yet by exploring the temporal features, some significant differences can be detected and it proves to be a practical way to compare the vulnerability of different nodes in terms of cascading failure, as the following simulations and discussions exhibit.

In Fig.17, the PoF curves obtained from our simulation results with respect to the number of rounds under various values of D are illustrated, where the X-axis is the round of cascading failure and the Y-axis is the failure percentage PoF . For some values of D , there will be no cascading failure observed within $3D$ rounds after the initial attacks on some of the victims, and thus the corresponding PoF curves are not shown in Fig.17 for better visual clearance.

First, we suppose that all devices have the same value of D . From Fig.17 it is clear that the time for each attack to reach its final impact varies from each other

Figure 17. The cascading failure caused by attacks for $T = 1.1$.

in terms of rounds, and the difference becomes more distinct with the increase of D . For some victim nodes, e.g. Node 38, 55 and 57, their cascading process exhibit stages of acceleration and slowdown in the rise of PoF until the failures finally reach the stable state. Also, under different values of D , e.g. $D = 1$ and $D = 0$, attacks on Node 29 and 53 allow first response moment to be sufficiently long since no additional failure occurs in $3D$ rounds; while for Node 77 as the victim, the first response moment n_0 will be doubled by increasing D to 1. Similar increase of n_0 can be found in attacks on victim nodes like Node 14, 15, 55 and 57 as well, with different values of D in the comparison. Moreover, for Node 55 and 57, with any non-zero values of D , the cascading process in each case displays two major leaps with a buffer period in-between, and the increase of D can introduce an extending buffer period between the leaps for each attack scenario.

However, for Node 14, 15, the presence of a relay will not be able break the

single leap into several like they do for Node 55 and 57, nor will they bring up any buffer periods; only a minor fluctuation of the growth of PoF is found in each attack. Nevertheless, the first response moment n_0 is indeed extended due to the extra time required to accumulate the thermal overload until a fatal level is reached. Meanwhile, it is noticed that for Node 38, the cascading process yields a slowdown at a late stage, even though it is not identified as a buffer period or a breakdown of a single leap in our criteria.

As the the simulation results suggest that D can significantly change the shape of PoF in the time-domain, it suggests the importance of their application in the power grids. Therefore, more general discussions on the relays as an individual factor affecting the temporal features will be included in Sect. 5.4.1

Also, take the cascading failure of attacking Node 57 as an example, given that we have the prior knowledge that $D = 3$. From Fig.18, we can identify three leaps during the cascading failure: a minor leap take place from Round 8 to Round 15, and a major leap from Round 26 to Round 35, respectively. Hence the first response time n_0 in this specific case is 8, while there is one buffer period from Round 16 to Round 25. These temporal features clearly highlight the critical moments to response to the cascading failure caused by attacking Node 55:

To avoid a cascading failure in the gird, actions must be made within 8 rounds to mitigate the 13 overloaded nodes caused by the failure Node 55, either by calling up backup resources or cutting off demands. If this critical period is missed, the failure propagation accelerates and it would be difficult to limit the cascading effect until Round 13, after which the cascading speed slows down to less than 1.5% each round for 13 rounds. And this will be the last chance to curb the cascading failure at a failure percentage of about 22%. It is observed that during this period, although there are 4 rounds with only one or no node failure, there are already

Figure 18. The change of failure percentage at each round for Node 57.

over 15% nodes failed with 8 to 34 nodes overloaded, so it requires much more effort to stop the cascading failure compared to the first response period. After Round 25, the cascading process will inevitably accelerates again until it reaches a finally stabilized yet disastrous state.

5.4 Discussions

With the simulations discussed above, it then becomes feasible to discuss the factors that can affect the temporal features, which can provide decision supports to enhance the power grid security accordingly.

5.4.1 Time-Delay Relay

As shown in Fig.17, the maximal time-delay D plays an important role in the cascading procedure. Most nodes only have one major leap because of the heavy load they are carrying, especially when D is low and allows little time before an overloading turns into a failure. In Fig.17, the cascading procedure for all these 9 nodes are quite similar when $D = 0$, and so it will be very challenging to intervene the cascading process at an early stage, in which the initial impact of the attack

has not shown up.

However, when the value of D is increased, some of nodes like Node 14, 38, 76, 57 and 55 will yield some leaps during the cascading, and buffer periods will emerge when D is increased large enough. In reality, if D is raised sufficiently large, the power system will have plenty of time to restore normal operation automatically or manually, hence eliminating the chance of cascading failure. For example for Node 53 and 29, by increasing D to any integers larger than 1, no cascading failure will occur in the Bay Area, even if they have the 4th and 5th largest load in the power grid with 510 nodes. Unfortunately, the installation of such highly resilient relays and branches can be not only expensive, but also risky since the tripping or cutoff also plays crucial roles in keeping the system stable when other faults are taking place.

Meanwhile, the time in which a leap is delayed by increased D is not a linear function of D , as shown in the figures. Comparing the PoF curves, it is shown that an increased value of D determines the total rounds of cascading failure before it stabilizes, the first response moment n_0 corresponding to the a major leap or a significant failure scale.

Based on the influence of D to the cascading process in the time-domain shown in Fig.17, we can categorize the victims and cascading failures into three general types:

1. Preventable: Victim nodes like Node 53, 29, 77 can fall into this category, all of which can be effectively defended by proper increase of D rather than post-attack responses, since for the potential cascading that may occur there is little variation in the development of a series of rapidly propagating failure;
2. Vulnerable/critical: Victims like Node 15, 14 can be the representative of the second category. Node failure included in this category yield significant

resistance to the increase of D , marking them more vulnerable and critical in the power system infrastructure;

3. Defensible: Victim nodes in the last category include Node 57 and 55, on which we have found significant influence of D to the first response moment, the buffer periods as well as the leaps. In other words, temporal analysis on these victim nodes can reveal more helpful information to the Smart Grid operators, facilitate proper and timely reaction to the attacks detected.

5.4.2 Spatial Connectivity

In addition to the time-delayed relays, from the PoF curves in Fig.17, we can see that the spatial location and connection can affect temporal features as well. First, when two nodes are spatially close to each other, their PoF curves exhibit similar patterns given the same system parameters, as shown in the cases of Node 15 and 14, and Node 55 and 57, suggesting that they are interdependent in the cascading failures. Second, while the buffer periods can start at arbitrary rounds with different lengths if the value of D is changed, they always correspond to a certain value or range of failure percentage PoF , which is associated with a given spatial area affected by the cascading failure. This observation implies that the buffer period is also related to the actual geo-spatial cluster of failed nodes.

5.4.3 System Tolerance

Finally, choosing the single victim attack on node 57 as an example, the effect of system tolerance T on the intermediate stages of cascading failure is shown in Fig.19, with $D = 1$. Increasing T from 1.0 to 1.3 can break down a large leap into smaller ones, thus generating a buffer period and increasing the length of it. Also, when T reaches a threshold, it can essentially prevent the cascading failure; for instance, it is observed that when T is equal or larger than 1.3, there will be

Figure 19. The influence of system tolerance

not cascading effect at all if the attacker chooses to initiate the cascading failure from Node 57. However, in reality the cost to construct and maintain such a high tolerance can be prohibitive, which means the temporal feature is still important in providing critical information for the timing of defense response.

5.5 Summary

In summary, in this chapter we reveal several critical temporal features in the cascading analysis of power system. While for the most loaded nodes in the power grid the cascading procedure after they have been attacked could lead to similar final failure percentage, the intermediate process varies significantly. Therefore, temporal features provide key information on the defense against Smart Grid attacks. These features includes the time-domain location, magnitude, duration, number of occurrence of leaps as well as the buffer period for a second chance to response. Among them we have explored three of the most critical and meaningful, i.e. the leaps, the buffer period and the first response moment, and the number of leaps. The study in this chapter can shed some light on an important dimension for cascading failure analysis in the development of a comprehensive understand-

ing of Smart Grid security, which can help in the operation, protection as well as planning of the Smart Grid.

CHAPTER 6

Conclusion and Future Work

6.1 Conclusion

The Smart Grid, while enjoying the latest intelligent technologies for efficient and reliable power delivery, is also facing some critical security issues raised by both the original structural vulnerability of traditional power systems as well as its integration with communication networks. This thesis has focused on the security analysis of Smart Grid on a specific type of threat, i.e the cascading failures caused by potential attackers in power grids. Simulations and discussions in this work are drawn from two perspectives, i.e. spatial patterns and temporal features, where the corresponding results are obtained on a carefully refined topological model.

In the analysis of spatial pattern, an integrated ArcGIS-MATLAB based visualization platform developed by the author and his teammate is first presented. The compact demo is then employed to study cascading failures of a smart grid under attack scenarios in the geographic space. Our detailed implementation strategy and simulation results demonstrate the complex spatial patterns observed in the simulation of power grid cascading events, the existence of critical moment of long distance failure propagation within a short time, and the relationship between the size of cascading failure with respect to the connectivity of each substation. Hopefully the specialized platform can allow power engineers and operators to effectively and efficiently model and simulate different attack strategies, facilitate understanding of power grid behaviors under complex cascading failures, and eventually help the development of advanced defense strategies to enhance the security and reliability of the Smart Grid.

In the analysis of temporal features, several critical temporal features have been revealed in the cascading analysis of power system. Although for the most

loaded nodes in the power grid the cascading procedure leads to similar final size of cascading failure, the intermediate stages vary significantly. Therefore, temporal features such as the location and magnitude of sudden change of failure/blackout size, the corresponding duration, the number of occurrence of such “leaps” as well as the “buffer periods” which allow a second chance to response, provide key information on the defense against smart grids attacks. Specific examples have been discussed in the related chapters with their practical meaning to the timely response of such attacks. This study on the temporal features of cascading procedure caused by malicious attacks can provide another important dimension to the comprehensive understanding of smart grid security and help power system managers in the operation, protection and planning of Smart Grid.

6.2 Future Work

In general, our future work includes the following parts, which will consist of the author’s work in his pursuit of PhD degree in the future:

- Improve the power grid model to an extended topology model [100] and power flow model as presented in [12];
- Reveal more information on the intelligent attack strategies in the selection of most vulnerable components in the power grid;
- Simulate defense strategies with limited strength and resources, and reveal the optimal timing and tactic to respond to different types and stages of smart grid attacks.

For the integrated visualization Smart Grid security platform, we are also working to extend it to a larger scale database such as the entire North America power grid, which contains thousands of substations as potential victim nodes and tens of thousands of transmission lines, making it a much more complicated

network. Since our structure of platform has not contained any limitation on the size of dataset, it should have good scalability on cascading on the visualization part. However, the computational cost may grow by a certain extent, which could pose some challenges for the computation core and its real-time performance. Our future work also aims at a highly integrated interface that is more versatile and compatible with other power system models, and the whole simulation can be embedded solely in ArcGIS, so it could provide more interactive control as well as real-time visualization of power grid response to complicated attacks. In general, all these works are expected to be helpful in defending the Smart Grid against the potential smart attacks.

LIST OF REFERENCES

- [1] “The smart grid: An introduction,” The U.S. Department of Energy, Tech. Rep., 2008. [Online]. Available: <http://energy.gov/oe/downloads/smart-grid-introduction-0>
- [2] “Demand reductions from the application of advanced metering infrastructure, pricing programs, and customer-based systems - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/demand_reductions_application_advanced_metering_infrastructure_pricing_programs_and_custome
- [3] “Operations and maintenance savings from advanced metering infrastructure - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/operations_and_maintenance_savings_advanced_metering_infrastructure_initial_results
- [4] “Reliability improvements from the application of distribution automation technologies - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/reliability_improvements_application_distribution_automation_technologies_initial_results
- [5] “Application of automated controls for voltage and reactive power management - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/application_automated_controls_voltage_and_reactive_power_management_initial_results
- [6] M. Amin, “Guaranteeing the security of an increasingly stressed grid,” *IEEE Smart Grid Newsletter*, feb. 2012.
- [7] “Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations,” U.S.-Canada Power System Outage Task Force, Tech. Rep., apr. 2004. [Online]. Available: <https://reports.energy.gov/>
- [8] “Report of the enquiry committee on grid disturbance in northern region on 30th july 2012 and in northern, eastern & north-eastern region on 31st july 2012,” The Enquiry Committee, Ministry of Power, Government of India, Tech. Rep., aug. 2012. [Online]. Available: http://www.powermin.nic.in/pdf/GRID_ENQ_REP_16.8.12.pdf

- [9] 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," *Power Systems, IEEE Transactions on*, vol. 27, no. 2, pp. 631–641, may 2012.
- [10] 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 1 - overview of methodologies," in *Power and Energy Society General Meeting, 2011 IEEE*, jul. 2011, pp. 1–10.
- [11] 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 *Power and Energy Society General Meeting, 2011 IEEE*, jul. 2011, pp. 1–9.
- [12] M. Eppstein and P. Hines, "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," *Power Systems, IEEE Transactions on*, vol. 27, no. 3, pp. 1698–1705, aug. 2012.
- [13] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 38–45, aug. 2012.
- [14] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 24–29, aug. 2012.
- [15] 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.
- [16] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, "Complex dynamics of blackouts in power transmission systems," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 14, no. 3, pp. 643–652, 2004.
- [17] R. Albert, H. Jeong, and A. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.
- [18] S. Buldyrev, R. Parshani, G. Paul, H. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.
- [19] "Smart grid conceptual model," 2013. [Online]. Available: <http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model>
- [20] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 57–64, jun. 2010.

- [21] P. W. Sauer and M. Pai, *Power system dynamics and stability*. Prentice Hall New Jersey, 1998.
- [22] A. Monticelli, “Electric power system state estimation,” *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.
- [23] S. Pajic, “Power system state estimation and contingency constrained optimal power flow-a numerically robust implementation,” Ph.D. dissertation, WORCESTER POLYTECHNIC INSTITUTE, 2007.
- [24] A. Gomez-Exposito, A. Abur, A. de la Villa Jaen, and C. Gómez-Quiles, “A multilevel state estimation paradigm for smart grids,” *Proceedings of the IEEE*, vol. 99, no. 6, pp. 952–976, 2011.
- [25] I. Dzafic, S. Henselmeyer, and H.-T. Neisius, “High performance state estimation for smart grid distribution network operation,” in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, jan. 2011, pp. 1–6.
- [26] S. Choi, B. Kim, G. J. Cokkinides, and A. P. S. Meliopoulos, “Autonomous state estimation for the smart grid - laboratory implementation,” in *Transmission and Distribution Conference and Exposition, 2010 IEEE PES*, april 2010, pp. 1–8.
- [27] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 4, no. 2.
- [28] N. Balu, T. Bertram, A. Bose, V. Brandwajn, G. Cauley, D. Curtice, A. Fouad, L. Fink, M. G. Lauby, B. F. Wollenberg, *et al.*, “On-line power system security analysis,” *Proceedings of the IEEE*, vol. 80, no. 2, pp. 262–282, 1992.
- [29] Y. Sun and T. J. Overbye, “Visualizations for power system contingency analysis data,” *Power Systems, IEEE Transactions on*, vol. 19, no. 4, pp. 1859–1866, 2004.
- [30] D. Sobajic and Y.-H. Pao, “An artificial intelligence system for power system contingency screening,” *Power Systems, IEEE Transactions on*, vol. 3, no. 2, pp. 647–653, 1988.
- [31] J. Refaee, M. Mohandes, and H. Maghrabi, “Radial basis function networks for contingency analysis of bulk power systems,” *Power Systems, IEEE Transactions on*, vol. 14, no. 2, pp. 772–778, 1999.
- [32] V. Donde, V. López, B. Lesieutre, A. Pinar, C. Yang, and J. Meza, “Severe multiple contingency screening in electric power systems,” *Power Systems, IEEE Transactions on*, vol. 23, no. 2, pp. 406–417, 2008.

- [33] B. C. Lesieutre, A. Pinar, and S. Roy, "Power system extreme event detection: The vulnerability frontier," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, 2008, pp. 184–184.
- [34] P. Varaiya, F. F. Wu, and R.-L. Chen, "Direct methods for transient stability analysis of power systems: Recent results," *Proceedings of the IEEE*, vol. 73, no. 12, pp. 1703–1715, 1985.
- [35] G. Aloisio, M. Bochicchio, M. La Scala, and R. Sbrizzai, "A distributed computing approach for real-time transient stability analysis," *Power Systems, IEEE Transactions on*, vol. 12, no. 2, pp. 981–987, 1997.
- [36] S. Lee, N. Chiang, K. Lee, and B. Ku, "Parallel power system transient stability analysis on hypercube multiprocessors," *Power Systems, IEEE Transactions on*, vol. 6, no. 3, pp. 1337–1343, 1991.
- [37] L. Wang, "Techniques for high performance analysis of transient stability," in *Power and Energy Society General Meeting, 2012 IEEE*. IEEE, 2012, pp. 1–6.
- [38] W. Xue, J.-W. Shu, J.-F. Yan, X.-f. WANG, and Y.-d. HAN, "Cluster-based parallel simulation for power system transient stability analysis," *Proceedings of the CSEE*, vol. 8, p. 008, 2003.
- [39] R. Zárate-Miñano, T. Van Cutsem, F. Milano, and A. J. Conejo, "Securing transient stability using time-domain simulations within an optimal power flow," *Power Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 243–253, 2010.
- [40] R. Ambrosino, M. Ariola, and F. Amato, "A convex condition for robust stability analysis via polyhedral lyapunov functions," *SIAM Journal on Control and Optimization*, vol. 50, no. 1, pp. 490–506, 2012.
- [41] H. Li, F. Li, Y. Xu, D. Rizy, and J. D. Kueck, "Adaptive voltage control with distributed energy resources: Algorithm, theoretical analysis, simulation, and field test verification," *Power Systems, IEEE Transactions on*, vol. 25, no. 3, pp. 1638–1647, 2010.
- [42] S. C. Marchiori, M. d. C. G. da Silveira, A. D. P. Lotufo, C. R. Minussi, and M. L. M. Lopes, "Neural network based on adaptive resonance theory with continuous training for multi-configuration transient stability analysis of electric power systems," *Applied Soft Computing*, vol. 11, no. 1, pp. 706–715, 2011.
- [43] L. Moulin, A. A. Da Silva, M. El-Sharkawi, R. J. Marks, *et al.*, "Support vector machines for transient stability analysis of large-scale power systems," *Power Systems, IEEE Transactions on*, vol. 19, no. 2, pp. 818–825, 2004.

- [44] F. R. Gomez, A. D. Rajapakse, U. D. Annakkage, and I. T. Fernando, "Support vector machine-based algorithm for post-fault transient stability status prediction using synchronized measurements," *Power Systems, IEEE Transactions on*, vol. 26, no. 3, pp. 1474–1483, 2011.
- [45] C. Lu, J. Si, and X. Xie, "Direct heuristic dynamic programming for damping oscillations in a large power system," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 38, no. 4, pp. 1008–1013, 2008.
- [46] Y. Tang, P. Ju, H. He, C. Qin, and F. Wu, "Optimized control of dfig-based wind generation using sensitivity analysis and particle swarm optimization," *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, pp. 1–12, 2013.
- [47] D. Bienstock, "Optimal control of cascading power grid failures," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*. IEEE, 2011, pp. 2166–2173.
- [48] B. Stott, J. Jardim, and O. Alsac, "Dc power flow revisited," *Power Systems, IEEE Transactions on*, vol. 24, no. 3, pp. 1290–1300, aug. 2009.
- [49] H. Ren and I. Dobson, "Using transmission line outage data to estimate cascading failure propagation in an electric power system," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 55, no. 9, pp. 927–931, Sep. 2008.
- [50] . Holmgren and S. Molin, "Using disturbance data to assess vulnerability of electric power delivery systems," *Journal of Infrastructure Systems*, vol. 12, no. 4, pp. 243–251, 2006.
- [51] E. Cotilla-Sanchez, P. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the north american electric power infrastructure," *Systems Journal, IEEE*, vol. PP, no. 99, p. 1, may 2012.
- [52] S. Jonnavithula and R. Billinton, "Topological analysis in bulk power system reliability evaluation," *Power Systems, IEEE Transactions on*, vol. 12, no. 1, pp. 456–463, feb. 1997.
- [53] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, F. Li, J. Li, Z. Li, C.-C. Liu, L. Mili, S. Miller, R. Podmore, K. Schneider, K. Sun, D. Wang, Z. Wu, P. Zhang, W. Zhang, and X. Zhang, "Initial review of methods for cascading failure analysis in electric power transmission systems," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, jul. 2008, pp. 1–8.
- [54] D. Newman, B. Carreras, V. Lynch, and I. Dobson, "Exploring complex systems aspects of blackout risk and mitigation," *Reliability, IEEE Transactions on*, vol. 60, no. 1, pp. 134–143, mar. 2011.

- [55] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, “Power grid vulnerability to geographically correlated failures-analysis and control implications,” *arXiv preprint arXiv:1206.1099*, 2012.
- [56] A. Chakraborty, J. Chow, and A. Salazar, “A measurement-based framework for dynamic equivalencing of large power systems using wide-area phasor measurements,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 1, pp. 68–81, mar. 2011.
- [57] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, “Matpower: Steady-state operations, planning, and analysis tools for power systems research and education,” *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 12–19, feb. 2011.
- [58] X. Wang and P. Yi, “Security framework for wireless communications in smart distribution grid,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 809–818, dec. 2011.
- [59] F. Boroomand, A. Fereidunian, M. Zamani, M. Amozegar, H. Jamalabadi, H. Nasrollahi, M. Moghimi, H. Lesani, and C. Lucas, “Cyber security for smart grid: A humanautomation interaction framework,” in *IEEE Innovative Smart Grid Technologies Conference Europe*, 2010, pp. 1–6.
- [60] S. Clements and H. Kirkham, “Cyber-security considerations for the smart grid,” in *Power and Energy Society General Meeting, 2010 IEEE*. IEEE, 2010, pp. 1–5.
- [61] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purpy, “Towards a framework for cyber attack impact analysis of the electric smart grid,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 244–249.
- [62] F. Cleveland, “Cyber security issues for advanced metering infrastructure (ami),” in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, jul. 2008, pp. 1–5.
- [63] A. Metke and R. Ekl, “Security technology for smart grid networks,” *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 99–107, june 2010.
- [64] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” *Security & Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, 2009.
- [65] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, “Smart-grid security issues,” *Security & Privacy, IEEE*, vol. 8, no. 1, pp. 81–85, 2010.
- [66] F. Garcia and B. Jacobs, “Privacy-friendly energy-metering via homomorphic encryption,” *Security and Trust Management*, pp. 226–238, 2011.

- [67] H. Li, R. Mao, L. Lai, and R. C. Qiu, “Compressed meter reading for delay-sensitive and secure load report in smart grid,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 114–119.
- [68] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, “Competitive privacy in the smart grid: An information-theoretic approach,” in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 220–225.
- [69] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, “A lightweight message authentication scheme for smart grid communications,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 675–685, 2011.
- [70] Q. Li and G. Cao, “Multicast authentication in the smart grid with one-time signature,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 686–696, 2011.
- [71] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, “Privacy for smart meters: Towards undetectable appliance load signatures,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 232–237.
- [72] C. Efthymiou and G. Kalogridis, “Smart grid privacy via anonymization of smart metering data,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 238–243.
- [73] O. Kosut, L. Jia, R. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 645–658, dec. 2011.
- [74] G. Dán and H. Sandberg, “Stealth attacks and protection schemes for state estimators in power systems,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 214–219.
- [75] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 220–225.
- [76] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, “A cyber security study of a scada energy management system: Stealthy deception attacks on the state estimator,” *arXiv preprint arXiv:1011.1828*, 2010.
- [77] Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 382–390, jun. 2011.

- [78] G. Hug and J. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *Smart Grid, IEEE Transactions on*, vol. 3, no. 3, pp. 1362–1370, sep. 2012.
- [79] A. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 667–674, dec. 2011.
- [80] G. N. Ericsson, "Cyber security and power system communication essential parts of a smart grid infrastructure," *Power Delivery, IEEE Transactions on*, vol. 25, no. 3, pp. 1501–1507, 2010.
- [81] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 865–873, 2011.
- [82] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, Z. Huang, M. Joung, J. Kim, D. Kirschen, S. Lee, F. Li, J. Li, Z. Li, C.-C. Liu, X. Luo, L. Mili, S. Miller, M. Nakayama, M. Papic, R. Podmore, J. Rossmair, K. Schneider, H. Sun, K. Sun, D. Wang, Z. Wu, L. Yao, P. Zhang, W. Zhang, and X. Zhang, "Vulnerability assessment for cascading failures in electric power systems," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, march 2009, pp. 1–9.
- [83] T. Chen, J. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 741–749, dec. 2011.
- [84] S. Pahwa, A. Hodges, C. Scoglio, and S. Wood, "Topological analysis of the power grid and mitigation strategies against cascading failures," in *Systems Conference, 2010 4th Annual IEEE*. IEEE, 2010, pp. 272–276.
- [85] M. Amin, "Balancing market priorities with security issues," *Power and Energy Magazine, IEEE*, vol. 2, no. 4, pp. 30–38, 2004.
- [86] K. J. Ross, "Application of game theory to improve the defense of the smart grid," DTIC Document, Tech. Rep., 2012.
- [87] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano, "Failure identification in smart grids based on petri net modeling," *Industrial Electronics, IEEE Transactions on*, vol. 58, no. 10, pp. 4613–4623, 2011.
- [88] H. Li, G. W. Rosenwald, J. Jung, and C.-C. Liu, "Strategic power infrastructure defense," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 918–933, 2005.
- [89] J. Singh and S. S. Sapatnekar, "Partition-based algorithm for power grid design using locality," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 25, no. 4, pp. 664–677, 2006.

- [90] M. Cannataro, A. Congiusta, A. Pugliese, D. Talia, and P. Trunfio, “Distributed data mining on grids: services, tools, and applications,” *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 34, no. 6, pp. 2451–2465, 2004.
- [91] F. Tang, M. Li, and J. Z. Huang, “Real-time transaction processing for autonomous grid applications,” *Engineering Applications of Artificial Intelligence*, vol. 17, no. 7, pp. 799–807, 2004.
- [92] W. Wang, Q. Cai, Y. Sun, and H. He, “Risk-aware attacks and catastrophic cascading failures in u.s. power grid,” in *Global Telecommunications Conference (GLOBECOM 2011)*, 2011 IEEE, dec. 2011, pp. 1–6.
- [93] R. Kinney, P. Crucitti, R. Albert, and V. Latora, “Modeling cascading failures in the north american power grid,” *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 46, no. 1, pp. 101–107, 2005.
- [94] 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.
- [95] Z. Shi, L. Shi, Y. Ni, L. Yao, and M. Bazargan, “Identifying chains of events during power system cascading failure,” in *Proceedings of the 2011 Asia-Pacific Power and Energy Engineering Conference*, ser. APPEEC ’11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 1–4.
- [96] 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, jul 2012, pp. 277–283.
- [97] “Esri shapefile technical description,” 2012. [Online]. Available: <http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf>
- [98] J. Yan, Y. Zhu, H. He, and Y. Sun, “Multi-contingency cascading analysis of smart grid based on self-organizing map,” *Information Forensics and Security, IEEE Transactions on*, in press.
- [99] J. Yan, Y. Zhu, H. He, and Y. Sun, “Revealing temporal features of attacks against smart grid,” in *Innovative Smart Grid Technologies (ISGT)*, 2013 IEEE PES, feb. in press, pp. 1–6.
- [100] E. Bompard, E. Pons, and D. Wu, “Extended topological metrics for the analysis of power grid vulnerability,” *Systems Journal, IEEE*, vol. 6, no. 3, pp. 481–487, sep. 2012.

BIBLIOGRAPHY

- “Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations,” U.S.-Canada Power System Outage Task Force, Tech. Rep., apr. 2004. [Online]. Available: <https://reports.energy.gov/>
- “The smart grid: An introduction,” The U.S. Department of Energy, Tech. Rep., 2008. [Online]. Available: <http://energy.gov/oe/downloads/smart-grid-introduction-0>
- “Application of automated controls for voltage and reactive power management - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/application_automated_controls_voltage_and_reactive_power_management_initial_results
- “Demand reductions from the application of advanced metering infrastructure, pricing programs, and customer-based systems - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/demand_reductions_application_advanced_metering_infrastructure_pricing_programs_and_custome
- “Esri shapefile technical description,” 2012. [Online]. Available: <http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf>
- “Operations and maintenance savings from advanced metering infrastructure - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/operations_and_maintenance_savings_advanced_metering_infrastructure_initial_results
- “Reliability improvements from the application of distribution automation technologies - initial results,” The U.S. Department of Energy, Tech. Rep., 2012. [Online]. Available: https://www.smartgrid.gov/document/reliability_improvements_application_distribution_automation_technologies_initial_results
- “Report of the enquiry committee on grid disturbance in northern region on 30th july 2012 and in northern, eastern & north-eastern region on 31st july 2012,” The Enquiry Committee, Ministry of Power, Government of India, Tech. Rep., aug. 2012. [Online]. Available: http://www.powermin.nic.in/pdf/GRID_ENQ_REP_16_8_12.pdf
- “Smart grid conceptual model,” 2013. [Online]. Available: <http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model>

- Albert, R., Jeong, H., and Barabási, A., “Error and attack tolerance of complex networks,” *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.
- Aloisio, G., Boichicchio, M., La Scala, M., and Sbrizzai, R., “A distributed computing approach for real-time transient stability analysis,” *Power Systems, IEEE Transactions on*, vol. 12, no. 2, pp. 981–987, 1997.
- Ambrosino, R., Ariola, M., and Amato, F., “A convex condition for robust stability analysis via polyhedral lyapunov functions,” *SIAM Journal on Control and Optimization*, vol. 50, no. 1, pp. 490–506, 2012.
- Amin, M., “Balancing market priorities with security issues,” *Power and Energy Magazine, IEEE*, vol. 2, no. 4, pp. 30–38, 2004.
- Amin, M., “Guaranteeing the security of an increasingly stressed grid,” *IEEE Smart Grid Newsletter*, feb. 2012.
- Baldick, R., Chowdhury, B., Dobson, I., Dong, Z., Gou, B., Hawkins, D., Huang, H., Joung, M., Kirschen, D., Li, F., Li, J., Li, Z., Liu, C.-C., Mili, L., Miller, S., Podmore, R., Schneider, K., Sun, K., Wang, D., Wu, Z., Zhang, P., Zhang, W., and Zhang, X., “Initial review of methods for cascading failure analysis in electric power transmission systems,” in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, jul. 2008, pp. 1–8.
- Baldick, R., Chowdhury, B., Dobson, I., Dong, Z., Gou, B., Hawkins, D., Huang, Z., Joung, M., Kim, J., Kirschen, D., Lee, S., Li, F., Li, J., Li, Z., Liu, C.-C., Luo, X., Mili, L., Miller, S., Nakayama, M., Papic, M., Podmore, R., Rossmair, J., Schneider, K., Sun, H., Sun, K., Wang, D., Wu, Z., Yao, L., Zhang, P., Zhang, W., and Zhang, X., “Vulnerability assessment for cascading failures in electric power systems,” in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, march 2009, pp. 1–9.
- Balu, N., Bertram, T., Bose, A., Brandwajn, V., Cauley, G., Curtice, D., Fouad, A., Fink, L., Lauby, M. G., Wollenberg, B. F., *et al.*, “On-line power system security analysis,” *Proceedings of the IEEE*, vol. 80, no. 2, pp. 262–282, 1992.
- Bernstein, A., Bienstock, D., Hay, D., Uzunoglu, M., and Zussman, G., “Power grid vulnerability to geographically correlated failures-analysis and control implications,” *arXiv preprint arXiv:1206.1099*, 2012.
- Bienstock, D., “Optimal control of cascading power grid failures,” in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*. IEEE, 2011, pp. 2166–2173.
- Bompard, E., Pons, E., and Wu, D., “Extended topological metrics for the analysis of power grid vulnerability,” *Systems Journal, IEEE*, vol. 6, no. 3, pp. 481–487, sep. 2012.

- Boroomand, F., Fereidunian, A., Zamani, M., Amozegar, M., Jamalabadi, H., Nasrollahi, H., Moghimi, M., Lesani, H., and Lucas, C., "Cyber security for smart grid: A humanautomation interaction framework," in *IEEE Innovative Smart Grid Technologies Conference Europe*, 2010, pp. 1–6.
- Buldyrev, S., Parshani, R., Paul, G., Stanley, H., and Havlin, S., "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.
- Calderaro, V., Hadjicostis, C. N., Piccolo, A., and Siano, P., "Failure identification in smart grids based on petri net modeling," *Industrial Electronics, IEEE Transactions on*, vol. 58, no. 10, pp. 4613–4623, 2011.
- Cannataro, M., Congiusta, A., Pugliese, A., Talia, D., and Trunfio, P., "Distributed data mining on grids: services, tools, and applications," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 34, no. 6, pp. 2451–2465, 2004.
- Carreras, B. A., Lynch, V. E., Dobson, I., and Newman, D. E., "Complex dynamics of blackouts in power transmission systems," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 14, no. 3, pp. 643–652, 2004.
- Chakraborty, A., Chow, J., and Salazar, A., "A measurement-based framework for dynamic equivalencing of large power systems using wide-area phasor measurements," *Smart Grid, IEEE Transactions on*, vol. 2, no. 1, pp. 68–81, mar. 2011.
- Chen, P.-Y., Cheng, S.-M., and Chen, K.-C., "Smart attacks in smart grid communication networks," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 24–29, aug. 2012.
- Chen, T., Sanchez-Aarnoutse, J., and Buford, J., "Petri net modeling of cyber-physical attacks on smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 741–749, dec. 2011.
- Choi, S., Kim, B., Cokkinides, G. J., and Meliopoulos, A. P. S., "Autonomous state estimation for the smart grid - laboratory implementation," in *Transmission and Distribution Conference and Exposition, 2010 IEEE PES*, april 2010, pp. 1–8.
- Clements, S. and Kirkham, H., "Cyber-security considerations for the smart grid," in *Power and Energy Society General Meeting, 2010 IEEE*. IEEE, 2010, pp. 1–5.
- Cleveland, F., "Cyber security issues for advanced metering infrastructure (ami)," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, jul. 2008, pp. 1–5.

- Cotilla-Sanchez, E., Hines, P., Barrows, C., and Blumsack, S., “Comparing the topological and electrical structure of the north american electric power infrastructure,” *Systems Journal, IEEE*, vol. PP, no. 99, p. 1, may 2012.
- Dán, G. and Sandberg, H., “Stealth attacks and protection schemes for state estimators in power systems,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 214–219.
- 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.
- Donde, V., López, V., Lesieutre, B., Pinar, A., Yang, C., and Meza, J., “Severe multiple contingency screening in electric power systems,” *Power Systems, IEEE Transactions on*, vol. 23, no. 2, pp. 406–417, 2008.
- Dzafic, I., Henselmeyer, S., and Neisius, H.-T., “High performance state estimation for smart grid distribution network operation,” in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, jan. 2011, pp. 1 –6.
- Efthymiou, C. and Kalogridis, G., “Smart grid privacy via anonymization of smart metering data,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 238–243.
- Eppstein, M. and Hines, P., “A “random chemistry” algorithm for identifying collections of multiple contingencies that initiate cascading failure,” *Power Systems, IEEE Transactions on*, vol. 27, no. 3, pp. 1698–1705, aug. 2012.
- Ericsson, G. N., “Cyber security and power system communicationessential parts of a smart grid infrastructure,” *Power Delivery, IEEE Transactions on*, vol. 25, no. 3, pp. 1501–1507, 2010.
- Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R., and Shen, X., “A lightweight message authentication scheme for smart grid communications,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 675–685, 2011.
- Garcia, F. and Jacobs, B., “Privacy-friendly energy-metering via homomorphic encryption,” *Security and Trust Management*, pp. 226–238, 2011.
- Gomez, F. R., Rajapakse, A. D., Annakkage, U. D., and Fernando, I. T., “Support vector machine-based algorithm for post-fault transient stability status prediction using synchronized measurements,” *Power Systems, IEEE Transactions on*, vol. 26, no. 3, pp. 1474–1483, 2011.

- Gomez-Exposito, A., Abur, A., de la Villa Jaen, A., and Gómez-Quiles, C., “A multilevel state estimation paradigm for smart grids,” *Proceedings of the IEEE*, vol. 99, no. 6, pp. 952–976, 2011.
- Holmgren, . and Molin, S., “Using disturbance data to assess vulnerability of electric power delivery systems,” *Journal of Infrastructure Systems*, vol. 12, no. 4, pp. 243–251, 2006.
- Hug, G. and Giampapa, J., “Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks,” *Smart Grid, IEEE Transactions on*, vol. 3, no. 3, pp. 1362–1370, sep. 2012.
- Jonnavithula, S. and Billinton, R., “Topological analysis in bulk power system reliability evaluation,” *Power Systems, IEEE Transactions on*, vol. 12, no. 1, pp. 456–463, feb. 1997.
- Kalogridis, G., Efthymiou, C., Denic, S. Z., Lewis, T. A., and Cepeda, R., “Privacy for smart meters: Towards undetectable appliance load signatures,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 232–237.
- Khurana, H., Hadley, M., Lu, N., and Frincke, D. A., “Smart-grid security issues,” *Security & Privacy, IEEE*, vol. 8, no. 1, pp. 81–85, 2010.
- Kinney, R., Crucitti, P., Albert, R., and Latora, V., “Modeling cascading failures in the north american power grid,” *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 46, no. 1, pp. 101–107, 2005.
- Kosut, O., Jia, L., Thomas, R., and Tong, L., “Malicious data attacks on the smart grid,” *Smart Grid, IEEE Transactions on*, 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 *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 220–225.
- Kundur, D., Feng, X., Liu, S., Zourntos, T., and Butler-Purpy, K., “Towards a framework for cyber attack impact analysis of the electric smart grid,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 244 –249.
- Kundur, P., Balu, N. J., and Lauby, M. G., *Power system stability and control*. McGraw-hill New York, 1994, vol. 4, no. 2.
- Lee, S., Chiang, N., Lee, K., and Ku, B., “Parallel power system transient stability analysis on hypercube multiprocessors,” *Power Systems, IEEE Transactions on*, vol. 6, no. 3, pp. 1337–1343, 1991.

- Lesieutre, B. C., Pinar, A., and Roy, S., "Power system extreme event detection: The vulnerability frontier," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, 2008, pp. 184–184.
- Li, H., Rosenwald, G. W., Jung, J., and Liu, C.-C., "Strategic power infrastructure defense," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 918–933, 2005.
- Li, H., Li, F., Xu, Y., Rizy, D., and Kueck, J. D., "Adaptive voltage control with distributed energy resources: Algorithm, theoretical analysis, simulation, and field test verification," *Power Systems, IEEE Transactions on*, vol. 25, no. 3, pp. 1638–1647, 2010.
- Li, H., Mao, R., Lai, L., and Qiu, R. C., "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 114–119.
- Li, Q. and Cao, G., "Multicast authentication in the smart grid with one-time signature," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 686–696, 2011.
- Li, X., Liang, X., Lu, R., Shen, X., Lin, X., and Zhu, H., "Securing smart grid: cyber attacks, countermeasures, and challenges," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 38–45, aug. 2012.
- Lu, C., Si, J., and Xie, X., "Direct heuristic dynamic programming for damping oscillations in a large power system," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 38, no. 4, pp. 1008–1013, 2008.
- Marchiori, S. C., da Silveira, M. d. C. G., Lotufo, A. D. P., Minussi, C. R., and Lopes, M. L. M., "Neural network based on adaptive resonance theory with continuous training for multi-configuration transient stability analysis of electric power systems," *Applied Soft Computing*, vol. 11, no. 1, pp. 706–715, 2011.
- McDaniel, P. and McLaughlin, S., "Security and privacy challenges in the smart grid," *Security & Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, 2009.
- Metke, A. and Ekl, R., "Security technology for smart grid networks," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 99–107, june 2010.
- Mohsenian-Rad, A. and Leon-Garcia, A., "Distributed internet-based load altering attacks against smart power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 667–674, dec. 2011.
- Monticelli, A., "Electric power system state estimation," *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

- Moslehi, K. and Kumar, R., “A reliability perspective of the smart grid,” *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 57–64, jun. 2010.
- Moulin, L., Da Silva, A. A., El-Sharkawi, M., Marks, R. J., *et al.*, “Support vector machines for transient stability analysis of large-scale power systems,” *Power Systems, IEEE Transactions on*, vol. 19, no. 2, pp. 818–825, 2004.
- Newman, D., Carreras, B., Lynch, V., and Dobson, I., “Exploring complex systems aspects of blackout risk and mitigation,” *Reliability, IEEE Transactions on*, vol. 60, no. 1, pp. 134–143, mar. 2011.
- Pahwa, S., Hodges, A., Scoglio, C., and Wood, S., “Topological analysis of the power grid and mitigation strategies against cascading failures,” in *Systems Conference, 2010 4th Annual IEEE*. IEEE, 2010, pp. 272–276.
- Pajic, S., “Power system state estimation and contingency constrained optimal power flow-a numerically robust implementation,” Ph.D. dissertation, WORCESTER POLYTECHNIC INSTITUTE, 2007.
- 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 *Power and Energy Society General Meeting, 2011 IEEE*, jul. 2011, pp. 1–9.
- Refaee, J., Mohandes, M., and Maghrabi, H., “Radial basis function networks for contingency analysis of bulk power systems,” *Power Systems, IEEE Transactions on*, vol. 14, no. 2, pp. 772–778, 1999.
- Ren, H. and Dobson, I., “Using transmission line outage data to estimate cascading failure propagation in an electric power system,” *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 55, no. 9, pp. 927–931, Sep. 2008.
- Ross, K. J., “Application of game theory to improve the defense of the smart grid,” DTIC Document, Tech. Rep., 2012.
- Sankar, L., Kar, S., Tandon, R., and Poor, H. V., “Competitive privacy in the smart grid: An information-theoretic approach,” in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. IEEE, 2011, pp. 220–225.
- Sauer, P. W. and Pai, M., *Power system dynamics and stability*. Prentice Hall New Jersey, 1998.
- Shi, Z., Shi, L., Ni, Y., Yao, L., and Bazargan, M., “Identifying chains of events during power system cascading failure,” in *Proceedings of the 2011 Asia-Pacific Power and Energy Engineering Conference*, ser. APPEEC ’11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 1–4.

- Singh, J. and Sapatnekar, S. S., “Partition-based algorithm for power grid design using locality,” *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 25, no. 4, pp. 664–677, 2006.
- Sobajic, D. and Pao, Y.-H., “An artificial intelligence system for power system contingency screening,” *Power Systems, IEEE Transactions on*, vol. 3, no. 2, pp. 647–653, 1988.
- Stott, B., Jardim, J., and Alsac, O., “Dc power flow revisited,” *Power Systems, IEEE Transactions on*, vol. 24, no. 3, pp. 1290–1300, aug. 2009.
- Sun, Y. and Overbye, T. J., “Visualizations for power system contingency analysis data,” *Power Systems, IEEE Transactions on*, vol. 19, no. 4, pp. 1859–1866, 2004.
- Tang, F., Li, M., and Huang, J. Z., “Real-time transaction processing for autonomous grid applications,” *Engineering Applications of Artificial Intelligence*, vol. 17, no. 7, pp. 799–807, 2004.
- Tang, Y., Ju, P., He, H., Qin, C., and Wu, F., “Optimized control of dfig-based wind generation using sensitivity analysis and particle swarm optimization,” *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, pp. 1–12, 2013.
- Teixeira, A., Dán, G., Sandberg, H., and Johansson, K. H., “A cyber security study of a scada energy management system: Stealthy deception attacks on the state estimator,” *arXiv preprint arXiv:1011.1828*, 2010.
- Ten, C.-W., Hong, J., and Liu, C.-C., “Anomaly detection for cybersecurity of the substations,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 865–873, 2011.
- 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 1 - overview of methodologies,” in *Power and Energy Society General Meeting, 2011 IEEE*, jul. 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,” *Power Systems, IEEE Transactions on*, vol. 27, no. 2, pp. 631–641, may 2012.
- Varaiya, P., Wu, F. F., and Chen, R.-L., “Direct methods for transient stability analysis of power systems: Recent results,” *Proceedings of the IEEE*, vol. 73, no. 12, pp. 1703–1715, 1985.
- 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, L., “Techniques for high performance analysis of transient stability,” in *Power and Energy Society General Meeting, 2012 IEEE*. IEEE, 2012, pp. 1–6.
- Wang, W., Cai, Q., Sun, Y., and He, H., “Risk-aware attacks and catastrophic cascading failures in u.s. power grid,” in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, dec. 2011, pp. 1–6.
- Wang, X. and Yi, P., “Security framework for wireless communications in smart distribution grid,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 809–818, dec. 2011.
- Xue, W., Shu, J.-W., Yan, J.-F., WANG, X.-f., and HAN, Y.-d., “Cluster-based parallel simulation for power system transient stability analysis,” *Proceedings of the CSEE*, vol. 8, p. 008, 2003.
- 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*, jul 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,” *Information Forensics and Security, IEEE Transactions on*, in press.
- Yan, J., Zhu, Y., He, H., and Sun, Y., “Revealing temporal features of attacks against smart grid,” in *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, feb. in press, pp. 1–6.
- Yuan, Y., Li, Z., and Ren, K., “Modeling load redistribution attacks in power systems,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 382–390, jun. 2011.
- Zárate-Miñano, R., Van Cutsem, T., Milano, F., and Conejo, A. J., “Securing transient stability using time-domain simulations within an optimal power flow,” *Power Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 243–253, 2010.
- Zimmerman, R., Murillo-Sandnchez, C., and Thomas, R., “Matpower: Steady-state operations, planning, and analysis tools for power systems research and education,” *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 12–19, feb. 2011.