2014

MULTIFACETED ATTACK ANALYSIS ON POWER GRIDS

Yihai Zhu
University of Rhode Island, yhzhu@ele.uri.edu

MULTIFACETED ATTACK ANALYSIS ON POWER GRIDS

BY

YIHAI ZHU

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

ELECTRICAL, COMPUTER & BIOMEDICAL ENGINEERING

UNIVERSITY OF RHODE ISLAND

2014

DOCTOR OF PHILOSOPHY DISSERTATION

OF

YIHAI ZHU

APPROVED:

Dissertation Committee:

Major Professor Yan (Lindsay) Sun

Haibo He

Joan Peckham

Nasser H. Zawia

DEAN OF THE GRADUATE SCHOOL

UNIVERSITY OF RHODE ISLAND

2014

ABSTRACT

Electrical grids have been developed over a century, which are considered as one of the most important infrastructures on the earth. In the past decade, the emergence of the Smart Grid, referred to the next generation of power grid, makes existing systems more complicated and vulnerable. Cyber-physical attacks against existing systems and future smart grids have drawn increasing attention, because such attacks could trigger large-scale cascading failures and result in major blackouts.

In the traditional power society, *contingencies* are widely considered as the causes that result in power outages. The contingency analysis is the predominant method to investigate the vulnerability of power grids. With the increasing *malicious attacks* against power transmission systems, however, studying the grid's security and reliability only from the contingency analysis perspective has apparent limitations. First, contingencies happen randomly and unintentionally; malicious attacks are mostly intentional. Second, it is rare that multiple contingencies happen simultaneously. Malicious attacks, however, can likely occur on a few, even more, the power grid components.

In this dissertation, the security and reliability of power grids is investigated. Briefly speaking, the attackers identify a few components in the grid as *targets* (e.g., substations, transmission lines, or both). Then, the attackers take down these targets by either physical sabotages or cyber intrusions, hoping that the initial failures can trigger large-scale cascading failures. The *goal* of the attackers is to find a group of targets, attacking on which can yield large damage to the power grid.

In particular, this dissertation investigate the attacks against the power system from the following aspects.

- It is a nature question that why attacking a few, even one, critical components can severely weaken the system. In manuscript 1 (i.e., chapter 2), the cascading process is visualized to help people under such complicated phenomena, as well as discovering different types of failure propagation.

- Attackers might only know the topological connection of the power grid, e.g., the topology. In manuscript 2 (i.e., chapter 3), a topology-based cascading model is adopted to study cascading failures. The metric *load distribution vector* (LDV) and LDV-based attack strategy are proposed and investigated.

- Attackers can possibly know some general information of the power grid, e.g., the topology, types of substations and length of transmission lines. In manuscript 3 (i.e., chapter 4), the extended topological model is used to mimic cascading failures. A novel metric, called the *risk graph*, is proposed to reveal the hidden relationship among critical substations/transmission lines. In addition, the risk-graph based attack strategies are developed regarding substations and transmission lines, respectively.

- Attacks can occur on substations and transmission lines simultaneously. In manuscript 4 (i.e., chapter 5), both the vulnerability analysis and the attacks are investigated from the joint substation-transmission line perspective.

- Attacks can be conducted not only synchronously but sequentially. In manuscript 5 (i.e., chapter 6), the sequential attack is introduced; the metric *sequential attack graph* (SAG) is constructed; the SAG-based sequential attack strategy is developed and evaluated.

ACKNOWLEDGMENTS

Foremost, I would like to express the deepest gratitude to my advisor, Dr. Yan Lindsay Sun. Being her student is and will be one of the greatest honors in my life. Dr. Sun gave many constructive suggestions in my study. Her instructions paved the way to this dissertation. Whenever, I discussed with her the ideas, she could find the vague points and gave concrete suggestions. In addition, Dr. Sun taught me many skills in writing and revising manuscripts. Last but not least, Dr. Sun is friendly. She let me choose the research topics based my interests, and encouraged me to learn different cultures and improve the spoken English. In summary, Dr. Sun is a great advisor.

I would like to sincerely thank Dr. He. Since 2011, I have been working with him on the project. Within the past three years, his hardworking and enthusiasm gave me great inspiration. He set up high, but achievable, standards for students. His concrete and useful suggestions gave me great help to finish this dissertation. Also, I appreciated that he could serve as my committee member.

I would also like to sincerely thank Dr. Joan Peckham, Dr. Lubos Thoma and Dr. Tao Wei for serving as my committee members and being available when I needed the consultant. I appreciated all your suggestions to improve the quality of this dissertation.

I would like to greatly thank Jun Yan and Yufei Tang. We worked in the same project during the past three years. They helped me understand the complicated cascading failure phenomena in power systems. The models they implemented were of great help to come out my research results.

I would like to thank many professors and staff members in my department, especially to Meredith Leach Sanders and Timothy Toolan. Meredith helped me to set up my office and gave concrete explanations of the department policy. Tim

gave me much convenience to use department resource for our projects and my researches.

Special thanks to my colleagues as well as friends in Network Security and Trust Laboratory Yongbo Zeng and alumni, Dr. Wenkai Wang and Dr. Yuhong Liu, for their support and help during my study.

Special thanks also to my friends, Daxian Yun, Zhen Ni, Miao Song, Quan Ding, Fu Luo, Xiaorong Zhao, Siyao Fu, and many others. They helped me in different aspects, e.g., early settle down, TA works and daily life.

Finally and most importantly, I would like to express the earnest thanks to my family. My wife, Na Li, came to URI in 2011. I appreciated her encouragement and support to my study as well as her hardwork in our lives. My father and mother raised and educated me. I would say, *the parents graciousness, heavier than the moutains*. I would like to express my deepest respect to my father-in-law and mother-in-law. Also, many thanks to other family members for their supports in my life.

PREFACE

This dissertation is organized in the manuscript format. In particular, it consists of seven chapters. The introduction is given in the chapter 1. From the chapter 2 to the chapter 6, five manuscripts are discussed in details. The dissertation is summarized in the chapter 7. Brief introduction of the five manuscripts are given as follows.

* Manuscript 1 in Chapter 2:

  Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, and Haibo He, "Failure Propagation and Visualization for Vulnerability Analysis in Power Grids," in submission to IEEE Conference on Communications and Network Security (CNS), 2014.

* Manuscript 2 in Chapter 3:

  Yihai Zhu, Yan (Lindsay) Sun, and Haibo He, "Load Distribution Vector Based Attack Strategies against Power Grid Systems," in Proceeding of IEEE Global Telecommunications Conference, Anaheim, CA, USA, Dec.3-7 2012.

* Manuscript 3 in Chapter 4:

  Yihai Zhu, Jun Yan, Yan (Lindsay) Sun, and Haibo He, "Revealing cascading failure vulnerability in power grids using risk-graph," IEEE Transactions on Parallel and Distributed Systems, 2014, in press.

* Manuscript 4 in Chapter 5:

  Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, and Haibo He, "Joint Substation-Transmission line Vulnerability Assessment against the Smart Grid," in submission to IEEE Transactions on Information Forensics and Security, 2014.

* Manuscript 5 in Chapter 6:

  Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, and Haibo He, "Resilience Analysis of Power Grids under the Sequential Attack," in submission to IEEE Transactions on Information Forensics and Security, 2014.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

Figure **Page**

CHAPTER 1

Introduction

The U.S. power grid has been developed over a century. Nowadays, this grid has involved into a extremely complicated system with more than 55,000 substations and nearly 300,000 miles of transmission lines. Such a big system is facing various security threats and reliability issues.

1.1 Public Voices on U.S. Grid Security

Recently, the U.S. power grid security and reliability has attracted increasing public concerns.

Janet Napolitano, the former U.S. Homeland Security Secretary, had a warning for her successor: A massive and "serious" cyber attack on the U.S. homeland is coming, and a natural disaster - the likes of which the nation has never seen - is also likely on its way [1]. An unreported study from the *Federal Energy Regulatory Commission* shows: the U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day [2]. A report from *Nature News and Comment*: U.S. electrical grid on the edge of failure [3]. *Adam Kredo*, a senior writer for the Washington Free Beacon, had reported: U.S. Electric Grid Inherently Vulnerable to Sabotage [4].

In the history, the U.S. power grid experienced several major *blackouts*, which caused catastrophic results to the societies.

Traditionally, the causes that can trigger major blackouts are mainly unintentional, such as natural disasters [5] (e.g., earthquakes, hurricanes, blizzards, tornadoes, lightnings, etc.), errors from computer hardware and software [6], misoperation from operators, vegetation sagging [7] and increasing energy demand [8].

Table 1.1. History of Major United States Blackouts

Date	Location	Reasons	Consequences
Nov. 1965	Northeastern of U.S., Ontario in Canada	Human errors	30 million people without power
Jul. 1977	New York City	An electrical substation stroke by lightning	9 million people without power
Jan. 1981	Utah	Knocking out transmission lines	1.5 million people lost power
Oct. 1989	Northern California	Electrical substations damaged by earthquakes	1.4 million people lost power
Jan. 1989	Northeastern of North America	Transmission towers destroyed by ice	3.5 million people affected
Aug. 2003	Northeastern of U.S., Ontario in Canada	Transmission lines tripped by trees	55 million people without power for days
Sep. 2011	California	Error made by a technician	7 million people without power
Jul. 2012	New York New Jersey	Hurricane Sandy	10 million people without power; some for weeks

These causes often occur in a unpredictable manner. Although many works have been done to enhance the security and reliability of the U.S. grid, major blackouts are still inevitable. Table 1.1[1] shows the history of U.S. notable blackouts in the past 50 years.

1.2 Malicious Attacks

Recently, *malicious attacks* against power systems have drawn increasing attention from many aspects, e.g., governments, industries, academies and even the public. Recent terrorist attacks have shown that U.S. are vulnerable to *physical sabotages* [10, 11]. With the emergence of the "Smart Grid", generally referred to as the next-generation power transmission system [12], power transmission systems are growing to rely on modern techniques, e.g., computer and communication networks and smart meters. The new techniques for traditional power systems have

[1]The information is collected from [9].

raised great concerns of *cyber intrusions* to the systems currently in use. Such attacks, physical sabotages or cyber intrusions, can be controlled by *attackers* to target on critical substations and transmission lines and likely cause national power outage [13].

Attackers are referred to as those people with strong willing carry out attacks to disable the power grid. Generally speaking, the attackers might include, but not limited to, those as follows.

- *Individuals*: The person who is disgruntled with the society could likely become the attacker [10]. The individual can target on those power grid components that are less protected, e.g., transmission lines. Individual attacks can be conducted by using simple physical sabotages.

- *Terrorists*: Terrorism is the critical issue to the United States. Terrorists possibly come from both inside and outside. Inside terrorists can directly attack substations by using sophisticated but low-tech physical sabotages [11]; outside terrorists can access and destroy power grid components through remote cyber intrusions [14].

- *Hostile Countries*: There are quite a few adversaries to the United States. Nuclear weapons from those hostile nations can release electromagnetic pulse (EMP) to destroy regional grids; the computer hackers in those hostile countries can remotely access and possibly shunt down target substations and transmission lines.

Individual attacks and terrorist attacks are highly possible, some of which already happened [10, 11]. Although attacks from hostile countries are less often than individual attacks and terrorist attacks, once the type of attacks occur, the entire U.S. grid might be shut down for weeks, even months [2].

Physical Sabotages refer to physically destroy the parts of power grids, e.g., transmission lines, transformers, generators, and even substations. Such sabotages can be conducted in different ways. Some ways can be easily done, e.g., failing down poles that support transmission lines [10]. Others can be complicated and powerful, e.g., terrorist attacks targeting on substations [11] and electromagnetic pulse (EMP) attacks to destroy reginal grid [15].

Examples of physical sabotages against the U.S. electric grids include the attacks on transmission lines in [10] and on substations in [11]. In 2013, a 37-year-old Arkansas man launched three attacks on the local power grid [10]. Specifically, the first attack occurred on August 21, 2013, with the sabotage of a 500 KV power line; the second attack occurred on September 29, 2013, at a switching station; the third attack occurred on October 6, 2013, destroyed two power poles that support a 115 KV transmission line.

In addition, on April 16 2013, two gunmen assaulted an electrical substation near San Jose, California [11]. During the 19 minutes of shooting, 17 transformers were knocked out, which then took nearly a month to repair. The attack raises great concerns on potential terrorist attacks against U.S. grid.

Finally, physical sabotages can possibly launched by military forces from hostile nations [15], e.g., EMP attacks and airforce attacks. The type of sabotages are powerful and possible to destroy many power grid components simultaneously.

Cyber intrusions to power systems are highly possible with the emergence of the Smart Grid [14, 16]. In March 2007, a simulated cyber attack was conducted at the Idaho National Laboratory to destroy a $1 million dollar large diesel-electric generator [17]. In particular, the generator turbine is forced to overheat dramatically and shut down, after receiving malicious commands from a hacker. The destroyed generator is similar to many now in use throughout the United States.

In order words, there exist many generators that could potentially be disabled the same way.

Furthermore, cyber worms could intrude into supervisory control and data acquisition (SCADA) systems [14]. For instance, the well-known Stuxnet worm were designed to target SCADA systems as well as nuclear power plants. With modifications, Stuxnet worm could become a serious threat to power grids.

Attacks caused by cyber intrusions, or cyber attacks, can be conducted remotely and secretely. The attackers will mainly adopt cyber intrusions to attack future smart grids.

1.3 Cascading Failure

Cascading failures are considered to be the leading reasons of large-scale power outages in power systems [18]. The cascading failure refers to a sequence of dependent failures of individual components that successively weakens the power system [19]. Generally speaking, the cascading failure includes initial failure(s) and dependent failures.

The *initial failure(s)* can occur on substations, transmission lines, or other components. Initial failures can be triggered by different causes. From the perspective of traditional contingency analysis, *random causes* are under great considerations. Such causes include natural disasters, e.g., earthquakes and hurricanes, operator errors, equipment failures, supply shortages, and so on [5]. It is predominant to check $N-1$ and $N-2$ system security [6], because it is rare that the system loses multiple components simultaneously by random causes. From the attack's perspective, malicious attacks, e.g., physical sabotages and cyber intrusions, are likely to trigger large-scale cascading failures. Different from random causes, malicious attacks are powerful. Attacks can be controlled in terms of selecting different targets and different number of targets. Attacks can be conducted in

CASCADE mode	• Topology	• Identical components • Randomly choosing load values between a range • Overloading when the load exceeds a threshold.
Wang-Rong model	• Topology	• Identical components • Using the degree to calculate load • Overloading when the load exceeds the capacity. • The capacity is proportional to the initial load.
Motter-Lai model	• Topology	• Identical components • Calculating the betweenness as the load • Overloading when the load exceeds the capacity • The capacity is proportional to the initial load.
Betweenness model	• Topology	• Identical components • Calculating betweenness to calculate the load • Overloading when the load exceeds a threshold.
Efficiency model	• Topology • Substation type	• Calculating the betweenness as the load. • Overloading components can be recovered. • Network efficiency
Extended model	• Topology • Substation type • Line impedance	• Calculating the extended betweenness as the load • Overloading when the load exceeds the capacity. • Net-ability
Hines model	• Topology • Substation type • Line impedance • DC power flows	• Calculating DC power flows • Generation dispatch and load shedding • Trip lines due to overheat. • Blackout Size
OPA model	• Topology • Substation type • Line impedance • DC power flows • Probability of line failure	• Calculating DC power flows • Generation dispatch and load shedding • Trip lines with probability. • Both fast and slow dynamics
Hidden failure model	• Topology • Substation type • Line impedance • DC power flows • Probability of line failure	• Calculating DC power flows • Generation dispatch and load shedding • Trip lines with probability. • Hidden failures
Manchester model	• Topology • Substation type • Line impedance • AC power flows	• Calculating AC power flows • Tripping lines • System convergence • Fast dynamics

Figure 1.1. Brief Summary of Cascading Models

different ways, simultaneously or sequentially.

Dependent failures are triggered by initial failure(s). The phenomenon is that many power grid components are failed subsequently after initial failure(s). These subsequent failures are referred to as the *failure propagation*. The reasons causing the failure propagation are very complicated [6]. Briefly speaking, massive power cannot be stored; the balance between power supply and demand should be met on time; initial failure(s) of critical components could cause great power loss or large-scale power redistribution; such disturbances trigger subsequent failures. In existing works, the cascading process is mimicked by using different models. Many models have been proposed to study the cascading failure from different aspects [6, 20–22]. From the attack's perspective, these models include CASCADE model [23], Wang-Rong model [22], Motter-Lai model [24], betweenness model [25], efficiency model [26], extended betweenness model or extended model [21], Hines model and [27, 28], OPA model [29], hidden failure model [30] and Manchester model [31]. (The models are named by either the popularly accepted name or the author's name who proposed the model.) The brief description of each model is shown in Fig. 1.1.

In this dissertation, three models, i.e., the efficiency model [26], the extended betweenness model, or the extended model in short [21] and the Hines model [28], will be employed to investigate the attack strategies. The adopted models will be introduced in details in each manuscript. For interested readers, the details of other models can be found in [6, 20–22].

1.4 Attack Strategy

If attackers want to launch successful and powerful attacks, they need to answer the following three questions.

1. In what ways can attackers initially attack the targets?

2. Which cascading model is the best one to predict the attack performance?

3. **Which and how many components should be identified as targets?**

Comprehensively answering any of aforementioned questions needs significant amount of research work. In the current literature, the power grid is considered as one of critical cyber-physical systems, and cyber-physical attacks against such power grids have attracted broad attentions [32–35]. These works can well answer the first question. In addition, many models have been developed by using different information of power grids [20, 21]. These models are helpful to answer the second question.

However, there are few works that specifically discuss the *attack strategies*. In this dissertation, the attack strategy refers to the following aspects.

- Which substations, transmission lines, or both, should be considered as targets?
- How many targets should be chosen to balance between the attack cost and performance?
- Should the targets be attacked synchronously or sequentially, aiming to obtain the best strength?

This dissertation focuses on tackling the third question from the attackers' perspective. The works in this dissertation also build the foundation for developing defense solutions. It is assumed that the attackers can completely conduct attacks and have enough knowledge about the cascading models. In particular, this dissertation will discuss *four* proposed attack strategies, which have strong performances and low complexity. Brief discussions of proposed attack strategies are given in Section 1.5.

Level	Information	Availability
Level 1	Topology	Easy
Level 2	• Topology • Substation type • Length of lines	Moderate
Level 3	Details of the grid: • Topology • Substation type • Impedance of lines • Power supply/demand on substations • etc.	Hard

Figure 1.2. Different levels of power grid information known by the attackers

1.5 Motivations and Highlights of Manuscripts

It is a nature assumption that different attackers might have different amonts of information on the power grid. In reality, power grid information can be obtained in different ways, e.g., gathering the topology from online Google Maps [10], purchasing the U.S. grid with raw data from commercial companies [36] and possibly hacking the details of power systems [37]. In this dissertation, it is not to specifically discuss how the attackers can obtain the information of power grids. Instead, developing attack strategies will be discussed based on three different levels of power grid information that are possibly known by attackers. Brief descriptions of the considered levels are given in Fig. 1.2. Under different levels of power grid information, we have adopted different cascading models to develop attack strategies.

1.5.1 Understanding Failure Propagation

Major blackouts, e.g., Northeast blackout of 2003 in Table 1.1, mainly result from cascading failures in power transmission systems. It is of great importance

for both attackers and defenders[1] to understood how failures propagate in power systems.

In **manuscript 1**, a useful tool is implemented to visualize cascading failures. Such a tool can let people "watch" how the failure propagates from a local point to the entire grid. It is of great help to understand the complicated cascading process. In addition, through investigating single-substation attacks, it is possibly to discover different failure propagation processes in the testing power grid.

1.5.2 LDV-based Attack Strategy

It is of importance for attackers to gather the information of the power grid. The more detailed the collected information is, the more accurate the cascading model can be adopted and the stronger the attack strategies can be developed.

In **manuscript 2**, it is assumed that the attackers have known the topology (i.e., level 1) of the power grid. Under this scenario, the efficiency model [26] is adopted to study cascading failures. In particular, a new metric, called the *load distribution vector* (LDV), is proposed to represent the feature of substations or transmission lines. The LDV can be used to design attack strategies on substations or transmission lines. Take substations as an example. Referring to LDV, if two substations have similar LDVs, they are close in terms of the Euclidean distance between the two LDVs. Therefore, it is possible to cluster all substations into different groups and then select a target from each group, which is referred to as the LDV-based node attack strategy.

1.5.3 Riskgraph-based Attack Strategy

Attackers are likely to obtain more information of the power grid, not just knowing the topology. One possible way is to purchase the power grid raw data

[1]Defenders refer to those who want to make power systems secure and reliable (e.g., power companies).

from business companies, e.g., Platts [36]. The raw data include the general information, e.g., the grid's topology, geographic coordinates of substations, power plants and generators, length of transmission lines and affiliations, but do not provide the details of power systems. The general information is enough for attackers to adopt a more accurate model to mimic cascading failures and discover strong attack strategies.

In **manuscript 3**, the extended model [21] is used to set up cascading simulator. Adopting the extended model needs the topology, types of substations (i.e., generator, demand substation and transmission substation), and the admittance of transmission lines. The needed information of the grid is either included in IEEE standard test benchmarks [38] or can be estimated for the purchased data [39, 40]. In particular, it is found that there are hidden relationship among substations in terms of vulnerability analysis. Such relationship is useful to design strong attack strategies with low complexity. A new metric, called *risk graph*, is proposed to show the hidden relationship. Based on the new metric, the riskgraph-based attack strategies against substations or transmission lines are proposed for attackers.

1.5.4 CIG-based Attack Strategy

Continuing the discussion in the previous manuscript, in **manuscript 4** it is of great interest to investigate the attacks that occur on substations and transmission lines simultaneously. Because, the previous two manuscripts and many existing works on analyzing the vulnerability of power grids are conducted from the substation-only perspective or the transmission-line-only perspective. In other words, it is assumed that attacks or contingencies occur on either substations or transmission lines.

However, it is reasonable that malicious attacks can occur on both substations and transmission lines. In this manuscript, the joint-substation-transmission-line

perspective is introduced to conduct vulnerability analysis in power grids. In addition, the metric *component interdependency graph* (CIG) is proposed by generalizing the idea of risk graph in manuscript 3. Balancing between choosing substations and transmission lines as targets, the CIG-based attack strategy is proposed to possibly find strong attacks.

1.5.5 SAG-based Attack Strategy

Attackers can be the experts in power systems and have the details of target power systems. For instance, the hostile countries can first obtain the entire or part of the U.S. power grid details by hacking or other means, and then organize the experts to launch possible attacks. Such possible attacks have attracted growing concerns in the U.S. (seeing the public voices in Section 1.1). In addition, multiple attacks can be conducted in different ways, e.g., synchronously or sequentially. In manuscripts 2, 3 and 4, attacks are assumed to occur synchronously to possibly trigger cascading failures, which is referred to as the *synchronous attack*. However, the synchronous attack have apparently missed the scenario that multiple attacks can be conducted sequentially.

In **manuscript 5**, a new attack scenario, called the *sequential attack*, is introduced for attackers with expertise. Similar idea on contingency analysis in the power society has rarely been reported. The Hines model [27, 28], a DC power-flow model, is adopted to mimic cascading failures on transmission lines in power systems. From the sequential attack perspective, there are many multiple-substation combinations that can yield large attack strength. Previously, these combinations cannot yield large strength from the synchronous attack perspective. In addition, a novel metric, called the *sequential attack graph* (SAG), is specifically designed to reveal the relationship among substations from the sequential attack perspective. Also, the SAG-based sequential attack strategy is proposed and compared with

some representative schemes.

1.6 Summary

As a summary, it is of great importance to comprehensively investigate the malicious attacks against power transmission systems. This dissertation focuses on tackling such critical issues. Generally speaking, this dissertation provides the reasonable answers to the following questions.

- Why can malicious attacks trigger large-scale power outages in power transmission systems? *The answer: initial failures of a few, even one in extreme cases, critical power grid components can trigger severe cascading failures in the entire grid and results in large-scale blackouts.*

- How can attackers determine the targets, the attacks on which can trigger major blackouts? *The answer: there are hidden relationships among power grid components in context of vulnerability analysis; such relationships are revealed in four proposed metrics, i.e.,* ***load distribution vector****,* ***risk graph****,* ***component interdependency graph*** *and* ***sequential attack graph****; relying on these metrics, attackers can easily identify targets for different attack strategies.*

List of References

[1] M. Levine, "Outgoing dhs secretary janet napolitano warns of serious cyber attack, unprecedented natural disaster," Aug.27 2013. [Online]. Available: http://abcnews.go.com/

[2] R. Smith, "U.S. risks national blackout from small-scale attack," Mar.12 2014. [Online]. Available: http://online.wsj.com/news

[3] J. Tollefson, "US electrical grid on the edge of failure," *Nature News and Comment*, Aug.25 2013.

[4] A. Kredo, "U.S. electric grid inherently vulnerable to sabotage," Apr.8 2014. [Online]. Available: http://freebeacon.com/author/adam-kredo/

[5] P. Hines, K. Balasubramaniam, and E. C. Sanchez, "Cascading failures in power grids," *IEEE Potentials*, vol. 28, no. 5, pp. 24–30, Sept. 2009.

[6] M. Vaiman et. al., "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[7] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.

[8] The Guardian. "India blackouts leave 700 million without power." [Online]. Available: http://www.guardian.co.uk/

[9] R. Richardsonh, "Power grid threats: EMPs, terror attacks and grid failures." [Online]. Available: http://offgridsurvival.com/powergrid-emps-terrorattacks-gridfailures/

[10] "FBI, joint terrorism task force arrest suspect in arkansas power grid attacks," 2013. [Online]. Available: http://www.forbes.com/

[11] R. Smith, "Assault on california power station raises alarm on potential for terrorism," Feb.18 2014. [Online]. Available: http://online.wsj.com/

[12] "The smart grid: An introduction." [Online]. Available: http://energy.gov/

[13] "Small-scale power grid attack could cause nationwide blackout, study says," Mar.13 2014. [Online]. Available: FoxNews.com

[14] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan. 2012.

[15] E. I. Bilis, W. Krger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 4, no. 7, pp. 854–865, Dec. 2013.

[16] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[17] R. Lemos, "DHS video shows potential impact of cyberattack," Sept.27 2007. [Online]. Available: SecurityFocus.com

[18] S. Mei, Y. Ni, X. Zhang, G. Wang, and G. Wang, "A study of self-organized criticality of power system under cascading failures based on AC-OPF with voltage stability margin," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1719–1726, Nov. 2008.

[19] R. Baldick et. al., "Initial review of methods for cascading failure analysis in electric power transmission systems," in *IEEE power engineering society general meeting*, Pittsburgh, PA, USA, July20-24 2008.

[20] S. Mei, X. Zhang, and M. Cao, *Power Grid Complexity*. Beijing: Tsinghua University Press, Aug. 2011.

[21] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, pp. 1334–1340, July 2011.

[22] 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, Dec. 2009.

[23] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 1, pp. 15–32, Jan. 2005.

[24] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, 065102(R), 2002.

[25] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, no. 5, May 2002.

[26] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, no. 4, Apr. 2004.

[27] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, Sept. 2010.

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

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

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

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

[32] X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[33] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, pp. 741–749, 2011.

[34] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[35] P. J. Hawrylak, M. Haney, M. Papa, and J. Hale, "Using hybrid attack graphs to model cyber-physical attacks in the smart grid," in *5th International Symposium on Resilient Control Systems*, Salt Lake City, UT, USA, Aug.14-16 2012.

[36] "Platts." [Online]. Available: www.platts.com

[37] E. K. Chow, "Forget hackers: Squirrels are a bigger threat to america's power grid," Jan.28 2014. [Online]. Available: http://theweek.com/article/index/255510/forget-hackers-squirrels-are-a-bigger-threat-to-americas-power-grid

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

[39] P. Kundur, *Power System Stability and Control*. New York: McGraw-Hill, Jan. 1994.

[40] A. Bernstein, D. Bienstockz, D. Hayx, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures - analysis and control implications," Columbia University, Electrical Engineering, Columbia University, Electrical Engineering, Tech. Rep., May 2011.

CHAPTER 2

Manuscript 1: Failure Propagation and Visualization for Vulnerability Analysis in Power Grids

Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, and Haibo He

Department of Electrical, Computer, and Biomedical Engineering

University of Rhode Island, Kingston, RI 02881

Manuscript status: in submission to 2014 IEEE Conference on Communications and Network Security (CNS'14)

Corresponding Author: Yihai Zhu

Kelley Annex, Room A115

4 East Alumni Ave.,

Kingston, RI 02881

Phone:+1-401-874-5846

Email: yhzhu@ele.uri.edu

2.1 Abstract

The cascading failure is considered to be the leading reason of large-scale power outages. One of the fundamental characteristics of cascading failures is that failures can propagate within the entire power grid and cause severe power loss. Investigating failure propagation significantly contributes to understanding large-scale power outages. In this work, we introduce a new platform that can visualize the failure propagation in power grids. The proposed platform not only let people "watch" how failures propagate, but enable investigation on the insights of cascading failure triggers. In particular, we adopt the extended model to simulate cascading failures, and develop the platform in ArcMap. The power grid around Bay Area, California, is used as the test benchmark. The proposed platform can successfully demonstrate how a failure propagates from a local point to the entire grid and eventually paralyzes the system. Through this platform, we investigate single-node (i.e. substation) failure problem. We discover three different and important types of failure propagation, which have different requirements on the system protection

2.2 Introduction

In the past decade, several major blackouts, e.g., the famous cases in [1–3], seriously affected the modern society and raised many concerns. Enhancing security and robustness of these cyber-physical power transmission systems becomes an increasingly urgent task [4–7]. Due to the complexity and significance of this problem, the investigation of blackouts attracts attentions from researchers, companies and governments.

The *cascading failure* is considered to be the main mechanism that results in major blackouts in power systems [8, 9]. Specifically, the failure of one or several power grid components (i.e., substations and transmission lines), due to natural

disasters, errors from equipments, etc., can trigger a series of successive failures of other components and progressively weaken the power transmission system.

An important research direction on the cascading failure is to understand the relationship between initial failures and the final damage to the power grid after the cascading process finishes. Specifically, it is to investigate the vulnerability of power grid components. In this type of research, the cascading failure process is mimicked by different models [10]. The inputs are substations/transmission lines that are initially failed; the outputs are the damage quantified in different measures, such as blackout size [5], net-ability [11], and network efficiency [12]. The detailed cascading process is often treated as a "black box".

Although the existing method is predominant in power grid vulnerability analysis, it is arguable that unfolding the "black box" gives opportunities to further understand cascading phenomena. There are three interesting questions that have not been answered. First, shall we treat the following two scenarios separately? (1) An initial failure can immediately trigger large-scale failures; (2) an initial failure can continually trigger trivial failures and eventually involve into large-scale failures. Second, two different initial failure cases might yield the same or very close cascading damage, e.g., net-ability. Do they have similar impact on the power grid? Finally, using two different cascading models, the damage for the same initial failure, e.g., net-ability or blackout size, can be different. Does this mean that at least one model is wrong?

Unfolding the "black box" can disclose the diversities of cascading failures. It has been found that the cascading failure has multifarious intermediate results [13]. Quantitative risk analysis can identify the criticality of components (i.e., substations/transmission lines) in a power grid. Generally speaking, the components that have equal or very close quantitative results are considered to be of similar signif-

icance to the power grid. In [13], however, even with equal quantitative results, the initial failures can demonstrate different failure accumulation processes. Such differences are the fundamental characteristics of cascading failures, and cannot be revealed or further investigated, if one only checks the eventual damage.

Power grids are man-made cyber-physical systems on the Earth, whose security and reliability issues also have strong relation with the geographical and regional information [14–16]. It is highly possible that malicious attackers can trigger the initial failures by failing substations in different regions [14], or fail several transmission lines in the same geographical area [15]. In addition, power failures can affect different areas and result in different impact [16]. Integrating the geographical and regional information into the existing quantitative analysis can help people comprehensively understand power grid vulnerability.

There exist different methods in analyzing cascading failures [5, 10, 17, 18], such as transient stability analysis (TSA), power-flow models and topological models. Comparisons among different methods or models can be conducted by looking into the details of cascading processes. TSA methods, based on differential algebraic equations, are predominant in power system control design; power-flow models, based on steady-state analysis, are widely adopted in power grid vulnerability analysis. In [17], the detailed power flow comparisons are conducted between a DC-power model with a TSA method. At the beginning of cascading failures, the power flow redistribution in the DC-power model is consistent to that in the TSA method. Topological models are developed from complex network theories. It is still necessary to further compare in detail the cascading processes of topological models with those of other methods and models [5, 18].

Based on the aforementioned discussions, it is necessary to develop such a tool that can reveal the insights of the cascading processes. It is of importance to

point out that different research communities use different terminologies, models and approaches when investigating the cascading failure. From the perspective of power systems, people often use detailed electrical information of power grids to perform analysis. From the perspective of complex networks, people mainly adopt the topological structure of power grids to set up simulations. We would like to give a solution that is meaningful to both aspects. A promising way is through visualization.

In this work, we develop a platform to visualize the failure propagation in detail. Such platform can lead to new discoveries of cascading failures. Generally speaking, there are three major challenges in developing such a platform. First, because of security reasons, the information of real-life power transmission systems are not publically available, or available, but incomplete. Second, it is necessary to develop reasonable cascading models based on the available power grid data. Finally, both the simulation and visualization of cascading failures need heavy computation, especially for large-scale power grids.

Specifically, we have purchased the real-life power grid data from Platts [19] and adopted the extended model [11] to set up cascading simulation on the power grid around Bay Area, California. In addition, we use ArcMap (i.e., a product from ESRI [20]) to store the power grid topology and visualize cascading failure processes.

Our **contributions** are as follows.

- We propose a new platform to investigate cascading failures in power grids. The proposed platform can successfully demonstrate how failures propagate and paralyze the power grid. The observations are consistent with recent discoveries [21]. In addition, the proposed system is implemented with real-life power grids, which provides not only quantitative analysis results but

geographical results of cascading damage.

- By investigating single-substation failures in the proposed platform, we discover three different initial failures that can trigger failure propagation with very different features in time domain. Such discoveries are of importance to understand the cascading failure and protect power grids.

The work is structured as follows. The related work is given in Section 4.3. System model and design are discussed in Section 2.4. Simulations and observations are made in Section 6.7. Finally, conclusions and future works are provided in Section 6.8.

2.3 Related Work

In the current literature, different models have been proposed to mimic failure propagation (i.e., the cascading failure) [11, 13, 22–29]. In [13, 22–24], pure topological models are adopted to model cascading failures. Although those models are not accurate to reveal the power distribution in power systems, they are still useful in conceptually setting up the cascading failure model and discovering stronger attack strategies. Pure power-flow models in [25–27] are mainly employed to identify critical components (i.e., substations and transmission lines). Those models are completely based on electrical theories. Such models, however, are with high computation cost as well as needing detailed electrical features in analyzing cascading failures. Although power-flow models are close to mimicking real cascading failures, they are limited in many cases, e.g., without enough information of power grids. Recently, the hybrid model, called the *extended model*, is proposed to investigate the vulnerability of power grids [11, 28]. The extended model adopts simple electrical features (e.g., impedance of transmission lines) and the topology information to set up the cascading model. The extended model has two key advantages.

First, the extended model adopts *Power Transfer Distribution Factors* (PTDFs) to calculate the power distribution [11, 30]. In other words, the extended model is based on calculating DC power flows and is more accurate than pure topological models in mimicking cascading failures. Second, the extended model needs much less electrical features than pure power-flow models, and is more suitable for setting cascading model to different power grid data. Different models for mimicking cascading failures are summarized and compared in [10].

Furthermore, the application of visualization approaches provides other ways to investigate the vulnerability of power grids [31–36]. The topology of U.S. power grids is visualized in [31], including important power plants and high-voltage transmission lines. Some visualization platforms, e.g. GreenGrid in [32] and 3D visualization scheme in [33], have been explored to monitor the American electricity infrastructure. To aid power system operators interpret contingency analysis results, a three-level visualization tool was proposed to visualize vulnerability and severity of substations [34]. Besides, there are two tools that can visualize cascading failures [35, 36]. However, the work in [35] adopted IEEE power grid benchmarks, which could not connect the vulnerability analysis with the geographical information of power grids; the work in [36] adopted the pure topological model to mimic cascading failures, where the model itself could not reveal failure propagation accurately.

In this work, we implement a new platform that can be used to investigate the failure propagation in power grids. In particular, we adopt the extended model to mimic cascading failures and choose the power grid around Bay Area, California, as the test benchmark.

2.4 System Model and Design

In this work, we adopt the power grid data that we purchased from Platts [19] as the test benchmark. Generally speaking, to conduct investigation with such commercial power grid data has advantages and disadvantages. The purchased data include the power grid that is operating in real life. Such power grid provides the possibility to study, even verify, the failure propagation in real power transmission systems. However, the purchased data lack the detailed electrical features of the power grids. In other words, the information about the purchased power grid is not enough to set up pure power-flow models to study the cascading failure. To balance between the availability of the power grid data and the accuracy of cascading model, we choose the extended model to mimic the cascading failure.

In the rest of this section, we briefly review the extended model and the setup of cascading simulator under this model in subsection 2.4.1. In subsection 2.4.2, we introduce the constriction of the test benchmark from raw data we purchased. In subsection 2.4.3, the design and implementation of the proposed platform is introduced in details.

2.4.1 Cascading Failure Simulator using the Extended Model

The extended model is first introduced in [28], and well developed in [11]. We briefly summarize the key features of this model as follows.

1. *Directed Graph*: The power grid under this model is considered to be a directed graph $\mathbf{G} = \{B, L\}$, where B represents the set of nodes (i.e. substations) and L represents the set of links (i.e. transmission lines). The direction of a link stands for the direction of the electricity. The nodes consist of generators, transmission nodes and load nodes. Generators are denoted as the set G ($G \subseteq B$); load nodes are denoted as the set D ($D \subseteq B$). In addition, N_B, N_L, N_G and N_D are adopted to represent the number of substations,

transmission lines, generators and load substations, respectively.

2. *PTDFs*: In power systems, power distribution basically follows electrical theories. Under the extended model, *Power Transfer Distribution Factors* (PTDFs) [11, 28, 30] are employed to reflect the sensitivities of power flow changes in links, caused by the real power injection and withdrawal at a pair of nodes. PTDFs are derived from DC power flow model, making the power distribution under the extended model be governed by the fundamental electrical theories. We adopt the PYPOWER in [37] to calculate all PTDFs in the simulations.

3. *Extended Betweenness*: In power systems, power is transmitted from generators to load nodes along links, which means the change of power flow in transmission lines is caused by each generator-load node pair. In other words, the summation of all power in a link caused by all generator-load node pairs could determine the total power in this link. The *extended betweenness* of a node is defined as half of the total summation of power in all links connecting to this node, as the summation double counts the inward and outward power flow which are equal in the magnitude,

4. *Net-ability*: In [11], the net-ability of a power grid network (e.g. $\mathbf{G}$), denoted as $E(\mathbf{G})$, is defined as $\frac{1}{N_G N_D}\sum_{g\in G}\sum_{d\in D}\frac{P_{gd}}{Z_{gd}}$, where P_{gd} and Z_{gd} are the maximum power injection and the impedance between the generator g and the load node d, respectively.

Cascading failures have already been well studied under pure topological models [24, 38]. Here, we defined the *cascading failure simulator* (CFS) under the extended model by redefining some important concepts as follows.

- *Load*: The extended betweenness of a node, e.g. node i, is employed as the

definition of its load, similar to the functionality of the *betweenness* in [38]. Before any failure, the load of node i is referred as its *initial load*. Once the occurrence of any failure in the power grid, the load of node i will be updated by recalculating its extended betweenness.

- *System Tolerance*: In cascading failure simulations, the system tolerance is an important parameter, which represents the stability of power grids. Generally speaking, the larger the system tolerance of a power grid is, the more robust this power grid is.

- *Capacity*: In reality, the capacity of a node represents the maximum load that it can tolerate. Due to many reasons, e.g., the cost of construction fee, the capacity cannot be infinity. In the work, the definition of the capacity of a node is similar to that in [24, 38], the multiplication of the system tolerance and its initial load.

- *Overloading*: When the load of a node exceeds its capacity, the overloading will happen. Under the extended model, the overloaded nodes and their links are assumed to be removed from a power grid.

- *Load Redistribution*: After removing the overloaded nodes and its corresponding links, the topological structure of the power grid network will change. Thus, the power that originally passes through the removed nodes needs to be detoured, which causes the power to be redistributed in the power gird. Under the extended model, the new load distribution is based on recalculating the PTDFs and the extended betweenness. The load redistribution may raise other nodes to be overloaded and removed from the power grid, which might cause the failure propagate from one point to the while grid. The load redistribution will stop until there is not any overloaded node in

the remaining power grid network.

- *Time Simulation*: In the CFS, the concept of "round" is adopted to describe the progress of cascading failures [13]. In the first round, initial failed nodes will removed from power grids. In the following each round, the CFS will first update the topological structure of power grids, then calculate the new load distribution for all nodes, and finally remove all overloaded nodes. The CFS will stop at the final round, in which there is not any overloaded node. The number of rounds of each attack might be different, which will be seen in Fig. 2.5.

The detail of the CFS is discussed in our previous works [29, 39].

2.4.2 Construction of the Test Benchmark

We have purchased the entire North American power grid data, which includes thousands of substations and transmission lines, from Platts [19]. Currently, it is computationally infeasible for us to conduct cascading simulations on such a big power grid. For demonstration purpose, we chip the power grid around Bay Area, California, as the test benchmark.

Originally, the raw GIS data consist of four types of layers (i.e., the shapefiles in ArcGIS [40]), the substation layer, the transmission line layer, the generator unit layer and the power plant layer. To construct the test benchmark from the raw data, there are three challenges. First, the notations of substations in the substation and transmission line layers are not completely consistent, due to the fact that Platts originally collects those information from different providers. Second, identifying the generators and load substations is difficult, because the IDs of power plants in the power plant layer are different from that of substations in the substation layer, and also no corresponding information is about the load

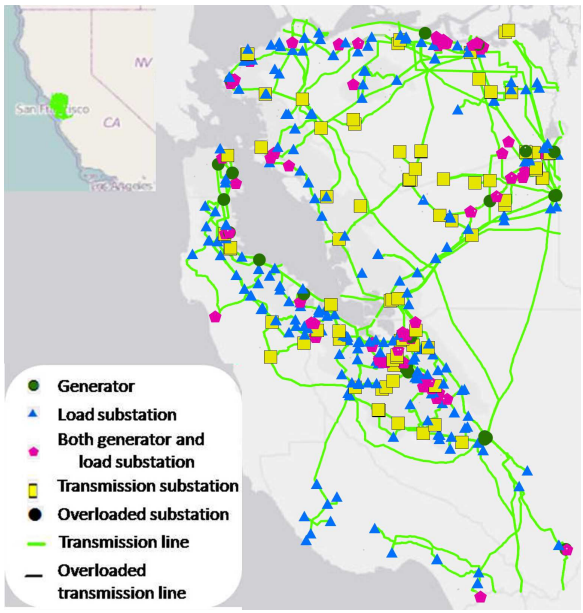


Figure 2.1. Bay Area power grid topology

distribution in the raw data. Finally, the raw data also lacks the corresponding information to discuss the electrical impedance of transmission lines.

In what follows we will briefly introduce how to set up the test grid network according to the introduction of American power transmission system [41] and some explanations from Platts [42].

First, originally there are 688 transmission lines and 532 substations in the transmission line layer and the substation layer, respectively. In the substation layer, every substation has an unique ID. In the transmission line layer, each line has two endpoints (i.e. substations in the substation layer), which can be represented by the unique IDs of the two endpoints. In addition, there are 23 fields in the transmission line layer to describe the properties of transmission lines, such as voltage, length in KM (kilometer) and so on. The voltage of transmission lines in USA is usually more or equal than 69 KV (kilovolt) [41]. When we dove into the voltage field of all transmission lines, we found that the voltage of some transmission lines are less than 69 KV, which are either 10 KV or a negative

number. In [19], we know transmission lines with the voltage as 10 KV are just used by Platts to connect a substation with a power plant, which only has one valid endpoint and is not included in the real transmission system. The lines with voltage as a negative number have two valid endpoints, and they are part of the transmission system. Also, some substations in the substation layer are redundant. When we filter out those transmission lines with the voltage as 10 KV and the redundant substations, the Bay Area power grid network can be easily set up.

Second, generators are decided according to explanations from Platts [19]. That is, substations, which associate with a 10 KV transmission line or geographically close to a power plant in power plant layer (within 1 KM in this work), are considered as generators. In a transmission system, load substations usually work in lower voltages [41]. In this work, substations that have the maximum voltage less or equal than 115 KV but more than 0 KV are viewed as the load substations. Other substations, not a generator or a load substation, are viewed as transmission substations. It should be stated that some substations not only work as generators, but work as load substations simultaneously.

Finally, the valid Bay Area power grid network consists of 614 transmission lines and 467 substations, which includes 120 generators and 320 load substations. Fig.2.1 shows this power grid and its generators and load substations.

Employing the extended model to analyzing the vulnerability of power grid networks basically needs the reactance of each transmission line, due to the lossless assumption of transmission lines [30]. The reactance of transmission lines is estimated according to [43], and the ratio is $0.4\Omega/KM$ (ohm per kilometer). For example, if the length of a transmission line is 15 KM, its estimated reactance is 6Ω. This estimation is similar to the way directly adopting the length of a

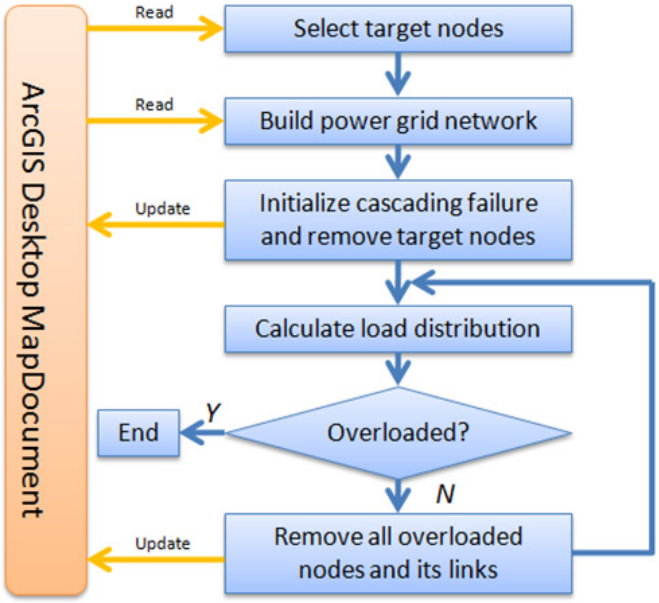


Figure 2.2. The flowchart of the proposed platform.

transmission line as its reactance in [15].

2.4.3 Platform Design

The proposed platform is to help people understand the principles of failure propagation in power grids. The new platform consists of three major functional modulations: visualization in ArcMap, user interface and CFS.

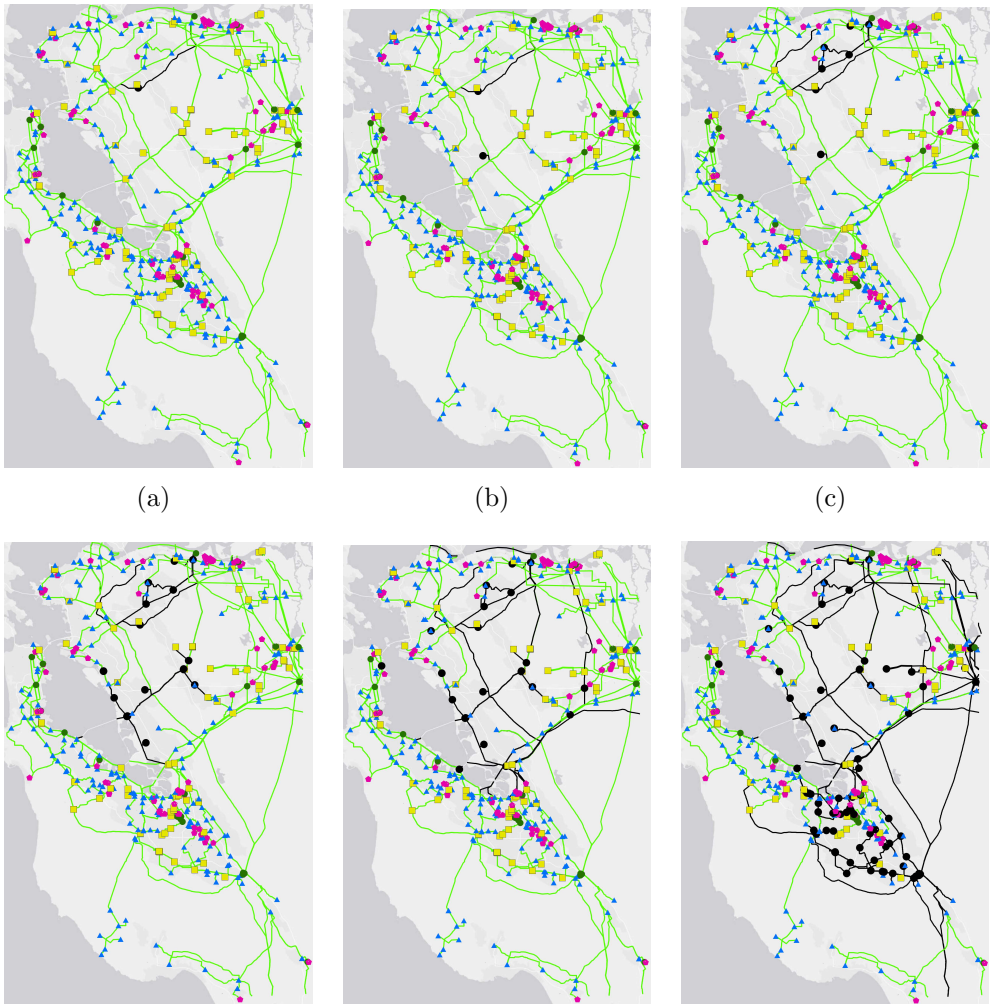
- *Visualization in ArcMap*: ArcMap is adopted as data storage and visualization in this platform. The test benchmark is visualized in ArcMap as different layers. The proposed platform adopts three of the four layers in the raw data, i.e. the substation, transmission line and power plant layers, to construct the grid network. In order to simulate the statuses and types of substations and transmission lines, e.g. alive and failed, one additional field, called "STATUS", is added into each of these layers. We assume each valid transmission line has two status, "failed" and "alive". In ArcMap, the two statuses are distinguished by using different colors (black and green). Also, substations

are divided into four categories, generator only, load substation only, both generator and load substation, and transmission substation. Originally, they are alive and symbolized as green circles, blue triangles, red polygons, and yellow squares, respectively. If a substation of any type is failed, it will be replaced by a black circle.

- *User Interface*: A toolbar, based on the Python add-in in ArcGIS desktop, is developed and added into ArcMap to control the procedures of the visualization. The toolbar consists of three buttons named as "build", "select" and "start", respectively. Each button has its corresponding functional script. The "build" button is responsible for constructing the power grid network from raw GIS data and resetting the statuses of substations and transmission lines. The "select" button is adopted to choose target substations in ArcMap, while "start" button is used to trigger the cascading failures and to refresh the statuses of substations and transmission lines in ArcMap.

- *CFS*: The extended model and the CFS, discussed in Section 2.4.1, are employed to simulate the load distribution and cascading failures after initial failures. Given a certain system tolerance value, a cascading failure process consists of one or more rounds. Within each round, the overloaded nodes are failed, and their statuses (including the statuses of the connecting links) are updated as "failed", visualized as black circle and black lines in ArcMap, respectively. If no more overloaded nodes, the cascading failure procedure will stop.

The flowchart of the proposed visualization platform is shown in Fig. 2.2. As a summary, the proposed visualization platform has the following features that are not presented in the existing visualization tools [31–34, 36],



(a) (b) (c)

(d) (e) (f)

Figure 2.3. An example of the cascading failure with six rounds.

- Providing a way to "watch" how cascading failures propagate in power grids, which can help people understand the cascading phenomenon.
- Providing the user interface to trigger and simulate different types of initial failures, e.g. selecting different initial nodes and different number of them.
- Providing a DC based model, i.e. the extended model, to investigate the vulnerability of power grids.

2.5 Simulation Results and Analysis

The proposed platform is developed in ArcMap and all scripts are written in Python. The power grid around Bay Area, California, is adopted as the test benchmark. The construction of the power grid network from the raw GIS data is discussed in Section 2.4.2. The simulations and discussions are made detailedly in the following subsections.

2.5.1 Failure Propagation

Understanding the failure propagation is an important aspect of studying the vulnerability of power grids. In reality, the failure propagation means when one or more substations/transmission lines fail, they will shift their load to other substations/transmission lines, which could trigger the successive failure of them. The proposed visualization platform could let people "watch" how a failure propagates from a point to the while grid network. In particular, we observe two critical failure propagation patterns that can collapse the power grid.

The first critical pattern is that the single initial failure can continually trigger other failures and paralyze the power grid after a few rounds. An example of such pattern is demonstrated in Fig. 2.3. The single failure is manually triggered, and the cascading failure finally stops after six rounds. In the subfigures, the failed nodes, together with their links, are marked as black circles and black lines, respectively. In Fig. 2.3(a), the failure begins after manually knocking down a node. The removal of this node and its links changes the topological structure of the power grid, then raises the power redistribution, and finally causes another node to be overloaded and failed, as shown in Fig. 2.3(b). From Fig. 2.3(c) to Fig. 2.3(e), the number of overloaded and failed nodes is increasing, and the failure propagates from the initial point to the global power grid. It is clearly seen in Fig. 2.3(f) that when the failure procedure stops, most nodes are failed and the power

grid is almost paralyzed.

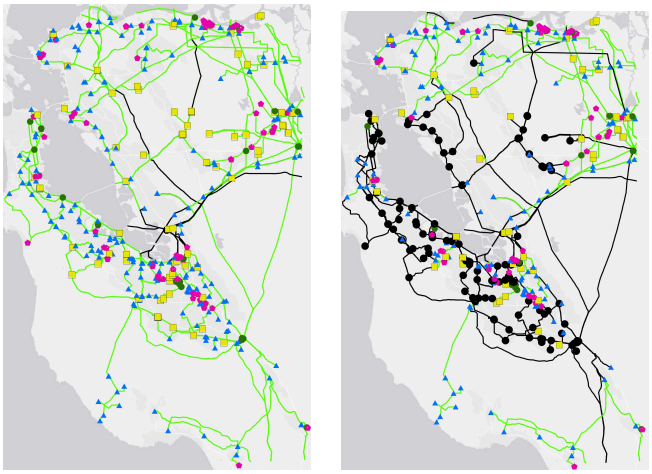
The second critical pattern is that the single initial failure can quickly trigger many other failures and paralyze the power grid with one or two rounds. One of such examples is shown in Fig. 2.4, where black circles and black lines have the same meanings with those in Fig. 2.3. In Fig. 2.4(a), the initial failure is manually triggered, which raises many nodes to be severely overloaded. Just after the second round, the power grid occurs large-scale avalanche, demonstrated in Fig. 2.4(b).

We have the following observations from Figs. 2.3 and 2.4.

- The power grid, as a type of man-made orderly network, has lots of critical node. The existence of such critical nodes significantly increase the instability of the power grid. For instance, the two single failures demonstrated in Figs. 2.3 and 2.4 can severely damage the power grid. This observation is consistent with the statement recently published in Nature News & Comment [21].

- Geographically, the failure propagation begins from the local point, where the initial failure is triggered, gradually involves into large-scale failures, and finally trigger failures that might be far from the initial point. This observation is similar to the failure propagation process that occurred in real cases, e.g., Northeast blackout [1].

- Different initial failures can affect different regions that the power grid serves. Compared Fig. 2.4(b) with Fig. 2.3(f), although both initial failures result in severe damage to the test benchmark, the regions that lose the power are partially different. Put differently, it is of importance to analyze the cascading damage from the perspective of the affected regions.



(a) (b)

Figure 2.4. An example of the cascading failure with two rounds

2.5.2 Different Initial Triggers of Cascading Failures

In Section 2.5.1, we discussed two different critical failure propagation patterns, which were caused by initially failing different nodes. Therefore, it is of great importance to investigate the classifications of nodes in the power grid based on the contribution to power outage. In the context of single node failures, we investigate that the initial failures of different nodes can result in different types of cascading failures in the power grid.

Using the proposed visualization platform, we observed that different initial failures could cause three types of power grid network failures: *non-critical*, *rapid-and-critical*, and *propagative-and-critical*. The brief description of them is given as follows.

- In the non-critical failures, the initial failure of a node could not cause severe damage to a power grid.
- In the rapid-and-critical failures, the initial failure of a node could cause severe damage to a power grid within very few rounds. In other words, the large-scale failure occurs quickly after the initial failure.

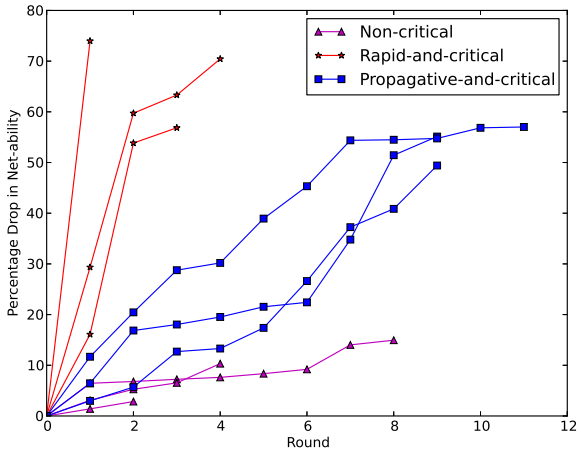


Figure 2.5. Three different types of initial failures.

- In the propagative-and-critical failures, the initial failure propagates to the whole power grid network within several rounds, and eventually causes severe damage. In other words, there is a certain amount of delay between the large-scale cascading failure and the initial failure.

The definition and classification consider two factors: the damage to the power grid and the number of rounds in each failure process. The amount of the damage can be measured by various metrics [11, 12, 27]. For illustration purpose, we adopt the metric *percentage of drop in net-ability* (PoDN), defined in [11]. The PoDN is defined as,

$$PoDN = \frac{E(\mathbf{G}) - E(\mathbf{G}^{'})}{E(\mathbf{G})} \tag{2.1}$$

where $E(\mathbf{G})$ and $E(\mathbf{G}^{'})$ represents the net-ability of a grid network before and after an initial failure, respectively. The more serious an initial failure is, the larger the PoDN this failure causes.

In particular, using the test benchmark, we illustrate these three types of initial failures. We set thresholds for PoDN and the corresponding number of rounds as follows. The severe damage means the finial PoDN is more or equal

than 15%. That is, if the final PoDN is below the threshold (i.e. $< 15\%$), this failure is marked as a non-critical failure. If the final PoDN is larger and equal than 15%, the failure is either rapid-and-critical or propagative-and-critical. If the PoDN increases more and equal than 20% in the first round or 30% within the first two rounds, with the total number of rounds less than 5, this failure is called as the rapid-and-critical failure, Otherwise, it is called the propagative-and-critical failure. All thresholds mentioned above should be adjusted according to different power grid networks. We use these numbers just for demonstration purpose. The simulation is performed when the system tolerance (described in Section 2.4.1) is 1.2. There are 367 nodes whose failure cause non-critical failures, 18 nodes causing rapid-and-critical failures, and 84 nodes causing propagative-and-critical failures.

For each type of initial failures, we show three typical cases in Fig. 2.5. The horizontal axis is the number of *rounds*, and the vertical axis is the PoDN. In addition, the magenta-triangle, blue-square and red-star curves present the non-critical, rapid-and-critical and propagative-and-critical failures, respectively. Generally speaking, the non-critical nodes are not critical to power grids, and approximately 80% of nodes in the Bay Area power grid network belong to this category. This is consistent with the observations made in [27]. The rapid-and-critical nodes are very important to power grids, the failure of which could seriously raise the power redistribution and cause lots of other nodes to be overloaded in a short time. The propagative-and-critical nodes are also very critical to power grids due to its severe damage. However, its severe damage is due to the accumulation of failures in each round. In Fig. 2.3, a case of the propagative-and-critical failure is shown. It is clearly seen that this initial failure continually triggers small-scale failures of other nodes in the test benchmark, and finally raises the overloading of many nodes and causes large-scale failure. From the perspective of PoDN, the

Table 2.1. Comparisons among different initial failures.

Failure Type	Non-critical	Rapid-and -critical	Propagative-and -critical
Trigger severe power redistribution	No	Yes	Yes
Critical to power grids	No	Yes	Yes
Number of such nodes in best benchmark	367	16	84

blue-square curves in Fig. 2.5 increase slowly within the beginning several rounds, suddenly jump up within the next several rounds (showing the rapid increase of the failed nodes), and finally reach the maximum PoDN.

From the perspective of protecting power grids, the classification presented in this section is important for the investigation on defense. For example, for the nodes that trigger rapid-and-critical failures, the protection should focus on preventing these nodes from initial failures. On the other hands, for the propagative-and-critical failures, the protection can be from several angles, including stopping the cascading process before the failures become large scale.

As a summary, in Table 2.1, we listed the main features of these three types of initial failures. Although the nodes causing rapid-and-critical and propagative-and-critical failures only take a small percentage of total nodes, around 22% in the test benchmark, these nodes are the pivot points that can affect the stability and security of man-made power transmission systems.

2.6 Conclusion

In this work, we developed a new platform to investigate the failure propagation in power grids. The proposed platform could successfully demonstrate the failure propagation, which was useful to help people understand such complicated cascading phenomena. We adopted the power grid around Bay Area, California,

as the test benchmark, and investigated single-node failures. Briefly speaking, we observed three different power grid network failures, and classified all nodes into three different groups. Such classification could help people effectively and efficiently protect power grids.

In the future, we plan to continue this work as follows. First, we will utilize the proposed platform to study large-scale power grids, e.g. the entire North America electrical infrastructure benchmark, where the key challenge is to improve the loading speed. Second, we will extend the extended model to visualize the consequence of link failures and study their features. Third, we will improve the accuracy of cascading modeling by adopting pure power-flow models. The key challenge is how to reasonably estimate more electrical features from the raw data. Finally, we will also study some real blackout cases with the proposed platform.

List of References

[1] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.

[2] Union for the co-ordination of transmission of electricity, "Final report system disturbance on 4 november 2006," Nov. 2006.

[3] The Guardian. "India blackouts leave 700 million without power." [Online]. Available: http://www.guardian.co.uk/

[4] D. H. Shin, J. Koo, L. Yang, X. Lin, S. Bagchi, and J. Zhang, "Low-complexity secure protocols to defend cyber-physical systems against network isolation attacks," in *Proceeding of IEEE Conference on Communications and Network Security*, National Harbor, MD, USA, Oct.14-16 2013.

[5] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, Sept. 2010.

[6] Y. Jiang, X. Guo, C. Li, H. Wen, C. Lei, and Z. Rui, "An efficient and secure search database scheme for cloud computing in smart grid," in *Proceeding of IEEE Conference on Communications and Network Security*, National Harbor, MD, USA, Oct.14-16 2013.

[7] H. Wen, X. Zhang, L. Cai, J. Tang, X. Zhu, Y. Jiang, and X. Guo, "A novel detection scheme for malicious nodes in smart meter system," in *Proceeding of IEEE Conference on Communications and Network Security*, National Harbor, MD, USA, Oct.14-16 2013.

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

[9] M. Vaiman et. al., "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[10] S. Mei, X. Zhang, and M. Cao, *Power Grid Complexity*. Beijing: Tsinghua University Press, Aug. 2011.

[11] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, pp. 1334–1340, July 2011.

[12] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in U.S. power grid," in *Proceeding of IEEE Global Telecommunications Conference*, Houston, Texas, USA, Dec.5-9 2011.

[13] J. Yan, Y. Zhu, Y. Sun, and H. He, "Revealing temporal features of attacks against smart grid," in *IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.

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

[15] A. Bernstein, D. Bienstockz, D. Hayx, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures - analysis and control implications," Columbia University, Electrical Engineering, Columbia University, Electrical Engineering, Tech. Rep., May 2011.

[16] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1676–1686, May 2013.

[17] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with dc power flow model and transient stability analysis," *IEEE Transactions on Power Systems*, 2014, submitted.

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

[19] "Platts." [Online]. Available: www.platts.com

[20] "Arcgis desktop 10.1," Environmental Systems Research Institute. [Online]. Available: http://www.esri.com/

[21] J. Tollefson, "US electrical grid on the edge of failure," *Nature News & Comment*, Aug.25 2013.

[22] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, no. 4, Apr. 2004.

[23] Y. Zhu, Y. Sun, and H. He, "Load distribution vector based attack strategies against power grid systems," in *Proceeding of IEEE Global Telecommunications Conference*, Anaheim, CA, USA, Dec.3-7 2012.

[24] J. Wang, L. Rong, L. Zhang, and Z. Zhang, "Attack vulnerability of scale-free networks due to cascading failures," *Physica A*, vol. 387, pp. 6671–6678, Nov. 2008.

[25] Q. Chen and J. D. McCalley, "Identifying high risk N-k contingencies for online security assessment," *IEEE Transactions on Power Systems*, vol. 20, pp. 823–834, May 2005.

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

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

[28] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 1, 2009.

[29] Y. Zhu, J. Yan, Y. Sun, and H. He, "Risk-aware vulnerability analysis of electric grids from attacker's perspective," in *Proceeding of IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.

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

[31] Visualizing The U.S. Electric Grid. [Online]. Available: http://www.npr.org

[32] P. C. Wong, K. Schneider, P. Mackey, H. Foote, G. Chin, R. Guttromson, and J. Thomas, "A novel visualization technique for electric power grid analytics," *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, no. 3, pp. 410–423, May 2009.

[33] P. Chopade, K. M. Flurchick, M. Bikdash, and I. Kateeb, "Modeling and visualization of smart power grid: Real time contingency and security aspects," in *Southeastcon, 2012 Proceedings of IEEE*, Mar. 2012, pp. 1–6.

[34] Y. Sun and T. J. Overbye, "Visualizations for power system contingency analysis data," *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1859–1866, Nov. 2004.

[35] Z. Wang, A. Scaglione, and R. J. Thomas, "TCIPG demo: Metrics of grid vulnerability to cascading failures," 2011. [Online]. Available: http://tcipg.org/news/research-demos

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

[37] "PYPOWER: a power flow and optimal power flow (opf) solver." [Online]. Available: http://www.pypower.org/

[38] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *Eur. Phys. J. B*, vol. 46, pp. 101–107, 2005.

[39] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Transactions on Parallel and Distributed Systems*, 2014, in press.

[40] "Esri shapefile technical description," Environmental Systems Research Institute. [Online]. Available: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf

[41] Electric Transmission Lines. [Online]. Available: http://psc.wi.gov/

[42] Some explanation from Platts: (1) substations can be identified as power plants, either connecting a 10 KV transmission lines or geographically near a power plant; (2) if the voltage of a transmission line is not sure, it is recorded as a negative number.

[43] P. Kundur, *Power System Stability and Control*. New York: McGraw-Hill, Jan. 1994.

CHAPTER 3

Manuscript 2: Load Distribution Vector Based Attack Strategies against Power Grid Systems

Yihai Zhu, Yan (Lindsay) Sun, and Haibo He

Department of Electrical, Computer, and Biomedical Engineering

University of Rhode Island, Kingston, RI 02881

Manuscript status: published in Proceeding of 2012 IEEE Global Communications Conference (GLOBECOM'12)

Corresponding Author: Yihai Zhu

Kelley Annex, Room A115

4 East Alumni Ave.,

Kingston, RI 02881

Phone:+1-401-874-5846

Email: yhzhu@ele.uri.edu

3.1 Abstract

Security issues in complex systems such as power grid, communication network, Internet, among others have attracted wide attention from academic, government and industry. In this paper, we investigate the vulnerabilities of power grid under a topology-based network model in the context of cascading failures caused by physical attacks against substations and transmission lines. In particular, we develop attack strategies from the attackers' points of view, aiming to cause severe damage to the network efficiency, as a way to revealing the vulnerability of the system. We propose a new and useful metric, load distribution vector (LDV), to describe the properties of nodes and links. Based on the LDV, we develop a multi-node attack strategy and a multi-link attack strategy, which are proved to be stronger attacks than the traditional load-based attacks using the Western North American power grid data. For example, the removal of only three critical nodes in the grid can reduce more than 30% of the original network efficiency, and the removal of only three critical links can reduce the network efficiency by 23%. In the above cases, the traditional load-based schemes reduce the network efficiency by 23.57% and 18.35%, respectively.

3.2 Introduction

With the continuous growing energy demand, accidents and natural disasters, power outage has become more and more frequent within recent years. The four largest power blackouts in the history occurred only within the recent 10 years [1]. This seriously affects economy and raises concerns from the homeland security points of view.

The problem of large scale power system failure has attracted wide research attention. In current literature, there are two prevalent types of analysis to power system failures: power flow based analysis [2–8] and topology based analysis [9–

15]. Power flow based analysis is rooted on the circuit theory with Kirchhoff's law to understand the power flows in the grid under system failures. Because such approaches are built on the foundation of the physical laws governing the electricity generation, transmission, distribution, and utilization, they can provide the most critical insights and fundamental understanding of the grid behavior under attacks or failures. IEEE Power and Energy Society (PES) has dedicated task forces to understand the grid reliability, predict its failure propagation, and restore electricity from cascading failures [2–5]. In addition to the power flow based analysis, recent topology based analysis motived from complex systems research has also been investigated to understand the power grid vulnerability and cascading failure. In these approaches, simplified topology based models are considered, such as the recoverable models and non-recoverable models to study the complex grid behavior under physical or cyber attacks, or a failure due to natural disasters such as hurricanes or snow storms. These approaches offer new possibilities for understanding and monitoring power grid behavior by, for example, using existing complex network analysis approaches. Our work presented in this paper is aligned with this direction and adopts topology based analysis. We would also like to note that most recently, a kind of hybrid approach with the integration of power flow based analysis and topology based analysis, named extended topological approach, has been proposed to study the power grid vulnerability [6–8]. This approach incorporates several key features of power grid such as flow path, transmission line limitation, and bus distribution together with topological models to assess the grid vulnerability under attacks.

In the complex network literature, the large scale power outage can be referred to as **cascading failure**, meaning when one of the components (substations and transmission lines) in power grids completely or partially fails, shifts its load to

nearby components and triggers the failure of successive components in the system. Many works in this field can contribute to analyzing errors, failures, attacks, and resilience of power grid systems. For instance, cascade-based attack on power grid network was presented in [9–11]. In [9], two types of attack methods, *random removals* and *intentional removals*, were compared and the latter was proved to be much stronger than the former. This comparison is done in the context of the *single node attack*, defined as only one node taken down by the attacker. In [10], *multiple-node attack*, defined as multiple nodes taken down by the attacker simultaneously, was presented. It was shown that the multiple-node attack can cause more severe damage to the power grid than the *single node* attack. The work in [12] adopted a model that calculates the load of a substation from local topology of the substation, when studying the multiple node attacks. The results in the paper indicate that attacking the nodes with small load can cause severe cascading failures under certain circumstances.

Many existing work on cascading failure assumes attacks occur on nodes. On the other hand, five out of six the largest power outage accidents (except 1999 Southern Brazil blackout) [1] were initially triggered by the damage to one or more transmission lines, and finally spread to whole power grid system. Some researchers studied the system behavior on basis of link removal [14, 15]. For example, in [14], range-based attacks on link was investigated, showing that scale-free networks were more sensitive to attacks on short-range than long-range links. In [15], efficient link attack strategies and lower cost protections on links were both investigated based on load model similar to [12].

In this paper, we develop a novel attack strategy. The motivation of our work comes from the observation that the existing multi-node attack strategies in [11, 16] are not the strongest attacks. Our goal is to investigate the vulnerabilities of power

grid network under different attack strategies, *node attack strategy (NAS)* and *link attack strategy (LAS)*. We found that although *load* plays very important role in attack strategies, it still does not represent the strongest strategy from both attack and defense points of view. Instead, we discover a new metric, called *load distribution vector (LDV)*, which gives us a new way to identify the importance of components in power grid network in the context of cascading failure. Utilizing this load distribution vector, we develop a new and much stronger attack strategy which can be used in both node and link attacks. The new attack strategy is tested and compared with existing load-based attack strategy using the Western North American power grid network data. The simulation results demonstrate that the proposed attack strategy is much stronger than the existing schemes.

The rest of this paper is organized as follows. Section 3.3 introduces the network model and assessment metrics. Section 3.4 describes the proposed work in details including load distribution vector, the proposed multi-node and multi-link attack strategies. Simulation results will be shown in Section 3.5. Finally, discussion and conclusion are made in Section 3.6.

3.3 System Model

3.3.1 Network Model

In practice, an power grid is an interconnected network for delivering electricity from generators to customers. It consists of substations (generators, transmission substations and distribution substations) and transmission lines. The topology of the power grid is often represented as an undirected and weighted graph, $\mathbf{G}$, with substations being as nodes and transmission lines being as links (or edges). In the topology-based system models, there are several very important concepts.

The first concept is *load*. Adopting the definition of betweenness on complex network [17], we define the load for nodes and links as betweenness. Specifically, the

load of node n_i, at time t, denoted by $L_{n_i}(t)$, is the number of most efficient paths (also known as the shortest paths) from generators to distribution substations that pass through n_i at time t. To obtain $L_{n_i}(t)$, one needs to find the most efficient paths between each pair of generators and distribution substations, and then count how many of such paths pass n_i. Here, the process of finding the most efficient paths is closely related to the definition of *link efficiency* and *path efficiency*, which will be introduced in Section 3.3.2. Similarly, the load of link l_k, denoted by $L_{l_k}(t)$, is the number of the shortest paths passing through l_k at time t. The definitions are just slight extension from the concept proposed in [18].

The second concept is *capacity*, defined as the maximum load that a node (or link) can carry. Let C_{n_i} (or C_{l_k}) denote the capacity of n_i (or l_k), and $L_{n_i}(0)$ (or $L_{l_k}(0)$) denote the initial load of n_i (or l_k) before any attacks occur. It is usually assumed that C_{n_i} (or C_{l_k}) is proportional to the initial load of node n_i (or link l_k) [11], as

$$\begin{aligned} C_{n_i} &= \alpha * L_{n_i}(0) \\ C_{l_k} &= \alpha * L_{l_k}(0) \end{aligned} \tag{3.1}$$

where $\alpha(> 1)$ is called the *system tolerance parameter*. Higher α means better capability to resist perturbation in the system.

3.3.2 Assessment Metrics

How does the network respond to node or link failures? To model the cascading failures in power grid, a topology-based *recoverable model* was first employed in [10], and then slightly modified and extended in [11]. Next, we briefly introduce the key concepts of this model.

Load Redistribution: If a node (or link) is taken down (i.e. removed from the network), some shortest paths between generators and distribution substations become unavailable. For these generator-to-distribution-substation pairs, they need

to find the new shortest paths, which will change the load of remaining nodes and links, according to the definitions of load in Section 3.3.1. This process is called the load redistribution.

Overloading occurs when the load exceeds the capacity of a node (or link). That is, node n_i is overloaded when $L_{n_i}(t) > C_{n_i}$, and link l_k is overloaded when $L_{l_k}(t) > C_{l_k}$. In the context of investigating cascading failures, overloading is caused by load redistribution.

Link Efficiency represents how well a link can carry the power flow. Let $e_{l_k}(t)$ denote the efficiency of link l_k at time t. Initially, for each existing link, $e_{l_k}(0) = 1$, meaning that this link works properly. When a node is overloaded (say node n_i), the efficiency of all links that connect to node n_i is reduced as [11],

$$e_{l_k}(t+1) = \begin{cases} e_{l_k}(0)\frac{C_{n_i}}{L_{n_i}(t)} & if \;\; L_{n_i}(t) > C_{n_i} \\ e_{l_k}(0) & otherwise \end{cases} \tag{3.2}$$

When a link is overloaded (say link l_k), the efficiency of this link is reduced, as

$$e_{l_k}(t+1) = \begin{cases} e_{l_k}(0)\frac{C_{l_k}}{L_{l_k}(t)} & if \;\; L_{l_k}(t) > C_{l_k} \\ e_{l_k}(0) & otherwise \end{cases} \tag{3.3}$$

When the link efficiency is smaller than 1, it means that the link partially losses its functionality and becomes less efficient. The amount of reduction in the link efficiency is proportional to the overload extent: $C_{n_i}/L_{n_i}(t)$ for node overloading and $C_{l_k}/L_{l_k}(t)$ for link overloading.

Path Efficiency is defined as harmonic composition of link efficiency [11]. From node n_i to n_j, there exists many paths. The path that has the highest path efficiency value is called as the *most efficient path* or the *shortest path* in this paper. We use $\epsilon_{ij}(t)$ to denote the efficiency of the shortest path at time t. It is defined as $\epsilon_{ij} = 1/(\sum_{p=1}^{P} 1/x_p(t))$, where P is the number of links on the path and $x_p(t)$ is the efficiency value of each link on the path.

Network Efficiency: Assume there are N_g generators and N_d distribution substations. Let set G contains all generators and set D contains all distribution

substations. The network efficiency at time t, denoted by $E(t)$, is defined as

$$E(t) = \frac{1}{N_g N_d} \sum_{n_i \in G} \sum_{n_j \in D} \epsilon_{ij}(t) \tag{3.4}$$

3.4 Load Distribution Vector Based Attack Strategies

To understand the vulnerabilities of power grid systems, one effective method is to study this problem from the attacker point of view. That is, to find the strong attack strategies that cause large damage to the grid. In the context of investigating cascading failure using topology-based model, the attacker's goal is to identify a set of *victim nodes or links*, whose failure will cause large reduction of the network efficiency. The methods of selecting victim nodes are referred to as *Node Attack Strategies* (NAS), and the method of selecting victim links are referred to as *Link Attack Strategies* (LAS).

3.4.1 Load-based Attack Strategies and Their Limitations

In the existing literature [10, 11], the prevalent attack strategies choose victim nodes/links according to their *load*, which can have different definitions in different network models. In the topology-based model discussed in Section 3.3.1, load is defined as betweennees. When the attacker aims to knock down M nodes or links, the load-based attack strategies are as follows.

* NAS^M_{load} : Selecting the top M largest load nodes as the victim nodes.

* LAS^M_{load} : Selecting the top M largest load links as the victim links.

Although load-based attack strategies are widely used, they often are not the strongest attacks. This has been shown in [13], which adopted a non-recoverable network model using degrees to compute the load. In this subsection, we discuss and demonstrate the **intrinsic limitation of betweenness (ILB)** (or load) as the victim node or link selection criteria.

If node A has large load (i.e. betweeness), it is highly likely that the nodes around A also have large load, since the shortest paths passing A often pass its neighbors too. According to NAS^{M}_{load}, the victim nodes tend to be "close" to each other, residing in a small area in the network. In this case, attacking A and its neighbors may not be much more damaging than attacking A alone.

To see this, let us examine a special example shown in Fig. 3.1. This power grid contains a set of 10 generators (denoted by S_G) and a set of 10 distribution substations (denoted by S_D). We find 100 shortest paths, and one path between each pair of generator and distribution substation. Assume that S_G and S_D are completely separated by a set of transmission substations, denoted by S_T. We also assume that 90 shortest paths pass through the A-G link and 10 shortest paths are through the B-N link. Thus, the loads of node A, G, B, N are 90, 90, 10, and 10 respectively.

Now, if we launch the traditional load-based node attack strategy, NAS^{2}_{load}, what will happen? The attacker should knock down node A and G, which will cause severe load redistribution, make node B and N carry much higher load, reduce link efficiency, and reduce network efficiency. However, is this the strongest attack? Obviously not. A smart attacker should choose the first victim node as either A or G, and the second victim node as either B or N. This new attack will make the network efficiency reduce to 0. This simple example illustrates the limitation of the betweenness (or load) as the sole metric in the selection of victim nodes.

3.4.2 Primary Idea

The *optimal multi-node attack strategy*, denoted by NAS^{M}_{opt}, surely exists and can be found through an exhaustive search. For instance, for NAS^{3}_{opt}, the attacker can run simulation for each three nodes combination as the victim nodes.

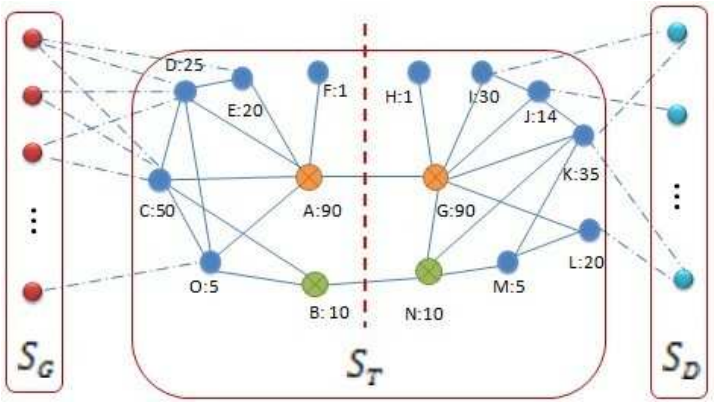


Figure 3.1. Demonstrating the limitation of the load-based attack strategies

This approach, however, has two major problems. First, the simulation has to be performed for a given system tolerance T value. The search results may not be generalized to different T values. Second, the computation complexity is prohibitively high because (a) the network size (N) is a very large number in practice, (b) the cost of finding all betweenness values in one round of iteration increases dramatically with N, and (c) the number of M nodes combinations increases sharply with N.

We propose a practical multi-node attack strategy. Here, *load* is still an important metric. Besides load, as discussed in Section 3.4.1, we would like to capture features such as (1) attacking both A and G in Fig. 3.1 has the similar effect as attacking node A alone, and (2) attacking A and attacking B leading to very different consequences. Our primary idea is to

* Select the nodes with reasonably large load as candidate nodes.

* Divide the candidate nodes into different groups. The nodes in the same group should cause load-redistribution in a similar area in the network if they are taken out of the network. The nodes in different groups should

impact different areas in the network if they are taken out.

* Pick one node from each group, and compose the victim nodes selection.

This idea also works for LAS, as long as you replace "node" with "link" in the above description. Obviously, the most challenging part is to determine how to divide nodes into groups, which is addressed by our newly proposed load distribution vector metric.

3.4.3 Load Distribution Vector

Before any attack, all nodes (or links) have their own load as betweenness. We define the *original node load distribution vector* as $ONLDV = [L_{n_1}(0), L_{n_2}(0), ..., L_{n_N}(0)]'$, and the *original link load distribution vector* as $OLLDV = [L_{l_1}(0), L_{l_2}(0), ..., L_{l_K}(0)]'$, where $'$ is vector transpose. If we remove a node or link, the load distribution vector changes. We define the $\hat{L}^j_{n_i}$ as the load of node n_i after node n_j is removed, and the $\hat{L}^k_{l_s}$ as the load of link l_s after link l_k is removed. Then, the *node load distribution vector* (NLDV) of node n_j is defined as

$$NLDV_j = [\hat{L}^j_{n_1}, \hat{L}^j_{n_2}, ..., \hat{L}^j_{n_i}, ..., \hat{L}^j_{n_N}]'. \tag{3.5}$$

Similarly, the *link load distribution vector* (LLDV) of link l_k is defined as

$$LLDV_j = [\hat{L}^k_{l_1}, \hat{L}^k_{l_2}, ..., \hat{L}^k_{l_s}, ..., \hat{L}^k_{l_K}]'. \tag{3.6}$$

Furthermore, for $i = j$, we set $\hat{L}^i_{n_i} = L_{n_i}(0)$, the original load of node n_i. For $s = k$, we set $\hat{L}^k_{l_k} = L_{l_k}(0)$, the original load of link l_k.

As a summary, a node's NLDV is just the new load distribution of all remaining nodes after this node is removed, and a link's LLDV is just the new load distribution of all remaining links after this link is removed.

Given the definition of load distribution vectors, we compute the **distance** between n_i and n_j, (denoted by $d_{n_i n_j}$) and the distance between l_s and l_k (denoted

by $d_{l_s l_k}$) as

$$\begin{aligned} d_{n_i n_j} &= \mathbf{Dist}(NLDV_i, NLDV_j) \\ d_{l_k l_s} &= \mathbf{Dist}(LLDV_k, LLDV_s) \end{aligned} \tag{3.7}$$

The function **Dist**(.) can be any distance definition, such as Euclidean distance, Mahalanobis distance et al [19]. In the paper, we adopt the Euclidean distance.

From the definitions of load distribution vector and distance metric, we expect that two nodes (links) with smaller distance cause similar impact to the network if they are taken out, and vice versa.

3.4.4 Load Distribution Vector Based Multi-node Attack Strategy

Following the primary idea in Section 3.4.2, we propose a load distribution vector based multi-node attack strategy, denoted by NAS^M_{LDV}, which contains the following steps.

- Step 1: Choose the top R ($R > M \geq 2$) largest load nodes and put them into a *candidate set*, denoted by S_c. The nodes in S_c are called the candidate nodes.

- Step 2: For each node $n_i \in S_c$, compute its load distribution vector $NLDV_i$. For each pair of nodes $n_i, n_j \in S_c$ and $i \neq j$, compute the distance $d_{n_i n_j}$.

- Step 3: Use the well-known hierarchical clustering algorithm, Ward's algorithm in [20], to get the hierarchical tree of candidate nodes and divide them into M unique groups.

- Step 4: Select one candidate node in S_c such that its average distance to all other candidate nodes is the largest. Put the selected node (say n_x) into the *victim set*, denoted by S_v. In order to make sure that only one node in each group (see step 3) can be added to the victim set, we remove the candidate nodes belonging to the same group as n_x from the candidate set S_c.

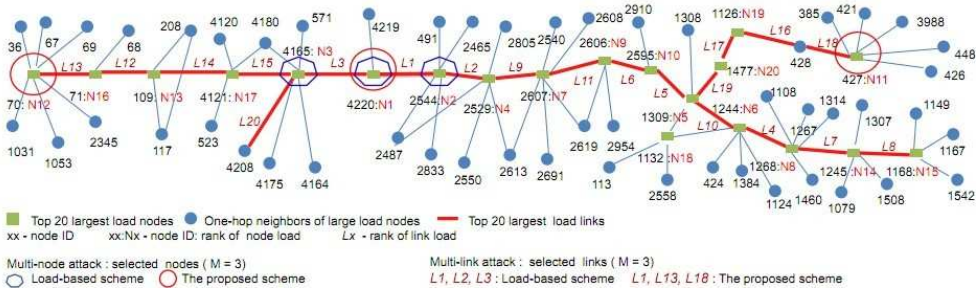


Figure 3.2. Demonstration of node attack strategies and link attack strategies under topology snapshot 1

- Step 5: For each remaining node in S_c, calculate its average distance to all nodes in S_v. This average distance is called the *to-Sv-distance*. Select the node in S_c that has the largest *to-Sv-distance* value, and put this node into S_v. If some nodes are in S_c and belong to the same group as the selected node, these nodes are deleted from S_c.

- Step 6: Repeat Step 5 until the candidate pool is empty. (There will be $M-1$ iterations.)

- Step 7: Finally, there are M nodes in S_v, which are the selected victim nodes.

In Fig. 3.2, we plot the local topology of top 20 largest load nodes under topology snapshot 1 of Western North American power grid network. The details of the data set can be found in Section 3.5. The selected victim nodes chosen by NAS^3_{load} are marked with blue octagons, and victim nodes selected by NAS^3_{LDV} are marked with red circles. It is clearly seen that the proposed scheme, NAS^3_{LDV}, is better in terms of finding victim nodes from different regions of the power grid network. It is also a stronger attack, which will be demonstrated in Section 3.5.

3.4.5 Load Distribution Vector Based Multi-link Attack Strategy

Most works in the current literature aim to model cascading failure of power grid based on the removal of nodes (substations). On the other hand, transmission lines can be more vulnerable [1]. We propose a link attack strategy (LAS), denoted by LAS^M_{LDV}, based on the concept of load distribution vector. The procedure to selecting victim links of LAS^M_{LDV} is very similar to the 7-step-procedure of NAS^M_{LDV} presented in Section 3.4.4. The only modifications are replacing (1) "node" with "link", (b) n_i with l_k, (c) n_j with l_s, (d) $NLDV_i$ with $LLDV_k$, (e) $d_{n_i n_j}$ with $d_{l_k l_s}$, and (f) n_x with l_x. In Fig. 3.2, we also demonstrate the selected victim links of the proposed scheme (LAS^3_{LDV}) and these of the load-based scheme (LAS^3_{load}). The bold red lines represent candidate links. We clearly see that the victim links of LAS^3_{LDV} (marked as $L1$, $L13$, and $L18$) are further apart than the victim links of LAS^3_{load} (marked as $L1$, $L2$, and $L3$).

In summary, we propose the novel concept of load distribution vectors and develop new attack strategies that have the following features. First, they cause more damage than the traditional load based attacks. The comparison results will be shown in Section 3.5. Second, the proposed attacks do not require extensive search or pre-determined system tolerance value (T).

3.5 Simulation Results

We use Matlab to simulate all attack strategies under recoverable model discussed in Section 3.3 and adopt the Western North American power grid network data [21], consisting of 4941 substations and 6594 transmission lines, as the benchmark. Since the Western North American power grid data does not specify the types of substations, we use the method in [22] to determine the generators and distribution substations. Particularly, there are 1226 nodes that have only one transmission line connected. Among those 1226 nodes, which are highly likely to

be distribution substations, we randomly select 800 nodes as the distribution substations. From the remaining nodes, we randomly select 600 nodes as generators. By doing so, we can create multiple snapshots of the power grid topology. In this paper, we will use two different snapshots to do the simulations.

The simulation results for node attack strategies (NAS) and link attack stragies (LAS) will be shown in Section 3.5.1 and 3.5.2 respectively, followed by a comparison between them in Section 3.5.3.

3.5.1 Simulation Results for Multi-node Attack Strategies

In this subsection, we first demonstrate how the network efficiency ($E(t)$) changes after the proposed NAS is launched. In Fig. 3.3, the x-axis is the index of iteration round, and the y-axis is network efficiency. In the simulation, we set the system tolerance (α in Equ. 3.1) to be 1.2 and the number of victim nodes (M) changes from 1 to 6.

When the iteration index is 0, the network is not under attack. When one or multiple nodes (also called as the victim nodes) are taken down, the network efficiency first drops sharply due to the overloading problem, then recovers a little because the network tries to find the new shortest paths to increase its efficiency, and finally starts to fluctuate. The reason for the occurrence of fluctuation is due to the reversibility of effects of overload, which was clearly explained in [11].

We observe that the network efficiency converges very quickly (usually after 4 iterations) and has some fluctuations after its convergence. In the simulation, we usually perform 12 rounds of iteration and compute the *stabilized average network efficiency (SANE)*, denoted by $E(G_f)$, as the average of $E(t)$ from round 5 to 12. Furthermore, we define η to measure the damage of the attack as $\eta = \frac{E(0)-E(G_f)}{E(0)}$.

Next, we compare the proposed load distribution vector based scheme with the traditional load based scheme. In Figure 3.4, the x-axis is the number of victim

nodes, and the y-axis is the $E(G_f)$ value. The curves marked with square represent the proposed scheme, NAS^M_{LDV}, and the curves marked with star represent the load-based scheme, NAS^M_{load}.

It is clearly shown that the proposed attack strategy is much more powerful than the load-based attacks. For instance, when $M = 3$ under the topology snapshot 1, NAS^3_{LDV} reduces the network efficiency from 0.0594 to 0.0415 leading to $\eta = 30.13\%$, whereas NAS^3_{load} reduces the network efficiency from 0.0594 to 0.0454 leading to $\eta = 23.57\%$. We see that NAS^3_{LDV} chooses node 4220, 427 and 70 as victim nodes, and NAS^3_{load} chooses node 4220, 2544 and 4165 as victim nodes. Obviously, the proposed attack chooses the victims that are further away and conquers the limitation of the betweenness discussed in Section 3.4.1.

We performed simulation for different topology snapshots, and observed similar results. Fig. 3.5 shows the results of another topology snapshot, which is similar to Fig. 3.4. The similarity indicates that the advantage of the proposed multi-node attack (from the attacker points of view) exists in different power grid network topologies. We also performed simulations for different choices of R value, which is the number of nodes selected in Step 1 of the proposed attack. We observed that the attack performance for $M \leq 6$ is not sensitive to R as long as $R > 30$.

3.5.2 Simulation Results for Multi-link Attack Strategies

In this subsection, we compare the proposed link attack strategy, LAS^M_{LDV}, with the traditional load strategy, LAS^M_{load}. Fig. 3.6 shows the stabilized average network efficiency ($E(G_f)$) under different numbers of victim links.

It is clearly shown that the proposed scheme is much more powerful than the load-based attack scheme. For instance, when $M = 3$ under the topology snapshot 1, LAS^3_{LDV} reduces the network efficiency from 0.0594 to 0.0458, leading

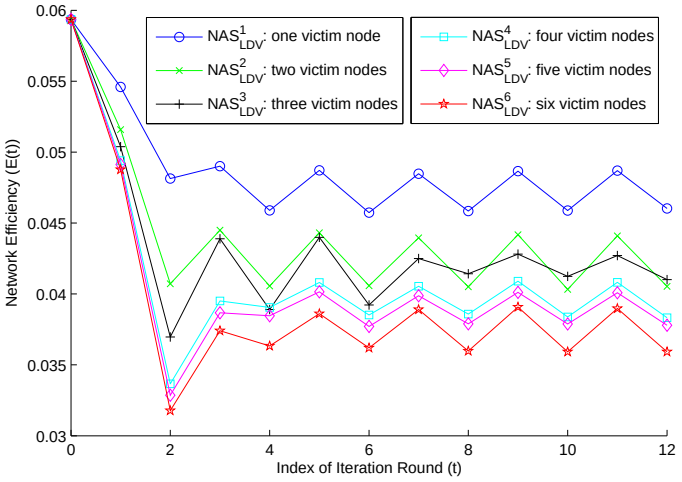


Figure 3.3. Network efficiency of the proposed node attack strategy

to $\eta = 22.9\%$, whereas LAS^3_{load} reduces the network efficiency from 0.0594 to 0.0485, leading to $\eta = 18.35\%$. Furthermore, LAS^3_{LDV} chooses link $L1$, $L13$ and $L18$ as victim links, and LAS^3_{load} chooses link $L1$, $L2$, and $L3$ as victim nodes. From Fig. 3.2, we see that the proposed scheme chooses the victim links that have not only relatively high load and but are further away from each other. The load-based scheme, however, chooses the victim links that are connected together.

We also conduct the simulation on topology snapshot 2 and observe the similar results. Due space limitation, we will not show that figure in the paper.

3.5.3 Multi-node Attack Strategies vs Multi-link Attack Strategies

In Fig. 3.7, we show an interesting comparison between node attacks and link attacks, given different numbers of victim nodes/links. We make the following observations.

- Given the same number of victim nodes/links, the node-based attacks (NAS) are obviously stronger than link-based attacks (LAS). *NAS* not only cuts off nodes themselves, but also links adherent to those nodes, whereas *LAS* only cuts off victim links from the network which causes less damage. For exam-

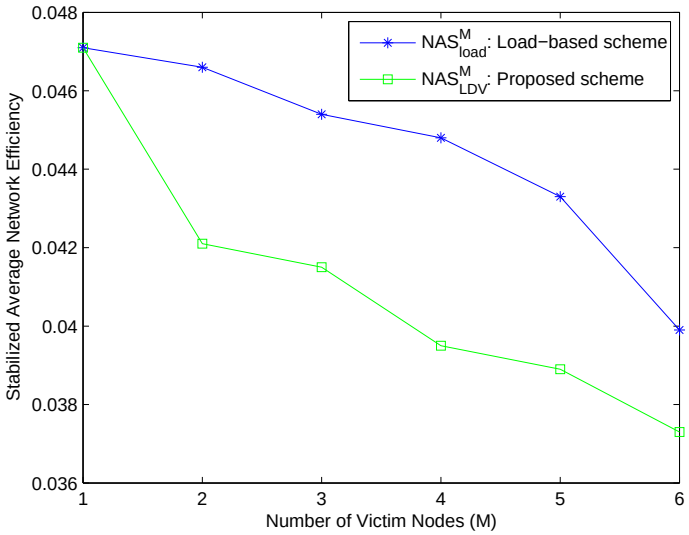


Figure 3.4. Comparison between the proposed node attack strategy and the comparison scheme on topology snapshot 1

ple, NAS^2_{LDV}, removing two critical nodes, can reduce the average network efficiency by 29.12%, whereas the η of LAS^6_{LDV}, which cuts off six critical links, is only 26.26%.

- Although weaker than NAS, the proposed LAS can cause severe damage to power grid. For example, LAS^1_{LDV}, only removing one critical link, can sharply reduce the network efficiency from 0.0594 to 0.0493, leading to $\eta =$ 17%. This is only a little bit weaker than NAS^1_{LDV} with $\eta = 20.54\%$.

- In practice, the attacker may choose to attack links because knocking down links are usually considered easier than knocking down nodes. For example, when the *cost of attacking a transmission line* is less than a third of the *cost of attacking a substation*, the attacker should launch LAS^3_{LDV}, instead of NAS^1_{LDV}. The former requires less resource, but causes severer damage.

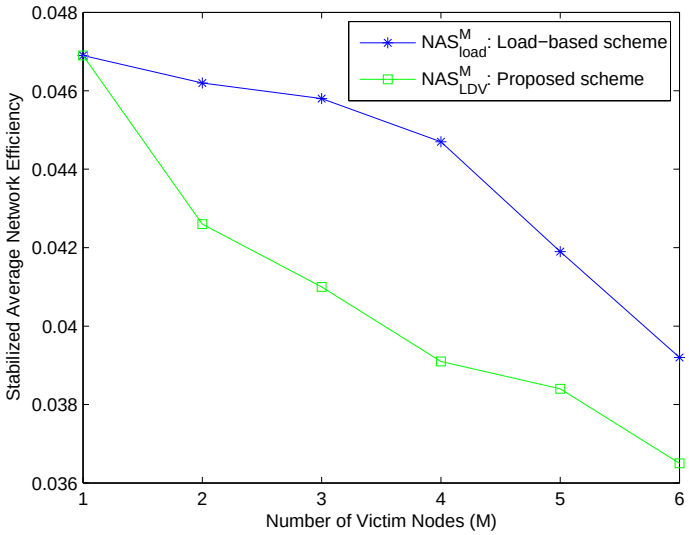


Figure 3.5. Comparison between the proposed node attack strategy and the comparison scheme on topology snapshot 2

3.6 Conclusions and Discussions

In this paper, we studied the vulnerabilities of US power grid under a betweeness based network model. After analyzing the intrinsic limitation of betweenness, we found that the traditional load-based attacks cannot represent the strongest attacks in the grid. Then, we propose a new metric, called *load distribution vector (LDV)*, to measure the functionality of nodes in the network, and extend this idea to links. Simulation results show that our proposed attack strategies generate much stronger attacks.

There are several important future research directions along this topic. First, the current work often investigates node failures and link failures separately. In practice, attackers can surely attack several nodes and several links simultaneously. It is highly desirable to study the vulnerability of power grids by joining node and link attacks together. Second, as we discussed in Section I, power grid is a unique complex system not only with complicated topological structure, more importantly it has the fundamental circuit theory (i.e., Kirchhoff's law) governing the electricity

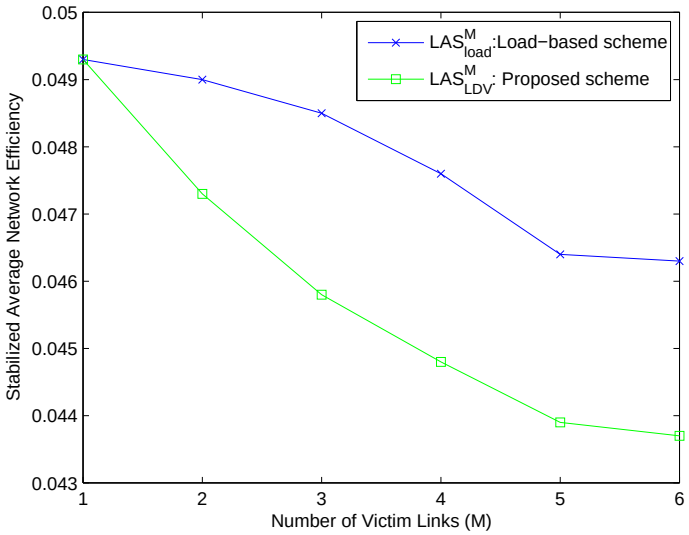


Figure 3.6. Comparison between the proposed link attack strategy and the comparison scheme on topology snapshot 1

generation, transmission and distribution in the grid. Therefore, it will be critical to go beyond the pure topological vulnerability analysis with the consideration of the physical laws governing the power systems. One natural extension is to integrate our approach with the extended topological model as discussed in [6–8] to see how our proposed method will perform with the consideration of several key features in power flow analysis. Finally, the data set we investigated in this work is based on the Western North American Power Grid data. It would be interesting to analyze and validate the observations from our research presented in this paper to other data sets, such as the IEEE-118-bus and IEEE-300-bus benchmarks, as well as the entire North America Electrical Infrastructure data that we recently obtained. We are currently investigating all these issues and the corresponding results will be reported in future work.

List of References

[1] "List of power outages." [Online]. Available: http://en.wikipedia.org/wiki/List_of_power_outages#Largest

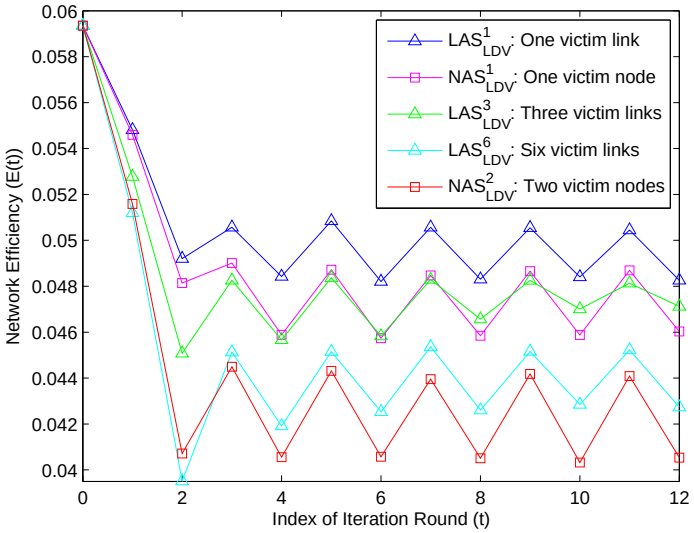


Figure 3.7. Comparisons between the proposed node attack strategies with the proposed link attack strategies

[2] R. Baldick et. al., "Initial review of methods for cascading failure analysis in electric power transmission systems," in *IEEE power engineering society general meeting*, Pittsburgh, PA, USA, July20-24 2008.

[3] C. Grigg et. al., "The IEEE reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.

[4] R. Baldick et. al., "Vulnerability assessment for cascading failures in electric power systems," in *IEEE Power Engineering Society Power System Conference and Exposition*, Seattle, WA, USA, Mar.15-18 2009.

[5] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.

[6] E. Bompard, R. Napoli, and F. Xue, "Analysis of structural vulnerabilities in power transmission grids," *International Journal of Critical Infrastructure Protections*, vol. 2, no. 12, pp. 5–12, May 2009.

[7] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, pp. 1334–1340, July 2011.

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

[9] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, 065102(R), 2002.

[10] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, no. 4, Apr. 2004.

[11] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *Eur. Phys. J. B*, vol. 46, pp. 101–107, 2005.

[12] 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, Dec. 2009.

[13] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in U.S. power grid," in *Proceeding of IEEE Global Telecommunications Conference*, Houston, Texas, USA, Dec.5-9 2011.

[14] Y. C. Lai, A. E. Motter, and T. Nishikawa, "Attacks and cascades in complex networks," *Lecture Notes in Physics*, vol. 650, pp. 299–310, 2004.

[15] J.-W. Wang and L.-L. Rong, "Robustness of the western united states power grid under edge attack strategies due to cascading failures," *Safety Science*, vol. 49, no. 6, pp. 807–812, July 2011.

[16] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A*, vol. 340, pp. 388–394, 2004.

[17] M. E. J. Newman, "Scientific collaboration networks. II. shortest paths, weighted networks, and centrality," *Phys. Rev. E.*, vol. 64, no. 1, June 2004.

[18] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, pp. 35–41, 1977.

[19] E. Deza and M. Deza, *Dictionary of Distances*. Elsevier, 2006.

[20] G. J. Szekely and M. L. Rizzo, "Hierarchical clustering via joint between-within distances: Extending ward's minimum variance method," *Journal of Classification*, vol. 22, no. 2, pp. 151–183, Sept. 2005.

[21] D. Watts and S. Strogatz, "An undirected, unweighted network representing the topology of the western states power grid of the united states," *Nature*, vol. 393, pp. 440–442, 1998.

[22] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the north american power grid," *Phys. Rev. E*, vol. 69, no. 2, Feb. 2004.

CHAPTER 4

Manuscript 3: Revealing Cascading Failure Vulnerability in Power Grids using Risk-Graph

Yihai Zhu, Jun Yan, Yan (Lindsay) Sun, and Haibo He

Department of Electrical, Computer, and Biomedical Engineering

University of Rhode Island, Kingston, RI 02881

Manuscript status: published in IEEE Transactions on Parallel and Distributed Systems, 2014

Corresponding Author: Yihai Zhu

Kelley Annex, Room A115

4 East Alumni Ave.,

Kingston, RI 02881

Phone:+1-401-874-5846

Email: yhzhu@ele.uri.edu

4.1 Abstract

Security issues related to power grid networks have attracted the attention of researchers in many fields. Recently, a new network model that combines complex network theories with power flow models was proposed. This model, referred to as the extended model, is suitable for investigating vulnerabilities in power grid networks. In this work, we study cascading failures of power grids under the extended model. Particularly, we discover that attack strategies that select target nodes (TNs) based on load and degree do not yield the strongest attacks. Instead, we propose a novel metric, called the *risk graph*, and develop novel attack strategies that are much stronger than the load-based and degree-based attack strategies. The proposed approaches and the comparison approaches are tested on IEEE 57 and 118 bus systems and Polish transmission system. The results demonstrate that the proposed approaches can reveal the power grid vulnerability in terms of causing cascading failures more effectively than the comparison approaches.

4.2 Introduction

Power grid is considered as one of the most significant infrastructures on the Earth. Within recent decades, several large-scale power outages around the world seriously affected the livelihood of many people and caused great damage [1]. For example, the well-known Northeast blackout in 2003 affected 55 million people and caused an estimated economic loss between $7 billions and $10 billions [2].

Large-scale power outage is often caused by *cascading failure*. A cascading failure refers to a sequence of dependent events, where the initial failure of one or more components (i.e. substations and transmission lines) triggers the sequential failure of other components [3, 4]. Triggers of the initial failures can be natural damage (e.g. the fall of trees), aging equipment, human errors, software and hardware faults, and so on. Within recent years, power grids are facing new threats,

e.g. cyber-physical attacks [5, 6]. Therefore, malicious attacks become new and potential triggers of cascading failures.

Many existing works have been proposed to investigate the vulnerability of power grids from the attack perspective. Important challenges, however, still remain. First, developing reasonable models that can mimic cascading failures in reality is still a critical challenge. In current literatures, there are three popular models, pure topological models [7–9], pure power flow models [4, 10] and hybrid models [11–13]. Each category has its own advantages and disadvantages. Second, finding stronger malicious attack strategies is one of the key ways to investigate cascading failures. Although the exhaustive search approach can yield the best attack from the attack performance point of view, it is sometimes computationally infeasible in practice [9]. Thus, practical and efficient attack strategies need to be found. Finally, attackers might have different knowledge of power grids, such as topological structures, electric features and real-time information. Under different levels of knowledge, attackers may adopt different attack strategies.

In this work, we do not tackle the first challenge. Instead, we choose a hybrid model, called the *extended model*. Although hybrid models [11, 13] have been adopted to study the vulnerability of power grids, few existing studies have discussed how cascading failures occur under hybrid models. A reasonable *cascading failure simulator* (CFS) under the extended model will be introduced.

To address the second challenge, we study the *node attack strategy* (NAS) under the extended model to address how to find stronger attacks. In this work, an *attack* means an attacker knocks down one or more nodes (i.e. substations). These removed nodes are referred to as *target nodes* (TNs). From the attacker's point of view, attackers need to carefully choose a few TNs, aiming to maximize the damage. the node attack strategy describes how the attacker chooses TNs.

In addition, a stronger attack means that the initial removal of the TNs could yield larger *percentage of drop in net-ability* (PoDN), which will be discussed in Section 5.4.4. If the attacker knows everything about a power grid and can model how cascading failures occur, the *exhaustive search node attack strategy* can yield the most serious damage. The exhaustive search, however, is often not practical due to its huge search space on a large-scale, even moderate-scale, power grid networks. Instead, we propose a *reduced search space node attack strategy* or *RSS node attack strategy* in short. The RSS node attack strategy can sharply reduce the search space and achieve comparable attack performance to that of the exhaustive search node attack strategy.

We also investigate the third challenge. To adopt the proposed RSS node attack strategy, an attacker needs to know the topology of power grid networks, as well as the *system tolerance factor* that is defined as the capacity divided by the initial load of a node. In practice, such tolerance factors may not be known to attackers. Therefore, as the third task of this work, we investigate attack strategies under the assumption that an attacker does not know the tolerance factors. We propose a novel metric, called the *risk graph* (RG), to show the criticality of important nodes in a grid network and the hidden relationship among them. Using the risk graph, we develop the *riskgraph-based node attack strategy*. The riskgraph-based node attack strategy is conducted on IEEE 118 bus system and Polish transmission system, and compared with the load-based, the degree-based and the proposed RSS node attack strategies. The simulation results demonstrate the surprising strength of the riskgraph-based approach even if an attacker has limited knowledge of power grids.

This work is structured as follows. The related work is presented in Section 4.3. In Section 5.4 we set up the cascading failure simulator under the extended model.

In Section 4.5 we describe the reduced search space node attack strategy, risk graph, and the riskgraph-based node attack strategy in detail. In Section 6.7, the details of simulation and observation are made. Discussions and conclusions are provided in Section 6.8. Finally, the supplementary file of this published manuscript is provided in Section 4.8.

4.3 Related Work

In this work, we study node attack strategies under the extended model considering two scenarios: attackers know or do not know the system tolerance factor. We briefly summarize existing works as follows.

In the current literature, from the attack perspective, there are three prevailing models in studying cascading failures, pure topological models, pure power flow models and hybrid models. Pure topological models [7, 8] are rooted in complex network theories, and useful to develop strong attack metrics, e.g. degree and load in [14], percentage of failure (PoF) and risk if failure (RIF) in [9], and load distribution vector (LDV) in [15]. Originating from circuit theories, e.g. Kirchoff's and Ohm's Laws, pure power flow models provide the fundamental insights and understanding of cascading behaviors. Recently, hybrid models [11, 13] are proposed to investigate the vulnerability of power grids by combining complex network theory with basic features of power systems, e.g. *power transmission distribution factors* (PTDFs). More discussions about existing cascading failure models are given in Section 4.8, the supplementary file of this work.

Different models have different advantages and disadvantages. First, although pure topological models are useful to develop malicious attack strategies, the related concepts and metrics are far from the physical characteristics of power grids. Thereby, these models are far from reflecting the fundamental behaviors of cascading failures. Second, pure power flow models are more accurate to reveal vulnera-

bility of power grids, and are mainly used to assess the security and reliability of power grid networks [10, 16]. However, a detailed analysis of large-scale power grid is usually computationally expensive due to its complexity, nonlinearity, and dynamics [4]. Finally, the extended model in [13] is a new angle in modeling cascading failures. The power distribution under the extended model is based on PTDFs [12]. Thus, the extended model is more accurate than pure topological models in terms of studying cascading failures. In addition, the calculation of PTDFs is less complex than the detailed analysis of power flows in a power grid [17]. That is, the extended model is less complex than pure power flow models.

When discussing about malicious attack strategies, we assume that attackers might have certain information of power grid networks, such as topological structures, electric features, and system tolerances. For instance, the topological structure information can be purchased from companies (e.g. Platts [18]), the electric features, such as impedance, can be estimated based on the topological information. The system tolerances of real power systems are hard to be clearly known by attackers due to various reasons [7–9]. Thus, the attack strategies in prior studies can be divided into two categories: unknown system tolerance, e.g. *degree*, *load*, *RIF* and *LVD*, and known system tolerance, e.g. *PoF* and the exhaustive search approach. The more information attackers know about power grids, the stronger attacks they might find.

4.4 The Extended Model for Cascading Failures Analysis in Power Grids

4.4.1 Network Topology

Generally speaking, a power grid composes of substations (e.g. generators, transmission and distribution substations) and transmission lines. In this work, we model the power grid network as a directed graph, $\mathbf{G} = \{B, L\}$, where B is the set of nodes (i.e. substations) and L is the set of links (i.e. transmission lines).

We put all generators and all distribution substations into different sets G and D, respectively, where $G \subseteq B$ and $D \subseteq B$. In addition, N_B, N_L, N_G and N_D are used to represent the number of nodes, links, generation nodes and distribution nodes, respectively.

4.4.2 Introduction of the Extended Model

The extended model was originally established in [12, 13]. The introduction of the extended model and comparisons among different models can be found in Section 4.8. We briefly summarize three important concepts about the extended model as follows.

1. *PTDFs*: Power Transfer Distribution Factors (PTDFs) can represent the sensitivity of power flow change in each transmission line for power injection/withdrawal at a pair of nodes [12, 17]. In reality, power is only transmitted from generation nodes to distribution nodes. Under the extended model, power flow on links is considered to be caused by the node pairs that one node is generator and the other node is transmission node.

2. *Extended Betweenness*: The *link extended betweenness* is the summation of power flows caused by each generation-distribution-node pair. The *node extended betweenness* is defined as the summation of extended betweenness on links that connect to a node. The extended betweenness is adopted as the load definition of nodes/links in this work.

3. *Net-ability*: For a grid network $\mathbf{G}$, the net-ability, denoted by $E(\mathbf{G})$, is defined as $\frac{1}{N_G N_D} \sum_{g \in G} \sum_{d \in D} \frac{P_{gd}}{Z_{gd}}$, where P_{gd} represents power injection limitation and Z_{gd} represents the impedance between the generator g and the distribution node d. Net-ability is the measure to evaluate how well a power grid supplies power [12].

4.4.3 Cascading Failure Simulator under the Extended Model

In the current literature [7–9], cascading failure simulators (CFSs) under pure topological models are well established. However, few researchers have conducted in-depth study on cascading failures under the extended model. In this subsection, we setup the CFS under the extended model by introducing several important concepts as follows.

- *Load*: We employ the extended betweenness as the definition of load. During cascading failures, the grid network is often broken into more than one subnets after several rounds. At round t, the load of node i, or n_i, is denoted by $A_{n_i}(t)$, and is updated by recalculating the extended betweenness of n_i in the subnet that contains n_i. In this work, the load of a node (e.g. n_i) before an attack is called the *initial load* of n_i and denoted by A_{n_i}.

- *Capacity*: The capacity of n_i, denoted by C_{n_i}, is the maximum amount of load that n_i can carry.

- *Overloading*: When the load of a node exceeds its capacity, the overloading will occur. Under the extended model, the overloaded nodes are assumed to be removed from the power grid network immediately.

- *System tolerance*: The system tolerance, α ($\alpha > 1$), is the parameter describing the relationship between the initial load of a node and its capacity. For example, the capacity of n_i is assumed to be $\alpha = C_{n_i}/A_{n_i}$ [7]. In general, we assume α values for all nodes are the same, and calculate the capacity as $C_{n_i} = \alpha \times A_{n_i}$.

- *Load redistribution*: When the topology of a grid network changes due to the removals of nodes, the load on nodes will be redistributed by recalculating the extended betweenness for all surviving nodes. If the entire grid network

is broken into more than one subnets, the calculation will be conducted in each subnet separately.

The CFS under the extended model includes three parts: (1) initializing the CFS and removing the TNs; (2) starting the cascading failures process till it stops; (3) measuring the damage using assessment metrics. A similar CFS under the extended model can be found in our previous work [19].

4.4.4 Assessment Metric

In this work, the primary assessment metric is *percentage of drop in net-ability* (PoDN), which is defined as follows.

$$\eta = \frac{E(\mathbf{G}) - E(\mathbf{G}')}{E(\mathbf{G})} \tag{4.1}$$

where $E(\mathbf{G})$ and $E(\mathbf{G}')$ represents the net-ability of power grids before and after the occurrence of cascading failures. The larger η is, the stronger the attack is.

The second and third assessment metrics are *average inverse geodesic length* (AIGL) [20] and *connectivity loss* (CL) [21]. *Geodesic length* is the shortest path between a pair of nodes in a graph [20]. When a pair of nodes are in different subnets, the geodesic length between this pair is ∞ (i.e. infinity). The metric AIGL, denoted by ℓ^{-1}, is defined as $\ell^{-1} = \frac{1}{N_B(N_B-1)} \sum_{n_i \in B} \sum_{n_j \neq n_i \in B} \frac{1}{d(n_i,n_j)}$, where B is the node set and $d(n_i, n_j)$ is the geodesic length between n_i and n_j. The metric CL represents the connectivity between generators and distribution nodes in a power grid. The definition of CL is $1 - \langle \frac{N_G^k}{N_G} \rangle_k$, where N_G is the number of generators and N_G^k is the number of generators connected to the distribution node k. The averaging, $\langle \bullet \rangle$, is done over all surviving distribution nodes after cascading failure. Referring to AIGL, the smaller ℓ^{-1} represents the stronger attack, while by using CL a stronger attack is with larger CL.

4.5 Attack Strategies under the Extended Model

In this section, we investigate malicious attack strategies by discussing *node attack strategy* (NAS). The similar *link attack strategy* (LAS) is introduced in Section 4.8. From the attack perspective, the biggest challenge is to find the attacks that can cause larger damage. In the context of studying cascading failures, an attacker's goal is to identify a set of TNs, whose simultaneous failures could yield as large PoDN as possible.

4.5.1 Complexity Measure of Attack Strategies

In this work, the complexity analysis of different attack strategies is based on the size of search space for each attack strategy. In order words, it is the calculation of how many times an attack strategy needs to launch CFS before finding its best attack. $O_{(CFS)}$ is adopted to represent the time of launching CFS once and as the *unit* to compare the complexity of different attack strategies. Theoretically, it is very hard to precisely analyze the computational complexity of CFS, due to different power grid network sizes, network topologies, system tolerances, attack strategies, and so on. However, the network size and topology are the major factors. For instance, in order to compute the extended betweenness, CFS needs to examine each pair of generation-distribution nodes. For each pair, it needs to determine the sensitivity value of each link. Roughly speaking, assume there are N_G generators, N_D distribution nodes, and N_L links in a grid network. The number of sensitivity values needed to be computed is close to $N_G \times N_D \times N_L$. After obtaining all sensitivity values, summation operation is performed for each node, in order to obtain the extended betweenness (i.e. load) for all nodes. The above operation is performed in each round of cascading failure. From the above discussion, we can see that it is very difficult to have a closed-form expression of $O_{(CFS)}$, because it depends on the network size and topology, as well as how a cascading failure

occurs. We do not address how to reduce the computation complexity of CFS itself. Instead, we focus on analyzing the complexity of different attack strategies based on the number of times launching CFS before making decision. For instance, if an attack strategy needs to launch $(N_B)^M$ times of CFS in order to find its best attack, the complexity of this attack strategy is $(N_B)^M \times O_{(CFS)}$, or $(N_B)^M$ in short.

4.5.2 Load-based and Degree-based Node Attack Strategies

In this subsection, we introduce the well-studied load-based and degree-based approaches [9, 20]. The load of a node is defined as the node extended betweenness, discussed in Section 4.8.1, while the degree of a node is defined the number of the links connecting to this node [20]. When an attacker aims to knock down M target nodes (TNs), the load-based and degree-based node attack strategies, denoted by NAS^M_{load} and NAS^M_{degree}, respectively, are shown as follows,

* NAS^M_{load}: Choose nodes with the top M largest load values as TNs.

* NAS^M_{degree}: Choose nodes with the top M largest degree values as TNs.

Let C^M_{degree} and C^M_{load} denote the complexity of NAS^M_{degree} and NAS^M_{load}. Because these approaches do not need to launch CFS before selecting TNs. Both C^M_{degree} and C^M_{load} are 0.

4.5.3 Exhaustive Search node Attack Strategy

For an attacker, the strongest node attack strategy is no doubt the exhaustive search. The exhaustive search NAS is denoted by NAS^M_{ES} and conducted below,

* NAS^M_{ES}: Find the M TNs, whose simultaneous failure yields the largest PoDN under a given α.

Table 4.1. The strongest target node combinations on IEEE 118 bus system

Index	NAS^1_{ES}		NAS^2_{ES}		NAS^3_{ES}	
	TNs	PoDN(%)	*TNs*	PoDN(%)	*TNs*	PoDN(%)
1	65	64.5	**30**,68	81.3	**30**,**65**,80	88
2	38	55.7	**30**,80	79.2	**30**,**65**,96	87.8
3	68	52.9	**30**,65	77.9	**30**,**68**,96	87.2
4	30	48.2	**65**,69	77.8	**30**,**68**,94	86.8
5	80	46.7	**38**,68	77.4	**30**,**68**,103	86.2
6	81	42.3	**38**,80	77.1	**38**,**69**,94	85.9
7	77	33.4	**38**,69	76.1	**30**,**65**,94	85.5
8	49	31.1	**17**,65	76.1	**38**,**69**,96	85.2
9	64	30.8	**38**,77	75.9	**30**,66,**68**	85.2
10	17	30.6	**30**,81	75.3	**30**,**68**,92	85

Let C^M_{ES} denote the complexity of NAS^M_{ES}. Theoretically, the complexity is,

$$C^M_{ES} = \binom{N_B}{M} \times O_{(CFS)} \tag{4.2}$$

where $\binom{N_B}{M} = \frac{N_B(N_B-1)\times\cdots\times(N_B-M+1)}{M!}$. Therefore, C^M_{ES} is the same order as $(N_B)^M$, which increases as a power function with N_B and explodes as an exponential function with M.

The exhaustive search is very time-consuming, and often computationally infeasible. Numerically, take IEEE 118 bus system as an example. Running CFS once on IEEE 118 bus system needs an average time of 0.06 second by using Matlab under Window 7 OS with 4 GB memory and dual-core i5 CPU (2.4GHz each). The time for simulating $\binom{118}{5} = 174,963,438$ node combinations is roughly 4 months. Note that, the real power grid networks are often much bigger than IEEE 118 bus system. Even if parallel computing is available, adopting NAS^M_{ES} on large-scale networks is still impractical.

4.5.4 Reduced Search Space Node Attack Strategy

It is the goal to develop practical attack strategy in this work. Although the exhaustive search is often infeasible, it is still doable at small M values on the

moderate-scale grid network, and can provide some useful insights. We conducted experiments on IEEE 118 bus system by using NAS^{M}_{ES}, where M is set to be 1, 2 and 3 and α is set to be 1.5. The node combinations of the top ten strongest attacks are shown in Table 5.3.

There is a helpful observation made from Table 5.3. For instance, in NAS^{2}_{ES}, at least one TN in the two-node combination is from the TNs of the top ten attacks in NAS^{1}_{ES}. In NAS^{3}_{ES}, all three-node combinations contains the two-node combinations that in NAS^{2}_{ES}. In Table 5.3, the highlighted nodes or node combinations illustrate such observation.

This observation is easy to understand. If a M-TN combination can result in severe damage to a power grid, adding another TN to this combination will most likely be a strong attack. It is important to point out that the new *(M+1)*-TN combination may not be the strongest attack of NAS^{M+1}_{ES}. However, as long as the resulted PoDN is large enough, the new combination will be a strong attack of NAS^{M+1}_{ES}.

Inspired by the above discussions, we propose a novel search based attack strategy, called *reduced search space attack strategy* or *RSS attack strategy* in short, which can be applied to both nodes and links. The RSS node attack strategy is denoted by NAS^{M}_{RSS}. Before discussing in detail about the algorithm procedure of NAS^{M}_{RSS}, we need to give some explanations. First, the procedure of searching TNs is an iterative process, which includes one initial round and $M-1$ successive rounds. Second, the *criticality* of a node combination (or a node) is determined by PoDN. The larger the PoDN is, the more critical the node combination is. Third, in each iterative round, e.g. m^{th} round ($1 \leq m \leq M$), the top R critical combinations are chosen as the *round recommended combination set* (RRCS), denoted by S^{m}_{RRC}. Those

Procedure 1 Initialize the iterative process and obtain the TN for NAS^1_{RSS}

1: Set up a system tolerance, e.g. $\alpha = 1.5$, and initialize a vector $\mathbf{x}$ with all values as 0.
2: //The indices of nodes are consecutive from 1 to N_B.
3: **for** $i = 1 :\ N_B$ **do**
4: Conduct one-node attack by knocking down node i under given α. Calculate the PoDN after the cascading failure and set the value of $\mathbf{x}_i$ as the corresponding PoDN value.
5: **end for**
6: Choose the node with the largest PoDN in $\mathbf{x}$ as the TN for NAS^1_{RSS}.
7: Choose the nodes with the top P largest PoDNs in $\mathbf{x}$ as candidate nodes, and put them into S_C.
8: Choose the nodes with the top R largest PoDNs in $\mathbf{x}$ as the 1^{st} round recommended combination, and put them into S^1_{RRC}.

There are three procedures working together to select TNs for NAS^M_{RSS}. Procedure 1 shows the steps to obtain the TNs for NAS^1_{RSS}. When $M = 1$ (launching one-node attack), attackers only need to use Procedure 1, without considering the other two procedures. When $M > 1$ (launching multi-node attack), attackers need to first use Procedure 1 to initialize the iterative process, then use Procedure 2 to complete the iterative process, and finally use Procedure 3 to find TNs for NAS^M_{RSS}.

Let C^M_{RSS} denote the complexity of NAS^M_{RSS}. Searching TNs for NAS^M_{RSS} is performed in M rounds. In the 1^{st} round, Procedure 1 needs to run CFS N_B times. In m^{th} round ($2 \leq m \leq M$), Procedure 2 needs to run CFS $P \times R$ times. Therefore, the theoretical complexity is,

$$C^M_{RSS} = \{P \times R \times (M-1) + N_B\} \times O_{(CFS)} \tag{4.3}$$

where P and R are set to limit the search space. At the worst case, when $P = R = N_B$, C^M_{RSS} equals to $(M-1) \times (N_B)^2$, the same order as $M \times (N_B)^2$. Therefore, C^M_{RSS} increases as a power function with N_B and increases linearly with M.

From the above discussions, we know that NAS^M_{RSS} has three advantages.

Procedure 2 Find the S_{RRC}^{m+1} under given S_{RRC}^{m}

1: Perform the **Procedure** 1, and obtain S_C.
2: Initialize a candidate combination set, S_{CC}, and a vector $\mathbf{y}$ with all values as 0.
3: //Construct the candidate combinations in $(m+1)^{th}$ round.
4: **for** $i = 1:\ R$ **do**
5: Get the i^{th} node combination in S_{RRC}^{m}, denoted by $\mathbf{C}_i$.
6: **for** $j = 1:\ P$ **do**
7: Get the j^{th} candidate node in S_C, denoted by n_j.
8: Combine $\mathbf{C}_i$ and n_j to get a new candidate combination, and put it into S_{CC}.
9: **end for**
10: **end for**
11: //Conduct multi-node attack for each candidate combination in S_{CC}.
12: **for** k^{th} combination in S_{CC} **do**
13: Conduct multi-node attack by knocking down all nodes in the k^{th} combination under given α. Calculate the PoDN when CFSor stops, and set $\mathbf{y}_k$ to the corresponding PoDN.
14: **end for**
15: Choose the candidate combinations with the top R largest PoDNs in $\mathbf{y}$ as the $(m+1)^{th}$ round recommended combination, and put them into S_{RRC}^{m+1}.

Procedure 3 Find TNs for NAS_{RSS}^{M} under given S_{RRC}^{M}

1: There are R node combinations in S_{RRC}^{M}. The nodes in the combination that can cause the largest PoDN are the TNs for NAS_{RSS}^{M}.

First, compared with NAS_{ES}^{M}, NAS_{RSS}^{M} has sharply-reduced complexity (or search space). C_{RSS}^{M} is approximate to $M \times (N_B)^2$, which is much lower than $(N_B)^M$ of C_{ES}^{M}. Given the available computing resources, NAS_{RSS}^{M} can analyze a much bigger network than NAS_{ES}^{M}. In other words, NAS_{RSS}^{M} scales much better than NAS_{ES}^{M}. Furthermore, we can adjust the parameters P and R to achieve a good balance between the complexity and the attack performance. For example, suppose NAS_{ES}^{M} and NAS_{RSS}^{M} are both tested on IEEE 118 bus system, where $M = 5$ for both schemes, and $N_B = 118$, $P = 118$, $R = 16$ for NAS_{RSS}^{M}. NAS_{ES}^{5} needs to launch $174,963,438$ times of CFS and its calculation probably needs four months;

whereas NAS^5_{RSS} only needs to launch $7,670$ times of CFS, which needs 7.8 minutes. The improvement about the complexity of NAS^M_{RSS} is a big step. Second, the performance of NAS^M_{RSS} is comparable to that of NAS^M_{ES}, which will be shown in Section 6.7. Finally, during the procedures to find the best attacks, NAS^M_{RSS} keeps the track of the *round recommended combination set*, which is useful to construct the *risk graph*. The details of the risk graph will be discussed in subsection 4.5.6.

4.5.5 Limitations of Reduced Search Space Attack Strategy

Although NAS^M_{RSS} can sharply reduce the complexity of NAS^M_{ES} and reach comparable attack performance, which will be discussed in Section 4.6.1, it still has limitations.

First, NAS^M_{RSS} relies on the system tolerance (α). As shown in Procedure 1, if attackers adopt NAS^M_{RSS} to launch attacks, they must first estimate the system tolerance. In reality, system tolerances of power grids are rarely known by attackers due to various reasons, e.g. security concerns. Furthermore, although many existing works assume that the capacity of a node is defined as the initial load multiplying α, and assume that α is the same for all nodes, these assumptions could be over-simplifying the case. The nodes in a power grid surely can have different tolerance factors. It is surely not an easy task for an attacker to estimate the tolerance factors for all nodes in a power grid. Therefore, from the attack point of view, requiring the knowledge of system tolerance is a drawback.

Second, although NAS^M_{RSS} has greatly reduced the complexity, it is still a search based approach and not suitable for real-time attacks. For example, if an attacker knows that a few substations are currently down due to some reasons, e.g. a winter storm, the attacker wants to determine TNs in this situation and launch an attack. Similarly, the defense side may also want to know the vulnerability of the power grid network in this situation. Recall that the worst case of the

complexity of NAS^M_{RSS} is $M \times (N_B)^2$, which is still much higher than 0 of NAS^M_{degree} and NAS^M_{load}, discussed in Section 4.8.2. Further reduction in the complexity of NAS^M_{RSS} is desirable.

In summary, a practical real-time attack strategy should have two features: fast and not depending on system tolerances.

4.5.6 Construction of Risk Graph

Is it possible to obtain an attack strategy without knowing the information of system tolerances? We find the "relationship" among nodes in a power grid and can conduct strong attacks based on such relationships. This is particularly useful to choose multiple TNs. In this subsection, we propose a novel metric, called the *risk graph* (RG), to describe such relationship. Here, we demonstrate the procedure of building the risk graph for nodes, called the *node risk graph* (NRG).

In the procedures to search the strongest attack for NAS^M_{RSS}, we keep a track of the top R strongest node combinations in each round, called RRCS and denoted by $S^1_{RRC}, S^2_{RRC}, ..., S^M_{RRC}$. One realization of the RRCS are shown in Table 6.2, from which we have basic observations. First, several nodes, e.g. nodes 30, 38, 68, 65 and 80, appear more frequently than others. Second, several node combinations, e.g. $\{30, 68\}$, $\{38, 69, 96\}$, happen frequently. These observations demonstrate there probably are some fixed node combinations, the failure of which may seriously threaten the safety of the power grid. Studying these fixed node combinations or the relationship among nodes is helpful to find strong malicious attack strategy.

To demonstrate such relationship of nodes, we construct NRG according to the intermediate results of NAS^M_{RSS} under a given system tolerance. Furthermore, we merge single NRGs under different system tolerances into an *node integrated risk graph* (NIRG) to describe such relationship among nodes. If several nodes are closely related in NIRG, their combination is expected to cause severe damage to

the power grid network.

Next, we describe the procedure of constructing single NRG under a given system tolerance value α.

* **Step 1**: Given an α, performing the procedures of NAS^{M}_{RSS} and obtain $S^{1}_{RRC}, ..., S^{M}_{RRC}$.

* **Step 2**: Examine those sets (an example is shwon in Table 6.2), and find how many times a node appears in such sets. If a node appears at least once, this node becomes a vertex of the risk graph. In addition, each vertex has a *vertex occurrence frequency* (VOF), defined as the number of the corresponding node appears in those sets.

* **Step 3**: Add an edge between each pair of vertices and assign the weight of this edge as zero. The edge weight is referred to as the *edge occurrence frequency* (EOF).

* **Step 4**: Examine the node combinations in each S^{k}_{RRC} $(k = 1, 2, \cdots, M)$. If a pair of nodes, say node i and node j, appears in the combination with m nodes, increase the EOF of the edge between node i and j by adding $\frac{2}{m(m-1)}$. For example, for the combination $\{30, 80, 65\}$, we increase the EOF of three edges, $edge_{30-80}$, $edge_{80-65}$, $edge_{30-65}$, by 1/3. If the pair of nodes appear in more than one node combinations, the final EOF of the edge between this pair of nodes is to summarize all EOF values from the combinations this pair of nodes are in. For another example, assume nodes 30 and 80 appear simultaneously in $\{30, 80\}$, $\{30, 80, 65\}$ and $\{30, 80, 65, 94\}$, the EOF of $edge_{30-80}$ is $1 + 1/3 + 1/6 = 3/2$.

* **Step 5**: Remove the edges having EOF values as zero.

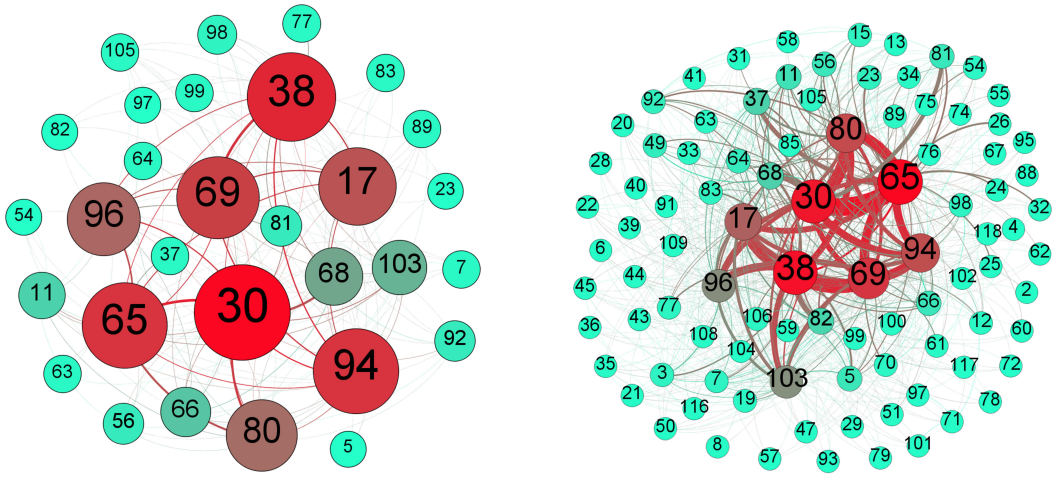
Table 4.2. An realization of RRCS on 118 bus system.

S^1_{RRC}	S^2_{RRC}	S^3_{RRC}	S^4_{RRC}	S^5_{RRC}	S^6_{RRC}
65	68,30	30,80,65	38,69,96,17	38,69,96,17,103	38,69,96,17,103,66
38	30,80	65,30,96	38,69,94,17	38,69,94,17,103	30,80,65,94,11,56
68	65,30	68,30,96	30,80,65,94	38,69,96,17,66	38,69,94,17,103,83
30	65,69	68,30,94	30,80,65,96	38,69,96,17,23	38,69,96,17,66,92
80	38,68	68,30,103	38,69,94,30	30,80,65,94,11	30,80,65,94,11,103
81	38,80	38,69,94	30,80,65,103	38,69,96,17,92	38,69,94,17,103,82
77	38,69	65,30,94	68,30,94,66	38,69,96,17,105	38,69,96,17,66,94
49	65,17	38,69,96	38,69,96,30	38,69,96,17,94	38,69,94,17,103,98
64	38,77	68,30,66	30,80,65,92	38,69,94,17,89	30,80,65,94,11,54
17	30,81	68,30,92	30,80,65,89	30,80,65,94,7	30,80,65,94,7,56
96	65,80	68,30,80	38,69,94,5	30,80,65,96,11	38,69,94,17,98,66
94	68,17	65,30,103	68,30,96,63	38,69,94,17,98	38,69,94,17,99,66
63	65,96	65,17,80	68,30,96,66	38,69,94,17,83	30,80,65,96,11,56
8	65,38	65,17,96	65,30,96,68	38,69,94,17,97	38,69,94,17,103,66
100	38,81	65,69,96	65,30,96,81	30,80,65,94,103	30,80,65,94,103,56
37	65,37	30,80,64	68,30,96,11	38,69,94,17,99	30,80,65,94,11,105

* **Step 6**: Remove the vertices that are not connected with other vertices. This occurs when some nodes are in S^1_{RRC} but not in other round recommend combination sets.

A NRG of IEEE 118 bus system, built directly from Table 6.2, is shown in Fig. 4.1(a). The size and color of a vertex is decided by its VOF. And the width and color of an edge is determined by its EOF. The bigger (wider) and redder of a vertex (or an edge), the larger its VOF (EOF). Fig. 4.1(a) is visualized by Gephi [22]

There are two important factors affecting the construction of risk graphs, the system tolerance (α) and the parameters (P and R). The former is the major factor and the latter is the minor factor. Different values of the parameters, P and R, may slightly change the nodes in the RRCS; whereas different values of the system tolerance, α, could probably lead to major changes of nodes in the RRCS. In other words, single risk graphs are sensitive to the system tolerance.



(a) Node Risk Graph (b) Node Integrated Risk Graph

Figure 4.1. The node risk graphs on IEEE 118 bus system

Risk Graph Additivity: The risk graphs constructed under different system tolerances of the same power grid network are additive. If two NRGs are added together, the vertices and edges in the new NRG are obtained as, (1) all vertices in the two NRGs will be in the new NRG, and the VOF of vertices in the new NRG is calculated as either adding the corresponding VOF of the vertex in the two NRGs, if the vertex appears in both NRGs; or keep its own VOF, if it just appears in one NRG; (2) for edges, the procedure is the same as vertices.

By adding single NRGs, we can obtain NIRG. As discussed above, single NRG is sensitive to α, while the NIRG is more robust in terms of reflecting the relationship between candidate nodes. Based on prior knowledge and construction restrictions of power grids [7, 8], the range of the system tolerance is set to be $1 < \alpha \leq 2$. Without losing the generality, the NIRG here is generated by adding 20 NRGs, where α is from 1.05 to 2 with an interval 0.05. The NIRG of IEEE 118 bus system is shown in Fig. 4.1(b).

4.5.7 Risk-Graph Based Node Attack Strategy

The NIRG provide a good way to find stronger attack strategy, which is not sensitive to system tolerances. Suppose attackers have already had the NIRG of a power grid, they can launch node attacks as follows,

* $NAS^{M}_{riskgraph}$: The riskgraph-based node attack strategy. If M equals 1, select the node with the largest VOF in the NIRG as the TN for $NAS^{1}_{riskgraph}$. Otherwise, we choose the M nodes from the NIGR as the TNs for $NAS^{M}_{riskgraph}$ by meeting two requirements. First, each pair of nodes should have a direct edge in the NIGR. In total, there are $\frac{M(M-1)}{2}$ edges among these M chosen nodes. Second, the summation of all EOF of those $\frac{M(M-1)}{2}$ edges is the largest among these of all other M nodes selections. In other words, we select the M TNs, whose summation of EOF is maximal.

Although the nodes with large VOF often have more impact on the power grid, their combination does not necessarily yield strong attacks. For instance, in Fig. 4.1(b) the vertices marked with labels as 17 and 30 are important candidate nodes, which have large VOF values and are represented by bigger circles. However, there is no direct edge between them. This means the node combination $\{17, 30\}$ is not a strong two-node attack. Therefore, the basic idea of $NAS^{M}_{riskgraph}$ is to find the set of M nodes with the strongest connection. The rationale behind the first requirement is to avoid including nodes that never appear together in any node combinations in RRCS. The rationale behind the second requirement is to choose the nodes, whose pair combinations appear most frequently in RRCS.

Let $C^{M}_{riskgraph}$ denote the complexity of $NAS^{M}_{riskgrph}$. $C^{M}_{riskgrph}$ includes two parts: the construction of the NIRG and the selection of TNs. The former has the similar complexity as that of NAS^{M}_{RSS}, because single risk graphs are based on the intermediate results of NAS^{M}_{RSS}. It is important to point out that this

Table 4.3. The summary of different node attack strategies

Attack Strategy	NAS^M_{degree}	NAS^M_{load}	$NAS^M_{riskgrph}$	NAS^M_{RSS}	NAS^M_{ES}
$O_{(CFS)}$	0	0	0	$M \times (N_B)^2$	$(N_B)^M$
Effectiveness	Low	Low	High	High	High
System tolerance	No	No	No	Yes	Yes

computation can be done "offline": first obtain single risk graphs under a set of representative system tolerances, and then construct the NIGR. The latter is to find TNs from the NIGR. This procedure does not rely on CFS, which means its complexity is 0, similar to that of the load-based and the degree-based approaches. This can be done in "real-time". For example, if an attacker has observed that n_{103}, node 103, in Fig. 4.1(b) is down for some reasons (e.g. nature disaster), the attacker can quickly identify an attack strategy adding one more TN, e.g. n_{38}, to the already-down n_{103}. Therefore, considering on-line attacks, $C^M_{riskgraph}$ is 0.

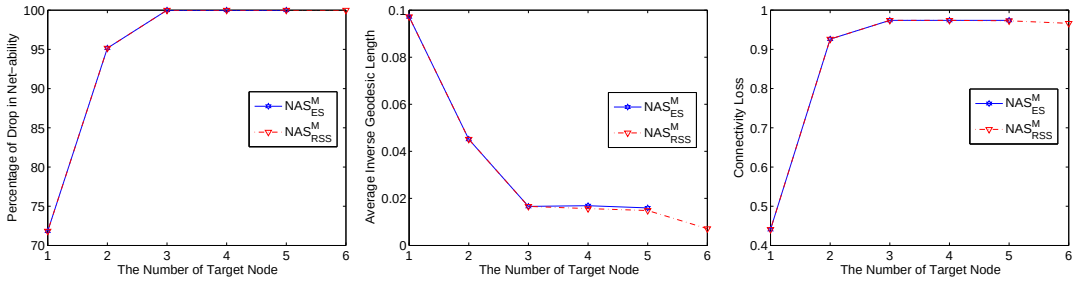
In summary, the comparison of the real-time complexity of different node attack strategies is $C^M_{degree} \approx C^M_{load} \approx C^M_{riskgraph} \ll C^M_{RSS} \ll C^M_{ES}$. More comparisons among different node attack strategies are shown in Table 4.3.

4.6 Simulation Results

In this section, the simulations and observations are presented in detail. The simulation experiments are conducted in Matlab, including the setup of power grid network, PDTFs calculation and the process of CFSor. The proposed attack strategies are tested on the well-known IEEE 57 and 118 bus systems [23], and Polish transmission system [17]. The details of the three benchmarks are listed in Table 6.3. Here, we will give our major experiment results and observations, and additional results are given in Section 4.8.

Table 4.4. The summary of different test benchmarks.

Test Benchmarks	N_B	N_L	N_G	N_D
IEEE 57 bus system	57	80	7	42
IEEE 118 bus system	118	179	54	99
Polish transmission system	2383	2896	327	1817

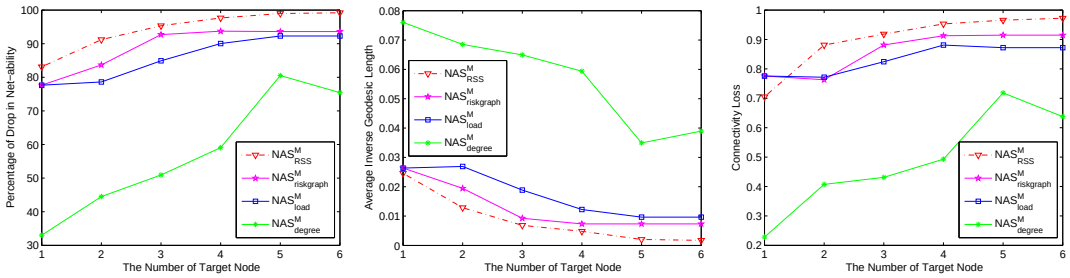


(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

Figure 4.2. The performances versus M between the ES and RSS attack strategies on IEEE 57 bus system.

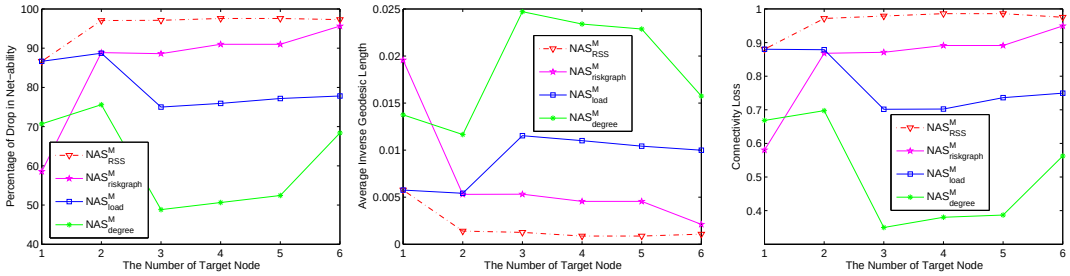
4.6.1 Performance Comparisons between the Exhaustive Search NAS and the Reduced Search Space NAS

In this subsection, the proposed RSS node attack strategy, NAS_{RSS}, is compared with the exhaustive search node attack strategy, NAS_{ES}. Both node attack strategies are tested on IEEE 57 bus system. Due to the huge search space of the exhaustive search, we conducted experiments for NAS^M_{ES} with $M \leq 5$. The maximum M for NAS^M_{RSS} is set to 6. The comparisons between NAS^M_{ES} and NAS^M_{RSS} are shown in Fig. 4.2. In the subplots, x-axis represents the number of TNs (M), while y-axis represents PoDN, AIGL, and CL, respectively. In each subplot, the solid blue-hexagram curves represents NAS^M_{ES}, and the dashdotted red-plus curves represents NAS^M_{RSS}. The system tolerance (α) is set to 1.5. Theoretically, it is very difficult to analyze how close the attack performance of NAS^M_{RSS} is to that of NAS^M_{ES}. The CFSor under the extended model is too complex to yield theoretical bounds for the attack performance. Therefore, researchers often judge



(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

Figure 4.3. The performances versus M among four node attack strategies on IEEE 118 bus system.



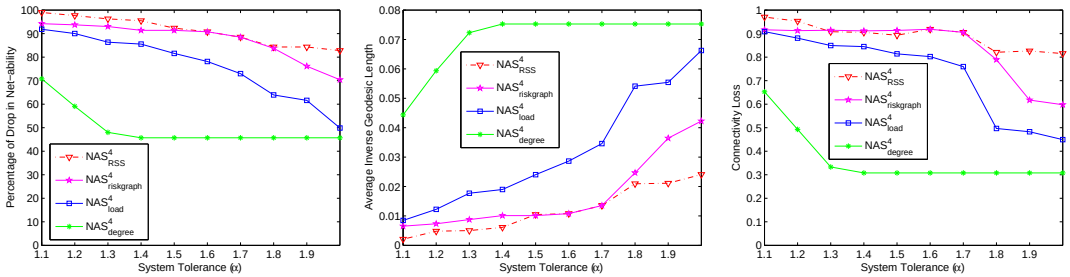
(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

Figure 4.4. The performances versus M among four node attack strategies on Polish transmission system.

the efficiency of different approaches based on numerical evaluation [7, 21, 24–26]. Several important observations are made from Fig. 4.2.

First, the attack performance of NAS^M_{RSS} can compete with that of NAS^M_{ES}. Within these subfigures, the dashdotted red-plus curves match the blue-square solid curves in terms of the three measurement metrics. The match is reasonable, because the TNs selected by NAS^M_{RSS} are often the same as those of NAS^M_{ES}. We do expect a small gap between those two approaches when M is large. Such results are not included because performing the exhaustive search for a large M value is computationally prohibitive.

Second, from the attackers point of view, launching attacks on a few critical



(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

Figure 4.5. The performances versus α among four node attack strategies on IEEE 118 bus system.

nodes will cause serious damage to power grid networks. In power grid networks, usually there are a few critical nodes, the failure of which will cause serious enough damage. The prior study shows that cascading failures have the power-law distribution of blackout sizes in both theoretical models and empirical blackouts [4]. Thus, from the attack perspective studying cascading failures by initially triggering a few TNs is practicable and meaningful.

Finally, NAS^M_{RSS} is an ideal substitution of NAS^M_{ES}. As discussed above, the attack performance of NAS^M_{RSS} is very close to that of NAS^M_{ES}. In addition, it is important for attackers to determine the number of TNs (i.e. M). When M is small, the attacker may not be able to cause serious damage to power grid networks. When M is large, the attacker needs to take down more nodes, which makes the attack difficult to be launched. Furthermore, increasing M will not significantly increase the attack performance if the smaller M value already causes large damage to power grids. More important, with appropriate parameter values, P and R, NAS^M_{RSS} has sharply-reduced complexity and is doable.

4.6.2 Comparison among Different Node Attack Strategies

In this subsection, comparisons are made among $NAS^M_{riskgraph}$, NAS^M_{load}, NAS^M_{degree}, and NAS^M_{RSS} on IEEE 118 bus system and Polish transmission system.

The comparisons among these four node attack strategies are shown in Figs. 4.3, 4.4 and 4.5. In simulations, there are two important parameters for all approaches, the number of TNs (M) and the system tolerance (α). Figs. 4.3 and 4.4 show the change of attack performance against M, while Fig. 4.5 shows the performance change against α. In addition, there are three subplots in each figure, which shows the results evaluated by the three different metrics. The y-axis noted by (a), (b) and (c) represents *percentage of drop in neb-ablity*, *average inverse geodesic length* and *connectivity loss*, respectively; the x-axis represents the number of TNs in Figs. 4.3 and 4.4, and the system tolerance in Fig. 4.5. In each subplot, the dash-dotted red-plus curve, solid magenta-pentagram curve, solid blue-square curve and solid green-star curve represent NAS^M_{RSS}, $NAS^M_{riskgraph}$, NAS^M_{load} and NAS^M_{degree}, respectively. For example, Fig. 4.3(a) demonstrates the comparison among the four node attack strategies on IEEE 118 bus system, when M is set from 1 to 6, α is set to 1.5, and results are measured by PoDN. From these figures, we have the following observations and discussions.

First, the attack performances of $NAS^M_{riskgraph}$ are a little weaker than that of NAS^M_{RSS}, but much stronger than those of NAS^M_{load} and NAS^M_{degree}. As discussed in Section 4.6.1, NAS^M_{RSS} could be employed as the substitution of the exhaustive search node attack strategy. From all subplots in Figs. 4.3 and 4.4, the attack performance against M, the solid magenta-pentagram curves are very close to the dashdotted red-plus curves, which means the attack performances of $NAS^M_{riskgraph}$ are close to those of NAS^M_{RSS}. In addition, the solid green-star curves are far from the dashdotted red-plus curves, while the solid blue-square curves are closer than those green-star curves, but still are not comparable with the magenta-pentagram curves. Similar observations are made in Fig. 4.5, the attack performance against α. In conclusion, from the attack performance perspective NAS^M_{RSS} is the best

achievable node attack strategy, and NAS^M_{degree} is the worst; while the $NAS^M_{riskgraph}$ is very close to NAS^M_{RSS}, and much better than NAS^M_{load} and NAS^M_{degree}.

Second, as M increases, the regression on the attack performance of $NAS^M_{riskgraph}$, NAS^M_{degree} and NAS^M_{load} might occur. Such examples could be found in Figs. 4.3 and 4.4. The reason of the regression happens is that the cascading failure under the extended model quickly stop when the whole power grid network is broken into more than one balanced subnets. NAS^M_{degree} and NAS^M_{load} do not consider this fact and select their TNs according to the degree or load distribution. The failure of those high-degree or high-load nodes might quickly break the whole power grid network into several subnets. For the $NAS^M_{riskgraph}$, the regression sometimes occurs, when the number of TNs is large, e.g. $M \geq 3$. The reason is that the NIRG is mainly reflecting the hidden relationship between a pair of nodes. Thus, when the number of TNs increases, the TNs selected from NIRG might not represent the strongest attacks, and then the attack performances downgrade a little.

As a summary, when the system tolerance value is unknown, $NAS^M_{riskgraph}$ is much stronger than NAS^M_{degree} and NAS^M_{load}. Furthermore, $NAS^M_{riskgraph}$ has similar performance to that of NAS^M_{RSS}, but do not require performing search in real time. In other words, after the NIRG is established, there is no need to launch CFSor before making attacks. The major advantages of $NAS^M_{riskgraph}$ are: (a) not requiring the knowledge of system tolerance, (b) low real-time complexity, and (c) comparable attack performance with that of NAS^M_{RSS}. Detailed comparisons are given in Table 4.3.

4.7 Discussion and Conclusion

In this work, we investigated cascading failures of power grids under the extended model. The major contributions are summarized as follows,

- Proposed a new search based node attack strategy, called the *reduced search space node attack strategy*, which can sharply reduce the complexity of the exhaustive search node attack strategy, and yields the attack performance very close to that of the exhaustive search. By using the proposed approach, we can analyze a much bigger network than using the exhaustive search. Furthermore, we can adjust the parameters in the proposed approach to achieve a good balance between the complexity and the attack performance.

- Proposed a novel metric, called the *risk graph*, to describe the hidden relationship among potential TNs in terms of causing cascading failures. In other words, if several nodes are closely tied together in the NIRG, the simultaneous failure of these nodes is more likely to raise serious cascading failures.

- Proposed a practical node attack strategy, called the *riskgraph-based node attack strategy*, whose attack performance is comparable to that of the reduce search space node attack strategy, but its complexity is extremely low when used in real-time situations.

Although we investigated cascading failures from the attack perspective, the results can be very useful for the research on defense side. In particular, the risk graph is a concise and effective way to describe the criticality of nodes in power grids. Furthermore, the RSS node attack strategy can be used to evaluate the effectiveness of defense approaches by finding the strong attacks after a certain defense approach is applied.

In the future work, the proposed approaches can be further improved from several aspects. First, the risk graph shows the hidden relationship of node pairs. The risk graph may not accurately describe the relationship among a group of nodes, when the group size is larger than 2. We have seen the degradation of

attack performance when $M > 5$. In the future, the risk graph construction procedure may consider more than two-node combinations. Second, the riskgraph-based NAS can handle the situation when each node has different tolerance factors. The next step may be evaluating its performance after being given some practical data, describing the distribution of tolerance factors. Third, the proposed node attack strategies can also work on links. Therefore, the proposed approaches can be extended to address joint-node-link attacks. Fourth, investigating the cascading failures in large-scale power grids, e.g. the entire North America power grid benchmark, will be more meaningful. Fifth, the RSS node attack strategy in this work is pretty intuitive and straightforward. As an interesting future research direction, more advanced methods could be used to improve the search efficiency and results. For instance, dynamic programming (DP) [27] and approximate dynamic programming (ADP) [28, 29] are the popular techniques in solving the problems that have the properties of overlapping subproblems. Integrating them with the search-based approach here will be an interesting and possible direction to improve the proposed approach. Finally, we plan to investigate the risk-graph idea in as stochastic models [30] and temporal features of cascading failures [31].

4.8 Supplementary File

4.8.1 Models for Investigating Cascading Failures

In current literatures, many simulation methods have been proposed to investigate the vulnerability of power grids [4]. Generally speaking, *high-level statistical models*, e.g. the CASCADE model [32], provide some statistical and probabilistic methods to study cascading failures; *historical data methods* try to find failure patterns from the historical blackout records [33]; *deterministic models* are the most important and prevalent models in studying the vulnerability of power grids, within which $N-x$ contingency analysis [10] is the biggest family; *network models* mainly

employ the topological properties of power grid networks, e.g. "betweenness" and "degree", to mimic the power distribution in power grids.

In addition, network theory models are widely adopted to study the malicious attack strategies against power grids. There are two prevailing network models, the *recoverable model* [24] and the *non-recoverable model* [8]. The major difference between them is the assumption of load definition and load redistribution after occurrences of failures or overloading of nodes/links [9]. Under the recoverable model, the load of each node/link is defined as *betweenness* [24]. To calculate the betweenness of nodes/links, we need to find the shortest path between each pair of generator and distribution substations. For example, if there are N_G generator and N_D distribution substations, there are $N_G \times N_D$ generator-distribution pairs. The betweenness of a node/link is then defined as the number of such shortest paths going through this node/link. When one or more nodes/links are knocked down, the shortest paths that originally pass through them need to be detoured, and then the load of surviving nodes/links is redistributed by recalculating the betweenness. Compared to the recoverable model, the load of a node/link under the *non-recoverable model* is defined as the multiplication of its degree with the summation of its neighbor's degree [8]. While a node/link is knocked down or overloaded, the load it holds will be proportionally redistributed to its surviving neighbors.

The Extended Model

The extended model is first discussed in [12], where *net-ability* was proposed to replace the *network efficiency* as the measure to evaluate how well a power grid supplies electricity. Then, the *extended beteweenness* was introduced in [13] to replace the *betweennees* as load of nodes/links. Generally speaking, the extended model is similar to the recoverable model [9]. We briefly summarize how to use

the extended model to investigate the vulnerability of power grids as follows.

1. First, the DC model of power grids [17] is adopted to calculate Power Transfer Distribution Factors (PTDFs), which represent the sensitivity of power flow change in each transmission line for power injection/withdrawal at a pair of nodes. In this work, PTDFs are denoted by $\boldsymbol{H}$, a $N_L \times N_B$ matrix. Each element in $\boldsymbol{H}$, e.g. h_{lj} (i.e. the element at lth row and jth column), reflects the change of real power flow in link l given per unit power injection at node j and withdrawal at the slack node. In this work, the MATPOWER [17], a well-known Matlab based tool for solving power flow analysis problems, is adopted to calculate PTDFs of power grids.

2. Second, power is only transmitted from generators to distribution substations in power grids. The power flow change on link l for power injection at the generator node (g) and withdrawal at the distribution node (d) is presented as $h_l^{gd} = h_{lg} - h_{ld}$, where h_{lg} and h_{ld} are the elements in $\boldsymbol{H}$ at row l with column g and d, respectively. Due to the stability and security concerns of power grids, each transmission line has its power limitation. Thus, for each generator-distribution node pair, the power injection at the generator side is limited. Under the extended model, the power injection limitation of each pair, denoted by P_{gd}, is defined as $\min_{l \in L}(\frac{P_l^{max}}{|h_l^{gd}|})$, where P_l^{max} is set to be 1 (p.u.).

3. Each generator-distribution node pair can raise power change more or less in all transmission lines, which represents the power distribution under the extended model. The accumulation of the power changes on each node/link is the *extended betweenness*, including the *node extended betweenness* and the *link extended betweenness*. In this work, the extended betweenness is adopted as the load of nodes/links.

4. Finally, the net-ability of a power grid network (i.e. $\mathbf{G}$), denoted by $E(\mathbf{G})$, is defined as $\frac{1}{N_G N_D}\sum_{g\in G}\sum_{d\in D}\frac{P_{gd}}{Z_{gd}}$, where Z_{gd} is the electric distance, equivalent to the impedance between the generator g and the distribution node d. Compared with the recoverable model in [24], the electric distance replaces the concept of the shortest path, and the net-ability replaces the concept of the global efficiency. If the failure of nodes/links occurs, the comparison of net-ability between before and after the failure will show how serious the failure is. In other words, the strength of an attack is measured as the reduction in the net-ability of the power grid network caused by the attack.

To interested readers, an example on the six-bus power system in [34] is shown here. The six-bus power system has six nodes and eleven links. In this power system, generators have indices of 1, 2, 3 and distribution nodes have indices of 4, 5, 6. In addition, MATPOWER includes this six-bus power system as one of its test cases. The original PTDFs of the six-node power system are shown in Table 4.5, where n_1, node 1, is selected as the slack bus. Take the generator-distribution node pair, n_2 and n_4, as an example. The power flow change in l_1, link 1, caused by this pair is: $h_{l_1}^{n_2 n_4} = h_{l_1 n_2} - h_{l_1 n_4} = -0.1557$. Similarly, the power flow changes in $l_2, l_3, \cdots, l_{11}$ caused by this node pair are 0.1895, -0.0338, 0.0384, 0.6904, 0.0701, 0.0453, 0.0439, -0.0055, -0.1201, -0.0399, respectively. Thus, the power injection limitation for (n_2, n_4) is $P_{n_2 n_4} = \min_{l\in L}(\frac{P_l^{max}}{|h_l^{gd}|}) = 1.4483$ (p.u.). The original net-ability, before an attack, of this six-bus system is around 21.2.

Comparison with Other Models

IEEE PES CAMS Task Force on Understanding, Prediction, Mitigation, and Restoration of Cascading Failures has listed a bunch of criteria in comparison of different risk assessment methodologies to power grids [4]. Those criteria include the accuracy of reproduction of real phenomena, the degree of dependency on large

Table 4.5. PTDFs of the six-bus power system

Link	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6
1	0	-0.4706	-0.4026	-0.3149	-0.3217	-0.4064
2	0	-0.3149	-0.2949	-0.5044	-0.2711	-0.2960
3	0	-0.2145	-0.3026	-0.1807	-0.4072	-0.2976
4	0	0.0544	-0.3416	0.0160	-0.1057	-0.1907
5	0	0.3115	0.2154	-0.3790	0.1013	0.2208
6	0	0.0993	-0.0342	0.0292	-0.1927	-0.0266
7	0	0.0642	-0.2422	0.0189	-0.1246	-0.4100
8	0	0.0622	0.2890	0.0183	-0.1207	0.1526
9	0	-0.0077	0.3695	-0.0023	0.0150	-0.3433
10	0	-0.0034	-0.0795	0.1166	-0.1698	-0.0752
11	0	-0.0565	-0.1273	-0.0166	0.1096	-0.2467

volumes of data, the accuracy of modeling of the power system (AC or DC power flow), and so on. From the attack perspective, we will compare the extended model and other models based on those criteria.

From the above discussions, we know the biggest difference between the pure topological models and the extended model is that the former are completely from the network theory without considering the features of power systems, whereas the latter partly root itself in electric circuit theories. For example, the definition of the load of a node/link under the non-recoverable model [8] only considers the degree distribution of nodes/links. If a node/link fails, its load is only redistributed to its neighbors. This model is far from the reality in power transmission systems. In addition, the load definition and redistribution under the recoverable model [24] are related to the shortest paths. This model is closer to the reality than the non-recoverable model, but still does not consider the features of power transmission systems. Compared with the above two representative pure topological models, the power distribution under the extended model is governed by using PTDFs following the basic circuit theories. This means that the extended model is more accurate in representing power distribution in power grids than the purely topological models.

Table 4.6. The summary of different models

Network model	Pure topological models		Extended model [13]	Pure power flow models [10]
	Non-recoverable [8]	Recoverable [24]		
Accuracy	Low	Low	Relatively accurate	Accurate
Information needed	Topology	Topology	Topology & PTDFs	Comprehensive structure & electrical features

On the other side, the pure power-flow models [10] are based on circuit theories, but they are too complex to analyze cascading failures from the attack perspective. First, those models require more information about power grids than other models. They not only need the topological structure of power grids, but more electrical features, e.g. the admittance matrix and voltage distribution. Such information is not easy to be known by attackers. Second, to analyze the vulnerability of power grids, pure power flow models require high computation cost. Sometimes, this kind of analysis is computationally infeasible for a simulator with any fidelity [4]. Meanwhile, the extended model makes several simplifications, with which it is less complex than the pure power flow models and more suitable for cascading failures analysis. In addition, there are an increasing number of researchers, who believe that the extended model is useful in identifying critical components in power grids [35]. The summation of different models is shown in Table 4.6.

4.8.2 Link Attack Strategies

In this section, we introduce the *link attack strategy* (LAS), which is similar to *node attack strategy* (NAS). The links that are initially removed are referred to as *target links* (TLs). Here, we will discuss the load-based LAS, the degree-based LAS, the exhaustive search LAS, the reduced search space LAS and the riskgraph-based LAS.

Load-based and Degree-based Link Attack Strategies

The definition of "degree of a link" is not straight forward. We adopt the definition in [20], in which the degree of a link is the summation of the degrees of the two nodes that this link connects. When an attacker aims to knock down M TLs, the degree-based LAS, denoted by LAS^M_{degree}, is shown as follows,

* LAS^M_{degree}: Select links with the top M largest degree as TLs.

We adopt the link extended betweenness as the load definition of links. The load-based LAS, denoted by LAS^M_{load}, is shown as follows,

* LAS^M_{load}: Choose links with the top M largest load as TLs.

The complexity of the load-based LAS and the degree-based LAS are both 0, because these approaches do not need to launch CFSor before selecting TLs.

Exhaustive Search Link Attack Strategy

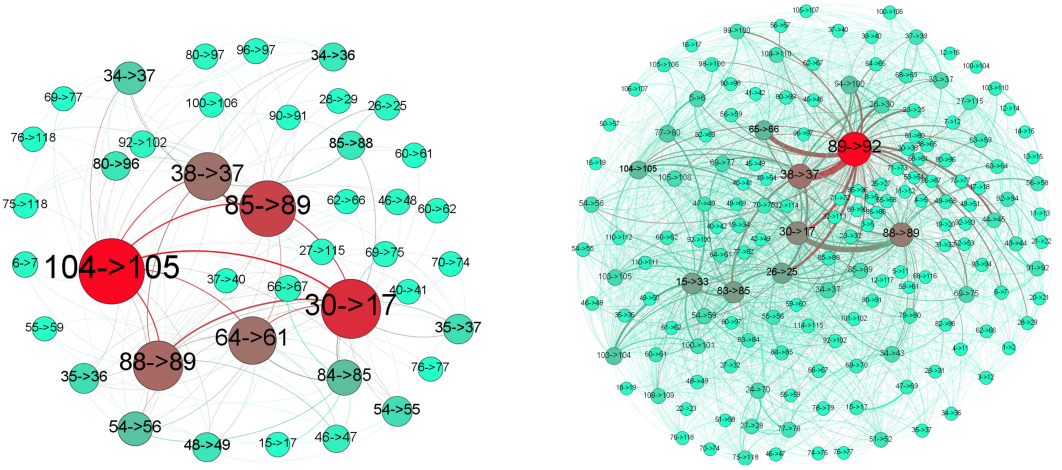
From the attackers' point of view, the strongest LAS is obtained by adopting the exhaustive search, denoted by LAS^M_{ES},

* LAS^M_{ES}: Find the M TLs, whose simultaneous failure yields the largest PoDN under a given α.

The complexity of LAS^M_{ES} is $(N_L)^M$, which is similar to $(N_B)^M$ of NAS^M_{ES}.

Proposed Link Attack Strategies

The proposed iterative procedures (i.e. Procedures 1, 2 and 3 in the main manuscript) can also be adopted to investigate the attack strategy on links. The *reduced search space link attack strategy* or *RSS link attack strategy* in short is denoted by LAS^M_{RSS}. The procedures of selecting TLs for LAS^M_{RSS} are similar to selecting TNs for NAS^M_{RSS}. The changes are to substitute the concepts related to nodes with those of links. The complexity of LAS^M_{RSS} is $M \times (N_L)^2$.

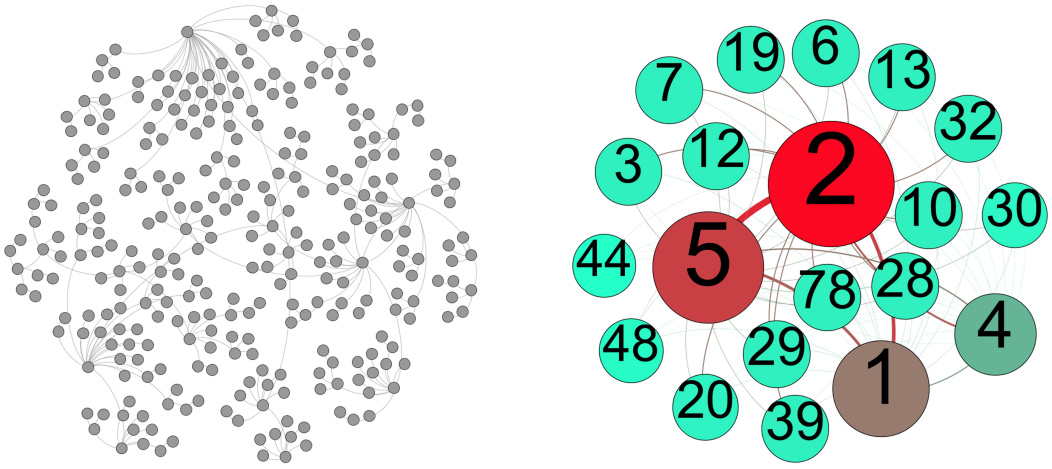


(a) Single Link risk graph (b) Link integrated risk graph

Figure 4.6. The link risk graphs on IEEE 118 bus system.

Similarly, the procedures for finding TLs for NAS^M_{RSS} will keep a record of *round recommended combination set* (RRCS), which can be used to construct *link risk graph* (LRG). The procedure of constructing single LRG is similar to the procedure of building single NRG. Instead of using link indices as labels, the labels of vertices in the LRG are the corresponding directed links, e.g. $30 \rightarrow 80$. Attackers can conduct single LRGs under different system tolerance values and combine them to generate *link integrated risk graph* (LIRG). The LRG and LIRG of IEEE 118 bus system are demonstrated in Fig. 4.6.

When attackers have already obtained the LIRG of a power grid, they can launch attacks based on the LIGR. This attack strategy is called the *riskgraph-based link attack strategy*, denoted be $LAS^M_{riskgraph}$. The procedure to select TLs for $LAS^M_{riskgraph}$ from the LIRG is similar to that of selecting TNs for $NAS^M_{riskgraph}$ from the NIRG. In addition, the real-time complexity of $LAS^M_{riskgraph}$ is 0, because choosing TLs from the LIRG does not require to launch CFSor.



(a) (b)

Figure 4.7. A scale-free synthetic network and its node risk graph

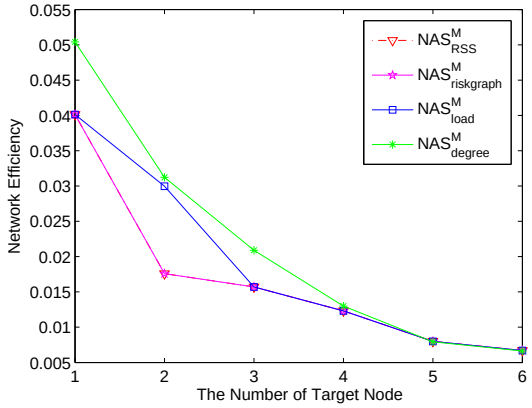


Figure 4.8. The performances versus M among four node attack strategies on the scale-free synthetic network.

4.8.3 Experiments on Synthetic Network

The scale-free complex network, which follows the power-law distribution of nodes and has the topological similarity to real man-made networks, is one of the important types of synthetic network [36]. A 300-node scale-free network was generated as the test benchmark of synthetic network. Its topological structure is shown in Fig. 4.7(a).

From the perspective of attack, the scale-free network is vulnerable to malicious attacks [24]. The proposed concepts and approaches are not restricted to

cascading failure models and types of complex networks. Due to the lack of electric features of the synthetic networks, we could not adopt the extended model and the corresponding measurement metrics in the main manuscript to simulate cascading failures and measure the damage of attacks. Instead, we adopted another cascading failure model, the *recoverable model* [24], to set up the simulations. In addition, the *network efficiency* was adopted as the measure metric. The details of the recoverable model and the network efficiency measure could be found in [9, 24].

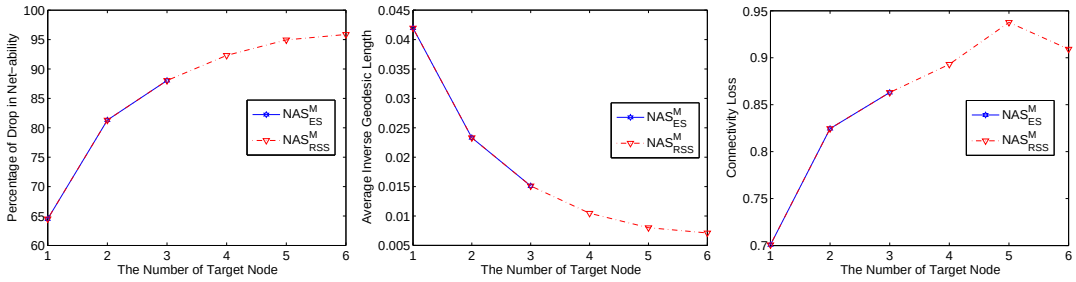
The procedures of conducting NAS^M_{RSS} and constructing risk graphs are similar to that in the main manuscript. The difference is that the system tolerance values for this synthetic network were chosen between 1 and 1.1. Due to the similarity of experiments on nodes and links, we only conducted experiments on node attacks. The node risk graph of the 300-node synthetic network is shown in Fig. 4.7(b). The comparison among NAS^M_{degree}, NAS^M_{load}, $NAS^M_{riskgraph}$ and NAS^M_{RSS} on the synthetic network is shown in Fig. 4.8, in which the horizontal and vertical axes represent the number of target nodes and the network efficiency, respectively. From the perspective of the attack performance measured by network efficiency, the lower the network efficiency is, the stronger the attack is. The dashdotted red-plus curve, the solid magenta-pentagram curve, the solid blue-square curve and the solid green-star curve represent NAS^M_{RSS}, $NAS^M_{riskgraph}$, NAS^M_{load} and NAS^M_{degree}, respectively. In Fig. 4.8, we could make similar observations from the comparison among the four node attack strategies as follows.

- The proposed NAS^M_{RSS} and $NAS^M_{riskgraph}$ are stronger than NAS^M_{degree} and NAS^M_{load}. In addition, the solid magenta-pentagram curve entirely overlaps the dashdotted red-plus curve in Fig. 4.8, which means $NAS^M_{riskgraph}$ and NAS^M_{RSS} have the same performance on this synthetic network.

- As the number of target nodes (i.e. M) increases, the increase of the attack

Table 4.7. Complexity analysis between the exhaustive search and the reduced search space attack strategies

P	$M=1$	$M=2$	$M=3$	$M=4$	$M=5$
16	$\epsilon=0$	$\epsilon=0$	$\epsilon=0.0625$	$\epsilon=0$	$\epsilon=0$
32	$\epsilon=0$	$\epsilon=0$	$\epsilon=0.0625$	$\epsilon=0.0313$	$\epsilon=0$



(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

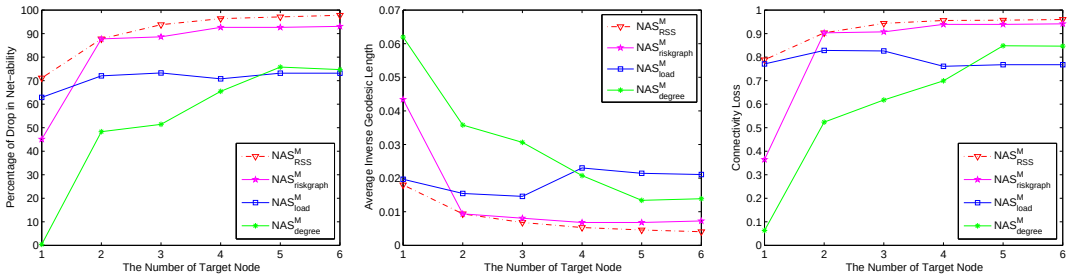
Figure 4.9. The performances versus α among the ES and RSS attack strategies on IEEE 118 bus system.

performance becomes slow and slow. From the attackers' perspective, choosing a few critical nodes will cause serious damage to the scale-free network.

4.8.4 Additional Experiments on Power Grid networks

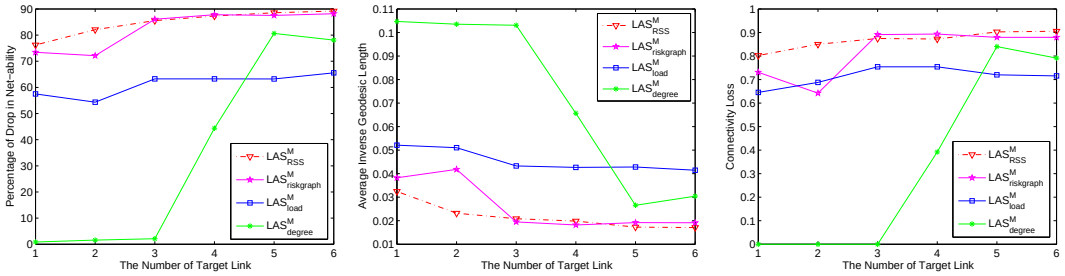
Additional Comparison between the Exhaustive Search NAS and the Reduced Search Space NAS

In this subsection, we continue to compare the proposed NAS^M_{RSS} with NAS^M_{ES} on IEEE 118 bus system. Due to the huge search space of the exhaustive search, we conducted experiments for NAS^M_{ES} with $M \leq 3$. The maximum M for NAS^M_{RSS} is set to 6. The results are shown in Fig. 4.9. Based on the subplots, it is clearly seen that the dashdotted red-plus curves, representing NAS^M_{RSS}, exactly match the blue-square solid curves, representing NAS^M_{ES}, in terms of the three measurement metrics. The match demonstrate that The TNs of NAS^M_{RSS}, when $M = 1, 2, 3$, are the same as those of NAS^M_{ES}, which can be verified from Table I and Table II in the main manuscript. In other words, from the perspective of performance the



(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

Figure 4.10. The performances versus α among four node attack strategies on IEEE 300 bus system



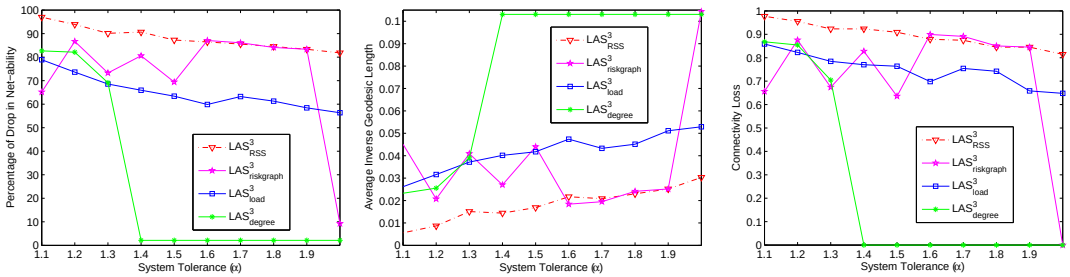
(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

Figure 4.11. The performances versus M among four link attack strategies on IEEE 118 bus system

proposed NAS^M_{RSS} is comparable to NAS^M_{ES}.

In addition, let Set^M_{ES} denote the set of M-node combination, identified as top R strongest attacks by NSA^M_{ES}, and Set^M_{RSS} denotes the set of M-node combinations, identified as top R strongest attacks by NSA^M_{RSS}. We compare Set^M_{ES} with Set^M_{RSS}. We define R' as the number of elements that are in Set^M_{RSS} but not in Set^M_{ES}. In other words, the reduced space search attack strategy would miss R' strong attacks, which would otherwise be found by the exhaustive search attack strategy. Then, we define metric ϵ as,

$$\epsilon = \frac{R'}{R} \tag{4.4}$$



(a) Measured by PoDN (b) Measured by AIGL (c) Measured by CL

Figure 4.12. The performances versus α among four link attack strategies on IEEE 118 bus system

When $\epsilon = 0$, the NSA^M_{RSS} did ont miss any top R strongest attacks. The larger ϵ is, the more attacks are missed by the NSA^M_{RSS}. On IEEE 57 bus system, we obtained ϵ through simulations, when M is set to be 1, 2, 3, 4 and 5, and R is set to be 16 and 32, respectively. The results of ϵ are shown in the following Table 4.7.

We made two observations according to Table 4.7. First, ϵ is small, meaning that the NSA^M_{RSS} captures most strong attacks. Second, ϵ is not necessarily larger for larger M values. Recall that NSA^M_{RSS} is conducted in M rounds, and the top M-node combinations are based on the top $(M-1)$-node combinations. Take $M = 4$ as an example. In third round, assume the strong 3-node combination $\{a, b, c\}$ is missed by the NSA^M_{RSS}. In fourth round, will the NSA^M_{RSS} surely miss the combination $\{a, b, c, d\}$, assuming $\{a, b, c, d\}$ is a strong 4-node combination? The answer is sometimes no. This is because a subset of $\{b, c, d\}$ could be included in Set^3_{RSS}, and $\{a, b, c, d\}$ can still be discovered in round 4.

Table 4.8. Description of IEEE 300 bus system.

Test benchmark	N_B	N_L	N_G	N_D
IEEE 300 Bus System	300	411	69	191

Additional Comparison Among Node Attack Strategies

By adjusting the two parameters, P and R, the proposed node attack strategies can be used to launch attacks on different sizes of power grid networks. Here, we choose a moderate-scale power grid network, IEEE 300 bus system, to test the four node attack strategies, which are NAS^M_{RSS}, $NAS^M_{riskgraph}$, NAS^M_{load} and NAS^M_{degree}. The description of IEEE 300 bus system, included in MATPOWER [17], is shown in Table 4.8. The experiment results are demonstrated in Fig. 4.10. The observations from Fig. 4.10 are consistent with those in the main manuscript.

Comparisons among Link Attack Strategies

In this subsection, comparisons are made among LAS^M_{RSS}, $LAS^M_{riskgraph}$, LAS^M_{load} and LAS^M_{degree} on IEEE 118 bus system. There are two important parameters for comparing different link attack strategies, the number of TNs (M) and the system tolerance (α). Fig. 4.11 demonstrates the change of attack performance against M, while Fig. 4.12 shows the change of attack performance against α. In addition, there are three subplots in each figure, which shows the results evaluated by the three different metrics, *percentage of drop in neb-ablity*, *average inverse geodesic length* and *connectivity loss*. In each subplot, the dash-dotted red-plus curve, solid magenta-pentagram curve, solid blue-square curve and solid green-star curve represent LAS^M_{RSS}, $LAS^M_{riskgraph}$, LAS^M_{load} and LAS^M_{degree}, respectively. According to these figures, we have the following observations and discussions on link attack strategies.

First, the performance of the proposed $LAS^M_{riskgraph}$ is close to that of LAS^M_{RSS}, and much better than those of the LAS^M_{degree} and LAS^M_{load}. In addition, $LAS^M_{riskgraph}$ can represent one of the best performances availably by adopting search-based approaches.

Second, as the number of TLs (i.e. M) increases, fluctuations occur in the performances of $LAS^M_{riskgraph}$, LAS^M_{load} and LAS^M_{degree}. The reason for the latter two is that the metrics, degree and load, only explore the information of grid networks before cascading failures. However, cascading failures are very complex and can not easily predicted by these simple metrics. While, the reason of $LAS^M_{riskgraph}$ is that the construction of link risk graphs only considers the relationship between a pair of links. However, when $M \geq 3$, the TLs from LIRG might not stand for the strongest attacks, therefore the attack performance downgrades a little.

List of References

[1] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.

[2] "The economic impacts of the august 2003 blackout," Feb. 2004, prepared by the Electricity Consumers Resource Council (ELCON).

[3] R. Baldick et. al., "Initial review of methods for cascading failure analysis in electric power transmission systems," in *IEEE power engineering society general meeting*, Pittsburgh, PA, USA, July20-24 2008.

[4] M. Vaiman et. al., "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[5] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, pp. 741–749, 2011.

[6] X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[7] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *Eur. Phys. J. B*, vol. 46, pp. 101–107, 2005.

[8] 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, Dec. 2009.

[9] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in U.S. power grid," in *Proceeding of IEEE Global Telecommunications Conference*, Houston, Texas, USA, Dec.5-9 2011.

[10] Q. Chen and J. D. McCalley, "Identifying high risk N-k contingencies for online security assessment," *IEEE Transactions on Power Systems*, vol. 20, pp. 823–834, May 2005.

[11] G. Chen, Z. Dong, D. J. Hill, G. H. Zhang, and K. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 389, no. 3, pp. 595–603, Feb. 2010.

[12] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 1, 2009.

[13] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, pp. 1334–1340, July 2011.

[14] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, 065102(R), 2002.

[15] Y. Zhu, Y. Sun, and H. He, "Load distribution vector based attack strategies against power grid systems," in *Proceeding of IEEE Global Telecommunications Conference*, Anaheim, CA, USA, Dec.3-7 2012.

[16] NERC standards, "Transmission system standards - normal andemergency conditions." [Online]. Available: www.nerc.com

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

[18] "Platts." [Online]. Available: www.platts.com

[19] Y. Zhu, J. Yan, Y. Sun, and H. He, "Risk-aware vulnerability analysis of electric grids from attacker's perspective," in *Proceeding of IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.

[20] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, no. 5, May 2002.

[21] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the north american power grid," *Phys. Rev. E*, vol. 69, no. 2, Feb. 2004.

[22] M. Bastian, S. Heymann, and M. Jacomy, "Gephi: An open source software for exploring and manipulating networks," in *Proceedings of the Third International ICWSM Conference*, San Jose, California, USA, May17-20 2009.

[23] "Power systems test case archive," University of Washington. [Online]. Available: http://www.ee.washington.edu/research/pstca/

[24] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, no. 4, Apr. 2004.

[25] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, Sept. 2010.

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

[27] D. P. Bertsekas, *Dynamic Programming and Optimal Control*. Athena Scientific, Jan.29 2007.

[28] F. Lewis and D. Liu, *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control*. Wiley-IEEE Press, Dec.26 2012.

[29] H. He, *Self-Adaptive Systems for Machine Intelligence*. Wiley-Interscience, Aug.9 2011.

[30] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 1, pp. 15–32, Jan. 2005.

[31] J. Yan, Y. Zhu, Y. Sun, and H. He, "Revealing temporal features of attacks against smart grid," in *IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.

[32] Q. Chen, C. Jiang, W. Qiu, and J. D. McCalley, "Probability models for estimating the probabilities of cascading outages in high-voltage transmission network," *IEEE Transactions on Power Systems*, vol. 21, no. 3, pp. 1423–1431, Aug. 2006.

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

[34] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control, 2nd Edition*. NY: John Wiley & Sons, 1996.

[35] G. Chen, Z. Dong, D. J. Hill, G. Zhang, and K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," *Physica A*, vol. 389, no. 3, pp. 595–603, Feb. 2010.

[36] A.-L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

CHAPTER 5

Manuscript 4: Joint Substation-Transmission line Vulnerability Assessment against the Smart Grid

Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, and Haibo He

Department of Electrical, Computer, and Biomedical Engineering

University of Rhode Island, Kingston, RI 02881

Manuscript status: in submission to IEEE Transactions on Information Forensics and Security in 2014

Corresponding Author: Yihai Zhu

Kelley Annex, Room A115

4 East Alumni Ave.,

Kingston, RI 02881

Phone:+1-401-874-5846

Email: yhzhu@ele.uri.edu

5.1 Abstract

The smart grids are often run near the operational limits because of increasing electricity demand, where even small disturbances could possibly trigger major blackouts. The *attacks* are the potential threats to trigger large-scale cascading failures in the smart grid. Specifically, the attacks mean to make substations/transmission lines lose functionality by either physical sabotages or cyber attacks. Previously, the attacks are investigated from node-only/link-only perspectives, assuming attacks can only occur on substations/transmission lines. In this work, we introduce the joint-substation-transmission-line perspective, which assumes attacks can happen on substations, transmission lines, or both. The introduced perspective is a nature extension to substation-only and transmission-line-only perspectives. Such extension leads to discovering many joint-substation-transmission-line vulnerabilities. Furthermore, we investigate the joint-substation-transmission-line attack strategies. In particular, we design a new metric, the *component interdependency graph* (CIG), and propose the CIG-based attack strategy. In simulations, we adopt IEEE 30 bus system, IEEE 118 bus system and Bay Area power grid as test benchmarks, and use the extended degree-based and load attack strategies as comparison schemes. The CIG-based attack strategy has stronger attack performance.

5.2 Introduction

The U.S. power grid has been developing over a century and becomes to a extremely complicated system that has more than 55,000 substations and nearly 500,000 kilometers of transmission lines. Such a complex system likely experiences severe blackouts, which cause catastrophe to modern societies. For instance, Northeastern blackout of 2003 left more than 55 million people in dark for days and resulted in estimated 10 billion economic loss [1, 2]. The emergence of the

"Smart Grid", the next-generation power transmission system [3], can significantly increase the risks of system failures caused by errors from computer software and hardware [4], cyber intrusions [5], and so on.

Generally speaking, large-scale blackouts are resulted from the cascading failure in power transmission systems [4, 6]. The triggers of cascading failures are various and mainly include *random causes* and *malicious attacks*. First, there are a wide variety of exogenous causes that can trigger cascading failures. Such causes include natural disasters [7] (e.g., earthquakes, storms, blizzards, tornadoes, etc.), errors from computer hardware and software [4], misoperation from operators, vegetation sagging [1], increasing energy demand [8], and so on. In existing power systems, although the failures resulted from random causes have been considered, major blackouts are still inevitable.

Second, different from random causes, *malicious attacks* can be manipulated. The well-designed attack strategies can choose a few critical components (i.e., substations and transmission lines) as targets. Successfully attacking these targets can trigger large-scale failures and severely weaken power transmission systems [9, 10, 14]. People who want to conduct attacks are referred to as *attackers*, including computer hackers, terrorist groups, disgruntled individuals, or hostile countries. Malicious attacks can be initiated by physical sabotages [20] or cyber intrusions [5, 21]. In reality, physical sabotages includes individual attacks on high-voltage transmission lines [22] and powerful EMP attacks from hostile countries [20]. Cyber intrusions are prevailing in smart grids [5] and can intentionally destroy targets. Examples include "Aurora Generator Test" [23]. Conducted by Department of Homeland Security (DHS) in 2007, this simulated cyber attack successfully damaged a $ 1 million dollar large diesel-electric generator. The destroyed generator is similar to many now in use throughout the U.S., which demonstrates

the high possibility of cyber threats to the U.S. power grid. Although malicious attacks have not yet resulted in large-scale blackouts, such attacks are greatly potential to trigger big events [24].

In this work, we study malicious attacks against the power transmission system. In particular, we introduce a new perspective to investigate the vulnerability of power grids.

In the current literatures [9–11, 14], substations are referred to as *nodes*; transmission lines are referred to as *links*. Attacks against power systems have been mainly investigated from *node-only* perspective [13, 16] and *link-only* perspective [17, 25, 26], which assume attacks occur on nodes and links individually. It is obvious that existing studies miss an important perspective: *joint-node-link*, which assumes attacks can occur on nodes and links concurrently. This perspective is a nature extension of node-only and link-only perspectives and has great impact on investigating power grid vulnerabilities.

The advantages of joint-node-link perspective are threefold. First, such perspective can reveal the complex mechanisms of failure propagation in power systems. In existing major blackout cases [1, 8], tripping of transmission lines can shut down power plants; failures of substations can trip transmission lines. Second, vulnerability analysis from the joint-node-link perspective can discover new vulnerabilities. Finally, from the attack's point of view, the joint-node-link perspective is insightful to find strong attack strategies.

In this work, we introduce the joint-node-link perspective to conduct the vulnerability analysis of power systems. In particular, we have done the following works.

- Adopt the extended model [18] to set up the cascading failure simulator (CFS) that can mimic the failures on both nodes and links.

- Conduct the vulnerability analysis from the joint-node-link perspective, and find extensive number of joint-node-link combinations that can yield severe damage.

- Design a new metric, called *component interdependency graph* (CIG), to reveal the relationship among critical nodes and links from the attack's perspective.

- Propose a novel joint-node-link attack strategy, called the *CIG-based attack strategy*. The proposed scheme can choose both nodes and links as target components (TCs).

- Perform extensive simulations to demonstrate the proposed CIG-based attack strategy. Specifically, we adopt IEEE 30 bus system, IEEE 118 bus system and Bay Area power grid as test benchmarks, and the extended degree-based and load-based attack strategies as comparison schemes. Experiment results show the CIG-based attack strategy has stronger attack performances.

The major **contributions** are (1) revealing many vulnerabilities that are not previously demonstrated; (2) designing a new metric, CIG; (3) proposing the CIG-based joint-node-link attack strategy.

This work is organized as follows. The related work is given in Section 5.3. In Section 5.4, we briefly introduce the system model, including the extended model and the cascading failure simulator. In Section 5.5, we demonstrate joint-node-link vulnerabilities. In Section 5.6, we construct a new metric, called *component interdependency graph* (CIG), and propose the *CIG-based attack strategy*. Section 5.7 includes all experiments and performance comparisons, followed by concluding this work in Section 6.8.

5.3 Related Work

In existing works, investigating attacks on power systems is mainly addressed from three angles: cascading failure models, metrics development, target selection on nodes or links.

Roughly speaking, cascading failure models include three categories, topological models [9, 10, 12, 14], power-flow models [16, 17, 26, 27] and the hybrid model [18]. Although topological models are useful to study new attack strategies [16], these models are far from mimicking power dynamics in power transmission systems, because they largely ignore the electric engineering properties [28]. Power-flow models, including ac and dc models, are accurate to mimic cascading failures. Such models, however, require the detailed information of power systems and need intensive computation [4]. The hybrid model is set up by combining complex network theory and power flows [18]. This model is less complex, as well as needing less information, than power-flow models, and more accurate than topological models. We compare this work with some representative works in Table 5.1. The first three columns show the models using in each work. In this work, we adopt the hybrid model in [18] to study cascading failures.

Many metrics have been developed to help attackers identify target components (i.e., target nodes or target links). Two metrics, degree and load, are predominant [9, 14–16, 16, 29]. They are developed by employing the structure or initial load information of power grids. Complicated metrics include risk if failure (RIF) [10], load distribution vector (LDV) [12], geographic information [13], risk graph [19], etc. Although complicated metrics are useful to find strong attack strategies, they are not prevailingly validated under different models. In Table 5.1, we show the metrics investigated in each work from the fifth column to the twelfth column. In this work, we compare the proposed metric, CIG, with the metrics,

Table 5.1. Summary of typical works in studying attacks on power grids

Reference	Cascading failure models			Metrics								Target components		
	Topological models	Power-flow models	Hybrid models	Random selection	degree	load	RIF	LDV	Geographic information	Risk graph	CIG	Node	Link	Node & link
[9]	✓				✓							✓		
[10]	✓			✓		✓	✓					✓		
[11]	✓			✓	✓	✓						✓		
[12]	✓					✓		✓				✓	✓	
[13]	✓					✓			✓			✓		
[14]	✓			✓	✓	✓						✓		
[15]	✓				✓	✓						✓	✓	
[16]		✓		✓	✓	✓						✓		
[17]		✓		✓									✓	
[18]			✓			✓						✓	✓	
[19]			✓			✓				✓		✓		
Proposed work			✓		✓	✓					✓			✓

degree and load, in terms of studying joint-node-link attack strategies.

As discussed in Introduction, lots of studies focus on node-only investigation [9–11, 13, 14, 29]; many studies highlight link-only investigation [17, 25, 26]; only a few studies discuss the investigation on both nodes and links [12, 15, 18, 30], but individually. It is obvious that existing works are not comprehensive, because they miss an important direction, which is conducting vulnerability analysis from the joint-node-link perspective. The last three columns in Table 5.1 clearly demonstrate one significant difference between this work and existing works.

5.4 System Model

5.4.1 Grid Network

In this work, the grid is represented as a network $\mathcal{H}$, where $\mathcal{H} = \{\mathcal{N}, \mathcal{L}\}$. $\mathcal{N}$ is the set of nodes (i.e., substations); $\mathcal{L}$ is the set of links (i.e., transmission lines). Nodes are divided into three groups, generation nodes (supplying power), demand nodes (delivering power to customers), and transmission nodes. Let $\mathcal{G}$ denote the set of generation nodes ($\mathcal{G} \subseteq \mathcal{N}$); let $\mathcal{D}$ denote the set of demand nodes ($\mathcal{D} \subseteq \mathcal{N}$). Let $K_{\mathcal{N}}$, $K_{\mathcal{L}}$, $K_{\mathcal{G}}$ and $K_{\mathcal{D}}$ represent the number of nodes, links, generator nodes and demand nodes, respectively. In addition, let n_i denote node i ($n_i \in \mathcal{N}$) and l_j denote link j ($l_i \in \mathcal{L}$).

5.4.2 The Extended Model

The hybrid model in [18] is referred to as the *extended model* in this work. This model was originally developed in [18, 31]. Generally speaking, using the extended model to mimic the load distribution in the power grid is conducted as follows.

- *Inputs*: the topology, the admittance matrix of links and the types of nodes. For IEEE standard benchmarks [32], these information is included. For the Bay Area power grid, these information can be estimated from the raw GIS

data (discussed in Section 5.7.1).

- *Outputs*: the extended betweenness and the net-ability. The extended betweenness is used to model the load of nodes/links; the net-ability represents how well the system works to supply power.

We briefly introduce the extended model as follows. For interested readers, more details can be found in [18, 31].

First, power transfer distribution factors (PTDFs) matrix is one of dc power-flow analysis methods [33]. Let $\boldsymbol{F}$ denote the PTDFs matrix, whose size is $K_{\mathcal{L}} \times K_{\mathcal{N}}$. Each element in $\boldsymbol{F}$, e.g., f_{ji}, represents the power change in l_j when a unit power is injected at n_i and withdrew at the reference node [32].

Second, the *extended betweennes* (EB) is developed to model the load of a node/link, which is calculated as follows.

- In power systems, power is transmitted from generation nodes to demand nodes. Therefore, each generation-demand-node pair can cause power change in links. Let g denote a generation node ($g \in \mathcal{G}$); let d denote a demand node ($d \in \mathcal{D}$). Let f_{gd}^{j} denote the power change in l_j (link j) caused by the pair of g and d. f_{gd}^{j} is defined as,

$$f_{gd}^{j} = f_{jg} - f_{jd} \tag{5.1}$$

  where f_{jg} and f_{jd} are the elements in $\boldsymbol{F}$ at l_j row gth column and l_j row dth column, respectively.

- Each link, e.g., l_j, has its own power flow limit, denoted by $P_{l_j}^{max}$. For the pair of g and d, let P_{gd} denote the capacity of power transmission between them. In order to secure all links, P_{gd} is defined as,

$$P_{gd} = \min_{l_j \in \mathcal{L}} \left(\frac{P_{l_j}^{max}}{|f_{gd}^{j}|} \right) \tag{5.2}$$

- The overall power distribution is determined by all generation-demand-node pairs. For a link, e.g., l_j, let EB_{l_j} denote its EB. EB_{l_j} is defined as,

$$EB_{l_i} = max(EB^+(l_i), |EB^-(l_i)|) \tag{5.3}$$

where $EB^+(l_i)$ represents the positive EB of l_i and $EB^-(l_i)$ represents negative EB of l_i,

$$EB^+(l_j) = \sum_{g\in\mathcal{G}} \sum_{d\in\mathcal{D}} P_{gd} f^j_{gd} \qquad \text{if} f^j_{gd} > 0$$
$$EB^-(l_j) = \sum_{g\in\mathcal{G}} \sum_{d\in\mathcal{D}} P_{gd} f^i_{gd} \qquad \text{if} f^j_{gd} < 0$$

For a node, e.g., n_i, let EB_{n_i} denote its EB. EB_{n_i} is defined as,

$$EB_{n_i} = \frac{1}{2} \sum_{g\in\mathcal{G}} \sum_{d\in\mathcal{D}} P_{gd} \sum_{l_j\in\mathcal{L}} |f^j_{gk}|, n_j \neq g \neq k \tag{5.4}$$

EB_{n_i} is half of the summation of power flows in the links connecting n_i.

Finally, the *net-ability* is used to evaluate how well the power system can supply power. Let $E(\mathcal{H})$ denote the net-ability of the power system $\mathcal{H}$. $E(\mathcal{H})$ is defined as [31],

$$E(\mathcal{H}) = \frac{1}{K_\mathcal{G} \times K_\mathcal{D}} \sum_{g\in\mathcal{G}} \sum_{d\in\mathcal{D}} \frac{P_{gd}}{Z_{gd}} \tag{5.5}$$

where Z_{gd} is the electric distance, equivalent to the impedance between the generation node g and the demand node d.

5.4.3 Cascading Failure Simulator

In our previous works [19, 34], we set up *cascading failure simulator* (CFS) for node-only failures in the extended model. In this work, we extend the CFS in [34] to study failures on both nodes and links. The extended CFS is demonstrated in Algorithm 1. We briefly explain it as follows.

1. *Load*: We adopt the EB to model the load of nodes/links. The EB before removals (or attacks) is called the initial load. After the occurrence of removals, the entire grid might be broken into subgrids. We recalculate the EB for all nodes/links in each subgrid separately, and update the load.

Function `CFS(`$\mathcal{H}$, α, RL`)`

Input: Input parameters
$\mathcal{H}$: the Power grid network, with $K_{\mathcal{N}}$ nodes and $K_{\mathcal{L}}$ links
α: system tolerance
RL: the list of target components
Output: $PoDN$, CL
`/* Obtain the initial load for all components */`
Calculate initial extended betweenness for all components in $\mathcal{H}$;
$\mathbf{EB}_{\mathcal{N}}^{init} \leftarrow$ Nodes' initial extended betweenness ;
$\mathbf{EB}_{\mathcal{L}}^{init} \leftarrow$ Links' initial extended betweenness ;
`/* Calculate the capacity for all components */`
$\mathbf{C}_{\mathcal{N}} \leftarrow \alpha \times \mathbf{EB}_{\mathcal{N}}^{init}$;
$\mathbf{C}_{\mathcal{L}} \leftarrow \alpha \times \mathbf{EB}_{\mathcal{L}}^{init}$;
`/* Failed Component List: FCL */`
$FCL \leftarrow RL$;
$overloading \leftarrow 1$;
while $overloading$ **do**
  $overloading \leftarrow 0$;
  $\mathcal{H}^{'} \leftarrow \mathcal{H}$ by removing all components in FCL ;
  Calculate new extended betweenness for all components in $\mathcal{H}^{'}$;
  $\mathbf{EB}_{\mathcal{N}}^{new} \leftarrow$ Nodes' new extended betweenness ;
  $\mathbf{EB}_{\mathcal{L}}^{new} \leftarrow$ Links' new extended betweenness ;
  for $i = 1, ..., K_{\mathcal{N}}$ **do**
    if $\boldsymbol{EB}_{\mathcal{N}}^{new}(i) > \boldsymbol{C}_{\mathcal{N}}(i)$ **then** `/* Node` i `is overloaded. */`
      $overloading \leftarrow 1$;
      $FCL \leftarrow FCL \cup$ node i ;
    end if
  end for
  for $j = 1, ..., K_{\mathcal{L}}$ **do**
    if $\boldsymbol{EB}_{\mathcal{L}}^{new}(j) > \boldsymbol{C}_{\mathcal{L}}(j)$ **then** `/* Link` j `is overloaded. */`
      $overloading \leftarrow 1$;
      $FCL \leftarrow FCL \cup$ link j ;
    end if
  end for
end while
`/* Cascading failures stop and measure the damage. */`
Measure the damage caused by the initial removals in terms of $PoDN$ and CL.
end

Algorithm 1: Cascading Failure Simulator

2. *System Tolerance*: We assume each substation/transmission line has the capacity, i.e., the maximum load it can tolerate [14]. The capacity of a node/link is proportional to its initial load. We introduce α to denote the proportional rate or system tolerance. For simplicity, α is assumed to be the same for all components [9, 14, 15].

3. *Overloading*: In the CFS, we check the overloading round by round. Within each round, we do the following steps. First, update the load for all components. Second, check the overloading for each node/link. If the load of a node/link in this round exceeds its capacity, this node/link is overloaded. If a link is overloaded, remove this link; if a node is overloaded, remove this node and all links connecting this node. Third, if there are not overloaded components in this round, the CFS stops; otherwise, the CFS continues for next round.

5.4.4 Assessment Measures

In this work, we adopt two measures to evaluate the damage caused by the attack. The primary measure is *percentage of drop in net-ability* (PoDN), which is defined as [18],

$$PoDN = \frac{E(\mathcal{H}) - E(\mathcal{H}')}{E(\mathcal{H})} \tag{5.6}$$

where $E(\mathcal{H})$ represents the net-ability before the attack and $E(\mathcal{H}')$ represents the net-ability after the attack. The larger PoDN is, the stronger the attack is.

The secondary measure is *connectivity loss* (CL), which is defined as [11],

$$CL = 1 - \langle \frac{K_{\mathcal{G}}^d}{K_{\mathcal{G}}} \rangle_d \tag{5.7}$$

where $K_{\mathcal{G}}$ is the number of total generation nodes, and $K_{\mathcal{G}}^d$ is the number of generation nodes connecting the demand node d. The averaging, $\langle \bullet \rangle$, is conducted over all remaining demand nodes after cascading failures. CL can evaluate how

Table 5.2. Joint-node-link vulnerability analysis on IEEE 30 bus system

M-component combination	Node-only		Link-only		Joint-node-link	
	# of combinations	% of vulnerabilities	# of combinations	% of vulnerabilities	# of combinations	% of vulnerabilities
$M = 2$	435	18.91%	820	33.13%	**1,230**	**47.95**%
$M = 3$	4,060	7.61%	10,660	18.59%	**42,435**	**73.8**%
$M = 4$	27,405	2.94%	101,270	10.35%	**842,960**	**86.71**%

well demand nodes structurally connect to generation nodes. The larger CL is, the stronger the attack is.

5.4.5 Summary

In this work, attacking/removing a node/link means to disconnect it from the entire grid. Investigating the strength of attacking targets (i.e., nodes, links, or both) is conducted through the CFS by removing targets to trigger cascading failures. The CFS adopts the extended betweenness to represent the load of nodes/links. Cascading failures occur when the load of a node/link exceeds its capacity, which is calculated by multiplying the system tolerance (α) with the initial load of the node/link. When the CFS stops, the damage is evaluated in terms of PoDN and CL.

5.5 Joint-node-link Vulnerability Analysis

5.5.1 Concepts of Combinations and Vulnerabilities

Before demonstrating joint-node-link vulnerabilities, we briefly introduce several concepts as follows.

- A *multiple-component combination* is referred to as a group of nodes, links or both. We conduct vulnerability analysis based on such combinations.

- In simulations, we perform the removals for a multiple-component combination to possibly trigger cascading failures. The *strength* of this combination is referred to as the damage, e.g., measured by PoDN in Equ. 5.6, after the cascading failure.

- The vulnerability of the power grid has broad meanings. In particular, we define *vulnerabilities* as the multiple-component combinations that can yield large strength.

- *Node-only vulnerabilities* are referred to as the node-only combinations with large strengths.

- *Link-only vulnerabilities* are referred to as the link-only combinations with large strengths.

- *Joint-node-link vulnerabilities* are referred to as the joint-node-link combinations with large strengths.

5.5.2 Demonstration of Joint-node-link Vulnerabilities

We adopt IEEE 30 bus system [32] as the test benchmark for demonstration. This power system consists of 30 nodes (i.e., $K_{\mathcal{N}} = 30$) and 41 links (i.e., $K_{\mathcal{L}} = 41$). There are in total 71 power network components (i.e., nodes and links). We label the nodes from n_1 to n_{30} and the links l_1 to l_{41} for discussion.

For demonstration, referring to the combination consisting of M components, there are in total $\binom{K_{\mathcal{N}}+K_{\mathcal{L}}}{M}$ M-component combinations. We divide these combinations into three categories as follows.

- *Node-only combination*: The combination consists of nodes only. There are in total $\binom{K_{\mathcal{N}}}{M}$ such node-only combinations.

- *Link-only combination*: The combination consists of links only. There are in total $\binom{K_{\mathcal{L}}}{M}$ such link-only combinations.

- *Joint-node-link combination*: The combination includes at least one node and at least one link. In other words, except node-only and link-only com-

Table 5.3. Top Ten strongest combinations in IEEE 30 bus system

Index	Two-component	Three-component	Four-component
1	n_6,l_{37}	l_6,l_{22},l_{29}	n_5,n_{12},n_{21},l_3
2	n_6,l_{38}	n_5,n_6,l_{37}	n_5,n_{12},l_3,l_{28}
3	n_5,n_6	n_5,n_6,l_{38}	n_5,n_{18},l_6,l_{29}
4	n_6,n_7	n_6,n_7,l_{37}	n_5,n_{21},l_6,l_{22}
5	n_6,l_5	n_6,n_7,l_{38}	n_7,n_{12},l_3,l_{29}
6	n_6,l_8	n_6,l_5,l_{37}	n_9,n_{13},n_{30},l_2
7	n_6,l_{39}	n_6,l_5,l_{38}	n_9,n_{30},l_2,l_{16}
8	l_6,l_{29}	n_6,l_8,l_{37}	n_{11},l_6,l_{22},l_{29}
9	n_6,n_9	n_6,l_8,l_{38}	n_{12},n_{21},l_3,l_5
10	n_6,n_{11}	n_6,n_9,l_{37}	n_{12},n_{21},l_3,l_8

binations, the remaining combinations are the joint-node-link combinations. There are in total $\binom{K_{\mathcal{N}}+K_{\mathcal{L}}}{M}-\binom{K_{\mathcal{N}}}{M}-\binom{K_{\mathcal{L}}}{M}$ such joint-node-link combinations.

In particular, we study all two-component, three-component and four-component combinations, i.e., $M = 2, 3, 4$. Take $M = 2$ as an example. In IEEE 30 bus system, there are in total $\binom{71}{2}$ = 2,485 two-component combinations. $\binom{30}{2}$ = 435 of them are node-only combinations; $\binom{41}{2}$ = 820 of them are link-only combinations; the reminding 1,230 of them are joint-node-link combinations.

Furthermore, for each two-component combination, we remove these two components in the CFS to possibly trigger cascading failures. When the CFS stop, the strength is evaluated in terms of PoDN. We introduce the threshold η to quantify the strong attack. Specifically, when $PoDN \geq \eta$, the multiple-component combination yields strong attack performance. We are interesting in these combinations yielding strengths. Numerically, we set η to be 0.2 (20% drop in net-ability is an important sign of system failure [30]). Among all 2,485 two-component combinations, there are 1,606 strong attacks, where joint-node-link vulnerabilities account for 47.95%, node-only vulnerabilities account for 18.91%, and link-only vulnerabilities account for 33.13%.

We conduct similar study for all three-component combinations and four-

component combinations, respectively. The analytical results are showed in Table 5.2. In addition, in Table 5.3 we show these combinations that yield top ten largest PoDN values. These combinations represent the strongest attack performances. Based on Tables 5.2 and 5.3, we have the following observations regarding joint-node-link vulnerability analysis.

- The joint-node-link perspective can significantly enlarge the number of multiple-component combinations. In Table 5.2, it is apparent that the number of joint-node-link combinations is much larger than those of node-only combinations and link-only combinations. For instance, when $M = 4$, there are 842,960 joint-node-link combinations. This number is much larger than 27,405 node-only combinations and 101,270 link-only combinations.

- Joint-node-link vulnerabilities contribute to a big portion of entire vulnerabilities. Seen from Table 5.2, joint-node-link vulnerabilities account for the biggest portion and increase sharply, from 47.95% at $M = 2$ to 86.71% at $M = 4$.

- Joint-node-link combinations can yield top strongest strengths. In Table 5.3, for instance, 6 out of 10 two-component combinations, 9 out of 10 three-component combinations and all 10 four-component combinations consist of both nodes and links. In other words, joint-node-link combinations can yield large strengths, even larger than those of the strongest node-only and link-only combinations.

In summary, joint-node-link combinations are of importance to investigate vulnerabilities and attack strategies in power transmission systems.

Input: $\mathcal{H} = \{\mathcal{N}, \mathcal{L}\}$, α, P, and Q
$Set_{CNs} \leftarrow \emptyset$, $Set_{CLs} \leftarrow \emptyset$
$Set^1_{RCC} \leftarrow \emptyset$
$\mathbf{x}_i \leftarrow 0$, $1 \leq i \leq K_{\mathcal{N}}$
$\mathbf{y}_j \leftarrow 0$, $1 \leq j \leq K_{\mathcal{L}}$
for $i = 1, ..., K_{\mathcal{N}}$ **do**
  $PoDN$ = CFS($\mathcal{G}$, α, RL = [node i])
  $\mathbf{x}_i = PoDN$
end
for $j = 1, ..., K_{\mathcal{L}}$ **do**
  $PoDN$ = CFS($\mathcal{H}$, α, RL = [link j])
  $\mathbf{y}_j = PoDN$
end
$\mathcal{N}^{'} \leftarrow$ sort $\mathcal{N}$ descendingly according to $\mathbf{x}$
$\mathcal{L}^{'} \leftarrow$ sort $\mathcal{L}$ descendingly according to $\mathbf{y}$
$Set_{CNs} \leftarrow$ first P nodes in $\mathcal{N}^{'}$
$Set_{CLs} \leftarrow$ first P links in $\mathcal{L}^{'}$
$Set^1_{RCC} \leftarrow$ first Q nodes in $\mathcal{N}^{'} \cup$ first Q links in $\mathcal{L}^{'}$

Algorithm 2: Iteration initialization

5.6 Joint-node-link Attack Strategy

In this section, we introduce joint-node-link attack strategies, which are referred to as the methods that can select both nodes and links together as *target components* (TCs). In particular, we design a new metric, called the *component interdependency graph* (CIG), and propose the *joint-node-link attack strategy*.

We introduce the design of CIG in Section 5.6.1 and the CIG-based joint-node-link attack strategy in Section 5.6.2.In Section 5.6.3 we extend existing load-based and degree-based node-only/link-only attack strategies to the load-based/degree-based joint-node-link attack strategies.

5.6.1 Introduction to Component Interdependency Graph

In our previous works [19, 34], we introduced the metric, risk graph (RG), which could be adopted to design strong node-only/link-only attack strategies. Previously, RGs of nodes and links were constructed separately. These RGs cannot accurately reveal the relationship among nodes and links in terms of finding joint-

Input: $\mathcal{H} = \{\mathcal{N}, \mathcal{L}\}$, α, P, Q, Set_{CNs}, Set_{CLs}, and Set_{RCC}^{m-1}
$Set_{RCC}^{m} \leftarrow \emptyset$
`/* Temporary combination set` Set_{tmp}`.` `*/`
$Set_{tmp} \leftarrow \emptyset$
for $i = 1, ..., m \times Q$ **do**
  $RCC_i \leftarrow$ the i^{th} combination in Set_{RCC}^{m-1}
  for $j = 1, ..., P$ **do**
    $cn_j \leftarrow$ the j^{th} candidate node in Set_{CNs}
    `/* Obtain a new component combination */`
    $newCombination \leftarrow RCC_i \cup cn_j$
    $Set_{tmp} \leftarrow Set_{tmp} \cup newCombination$
  end
  for $j = 1, ..., P$ **do**
    $cl_j \leftarrow$ the j^{th} candidate link in Set_{CLs}
    `/* Obtain a new component combination */`
    $newCombination \leftarrow RCC_i \cup cl_j$
    $Set_{tmp} \leftarrow Set_{tmp} \cup newCombination$
  end
end
`/* There are` $m \times Q \times 2P$ `new combinations in` Set_{tmp}`.` `*/`
$\mathbf{z}_o \leftarrow 0$, $1 \leq o \leq m \times Q \times 2P$
for $o = 1, ..., m \times Q \times 2P$ **do**
  $RL \leftarrow$ the o^{th} combination in Set_{tmp}
  $PoDN =$ CFS($\mathcal{H}$, α, RL)
  $\mathbf{z}_j = PoDN$
end
$Set_{tmp}^{'} \leftarrow$ sort Set_{tmp} descendingly according to $\mathbf{z}$
`/* Determine` $m+1$ `groups for` Set_{RCC}^{m}`.` `*/`
for $k = 1, ..., m + 1$ **do**
  $Set_{RCC}^{m} \leftarrow Set_{RCC}^{m} \cup$ first Q combinations in $Set_{tmp}^{'}$, each of which consists of $k - 1$ nodes and $m - k + 1$ links.
end
Finally, Set_{RCC}^{m} includes $(m + 1) \times P$ combinations.

Algorithm 3: Find Set_{RCC}^{m} under given Set_{RCC}^{m-1} $(2 \leq m \leq M)$

node-link combinations with strong strengths. In this work, we generalize the idea of RG to the idea of CIG for specifically investigating the joint-node-link attack strategy.

Iterative Procedure

The iterative procedure in [34] is very useful to obtain node-only/link-only combinations that can yield strong strengths. This rationale can be generalized to obtain joint-node-link combinations that can yield strong strengths. Briefly speaking, we make two modifications. First, we extend the procedure of finding node-only/link-only combinations to obtain joint-node-link combinations. Second, we change the conditions to keep the required multiple-component combinations. The new conditions are (1) the strengths of the kept combinations are as large as possible, (2) the number of links in final combinations should be equal to that of nodes, the goal of which is to balance numbers of links and nodes.

The modified procedure is presented in Algorithms 2 and 3. In particular, Algorithm 2 is to initialize the iteration; Algorithm 3 shows the details of one-round iteration. Introduction of the iterative procedure is given as follows.

- Suppose the power network has $K_{\mathcal{N}}$ nodes and $K_{\mathcal{L}}$ links, where there are in total $K_{\mathcal{N}} + K_{\mathcal{L}}$ grid components.

- Suppose the iterative procedure has M rounds, including an initial round (i.e., 1^{st} round) and $M-1$ iteration rounds (i.e., from the 2^{nd} round to the M^{th} round). In each round, the task is to choose the multiple-component combinations that meet the two aforementioned conditions. The chosen combinations are referred to as *round chosen combination set* (RCCS), denoted by Set_{RCC}. The combinations chosen in each round, e.g., the m^{th} round ($1 \leq m \leq M$), is denoted by Set^{m}_{RCC}.

Table 5.4. An realization of RCCS on IEEE 30 bus system

Index	Set^1_{RCC}	Set^2_{RCC}	Set^3_{RCC}	Set^4_{RCC}	Set^5_{RCC}	Set^6_{RCC}
1	n_6	n_6,n_7	n_6,n_7,n_9	n_5,n_6,n_7,n_9	n_5,n_6,n_7,n_9,n_{11}	n_3,n_6,n_7,n_9,n_{11},n_{18}
2	n_9	n_5,n_6	n_5,n_6,n_7	n_6,n_7,n_9,n_{11}	n_6,n_7,n_9,n_{11},n_{18}	n_3,n_5,n_6,n_7,n_9,n_{18}
3	n_{10}	n_6,n_9	n_6,n_7,n_{11}	n_5,n_6,n_7,n_{11}	n_5,n_6,n_7,n_9,n_{18}	n_3,n_5,n_6,n_7,n_{11},n_{18}
4	n_{15}	n_6,n_{21}	n_5,n_6,n_9	n_5,n_6,n_9,n_{11}	n_5,n_6,n_7,n_{11},n_{18}	n_5,n_6,n_7,n_9,n_{11},n_{18}
5	l_6	n_6,l_{37}	n_6,n_7,l_{37}	n_6,n_7,n_9,l_{37}	n_5,n_6,n_7,n_9,l_{37}	n_5,n_6,n_7,n_9,n_{11},l_{37}
6	l_{11}	n_6,l_6	n_5,n_6,l_{37}	n_5,n_6,n_7,l_{37}	n_6,n_7,n_9,n_{11},l_{37}	n_5,n_6,n_7,n_9,n_{11},l_6
7	l_{14}	n_6,l_{11}	n_6,n_9,l_{37}	n_6,n_7,n_{11},l_{37}	n_5,n_6,n_7,n_{11},l_{37}	n_5,n_6,n_7,n_9,n_{11},l_{11}
8	l_3	n_6,l_{14}	n_6,n_{21},l_{37}	n_5,n_6,n_9,l_{37}	n_5,n_6,n_9,n_{11},l_{37}	n_5,n_6,n_7,n_9,n_{11},l_{14}
9		l_6,l_{29}	n_6,l_6,l_{37}	n_6,n_7,l_6,l_{37}	n_6,n_7,n_9,l_6,l_{37}	n_5,n_6,n_7,n_9,l_6,l_{37}
10		l_3,l_{11}	n_6,l_{11},l_{37}	n_6,n_7,l_{11},l_{37}	n_6,n_7,n_9,l_{11},l_{37}	n_5,n_6,n_7,n_9,l_{11},l_{37}
11		l_3,l_{14}	n_6,l_{14},l_{37}	n_6,n_7,l_{14},l_{37}	n_6,n_7,n_9,l_{14},l_{37}	n_5,n_6,n_7,n_9,l_{14},l_{37}
12		l_6,l_{36}	n_6,l_3,l_{37}	n_6,n_7,l_3,l_{37}	n_6,n_7,n_9,l_3,l_{37}	n_5,n_6,n_7,n_9,l_3,l_{37}
13			l_6,l_{22},l_{29}	n_{11},l_6,l_{22},l_{29}	n_6,n_7,l_6,l_{11},l_{37}	n_6,n_7,n_9,l_6,l_{11},l_{37}
14			l_6,l_{29},l_{35}	n_6,l_6,l_{11},l_{37}	n_6,n_7,l_6,l_{14},l_{37}	n_6,n_7,n_9,l_6,l_{14},l_{37}
15			l_6,l_{29},l_{32}	n_6,l_6,l_{14},l_{37}	n_6,n_7,l_3,l_6,l_{37}	n_6,n_7,n_9,l_3,l_6,l_{37}
16			l_6,l_{26},l_{29}	n_6,l_3,l_6,l_{37}	n_6,n_7,l_6,l_{29},l_{37}	n_6,n_7,n_9,l_6,l_{29},l_{37}
17				l_6,l_{19},l_{22},l_{29}	n_6,l_6,l_{11},l_{14},l_{37}	n_6,n_7,l_6,l_{11},l_{14},l_{37}
18				l_6,l_{22},l_{29},l_{35}	n_6,l_3,l_6,l_{11},l_{37}	n_6,n_7,l_3,l_6,l_{11},l_{37}
19				l_6,l_{16},l_{29},l_{35}	n_6,l_6,l_{11},l_{29},l_{37}	n_6,n_7,l_6,l_{11},l_{29},l_{37}
20				l_6,l_{26},l_{29},l_{35}	n_6,l_6,l_{11},l_{28},l_{37}	n_6,n_7,l_6,l_{11},l_{28},l_{37}
21					l_6,l_{16},l_{29},l_{35},l_{37}	n_{13},l_6,l_{16},l_{29},l_{35},l_{37}
22					l_1,l_6,l_{22},l_{29},l_{35}	n_{11},l_6,l_{16},l_{29},l_{35},l_{37}
23					l_3,l_6,l_{16},l_{29},l_{35}	n_{29},l_3,l_6,l_{16},l_{29},l_{35}
24					l_6,l_{16},l_{29},l_{35},l_{41}	n_6,l_3,l_6,l_{11},l_{14},l_{37}
25						l_6,l_{16},l_{29},l_{35},l_{37},l_{41}
26						l_6,l_{16},l_{26},l_{29},l_{35},l_{37}
27						l_3,l_6,l_{16},l_{28},l_{29},l_{35}
28						l_3,l_6,l_7,l_{16},l_{29},l_{35}

- In the 1^{st} round, the procedure is initialized, which is shown in Algorithm 2. The initialization process is conducted as follows. First, set up the system tolerance α and conduct all one-node and one-link attacks. Second, among all one-node attacks, select P nodes with top largest attack strengths as candidate nodes, denoted by Set_{CNs}; among all one-link attacks, select P links with top largest strengths as candidate links, denoted by Set_{CLs}. (Briefly speaking, we select these critical nodes and links as candidate nodes and links.) Finally, we determine Set^1_{RCC} by selecting Q nodes with top largest attack strengths among all nodes, as well as selecting Q links similarly.

- In the following each found, e.g., the m^{th} round, Set^m_{RCC} is determined, which

is shown in Algorithm 3. In particular, Set^m_{RCC} includes $(m+1)$ groups, and each group includes Q multiple-component combinations. In other words, there are in total $Q \times (m+1)$ combinations in Set^m_{RCC}. In the k^{th} group $(1 \leq k \leq m+1)$, the combination consists of $k-1$ nodes and $m-k+1$ links. For instance, when $m=4$ and $k=2$, Set^4_{RCC} has 5 groups, and the combination in the 2^{nd} group consists of 2 nodes and 2 links. The rationale behind this design is to ensure that the number of links is the same as that of nodes in Set^m_{RCC}.

- When the iterative procedure stops, the determined Set_{RCC} includes $\{Set^1_{RCC}, Set^2_{RCC}, ..., Set^M_{RCC}\}$.

In particular, based on the aforementioned discussions, the proposed iterative procedure in this work is different from that in [34] in two aspects. First, we initialize the iteration, in the first round, by selecting both candidate nodes and candidate links, denoted by Set_{CNs} and Set_{CLs}, respectively. Also, Set^1_{RCC} includes equal numbers of first round chosen nodes and links. Previously, we only considered the scenario of node-only/link-only combinations [34]. Second, we keep $Q \times (m+1)$ combinations in each iteration round, which increases as m increases. Nodes and links can cause different damages to the power system, and the new procedure can balance the numbers of links and nodes appearing in Set^m_{RCC}. In [34], however, we kept a constant number (i.e., Q) of node-only/link-only combinations in each iteration round.

In Table 5.4, we present a realization of RCCS (i.e., Set_{RCC}) on IEEE 30 bus system, where $\alpha = 1.5$, $M = 6$, $P = 30$ and $Q = 4$. Take $m = 3$ (the third found) as an example. Set^3_{RCC} includes 4 (i.e., $m+1$) groups, and each group has 4 (i.e., Q) three-component combinations. In the first group, the combination consists of 3 nodes; in the second group, the combination consists of 2 nodes and 1 link; in the

third group, the combination consists of 1 node and 2 links; in the fourth group, the combination consists of 3 links.

There are four parameters, α, M, P and Q. First, α represents the system tolerance. This parameter has big effect on the nodes and links kept in Table 5.4, which will be discussed late in Section 5.6.1. Second, M represents the maximum number of nodes/links that the attacker wants to remove from the power system. Because of the orderly network structure, the power system has critical grid components, removing a few of which can collapse the entire grid [35]. Therefore, in practical attack scenario, M can be a small number, e.g., $M = 6$ in Table 5.4. Finally, P and Q are of importance to limit the search space in Algorithm 3. For P, its value is determined according to the scale of power systems (i.e., $K_{\mathcal{N}}$). For the small-scale system, P can be set to $K_{\mathcal{N}}$. For the large-scale grid, P can be a number that is much smaller than $K_{\mathcal{N}}$. That is to select critical nodes and links as candidate nodes and links. For Q, its value is not necessary to be large, e.g., $Q = 4$ in Table 5.4, because choosing a few strongest multiple-component combinations within each iteration round are enough to find strong attacks.

Construction of Component Interdependency Graph

With the availability of RCCS (a realization is shown in Table 5.4), we can construct a new metric, *component interdependency graph* (CIG). The procedure of constructing CIG is similar to that of constructing RG in [34]. We briefly introduce the construction idea. For interesting readers, the details are included in [19, 34].

- The nodes and links in Set_{RCC} (or Table 5.4) become the vertexes individually in CIG. For the repetitive ones, merge them together as one vertex. Assign the weight for each vertex, referred to as *vertex occurrence frequency* (VOF). The VOF value is the number of times that the vertex appears in Set_{RCC}.

- Add an edge between each pair of vertexes in CIG and assign the weight for each edge, referred to as *edge occurrence frequency* (EOF). Initially, EOF value is 0.

- Examine each combination in Set_{RCC} and update EOF. Take the combination $\{n_6, n_7, l_{37}\}$ in Table 5.4 as an example. Assign the overall weight of the combination as 1, and add the EOF of three edges by $\frac{1}{3}$, which are $edge_{n_6-n_7}$, $edge_{n_6-l_{37}}$ and $edge_{n_7-l_{37}}$.

- Delete the edges, whose EOF value equals to 0, and obtain CIG.

Construction of CIG highly depends on RCCS. For a given power system, the system tolerance α is the major factor of generating RCCS, as well as constructing CIG. In other words, CIG is sensitive to α. In reality, however, system tolerance values are rarely known by attackers [15]. In existing studies [9, 14], researchers usually assume that all components have the same α, and choose representative values.

In this work, we choose three representative α values, 1.2, 1.5 and 1.8, to simulate the "low", "middle" and "high" system tolerance scenarios, respectively. Under each chosen system tolerance, we construct one CIG. Then, we merge the three CIGs together to generate *integrated component interdependency graph* (ICIG). Compared with single CIG, ICIG is more robust and representative. The ICIG on IEEE 30 bus system is demonstrated in Fig. 5.1, where sizes and colors of vertices (edges) are determined by VOF (EOF) values. For simplification of demonstration, we use the index of a node to represent the node and two endpoints of a link to represent the link. In Fig. 5.1, for instance, n_6 is shown as 6 and l_{29} is shown as 21-22.

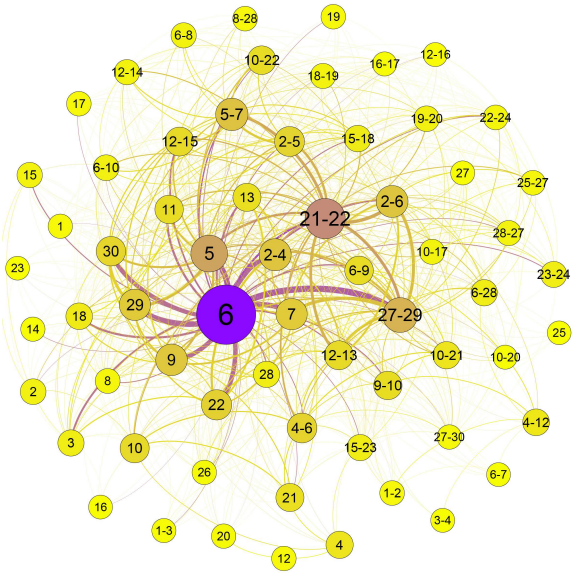


Figure 5.1. The integrated component interdependency graph of IEEE 30 bus system

5.6.2 CIG-based Attack Strategy

In ICIG, the criticality of single node/link is determined by the VOF, highlighted by the size and color of the vertex in Fig. 5.1. The bigger and darker a vertex is, the more critical the corresponding node/link is. The relationship of a pair of components is decided by the EOF, highlighted by the size and color of the edges. The wider and darker an edge is, the higher possibility this pair of components can yield large strength against the power system. Such information is useful to design strong attack strategy.

Based on ICIG, we propose the *CIG-based attack strategy*, denoted by AS_{CIG}. Suppose the attacker wants to choose U nodes and V links as target components (TCs). U and V are both integers and $U + V \geq 1$, where $0 \leq U \leq M$ and $0 \leq V \leq M$. (Recall M is one of parameters to construct CIG in Section 5.6.1.) AS_{CIG} is conducted as follows.

- Construct ICIG for a power system. M is chosen to be larger than both U and V.

- If $U + V = 1$, a TC is chosen from ICIG. There are two cases, $U = 1$ & $V = 0$ (i.e., single-node attack) or $U = 0$ & $V = 1$ (i.e., single-link attack). For the first case, the node with the largest VOF value in ICIG is selected as target node (TN). For the second case, the link with the largest VOF in ICIG is selected as target link (TL).

- If $U + V > 1$, multiple TCs are chosen from ICIG. These TCs are determined as follows. First, find all multiple-component combinations in ICIG. Each combination consists of U nodes and V links, and each pair of these components should have a direct edge. Second, for each combination, the summation of EOF on all edges is computed. The combination that has the largest EOF summation is chosen as TCs.

According to Fig. 5.1, for instance, the attacker can choose node 6 as TC for single-node attack and link 21-22 as TC for single-link attack. If the attacker wants to two TCs, a node and a link, node 6 and link 21-22 are together chosen as TCs.

The rationale behind choosing single TC or multiple TCs is different. When launching single-component attack, the TC is recommended by using VOF, similar to the functionality of the metrics, degree and load. When launching multiple-TC attack, these TCs are determined by EOF, because these TCs are tightly connected in ICIG, which means their pairs appear most frequently in RCCS (or in Table 5.4).

5.6.3 Degree-based and load-based Attack Strategies

In existing works [14–16, 36], two metrics, degree and load, have been prevailingly studied for the node-only/link-only attack strategies. In this section, we extend existing load-based and degree-based node-only/link-link attack strategies

to load-based and degree-based joint-node-link attack strategies.

In power networks, "node degree" is defined as the number of links connecting with the node [14]. Definition of "link degree" is related to the definition of "node degree" [15]. Specifically, the degree of a link is defined as the summation of two nodes' degrees that this link connects. Let AS_{degree} denote the *degree-based attack strategy*. When the attacker wants to choose U nodes and V links as TCs, AS_{degree} is conducted as follows,

- Sort all nodes descendingly according to their degrees, and select top U nodes; sort all links descendingly according to their degrees, and select top V links.

In this work, we adopt the extended betweenness as the load definition of nodes/links (discussed in Section 5.4). Let AS_{load} denote the *load-based attack strategy*. AS_{load} is conducted similarly as AS_{degree}, by replacing "degree" with "load".

Although we mainly discuss the joint-node-link attack strategy in this work, these three aforementioned attack strategies, i.e., AS_{CIG}, AS_{degree} and AS_{load}, can be specialized to node-only/link-only attack strategies as follows.

- When $V = 0$, the joint-node-link attack strategy turns to the node-only attack strategy.

- When $U = 0$, the joint-node-link attack strategy turns to the link-only attack strategy.

5.7 Performance Evaluations and Discussions

In this work, we conduct all simulations in MATLAB environment. Three power systems are employed as test benchmarks, IEEE 30 bus system, IEEE 118 bus system and Bay Area power grid in California, United States. The first two are

included in MATPOWER [32]; the last one is the power system that are currently in use. We purchased the raw power system data from Platts [37]. The brief description of three test benchmarks is given in Table 5.5.

Table 5.5. Brief description of test benchmarks

Test Benchmarks	$K_{\mathcal{N}}$	$K_{\mathcal{L}}$	$K_{\mathcal{S}}$	$K_{\mathcal{D}}$
IEEE 30 bus system	30	41	6	20
IEEE 118 bus system	118	179	54	99
Bay Area power grid	603	846	146	184

5.7.1 Construction of Bay Area Power Grid

In this section, we introduce the construction of Bay Area power grid from the raw data. The original data format is provided with GIS shapefiles, including substation layer, transmission line layer, generator unit layer and power plant layer. Generally speaking, building the grid from the raw GIS data includes three aspects, (1) chipping the grid raw data, (2) constructing the grid topology, (3) identifying the electric features, such as substation types and transmission line reactance. We briefly introduce the construction of Bay Area power grid according to [38] and [39] as follows.

- **Chipping the grid raw data**: Bay Area power grid data is chipped from the entire North American power network in ArcGIS desktop [40].

- **Building the grid topology**: The topology of Bay Area power grid is constructed mainly according to raw data in the transmission line layer. Transmission lines are viewed as links; the endpoints of transmission lines are viewed as nodes. The raw power network include one large-scale network and a few small-scale networks. After manually eliminating the small-scale ones, Bay Area power grid topology is set up.

- **Determining electric features**: In this work, we adopt the extended model to set up CFS. This model needs the electric information about substation types (i.e., generation substation, demand substation and transmission substation) and the reactance of transmission lines. We estimate those information as follows. First, the type of nodes is determined by exploiting the information in raw data. According to the explanations from Platts [39], two types of nodes are identified to be generation nodes, (1) the node is associated with a 10 KV (kilovolt) transmission line, (2) the node is geographically close to a power plant (within 1 KM in this work). According to the introduction of North American power transmission system [38], the nodes, whose maximum voltage is less or equal to 69 KV but more than 0 KV, are considered to be demand nodes. Other nodes are viewed as transmission nodes. Second, the reactance of a transmission line is determined by its physical properties. There is a linear relation between the length and the reactance. According to [41], we set the ratio between the length and the reactance as $0.4\Omega/KM$(ohm/kilometer). That is, the reactance of a 20 KM length transmission line is 8Ω. With the availability of the length of transmission lines in raw data, we can simply estimate the reactance.

In summary, Bay Area power grid has 846 transmission lines and 603 nodes, where there are 146 generation nodes and 184 demand nodes.

5.7.2 Comparison Set-up

When discussing the joint-node-link attack strategy, a question comes out naturally that how to balance between choosing nodes and links as TCs. In reality, attacking substations and transmission lines are both highly possible [42, 43]. In this work, it is not our focus to specifically discuss how hard for attackers to fail a substation or a transmission line. Instead, we conduct the comparison as follows.

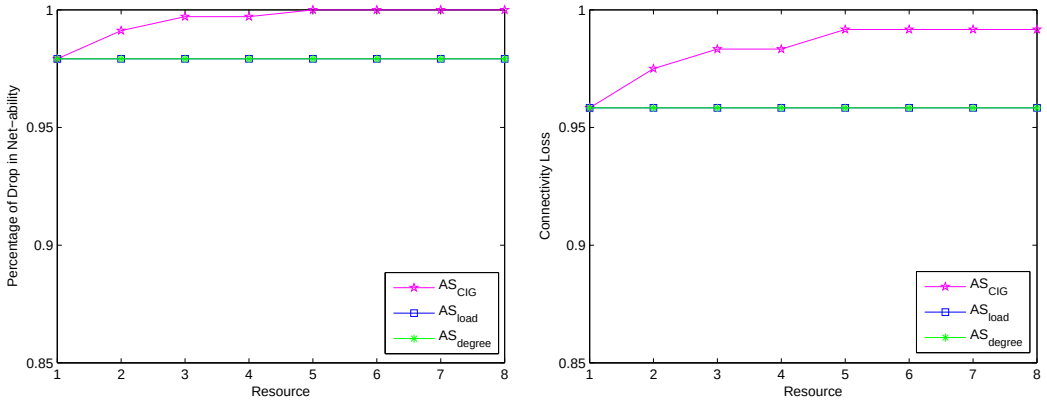
- It is a fact that attacking substations or transmission lines both needs the *resource* from the attacker. Specifically, we assume that attacking a substation needs γ_1 units resource and attacking a transmission line needs γ_2 units resource.

- Also, the attacker has the overall *resource* to launch attacks. Suppose the attacker has in total Γ units resource. In particular, we assume that γ_1, γ_1 and Γ are all integers, where $1 \leq \gamma_1, \gamma_2 \leq \Gamma$.

- Having Γ units resource, the attacker can make different decisions, depending on how to use the resource. For instance, the attacker can fully or partially utilize these Γ units resource, aiming to obtain the maximum damage to the power system. When the attacker wants to choose U nodes and V links as TCs under given γ_1, γ_2 and Γ, pairs of U and V are calculated as follows.

$$\begin{aligned} &Find: (U, V) \\ &s.t. \begin{cases} U * \gamma_1 + V * \gamma_2 \leq \Gamma \\ U + V \geq 1 \\ U \geq 0 \\ V \geq 0 \end{cases} \end{aligned} \tag{5.8}$$

- Recall U and V are non-negative integers, presenting the number of nodes and links chosen by the attacker. We can search for all qualified pairs of (U,V) and put them into a set, denoted by Λ. Take $\Gamma = 4$, $\gamma_1 = 2$ and $\gamma_1 = 1$ as an example. Λ includes eight pairs, i.e., $\{(0,1),(0,2),(0,3),(0,4),(1,0),(1,1),(1,2),(2,0)\}$. Take the pair $(1,2)$ as an example. This pair mean that the attacker chooses 1 node (i.e., $U = 1$) and 2 links (i.e.,$V = 2$) as TCs. Specifically choosing which node and links depends on different attack strategies. For instance, AS_{degree} will choose the node with the largest node degree and two links with top two largest link degrees as TCs (discussed in Section 5.6.3).



(a) Measured By PoDN (b) Measured By CL

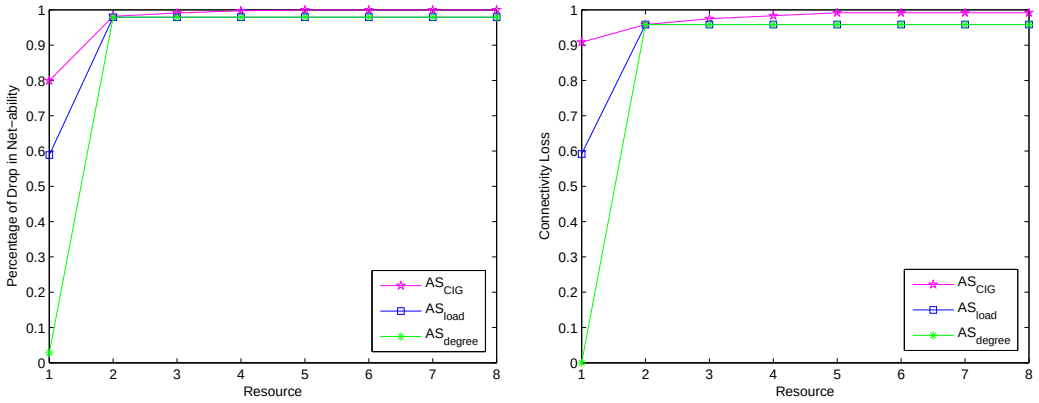
Figure 5.2. Performance comparisons among three attack strategies on IEEE 30 bus system, where $\gamma_1 = 1$ and $\gamma_2 = 1$

- Under given γ_1, γ_2 and Γ, an attack strategy, e.g., AS_{CIG}, might have multiple choices, i.e., the pairs in Λ. We conduct the simulation for all pairs and can obtain the maximum attack performance in terms of PoDN for AS_{CIG}. We do similar simulations and operation for AS_{load} and AS_{degree}, and conduct performance comparison among these attack strategies.

5.7.3 Performance Comparison among CIG-based, degree-based and load-based attack strategies

We specialize performance comparisons as follows. First, we adopt IEEE 30 bus system, IEEE 118 bus system and Bay Area power grid as test benchmarks. Second, we assume the attacker has limited resource. In particular, Γ is set to be 1, 2, ..., or 8 (i.e., $1 \leq \Gamma \leq 8$). Finally, in order to mimic different ways of distributing resource on selecting TNs and TLs, we set γ_1 and γ_2 as the following two scenarios,

- *Scenario I*: $\gamma_1 = 2$ and $\gamma_2 = 1$. Attacking a node needs 2 units resource; attacking a link needs 1 unit resource.



(a) Measured By PoDN (b) Measured By CL

Figure 5.3. Performance comparisons among three attack strategies on IEEE 30 bus system, where $\gamma_1 = 2$ and $\gamma_2 = 1$.

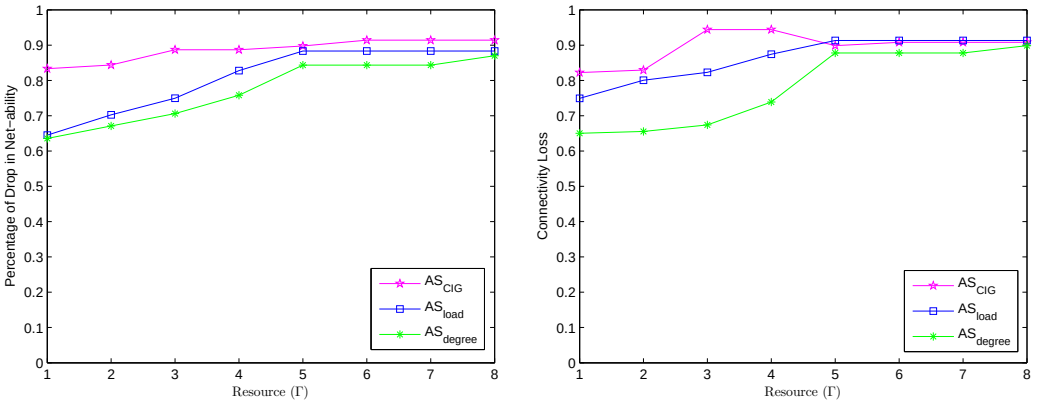
- *Scenario II*: $\gamma_1 = 1$ and $\gamma_2 = 1$. Attacking a node or a link both needs 1 unit resource.

The meaning of Scenario I is straightforward. Substations are harder to be attacked. In reality, substations are complicated and under well protection; transmission lines usually spread in very long distances (typically hundreds of kilometres), which can be easily found and attacked. In 2013, for instance, it was reported that a man in Arkansas launched a series of attacks on local high-voltage transmission lines [22]. The emergence of the Smart Grid, however, can dramatically increase the chances of cyber intrusions [21], which make substations possibly as vulnerable as transmission lines. Therefore, Scenario II is likely with consideration of cyber attacks in smart grids.

It is definite that the attacker can have more resource and the values of γ_1 and γ_2 can be others. We select the group of Γ values and two scenarios of setting γ_1 and γ_2 for demonstration purpose only.

Table 5.6. Target components for three attack strategies on Bay Area power grid

Attack	$\Gamma = 1$		$\Gamma = 2$		$\Gamma = 3$		$\Gamma = 4$		$\Gamma = 5$		$\Gamma = 6$		$\Gamma = 7$		$\Gamma = 8$	
Strategy	TCs	PoDN	TCs	PoDN	TCs	PoDN	TCs	PoDN	TCs	PoDN	TCs	PoDN	TCs	PoDN	TCs	PoDN
AS_{degree}	n_{13}	0.53	n_{12},n_{13}	0.62	n_{12},n_{13}, n_{39}	0.70	n_{12},n_{13}, n_{39},l_{73}	0.70	n_{12},n_{13}, n_{39},n_{68}, n_4	0.72	n_{12},n_{13}, n_{39},n_{68}, n_4,n_{54}	0.73	n_{12},n_{13}, n_{39},n_{68}, n_4,n_{54}, n_{56}	0.74	n_{12},n_{13}, n_{39},n_{68}, n_4,n_{54}, n_{56},l_{73}	0.74
AS_{load}	l_{185}	0.57	n_{13},n_{39}	0.68	n_{13},n_{39}, l_{185}	0.71	n_{13},n_{39}, l_{185}, l_{40}	0.75	n_{13},n_{39}, l_{185},l_{40}, l_{564}	0.75	n_{13},n_{39}, l_{185},l_{40}, l_{564},l_{549}	0.82	n_{13},n_{39}, l_{185}, l_{40}, l_{564},l_{549}, l_{144}	0.82	n_{13},n_{39}, l_{185}, l_{40}, l_{564},l_{549}, l_{144},l_{121}	0.83
AS_{CIG}	n_{207}	0.66	n_{207},n_{253}	0.77	n_{207},n_{253}, l_{457}	0.87	l_{235},l_{294}, l_{457},l_{586}	0.89	n_{13},n_{41}, n_{58},n_{85}, l_{549}	0.92	n_{13},n_{41}, n_{58},n_{85}, l_{549},l_{701}	0.94	n_{13},n_{41}, n_{58},n_{85}, l_{549},l_{567}, l_{701}	0.96	n_{13},n_{41}, n_{54}, n_{58}, n_{85},l_{549}, l_{567},l_{701}	0.97



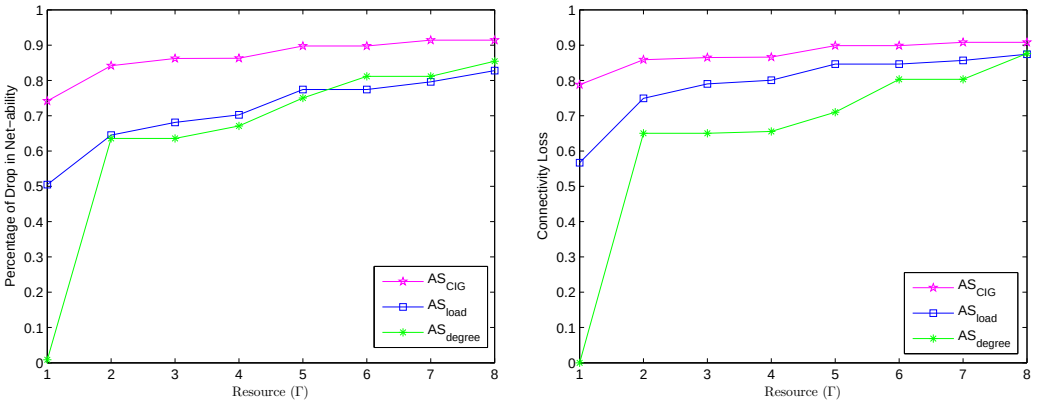
(a) Measured By PoDN (b) Measured By CL

Figure 5.4. Performance comparisons among three attack strategies on IEEE 118 bus system, where $\gamma_1 = 1$ and $\gamma_2 = 1$.

Performance comparisons among AS_{degree}, AS_{load} and AS_{CIG} are shown in Figs. 5.2 and 5.3 on IEEE 30 bus system, in Figs. 5.4 and 5.5 on IEEE 118 bus system and in Figs. 5.6 and 5.7 on Bay Area power grid. In each figure, there are two subfigures, which represent the performances are measured in terms of *percentage of drop in net-ability* (PoDN) and *connectivity loss* (CL). In each subfigure, x-axis represents the amount of resources (i.e., Γ); y-axis represents PoDN or CL. The green-star curve, blue-square curve, and magenta-pentagram curve represent the attack performance of AS_{degree}, AS_{load} and AS_{CIG}, respectively. In addition, in Table 5.6 we demonstrate the target components (TCs) that result in the performances for AS_{degree}, AS_{load} and AS_{CIG} in Fig. 5.6(a).

Based on Figs. 5.2, 5.3, 5.4, 5.5, 5.6 and 5.7 and Table 5.6, we have the following observations and discussions.

First, AS_{CIG} can obtain better performance than AS_{degree}, AS_{load}. In Figs. 5.2(a), 5.3(a), 5.4(a), 5.5(a), 5.6(a) and 5.7(a), the performances are measured in terms of PoDN. It is apparent that the magenta-pentagram curves are higher than the green-star curves and the blue-square curves. In Figs. 5.2(b), 5.3(b),

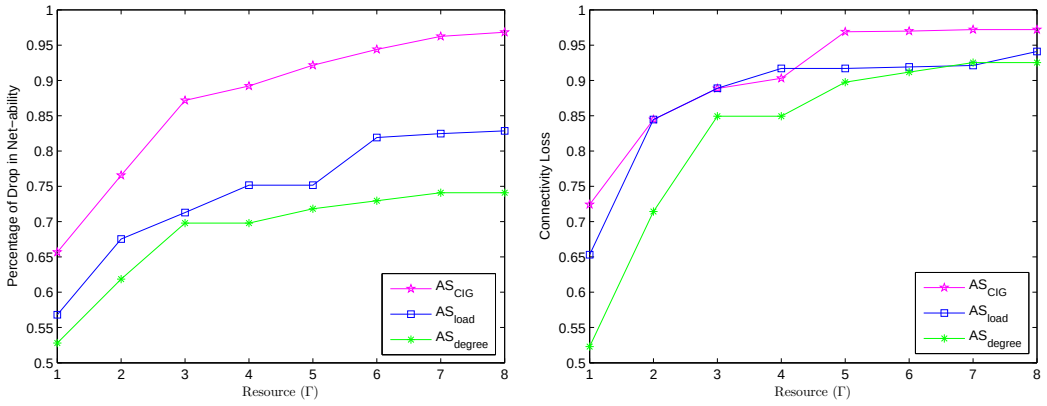


(a) Measured By PoDN (b) Measured By CL

Figure 5.5. Performance comparisons among three attack strategies on IEEE 118 bus system, where $\gamma_1 = 2$ and $\gamma_2 = 1$.

5.4(b), 5.5(b), 5.6(b) and 5.7(b), the performances are measured in terms of CL. The magenta-pentagram curves are still higher than the green-star curves and only lower than the blue-square curves at some cases, e.g., $\Gamma = 4$ in Fig. 5.6(b). These observations are reasonable. The proposed metric, CIG, is specifically designed and can be used to find these joint-node-link combinations that yield large strengths. The metrics, degree and load, are not carefully designed for investigating joint-node-link attack strategies. From the performance's point of view, AS_{CIG} is stronger than AS_{degree}, AS_{load}.

Second, from the attack's perspective, attacking a few pivot components can trigger severe cascading failures in power systems. Take IEEE 30 system as an example. Only attacking one component AS_{CIG} can obtain the performance $PoDN = 0.98$, which is shown in Fig. 5.2. Similar observations can be made in Fig. 5.4 and Fig. 5.6, i.e., the results on IEEE 118 bus system and Bay Area power grid, respectively. Generally speaking, there are some components that are critical to the power transmission system [35]. Attacking a few, even one, of critical components can collapse the entire grid. Because, power transmission systems



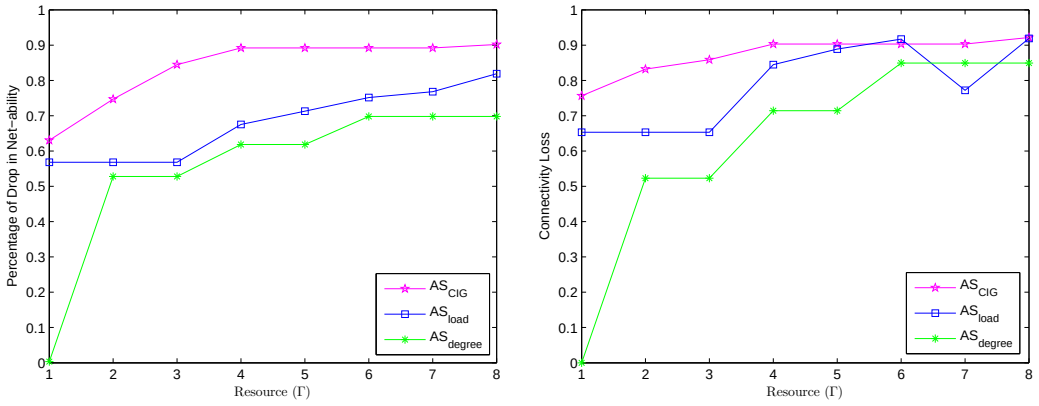
(a) Measured By PoDN (b) Measured By CL

Figure 5.6. Performance comparisons among three attack strategies on Bay Area power grid, where $\gamma_1 = 1$ and $\gamma_2 = 1$.

have the characteristic of self-organized criticality [26]. If they are operating closely to limitations, the disturbances caused by removing critical components are severe enough to trigger large-scale cascading failures and result in serious power outage in the grid.

Third, as the network size increases, the number of TCs should increase, if the attacker wants to entirely paralyze the grid. For instance, suppose the attacker wants to obtain more than 90% drop in net-ability (i.e., $PoDN \geq 0.9$). By using AS_{CIG}, the attacker needs to attack 1 TC on IEEE 30 bus system, at least 3 TCs on IEEE 118 bus system and at least 5 TCs on Bay area power grid. The observation is consistent with that in [24]. In order to cause national blackout, it is necessary to attack at least 9 substations in the U.S. power grid, which has in total 55,000 substations.

Finally, the joint-node-link attack strategy is the generalization of the node-only and link-only attack strategies. In Table 5.6, we show the combinations of TCs for AS_{degree}, AS_{load} and AS_{CIG} on Bay Area power grid. It is apparent that these combinations include three groups, node-only, link-only and joint-node-link.



(a) Measured By PoDN (b) Measured By CL

Figure 5.7. Performance comparisons among three attack strategies on Bay Area power grid, where $\gamma_1 = 2$ and $\gamma_2 = 1$.

Previously, the node-only/link-only attack strategies only select nodes/links as TCs [10, 11]. The joint-node-link attack strategies are the general cases, in which TCs can be nodes, links or both. In addition, there are in total 24 TC combinations in Table 5.6, including 10 node-only combinations, 2 link-only combinations and 12 joint-node-link combinations. The joint-node-link TC combinations are of importance to find strong attack performances.

5.8 Conclusions and Future Works

In this work, we introduced the joint-node-link perspective to investigate the power grid vulnerabilities and attack strategies . In particular, it was found that the power system had many joint-node-link vulnerabilities. In addition, we proposed the CIG-based joint-node-link attack strategy based on the specifically-designed metric, CIG. Through intensive experiments, it was shown that the proposed scheme shew better attack performances than comparison schemes.

In future, there are a few interesting directions along this topic. First, it is likely that multiple attacks are launched sequentially on substations and transmis-

sion lines, but not simultaneously. Second, the CFS can be further improved by introducing the stochastic analysis. Finally, validating existing blackouts is useful for the society to understand the cascading failure and major blackouts.

List of References

[1] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.

[2] "The economic impacts of the august 2003 blackout," Feb. 2004, prepared by the Electricity Consumers Resource Council (ELCON).

[3] "The smart grid: An introduction." [Online]. Available: http://energy.gov/

[4] M. Vaiman et. al., "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[5] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

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

[7] P. Hines, K. Balasubramaniam, and E. C. Sanchez, "Cascading failures in power grids," *IEEE Potentials*, vol. 28, no. 5, pp. 24–30, Sept. 2009.

[8] The Guardian. "India blackouts leave 700 million without power." [Online]. Available: http://www.guardian.co.uk/

[9] J. Wang, L. Rong, L. Zhang, and Z. Zhang, "Attack vulnerability of scale-free networks due to cascading failures," *Physica A*, vol. 387, pp. 6671–6678, Nov. 2008.

[10] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in U.S. power grid," in *Proceeding of IEEE Global Telecommunications Conference*, Houston, Texas, USA, Dec.5-9 2011.

[11] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the north american power grid," *Phys. Rev. E*, vol. 69, no. 2, Feb. 2004.

[12] Y. Zhu, Y. Sun, and H. He, "Load distribution vector based attack strategies against power grid systems," in *Proceeding of IEEE Global Telecommunications Conference*, Anaheim, CA, USA, Dec.3-7 2012.

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

[14] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *Eur. Phys. J. B*, vol. 46, pp. 101–107, 2005.

[15] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, no. 5, May 2002.

[16] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, Sept. 2010.

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

[18] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, pp. 1334–1340, July 2011.

[19] Y. Zhu, J. Yan, Y. Sun, and H. He, "Risk-aware vulnerability analysis of electric grids from attacker's perspective," in *Proceeding of IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.

[20] E. I. Bilis, W. Krger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 4, no. 7, pp. 854–865, Dec. 2013.

[21] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan. 2012.

[22] "FBI, joint terrorism task force arrest suspect in arkansas power grid attacks," 2013. [Online]. Available: http://www.forbes.com/

[23] R. Lemos, "DHS video shows potential impact of cyberattack," Sept.27 2007. [Online]. Available: SecurityFocus.com

[24] "Small-scale power grid attack could cause nationwide blackout, study says," Mar.13 2014. [Online]. Available: FoxNews.com

[25] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 1, pp. 15–32, Jan. 2005.

[26] S. Mei, Y. Ni, X. Zhang, G. Wang, and G. Wang, "A study of self-organized criticality of power system under cascading failures based on AC-OPF with voltage stability margin," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1719–1726, Nov. 2008.

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

[28] S. Mei, X. Zhang, and M. Cao, *Power Grid Complexity*. Beijing: Tsinghua University Press, Aug. 2011.

[29] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, no. 4, Apr. 2004.

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

[31] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 1, 2009.

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

[33] X. Cheng and T. J. Overbye, "PTDF-based power system equivalents," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1868–1876, Nov. 2005.

[34] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Transactions on Parallel and Distributed Systems*, 2014, in press.

[35] J. Tollefson, "US electrical grid on the edge of failure," *Nature News and Comment*, Aug.25 2013.

[36] P. C. Wong, K. Schneider, P. Mackey, H. Foote, G. Chin, R. Guttromson, and J. Thomas, "A novel visualization technique for electric power grid analytics," *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, no. 3, pp. 410–423, May 2009.

[37] "Platts." [Online]. Available: www.platts.com

[38] "Electric transmission lines." [Online]. Available: http://psc.wi.gov/thelibrary/publications/electric/electric09.pdf

[39] Some explanation from Platts: (1) substations can be identified as power plants, either connecting a 10 KV transmission lines or geographically near a power plant; (2) if the voltage of a transmission line is not sure, it is recorded as a negative number.

[40] "ArcGIS Desktop." [Online]. Available: http://www.esri.com/software/arcgis/arcgis-for-desktop

[41] P. Kundur, *Power System Stability and Control*. New York: McGraw-Hill, Jan. 1994.

[42] M. A. Rahman, E. Al-Shaer, and P. Bera, "A noninvasive threat analyzer for advanced metering infrastructure in smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 273–287, Mar. 2013.

[43] D. S. Fava, S. R. Byers, and S. J. Yang, "Projecting cyberattacks through variable-length markov models," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 359–369, Sept. 2008.

CHAPTER 6

Manuscript 5: Resilience Analysis of Power Grids under the Sequential Attack

Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, and Haibo He

Department of Electrical, Computer, and Biomedical Engineering

University of Rhode Island, Kingston, RI 02881

Manuscript status: published in IEEE Transactions on Information Forensics and Security, 2014

Corresponding Author: Yihai Zhu

Kelley Annex, Room A115

4 East Alumni Ave.,

Kingston, RI 02881

Phone:+1-401-874-5846

Email: yhzhu@ele.uri.edu

6.1 Abstract

The modern society has increasingly relied on electrical service, which also brings risks of catastrophic consequences, e.g., large-scale blackouts. In the current literature, researchers reveal the vulnerability of power grids under the assumption that substations/transmission lines are removed or attacked synchronously. In reality, however, it is highly possible that such removals can be conducted sequentially. Motivated by this idea, we discover a new attack scenario, called the *sequential attack*, which assumes substations/transmission lines can be removed sequentially, not synchronously. In particular, we find the sequential attack can discover many combinations of substation whose failures can cause large blackout size. Previously, these combinations are ignored by the synchronous attack. In addition, we propose a new metric, called the *sequential attack graph* (SAG), and a practical attack strategy based on SAG. In simulations, we adopt three test benchmarks and five comparison schemes. Referring to simulation results and complexity analysis, we find that the proposed scheme has strong performance and low complexity.

6.2 Introduction

Electric grids have been developed over decades and become increasingly interconnected and complex. Although mechanisms and regulations have been applied to maintain the stability and security of power transmissions, large-scale blackouts are still not inevitable. In the past decade, large-scale blackouts have caused catastrophic results. Examples include 2003 Northeast American blackout affecting 55 million customers [1] and 2012 India blackout leaving 700 million people without power [2]. In these cases, initial failures of one or a few power grid components (i.e., substations and transmission lines) can trigger the successive failures of other components. In other words, a sequence of dependent failures of individual com-

ponents successively weakens power grids, which is referred to as the *cascading failure* [3].

The triggers of cascading failures can be diverse, such as natural reasons, aging of equipment, and human errors [4]. Recently, malicious attacks become significant and potential triggers of cascading failures. For instance, there are increasing evidences of malicious intention and actions that aim to destruct the US power systems [5–7]. To understand the vulnerability of power grids, an important approach is to investigate malicious attacks, in terms of possible attack strategies, features, and consequence. Such investigation would also facilitate the study on mitigating or even preventing cascading failures in the future.

In the current literature [8–12], designing attack strategies is an important direction to investigate malicious attacks on power grids. In particular, attackers can obtain information of the power grid, choose a set of nodes (i.e., substations), referred to as *victim nodes* (VNs), or a set of links (i.e., transmission lines), referred to as *victim links* (VLs), and assume to remove these VNs/VLs through either cyber penetration [7] or physical sabotages [6, 13]. In reality, attackers can collect the power grid information in different ways, e.g., purchasing the entire North American power grid from commercial companies [14]. In addition, both cyber and physical attacks on power grids are highly possible. A simulated cyber attack on the U.S. power grid has shown power grid's components can be remotely accessed and destroyed by hackers [15]. Physical attacks can be conducted in easy ways, such as cutting down a tree to trip transmission lines [1], or in complex ways, such as using electromagnetic pulse (EMP) to destroy substations and transmission lines [16, 17].

Attack strategies in existing works [8–12, 18–25] can be classified from different angles. The *first* angle is the number of VNs/VLs. Single-node/link attacks are

studied in [8, 18, 19]; many industry reliability criteria require power grids can tolerate failure of single node/link [4]. Multiple-node/link attacks often cause larger damage and receive more research attention [10–12, 21, 22, 24, 26]. The *second* angle is whether nodes, links, or both are removed. There are some studies that investigate attacks on links [10, 18, 22, 23], whereas many investigate attacks on nodes [8–12, 18, 19, 21, 22, 24–26]. Very few studies address attacks on both together [27]. The *third* angle differentiates attack strategies according to the underlying cascading failure models they assumed. Some attack strategies are only meaningful for a given model [9, 24, 26], whereas others are useful under various assumptions [8, 11, 21].

We argue that the above three classification angles are not sufficient. An important classification angle is missing. In the current literature, the investigation of multiple-node/link attacks assumes that VNs/VLs are removed synchronously. This assumption, however, omits the fact that multiple removals can occur sequentially. In other words, *the attacker can remove VNs/VLs according to a carefully designed time sequence*.

Furthermore, cascading failures in real life involved the sequences of various events, such as voltage collapse, generators shunt down, and transmission lines tripping [4]. The cascade process lasts probably minutes, or even hours [1, 2]. Thus, time domain is an essential dimension to cascading failures. The assumption of synchronous removals has apparent limitations to comprehensively exploit the characteristics of cascading failures. In this work, we discover a new attack scenario, called the *sequential attack*. From the perspective of the new angle, attack strategies can be divided into newly-discovered *sequential attack strategy* (SeqAS) and existing *synchronous attack strategy* (SynAS).

Is the sequential attack more dangerous than the synchronous attack? Can the

new attack scenario reveal new vulnerabilities of power grids? Are existing metrics useful to design the SeqAS? In this work, we answer these questions by investigating the sequential attack and the SeqAS on nodes. The major contributions are summarized as follows.

- First, we find strong sequential attacks by using the exhaustive search on IEEE 39 bus system. On this small-scale power grid, we discover that the sequential attack generally cause more severe cascading failures, measured by the blackout size, than the synchronous attack.

- Second, we propose a novel metric, called the *sequential attack graph* (SAG). Compared with existing metrics, e.g., degree and load, this metric can intuitively capture the combination of vulnerable nodes and indicate the order of their removals, which would lead to stronger sequential attacks.

- Third, we design a new SeqAS based on SAG, called the *SAG-based SeqAS*, which can achieve good attack performance with low complexity.

- Finally, we perform extensive testing to demonstrate the features of the sequential attack, the proposed metric, SAG, and the proposed SeqAS. Briefly speaking, we adopt three different power grids as test benchmarks. The proposed SAG-based SeqAS is compared with five other schemes. The comparison schemes include the straightforward degree-based SeqAS and load-based SeqAS, and three existing synchronous attack strategies. The results demonstrate that the proposed SeqAS strategy yield strong attacks against power grids. The complexity of the proposed scheme and the comparison schemes are also analyzed.

The rest of this work is organized as follows. Related work is discussed in Section 6.3. In Section 6.4, the *cascading failure simulators* (CFS) used in this work

are presented in detail. In Section 6.5, we define the sequential attack and demonstrate the new vulnerabilities. In Section 6.6, we propose a new metric, called *sequential attack graph* (SAG), and the SAG-based sequential attack strategy. Experiments and discussions are given in Section 6.7, followed by the conclusion in Section 6.8.

6.3 Related Works

Traditionally, investigating the attack strategy is from the perspective of the SynAS. We briefly summarize the existing attack strategies as follows.

The *random removal*, randomly choosing VNs, is to mimic unintentional failures, e.g., vegetation sagging, earthquakes, lightening, or software and hardware faults. Power grids have been proven to be insensitive to random removals [21, 25].

The *search-based* approaches provides attackers a possible way to search for a set of VNs whose synchronous removals can yield the strongest performance. However, the exhaustive search [9], or called *contingency analysis* in the power society [4], usually has extensive search space and is computationally infeasible [4, 9]. In order to improve search efficiency, some heuristic approaches [11, 22] are proposed to reduce the search space. The key problem of search-based approaches is that they can not make quick attack decisions because of the large search space.

The *metric-based* approaches are prevailing in studying attack strategies. Many *metrics* have been proposed. Some metrics are straightforward, e.g., degree [25], load [8] and risk if failure (RIF) [9]. These metrics directly exploit the features of power grids, e.g., the topology and initial power flows. Other metrics are more complex, such as load distribution vector (LDV) [10], risk graph (RG) [11] and geographic information [12]. These metrics can find stronger attacks than the straightforward metrics. Existing metrics, however, are specifically designed for the SynAS. It is unknown for whether the existing metrics can yield SeqAS.

Table 6.1. Comparison between the proposed work and some existing studies

Attack Strategy		Single-node Synchronous	Multiple-node Synchronous	Multiple-node Sequential
Random removal [25]		✓	✓	
Search-based approaches [4]		✓	✓	
Attack metrics	Degree [25]	✓	✓	
	Load [21]	✓	✓	
	RIF [9]	✓	✓	
	LDV [10]		✓	
	Geographic information [12]		✓	
	RG [11]	✓	✓	
	Proposed work			✓

Furthermore, a few recent works have studied the vulnerability of power grids from the perspective of *time domain* [28, 29]. Cascading failures in power grids can have dramatically different intermediate processes, which reveals various evolution of cascading failures [28]. In addition, multiple triggers can be applied consecutively [29], with intervening time between two consecutive removals.

In this work, we consider the *time domain* in revealing the vulnerability of power grids and developing practical and strong attack strategy. Particularly, we are interested in investigating the sequential attack. A brief summary is shown in Table 6.1.

6.4 Cascading Failure Simulator

In this work, we use two types of *cascading failure simulator* (CFS), the sequential attack CFS and the synchronous attack CFS. Our CFSs are modified from the CFS in [22], based on the DC power-flow model. Briefly speaking, we conduct the modifications as follows.

- In our CFSs, multiple removals can be conducted either sequentially or

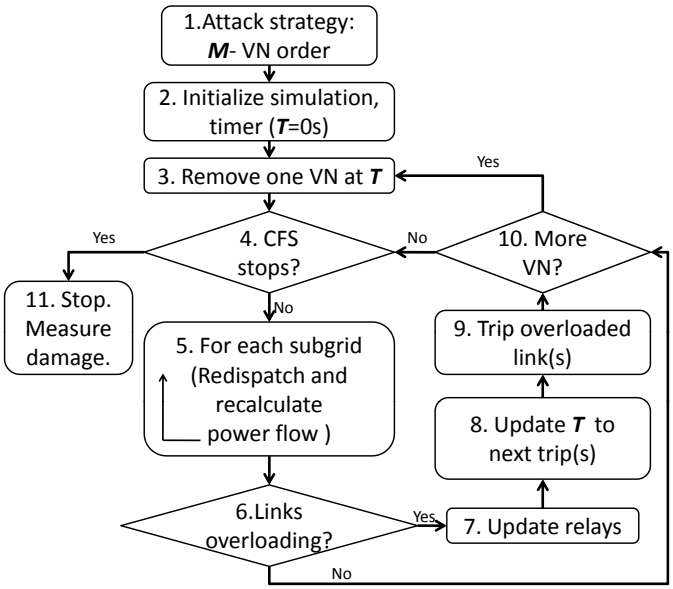


Figure 6.1. The diagram of sequential attack CFS.

synchronously; in the CFS from [22], multiple removals are conducted synchronously.

- Our CFSs will stop when there is no more attacks and no overloading links; the CFS from [22] will terminate when 10% of the nodes are no longer connected to the largest island.

- In our CFSs, we adopt the blackout size (defined in Equ. 6.4) to measure the damage of the attack; in the CFS from [22], there is no such measurement.

We first introduce the sequential attack CFS. Fig. 6.1 illustrates its flow diagram; the description of each step is given as follows.

CFS Step 1: Suppose an attack strategy has determine M victim nodes (VNs) and the order to remove them, e.g., $\{VN_1, VN_2, ..., VN_M\}$, where VN_i represents i^{th} VN ($1 \leq i \leq M$). These M removals are performed individually at M different times, e.g., $\{T_1, T_2, ..., T_M\}$, during cascading failures.

CFS Step 2: Initialize CFS, e.g. set up timer $\boldsymbol{T}$ and calculate initial power lows.

CFS Step 3: Remove one VN each time at time $\boldsymbol{T}$ to mimic the sequential attack. That is, remove VN_i at time T_i. After each removal, update the topological and electrical features of the power grid. The calculation of T_i will be discussed below.

CFS Step 4: Check whether CFS needs to stop. If yes, quit CFS and goto CFS Step 11. The criterion to terminate CFS include (1) all removals are finished, (2) there is no overloaded link.

CFS Step 5: If the power grid is broken into additional subgrids due to removals of VNs or trips of links from CFS Steps 3 to 9, re-dispatch generation and shed load to meet power supply/demand balance in each subgrid as follows. First, ramp up or down the supply of generators to meet the demand as closely as possible. These adjustments are restricted by the capacity of generators and ramping time [22]. Second, after re-dispatching generators in a subgrid, if the generation is surplus ($\eta = (\sum_{g \in G}(P_g) - \sum_{d \in D}(P_d)) > 0$, where G and D represent the sets of generation nodes and demand nodes in the subgrid, respectively), trip the generators sequentially, beginning from the smallest one, until $\eta \leq 0$ [22]. Third, after ramping the generation and tripping the surplus generators, if the supply is insufficient (i.e., $\eta < 0$), tripping the demand nodes sequentially, beginning from the smallest one, until $\eta \geq 0$. Then, if $\eta > 0$, recover the last tripped demand node partially to the demand η to meet supply/demand balance. When a subgrid reaches the balance, DC power-flows are recalculated to check the overloading on links.

CFS Step 6: Check link overloadings. If there is (are) overloaded link(s),

go through CFS Steps 7 to 9 to deal with the overloading; otherwise go to CFS Step 10 to check next possible removal.

CFS Step 7: Update relays. For the link(s) with overloading, use the time-delayed overcurrent relay to determine whether/when next link is tripped [22]. Here, the "relay modeling" is to mimic a number of processes by which links may shut down, such as the overheating of a transmission line due to sagging into vegetation. If a link is overloaded at time $\boldsymbol{T}$, the timer begins to count the overloading time. We assume that each link can tolerate the overloading for certain time, denoted by τ. The τ for link j, denoted by τ_j, is defined as,

$$\tau_j = \begin{cases} \frac{O_j}{f_j - F_j} & \text{if} f_j > F_j \\ 0 & \text{otherwise} \end{cases} \tag{6.1}$$

where f_j is the current power flow, F_j is the flow limit, and O_j is the threshold, which is chosen such that link j can tolerate 5 seconds of being 50% above its power flow limit. For instance, suppose the flow limit of link j is 45 (i.e., $F_j = 45$), the threshold O_j is calculated as $0.5 * 45 * 5 = 112.5$. If the current flow in link j is 55 (i.e., $f_j = 55$), τ_j is $11.25 = \frac{112.5}{55-45}$ s. The definition indicates that how fast a link is tripped depends how seriously this link is overloading. Among all overloaded links, the link(s) with the smallest τ value is chosen to be tripped in CFS Step 9. The corresponding τ value is referred to as τ_{min}.

CFS Step 8: Update the timer to when next trip happens, as $\boldsymbol{T} = \boldsymbol{T} + \tau_{min}$, the smallest τ in CFS Step 7.

CFS Step 9: Trip the chosen link(s) in CFS Step 7, and update the topological structure and the electrical features of the power grid network.

CFS Step 10: Check whether all removals are finished. If not, current time

$\boldsymbol{T}$ is the "time" for next removal.

CFS Step 11: When CFS stops, evaluate the damage by exploiting the *blackout size*, defined in Equ. 6.4.

In CFS Step 3, T_i is calculated as follows. First, when $i = 1$, $T_1 = 0$, meaning the first removal, VN_1, occurs at the beginning of cascading failures. Second, when $2 \leq i \leq M$, T_i is obtained depending on whether there are overloaded links after removing VN_{i-1} at T_{i-1}. If there exist overloaded links, $T_i = T_{i-1} + \tau_{min}$, where τ_{min} is decided in CFS Step 7. That is, the removal of VN_i at T_i occurs after tripping an overloaded link in CFS Step 9. Otherwise, $T_i = T_{i-1} + \epsilon$ (ϵ is a small interval, e.g., 0.001.). That is, the removal of VN_i at T_i occurs just after the removal of VN_{i-1} at T_{i-1}.

Note that if we use different policies to determine T_i, the sequential attack performances may be different. In this work, we specifically use the above policy to demonstrate the sequential attack. In the future works, we will surely consider to further investigate various policies in determining the removal time.

The procedures of the synchronous attack CFS is similar to that of the sequential attack CFS. The only difference is that in CFS Step 3 all M VNs are removed simultaneously at the begging of cascading failures. That is, $T_1 = T_2 = \cdots = T_M = 0$.

6.5 The Sequential Attack and New Vulnerabilities

Before introducing the sequential attack scenario, we introduce several concepts as follows.

- The *removal of a node* means physically disconnecting this node from the power grid by removing its incoming and outgoing links. In reality, such removals can be conducted by either cyber attacks or physical attacks [13].

- A *multiple-node combination* is referred to as a set of nodes. An attack strategy is to select one such multiple-node combination as its VNs.

- For a multiple-node combination, we can perform the removals either sequentially or synchronously. Either attack strategy can cause damage (in terms of blackout size defined in Equ. 6.4) to the power grid. The *strength* of the multiple-node combination for the SeqAS (or SynAS) is referred to as the damage caused by sequentially (or synchronously) removing these nodes.

- The *vulnerability* of the power grid can have broad meanings in the current literature. In this work, the vulnerability analysis is to specifically find these multiple-node combinations that have large strengthes.

- *Known vulnerabilities* are referred to as strong multiple-node combinations found by the synchronous attack.

- *New vulnerabilities* are referred to as strong multiple-node combinations that are discovered by the sequential attack, but are not found by the synchronous attack.

In the rest of this section, we first introduce the formal definition of the sequential attack in Section 6.5.1, then introduce several concepts related to setting up the demonstration in Section 6.5.2, and finally discuss the new vulnerability of the power grid in Section 6.5.3.

6.5.1 The Sequential Attack

For a multiple-node combination with M nodes, suppose the removals of them occur at T_1, T_2, ..., T_M. If all removals happen at the same time (i.e., usually at the beginning of cascading failures or time 0), this attack scenario is referred to as

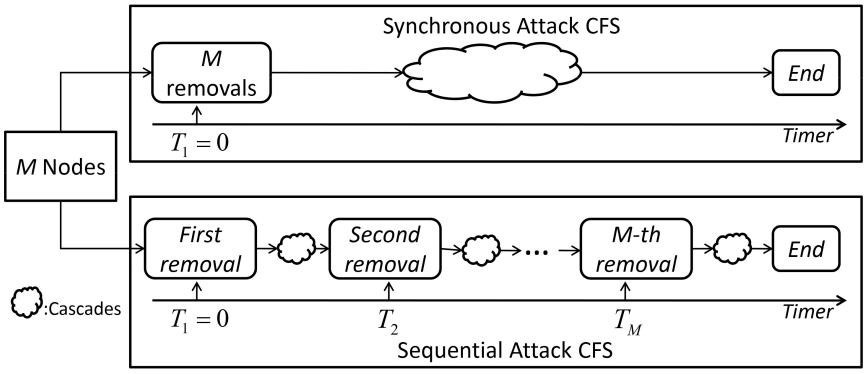


Figure 6.2. The sequential attack versus the synchronous attack.

the synchronous attack in this work. That is,

$$T_1 = T_2 = \cdots = T_M \tag{6.2}$$

If Equ. 6.2 dose not satisfy, this attack scenario is referred to as the general definition of the sequential attack. In particular, in this work we are interested in the special case that all removals occur at different times. That is,

$$T_1 < T_2 < \cdots < T_M \tag{6.3}$$

The definition of the sequential attack in Equ. 6.3 is assuming to remove one node each time. This definition is extensible. In Fig. 6.2, we demonstrate the two attack scenarios in this work. Roughly speaking, under the synchronous attack scenario M removals are conducted simultaneously at $T_1 = 0$, while under the sequential attack scenario the first removal occurs at $T_1 = 0$ and the rest removals (i.e., $M - 1$ removals) occur sequentially at T_2 till T_M during cascading failures.

6.5.2 Concepts Related to Demonstration Setup

We show the features of the sequential attack through demonstrations, and explain some concepts for the demonstration as follows.

- *Grid Network*: A power grid is viewed as a network, where substations and transmission lines are viewed as nodes and links, respectively. The set of

nodes is denoted by $\mathcal{B}$; the set of links is denoted by $\mathcal{L}$. Due to different functionalities, nodes are generally categorized into three sets, generation nodes (or generators that produce electricity), transmission nodes, and demand nodes (delivering electricity to customers) [9]. The set of generation nodes is denoted by $\mathcal{G}$; the set of demand nodes is denoted by $\mathcal{D}$. The number of nodes, links, generation nodes and demand nodes are represented as $N_{\mathcal{B}}$, $N_{\mathcal{L}}$, $N_{\mathcal{G}}$ and $N_{\mathcal{D}}$, respectively.

- *Test Benchmark*: We adopt IEEE 39 bus system [26] as the test benchmark to demonstrate new vulnerabilities. IEEE 39 bus system consists of 39 nodes (10 generation nodes and 29 demand nodes) and 46 links, which means $N_{\mathcal{B}} = 39$, $N_{\mathcal{L}} = 46$, $N_{\mathcal{G}} = 10$ and $N_{\mathcal{D}} = 29$.

- *Blackout Size*: We adopt the blackout size to measure the strength of a multiple-node attack. Blackout size is defined as [21],

$$\Delta = 1 - \frac{\sum_{d \in \mathcal{D}} P'_d}{\sum_{d \in \mathcal{D}} P_d} \tag{6.4}$$

  where P_d and P'_d represent the power on the demand node before and after the attack, respectively. This definition, similar to that in [21], is the normalized power loss, which means $0 \leq \Delta \leq 1$. The larger Δ is, the stronger the multiple-node attack is.

- *Strong Attack*: We define a threshold, η. Numerically, if the strength of a multiple-node attack, denoted by Δ, is larger or equal to η (i.e., $\Delta \geq \eta$), this multiple-node attack is called a strong attack; otherwise it is called a weak attack (i.e., $\Delta < \eta$).

- *Sequential Attack CFS*: *Cascading failure simulator* (CFS) is employed to mimic the occurrence of removing nodes and the evolution of cascading failures. The sequential attack CFS in this work is modified from the CFS

in [22]. In Section 6.4, we give the detailed discussion on both the sequential attack CFS and the synchronous attack CFS adopted in this work.

Next, for a multiple-node combination with M nodes, we perform both the synchronous attack and the sequential attack. The strength of the M-node synchronous attack is denoted by Δ_{syn}^{M}; the strength of the M-node sequential attack is denoted by Δ_{seq}^{M}. They are obtained as follows.

- Δ_{syn}^{M}: Perform the synchronous attack on M nodes in the synchronous attack CFS. Δ_{syn}^{M} is measured in terms of blackout size when the synchronous attack CFS stops.

- Δ_{seq}^{M}: There are $M!$ orders of the M-node combination. Perform the sequential attack for each order in the sequential attack CFS, and record all strengthes in terms of blackout size. The largest strength value is Δ_{seq}^{M}.

6.5.3 Demonstration of New Vulnerabilities

We conduct two-node attacks (i.e., $M = 2$) on IEEE 39 bus system. There are in total $\binom{39}{2} = 741$ two-node combinations. For each two-node combination, we obtain two strength values, Δ_{syn}^{2} and Δ_{seq}^{2}. The relation between the sequential attack and the synchronous attack is demonstrated in Fig. 6.3 by plotting Δ_{seq}^{2} versus Δ_{syn}^{2}. There are 741 dots in Fig. 6.3, each of which represents a two-node combination. The relation between Δ_{seq}^{2} and Δ_{syn}^{2} is not straightforward based on Fig. 6.3, because the dots are scattered in the plane. For demonstration purpose, we conduct two classifications among all dots.

First, we compare both Δ_{seq}^{2} and Δ_{syn}^{2} with η (i.e., the threshold of defining a strong attack). If $\Delta_{seq}^{2} \geq \eta$ (or $\Delta_{syn}^{2} \geq \eta$), the two-node sequential attack (or the two-node synchronous attack) is strong; otherwise, this attack is weak. By setting $\eta = 0.2$ (20% power loss is a big enough event for a power grid [21, 22]), we divide

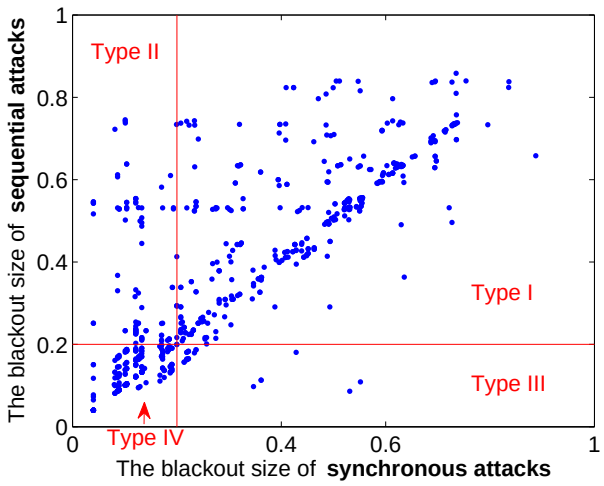


Figure 6.3. The correlation between the sequential attack and the synchronous attack.

the 741 dots in Fig. 6.3 into four types as follows.

- *Type I*: Both the sequential attack and the synchronous attack are strong. That is, $\Delta_{seq}^2 \geq \eta$ and $\Delta_{syn}^2 \geq \eta$.

- *Type II*: The sequential attack is strong, while the synchronous attack is weak, which means $\Delta_{seq}^2 \geq \eta$ and $\Delta_{syn}^2 < \eta$.

- *Type III*: The sequential attack is weak, while the synchronous attack is strong, which means $\Delta_{seq}^2 < \eta$ and $\Delta_{syn}^2 \geq \eta$.

- *Type IV*: Both the sequential attack and the synchronous attack are weak. That is, $\Delta_{seq}^2 < \eta$ and $\Delta_{syn}^2 < \eta$.

Type II is particularly interesting. From the perspective of the synchronous attack (i.e., according to x-axis), dots belonging to Type I and Type III are strong attacks, while dots in Type II and Type IV are weak attacks. However, if refer to y-axis, from the sequential attack's point of view, dots in Type II are viewed as strong attacks. It is clearly seen from Fig. 6.3 that there are a considerable

number of dots belonging to Type II. In particular, the dots in Type II are of importance to reveal new vulnerability of power grids, which are not discovered in previous works.

Second, from Fig. 6.3, we see that the sequential attack can not only discover new vulnerabilities but improve the strength of many two-node attacks. We compare Δ^2_{seq} with Δ^2_{syn} and categorize these 741 dots into three groups.

- *Group 1*: The performances of the sequential attack and the synchronous attack are similar. If the difference between Δ^2_{seq} and Δ^2_{syn} is less or equal to the threshold θ (i.e., $|\Delta^2_{seq} - \Delta^2_{syn}| \leq \theta$), we put this dot (i.e., a two-node combination) into group 1.

- *Group 2*: The sequential attack is stronger than the synchronous attack. If $\Delta^2_{seq} - \Delta^2_{syn} > \theta$, the dot is put into group 2.

- *Group 3*: The synchronous attack is stronger than the sequential attack. If $\Delta^2_{syn} - \Delta^2_{seq} > \theta$, the dot is put into group 3.

For the dots in Group 2, the sequential attack reaches better strength than the synchronous attack. We set θ to be 0.1. Among the 741 dots in Fig. 6.3, 75.44% belong to Group 1, 22.94% belong to Group 2, and only 1.62% belong to Group 3. This statistic demonstrates the sequential attack can find more strong attacks.

More demonstrations and analysis on the features of the sequential attack are discussed in Section 6.7.

6.6 Sequential Attack Strategy

The *sequential attack strategy* (SeqAS) is referred to as the method to identify multiple VNs and the order of sequentially removing. In this section, we extend

three existing synchronous attack strategies to the sequential attack scenarios in Sections 6.6.1 and 6.6.2, and propose a new SeqAS in Section 6.6.3.

6.6.1 Degree-based and Load-based Sequential Attack Strategies

Two metrics, degree and load, have been widely used in the SynAS [8, 9, 17, 21, 24, 25, 30, 31]. We straightforwardly extend the degree-based and load-based synchronous attack strategies to obtain the degree-based and load-based sequential attack strategies. The *degree of a node* is defined as the number of the links connecting to this node [9]; the *load of a node* is defined as the summation of the absolute values of power injection into this node by all generation-demand-node pairs [21]. This load definition is similar to the functionality of other definitions, e.g., betweenness in [8] and extended betweenness in [18].

We present the degree-based SeqAS with M VNs, denoted by $SeqAS^{M}_{degree}$ as follows. There are two steps. In the first step, select M nodes with maximum degrees as the VNs. This is the same as the degree-based SynAS in [8, 21, 24]. In the second step, we determine the order of removal of these VNs. We study two orders: (1) from higher degree to lower degree, and (2) from lower degree to higher degree. We choose the order that yields the stronger attack strength. In other words, we need to perform twice the sequential attack CFS to determine the order of removal.

The specific time of removing these M VNs is presented in Section 6.4 and briefly described as follows. The first removal is conducted as at the beginning. The m^{th}, $2 \leq m \leq M$, removal is conducted either after the $(m-1)^{th}$ removal or after tripping an overloaded link. Take removing two VNs as an example. Removing the first VN occurs at the beginning. After the removal, if there exists overloaded link(s), removing the second VNs will be conducted after tripping an such overloaded link; otherwise, the second removal is conducted after the first

removal.

The load-based SeqAS with M VNs, denoted by $SeqAS^M_{load}$, uses the same procedure, except replacing "degree" by "load".

6.6.2 Exhaustive Search Based Sequential Attack Strategy

The strongest multiple-node sequential attack can be found through the exhaustive search. Let $SeqAS^M_{ES}$ denote the exhaustive search based SeqAS with M VNs. In a power grid with $N_{\mathcal{B}}$ nodes, $SeqAS^M_{ES}$ needs to launch $\binom{N_{\mathcal{B}}}{M} \times M!$ times of the sequential attack CFS. Obviously, for a large-scale power grid, $SeqAS^M_{ES}$ is computationally infeasible. We use $SeqAS^M_{ES}$ as the comparison scheme to analyze the complexity of other attack strategies, which will be discussed in Section 6.7.5.

6.6.3 Proposed Sequential Attack Strategy

In this substation, we present a practical and strong SeqAS with three steps. The first step is to use the iterative procedure (Section 6.6.3) to search multiple-node combinations that yield strong sequential attacks. The second step is to construct the *sequential attack graph* (SAG) (Section 6.6.3). The final step is to determine the VNs and removal order based on the SAG (Section 6.6.3). This proposed scheme is called the *SAG-based SeqAS*, denoted by $SeqAS^M_{SAG}$.

Iterative Procedure

The iterative procedure in [11] is an effective and efficient way to find node combinations that yield strong synchronous attacks. The rationale behind is that if a m-node combination can yield strong synchronous attack, by combining these m nodes with another important node, the new $(m+1)$-node combination likely become another strong synchronous attack. Here, the important node refers to these nodes that has strong single-node attack performance; the selection of important nodes (also referred to as candidate nodes) is discussed in the following

Table 6.2. The realization of RRCS on IEEE 39 bus system.

Index	Set^2_{RRC}	Set^3_{RRC}	Set^4_{RRC}	Set^5_{RRC}
1	21,33	21,33,39	26,31,39,20	26,31,39,20,21
2	31,21	24,33,39	26,31,39,3	26,31,39,20,27
3	6,21	26,31,39	6,33,39,34	26,31,39,20,24
4	24,33	6,33,39	31,35,39,20	26,31,39,20,6
5	31,24	31,22,39	31,22,39,20	26,31,39,20,2
6	6,24	31,35,39	31,33,39,20	26,31,39,20,11
7	6,33	31,33,39	31,36,39,20	26,31,39,20,14
8	2,31	31,36,39	21,33,39,34	26,31,39,20,16
9	27,6	6,24,39	21,33,39,20	26,31,39,20,38
10	26,31	31,21,39	24,33,39,20	26,31,39,20,29
11	14,39	27,6,39	24,33,39,34	26,31,39,20,15
12	31,22	14,39,24	14,39,8,19	26,31,39,20,3
13	31,35	14,39,8	21,33,39,8	26,31,39,20,35
14	31,33	24,33,31	21,33,39,4	26,31,39,20,22
15	31,36	31,21,20	24,33,39,8	26,31,39,20,33
16	31,23	31,21,7	24,33,39,4	26,31,39,20,19

part of this section. We extend this rationale to exploit node combinations that yield strong sequential attacks.

Next, we briefly introduce the iterative procedure used in this work. This brief introduction focuses on the main idea of the procedure. For interesting readers, more details can be found in [11, 32].

- Assume the power grid has $N_{\mathcal{B}}$ nodes, and the total number of iteration rounds is $\hat{M}$.

- The rationale is to design a $\hat{M}$-round iterative process to search the node combinations that yield strong sequential attacks. We consider two restrictions. First, we select P nodes as *candidate nodes*, denoted by Set_C. Second, in each round we select R node combinations as *round recommended combination set* (RRCS). The m^{th} RRCS ($1 \leq m \leq \hat{M}$) is denoted by Set^m_{RRC}. The parameter P and R will be introduced later.

- The strength of a node or a node combination is measured in terms of the blackout size defined in Equ. 6.4. Stronger nodes or node combinations yield larger blackout size.

- In the 1^{st} round, the iteration is initialized. We first conduct $N_{\mathcal{B}}$ one-node attacks, then select the top P strongest nodes as candidate nodes and put them into Set_C, and finally select the top R strongest nodes as 1^{th} RRCS and put them into Set^1_{RRC}.

- In the following each round, e.g., m^{th} round, we do three steps. First, combine each candidate node in Set_C with each node combination in Set^{m-1}_{RRC} to obtain $P \times R$ m-node combinations. Then, conduct the sequential attack using nodes in each m-node combination as VNs. Finally, select top R strongest combinations, out of $P \times R$ combinations, as m^{th} RRCS and put them into Set^m_{RRC}.

- The set-up of parameters R and P are of importance to limit the search space. For R, we choose a small value, e.g., 16 in this work, because selecting a few strongest node combinations within each round are enough to find strong attacks [11]. For P, it can vary according to the scale of a power grid (i.e., $N_{\mathcal{B}}$). For a small-scale power grid, e.g., IEEE 39 bus system, P can be $N_{\mathcal{B}}$. For a large-scale power grid, e.g., Polish transmission system with $N_{\mathcal{B}} = 2383$ nodes, P can be a value that is much smaller than $N_{\mathcal{B}}$, e.g., $P = 150$. Because these most vulnerable nodes are more critical than others in finding strong attacks [8, 9, 21].

Referring to multiple-node attacks, node combinations in $\{Set^2_{RRC}, Set^3_{RRC}, ..., Set^{\hat{M}}_{RRC}\}$ are the strong sequential attacks found. Take IEEE 39 bus system as an example, when the parameters P, R and $\hat{M}$ are set to

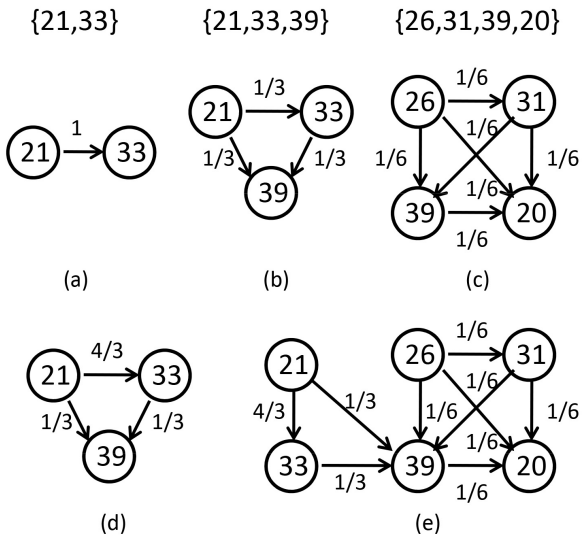


Figure 6.4. The demonstration of constructing SAG

be 39, 16 and 5, respectively, a realization of $\{Set^2_{RRC}, Set^3_{RRC}, Set^4_{RRC}, Set^5_{RRC}\}$ is shown in Table 6.2. It is seen that the iterative procedure identifies top R strongest node combinations within each iteration round.

Sequential Attack Graph

We specifically design a new metric, called *sequential attack graph* (SAG), to find VNs and their removal order. The SAG metric is constructed according to RRCS obtained in Section 6.6.3. The construction of SAG includes the following steps.

- **Step 1**: For a given power grid, set up parameters P, R and $\hat{M}$ and obtain RRCS (i.e., $\{Set^2_{RRC}, ..., Set^{\hat{M}}_{RRC}\}$). An example of RRCS is demonstrated in Table 6.2.

- **Step 2**: Generate the *combination-SAG* for each node combination. Take the combination $\{b_1, b_2, b_3\}$ as an example. First, add three vertexes, labeled as b_1, b_2 and b_3. Second, for each pair of nodes in this combination, add a directed edge with the direction pointing from the node at front to the

node behind. That is, $b_1 \rightarrow b_2$, $b_1 \rightarrow b_3$ and $b_2 \rightarrow b_3$. Finally, assign the weight to each edge, referred to as the *edge occurrence frequency* (EOF). If a combination has m nodes, there are $\frac{m(m-1)}{2}$ edges and the EOF of each edge is $\frac{2}{m(m-1)}$, such that the total weight introduced by this combination is 1. Referring to the example, m equals to 3 and the EOF of each edge is $\frac{1}{3}$. Figs. 6.4(a), 6.4(b) and 6.4(c) demonstrate the examples of the combination-SAG.

- **Step 3**: Merge all combination-SAGs to generate the SAG. We give an example of merging two combination-SAGs as follows. First, put all vertexes in both combination-SAGs into a new combination-SAG, and merge the repeated vertexes. Second, put all edges in both combination-SAGs into the new combination-SAG. For the repeated edges, merge them and sum their EOF as the new EOF; for the non-repeated edge, keep this edge and its EOF. Figs. 6.4(d) and 6.4(e) demonstrate the results of merging two combination-SAGs. Fig. 6.4(d) is generated by merging Fig. 6.4(a) and Fig. 6.4(b); Fig. 6.4(e) is generated by merging Fig. 6.4(c) and Fig. 6.4(d).

The SAG of IEEE 39 bus system, for example, is constructed based on Table 6.2 and demonstrated in Fig. 6.5, where the width and color of an edge is determined by its EOF. The wider and darker an edge is, the larger the EOF is.

SAG-based Sequential Attack Strategy

The direction and weight of an edge in SAG convey important information. The higher the weight of an edge is , the more likely the pair of nodes connected by this edge is a strong sequential attack. The direction represents the removal order of these two nodes.

Recall that SAG is constructed base on RRCS, $\{Set^2_{RRC}, ..., Set^{\hat{M}}_{RRC}\}$. This SAG can be used to find strong sequential attacks, as long as the number of VNs

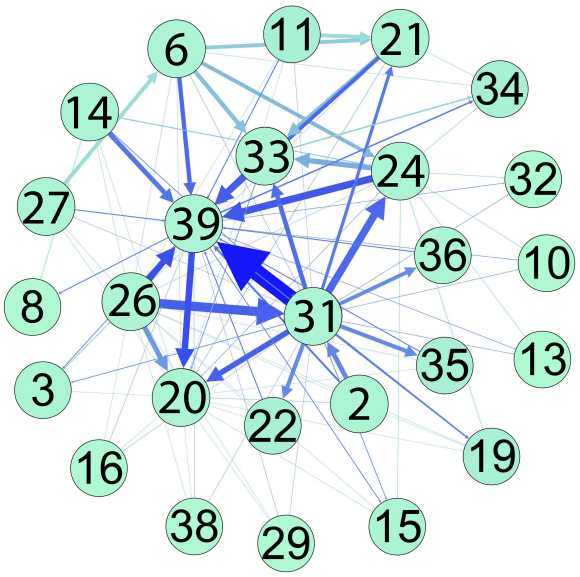


Figure 6.5. The sequential attack graph of IEEE 39 bus system.

(i.e., M) is no larger than $\hat{M}$ (i.e., $M \leq \hat{M}$).

We propose a sequential attack strategy, called the *SAG-based SeqAS*. Let $SeqAS^{M}_{SAG}$ denote the SAG-based SeqAS with M VNs. $SeqAS^{M}_{SAG}$ is conducted as follows.

- Construct the SAG, where $\hat{M} \geq M$.
- Find all interesting M-VN combinations in SAG. Each interesting combination, e.g., $\{b'_1, b'_2, ..., b'_M\}$, satisfies the condition that for any pair of i and j, $1 \leq i < j \leq M$, there exists an edge between b'_i and b'_j, and the direction is $b'_i \rightarrow b'_j$.
- For each interesting combination, compute the summation of EOF for all edges. The combination that yields the largest EOF summation is chosen as the VNs for $SeqAS^{M}_{SAG}$. In this combination, the removal order already exists. That is, b'_i is removed earlier than b'_j, if $i < j$. The corresponding removal order is $1, 2, \cdots, M$.

For instance, according to SAG in Fig. 6.5, if attackers want to choose three VNs (i.e., $M = 3$) for $SeqAS^3_{SAG}$, the VNs chosen by the above procedure is $\{26, 31, 39\}$. The removal order is first node 26, then node 31, and finally node 39. Determining removal time is discussed in Section 6.4. For example, the node 26 is initially removed, which might cause some links to be overloaded. The second removal, removing node 31, occurs either after removing node 26 or after tripping an overloaded link caused by removing node 26. The time to remove node 39 is similarly determined.

The basic idea behind $SeqAS^M_{SAG}$ is to find these VNs whose node pairs occur most frequently in RRCS. Obviously, it is not guaranteed that the above procedure can discover the strongest M-node sequential attack, which can be found by $SeqAS^M_{ES}$. The complexity of $SeqAS^M_{SAG}$, however, is much lower than that of $SeqAS^M_{ES}$, as demonstrated in Section 6.7.5.

6.7 Simulations and Discussions

We investigate the sequential attack on three different test benchmarks, IEEE 39 and 300 bus systems and Polish transmission system, which are all available in MATPOWER [33]. The brief description of these test benchmarks is given in Table 6.3. IEEE 39 bus system, a small-scale power grid, is used to demonstrate new vulnerabilities discovered by the sequential attack. All test benchmarks are adopted to compare the proposed SAG-based SeqAS with comparison schemes. Simulations are conducted in Matlab environment.

Table 6.3. Description of test benchmarks

Test Benchmarks	$N_{\mathcal{B}}$	$N_{\mathcal{L}}$	$N_{\mathcal{G}}$	$N_{\mathcal{D}}$
IEEE 39 bus system	39	46	10	21
IEEE 300 bus system	300	411	69	191
Polish transmission system	2,383	2,896	327	1,817

6.7.1 Further Demonstration of the Sequential Attack

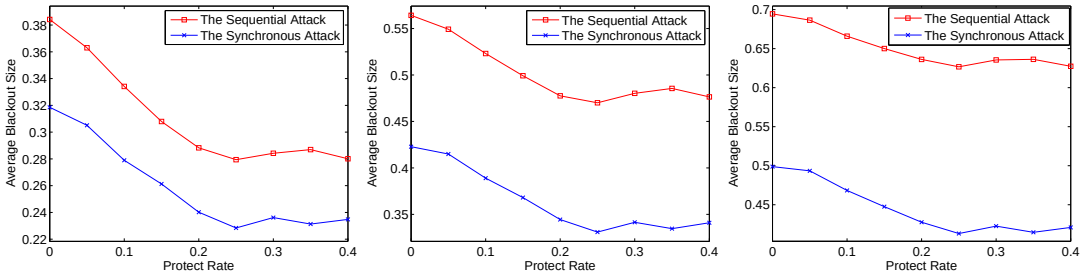
In this subsection, we extend the demonstration of the sequential attack. In Section 6.5 we have demonstrated the new vulnerabilities discovered by the sequential attack. Here, we extend the demonstration by conducting three-node attacks and four-node attacks on IEEE 39 bus system.

Similar to the discussion in Section 6.5.3, we conduct both the sequential attack and the synchronous attack for each three-node/four-node combination, obtain two strength values, and perform two types of classifications. Take three-node attacks as an example. There are in total 9,139 three-node combinations. For each combination, we obtain Δ^3_{seq} and Δ^3_{syn}. By comparing both Δ^3_{seq} and Δ^3_{syn} with the threshold η (i.e., $\eta = 0.2$), we divide these 9,139 combinations into four types (i.e., Type I, Type II, Type III and Type IV). Note that the combinations in Type II represent the new vulnerabilities. Recall that new vulnerabilities refer to the strong multiple-node combinations that are individually discovered by the sequential attack. If only the synchronous attack is used in vulnerability analysis, these new vulnerable combinations will not be recognized as critical ones, in terms of causing cascading failures. In addition, we can divide these combinations into three groups (i.e., Group 1, Group 2 and Group 3). The combinations in Group 2 lead to sequential attacks that are stronger than synchronous attacks.

There are 82,251 four-node combinations; similar classifications are conducted. Comparison results are shown in Table 6.4 and Table 6.5, respectively. We have the following observations.

- As M increases, the number of multiple-node combinations belonging to Type II increases sharply, which is highlighted in bold in Table 6.4. This means that the sequential attack can discover more new vulnerabilities.

- As M increases, the percentages of Group 2, highlighted in bold in Table 6.5,



(a) Two-node (b) Three-node (c) Four-node

Figure 6.6. Comparisons between the sequential attack and the synchronous attack

go up quickly, which means the sequential attack can exploit more strong attacks.

Table 6.4. The number of node combinations belonging four types on IEEE 39 bus system.

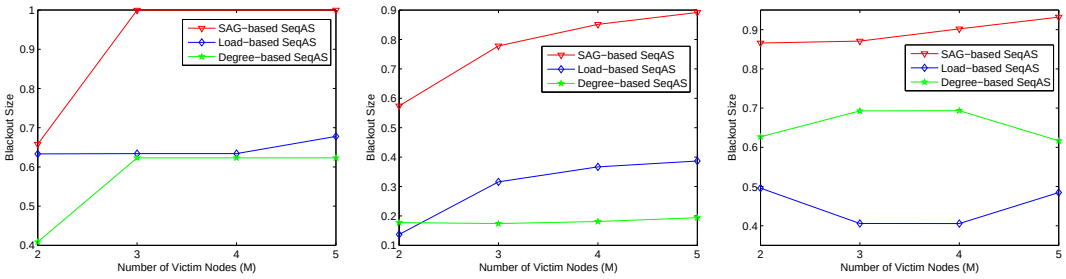
$M-$node removals	Type I	Type II	Type III	Type IV
Two-node	415	**93**	21	212
Three-node	7,307	**1,342**	99	391
Four-node	76,136	**5,742**	117	256

Table 6.5. The percentage of node combinations belonging three groups on IEEE 39 bus system.

$M-$node removals	Group 1	Group 2	Group 3
Two-node	75.44%	**22.94%**	1.62%
Three-node	51.15	**47.18%**	1.66%
Four-node	34.17%	**65.43%**	0.40%

6.7.2 Comparison Between the Sequential Attack and the Synchronous Attack in terms of Attack Strength

Although we focus on studying the attack in the work, we want to understand the attack strength under simple defense scheme. It is reasonable to assume that some critical nodes in a power grid have strong physical and/or cyber protection such that the attacker cannot successfully remove them [6, 34]. In this subsection,



(a) (b) (c)

Figure 6.7. Blackout size versus the number of victim nodes

we compare the sequential attack with the synchronous attack in terms of the average strength, under the condition that some critical nodes are protected from the initial removal. In particular, the comparison is conducted as follows.

- We sort all nodes of a power grid in a list by Δ^1_{syn}, i.e., the strength of one-node attacks, from the largest to the smallest. Note that Δ^1_{syn} and Δ^1_{seq} are the same since there is no sequential concept when considering one-node attacks. The nodes on the top of the list are the ones to be protected.

- We introduce the *protection rate*, denoted by α. Assume that the top $\lceil N_{\mathcal{B}} \times \alpha \rceil$ nodes on the above list are protected, where $\lceil \bullet \rceil$ is to obtain the nearest integer towards infinity. That is, these nodes cannot be initially removed by the attacker, but can be failed due to the overloading during the cascading process.

- We consider multiple-node attacks, where nodes can only be chosen from the $N'_{\mathcal{B}} = N_{\mathcal{B}} - \lceil N_{\mathcal{B}} \times \alpha \rceil$ unprotected nodes. Let $\overline{\Delta}_{seq}$ and $\overline{\Delta}_{syn}$ denote the *average blackout size* for the sequential attack and the synchronous attack, respectively. Considering M-node attacks, there are in total $\binom{N'_{\mathcal{B}}}{M}$ combinations. We perform the sequential attack on each combination, and average all

$\binom{N'_{\mathcal{B}}}{M}$ strength values as $\overline{\Delta}_{seq}$. Similarly, we conduct the synchronous attack on all combinations and obtain $\overline{\Delta}_{syn}$.

- In simulations, α is chosen from 0 to 0.4 with the step size as 0.05; M is set to be 2, 3 and 4, respectively.

Comparisons are demonstrated in Fig. 6.6, where three subfigures show comparisons regarding two-node attacks, three-node attacks and four-node attacks, respectively. In each subfigure, the x-axis represents the *protect rate*; y-axis represents the *average blackout size*. In addition, the red-square curve represents $\overline{\Delta}_{seq}$; the blue-star curve represents $\overline{\Delta}_{syn}$. The observations and discussions made from Fig. 6.6 are given as follows.

First, on average, the sequential attack is stronger than the synchronous attack. In the three subfigures, the red-square curves are higher than the blue-star curves. That is, the sequential attack can obtain better average attack performance. For instance, when the protect rate is zero ($\alpha = 0$), meaning no nodes are protected, $\overline{\Delta}_{seq}$ are 0.38, 0.56 and 0.69, while $\overline{\Delta}_{syn}$ are relatively 0.32, 0.42 and 0.5 (see in Fig. 6.6).

Second, the protection scheme can reduce the damage caused by initial removals to the power grid. As α increases from 0 to 0.25, all curves in Fig. 6.6 decrease. This is reasonable. Because, as the number of critical nodes that are protected from initial removals increases, there will be less and less multiple-node combinations that can yield strong attack performance. Therefore, as α further increases from 0.3 to 0.4, the curves do not reduce monotonically. The small fluctuations occur because the total number of combinations at these α values are different and their average blackout size fluctuates. In general, both $\overline{\Delta}_{syn}$ and $\overline{\Delta}_{syn}$ go down as α increases in a range, from 0 to 0.25 on IEEE 39 bus system.

Third, the protection scheme alone cannot solve the cascading failure problem. The simulation is conducted under the assumption that up to 40% of nodes are initially protected, which is really high percentage in any realistic systems. However, even α is chosen as 0.4, on IEEE 39 bus system the average blackout size caused by the sequential attack is still around 0.28 for two-node attacks, 0.47 for three-node attacks, and 0.62 for four-node attacks. Besides the protected nodes, there are many remaining nodes, whose single removals might not cause serious cascading failures. The combination of these nodes, however, can cause moderate-scale, even large-scale, power outages. Note that our discussion here bases on the assumption that people can only choose and protect a limited number of critical nodes. It is not practical to protect a large number of, or even all, nodes in a power grid.

Finally, as M increases, the sequential attack yields better attack strength. We can see from the three subfigures in Fig. 6.6 that the gap between the two curves becomes larger while M increases from 2 to 4. This is reasonable. In this work, for a M-node combination, we perform the exhaustive search to find the removal order with the largest Δ for the sequential attack (discussed in Section 6.5.2). When M increases, the total number of removal orders (i.e., $M!$) increases sharply. The sequential attack has more flexibility, and the synchronous attack is a special case of the sequential attack.

6.7.3 Comparison among Different Sequential Attack Strategies

In this subsection, we compare the proposed the SGA-based SeqAS with the straightforward degree-based SeqAS and load-based SeqAS. Comparisons are conducted on IEEE 39 and 300 bus systems and Polish transmission system, where the number of VNs (M) is set to be 2, 3, 4 or 5. Results are shown in Fig. 6.7, where three subplots represent comparisons on different test benchmarks. In each subplot, x-axis represents the number of victim nodes (VNs); y-axis represents

the blackout size. In addition, red-triangle curves, blue-square curves and green-pentagram curves represent the strength of $SeqAS^M_{SAG}$, $SeqAS^M_{load}$ and $SeqAS^M_{degree}$, respectively. Based on Fig. 6.7, we have the following observations and discussions.

First, the proposed metric, *SAG*, is better than the widely-studied metrics, *degree* and *load*, in terms of finding stronger sequential attacks. It is clearly seen from Fig. 6.7 that the proposed $SeqAS^M_{SAG}$ is much stronger than $SeqAS^M_{load}$ and $SeqAS^M_{degree}$. In Fig. 6.7(b), for instance, the strengths of $SeqAS^3_{SAG}$, $SeqAS^3_{load}$ and $SeqAS^3_{degree}$ are 0.78, 0.32 and 0.17, respectively. These results are reasonable. The metrics, degree and load, are not specifically designed for the sequential attack. These metrics cannot accurately find VNs and the removal order, which can yield strong sequential attack. However, the proposed metric, SAG, can reveal not only vulnerable nodes but orders of their removals (an example is shown in Fig. 6.5). From the perspective of the sequential attack, SAG is an effective metric.

Second, it is highly possible to cause serious power loss to a power grid by only sequentially removing several VNs. This observation agrees with a recent discovery in [35]. In this article published at Nature news, the author discussed that in power grids failure in one place leads to failure in another place, which cascades into collapse. $SeqAS^M_{SAG}$ is powerful to cause serious power loss. In Fig. 6.7(c), for example, if only two VNs are chosen and removed from Polish transmission system (less than 1‰ of the total number of nodes), $SeqAS^2_{SAG}$ can cause nearly 87% power loss, a serious blackout case. It is clearly seen that $SeqAS^M_{SAG}$ is a strong attack strategy against power grids.

6.7.4 Comparison Between the proposed SeqAS and Synchronous Attack Strategies

In this subsection, we compare the SAG-based SeqAS with three synchronous attack strategies, the degree-based SynAS, denoted by $SynAS^M_{degree}$, the load-

Table 6.6. Comparisons between the proposed attack strategy with other attack strategies

Test Benchmark	Attack Strategy	$M = 2$	$M = 3$	$M = 4$	$M = 5$
IEEE 39 Bus System	$SeqAS^M_{SAG}$	0.66	**1**	**1**	**1**
	$SynAS^M_{degree}$	0.43	0.63	0.63	0.63
	$SynAS^M_{load}$	0.63	0.63	0.63	0.74
	$SynAS^M_{RG}$	**0.89**	0.65	1	1
IEEE 300 Bus System	$SeqAS^M_{SAG}$	**0.57**	**0.78**	**0.85**	**0.89**
	$SynAS^M_{degree}$	0.23	0.22	0.22	0.26
	$SynAS^M_{load}$	0.15	0.30	0.35	0.37
	$SynAS^M_{RG}$	0.48	0.77	0.84	0.86
Polish System	$SeqAS^M_{SAG}$	**0.86**	**0.87**	0.90	**0.93**
	$SynAS^M_{degree}$	0.63	0.67	0.67	0.39
	$SynAS^M_{load}$	0.53	0.39	0.39	0.38
	$SynAS^M_{RG}$	0.78	0.86	**0.93**	0.87

based SynAS, denoted by $SynAS^M_{load}$, and the RiskGraph-based SynAS, denoted by $SynAS^M_{RG}$. In the current literature [8, 9, 11, 21, 25], there schemes represent the most popular ones and are conducted as follows.

- $SynAS^M_{degree}$: Calculate the degree for all nodes, and select M nodes with top largest degree as VNs [9].
- $SynAS^M_{load}$: Calculate the load for all nodes, and select M nodes with top largest load as VNs [21].
- $SynAS^M_{RG}$: Construct the metric, *Risk Graph* (RG), and select M nodes that are tightly connected in RG as VNs [11].

All three benchmarks are used in this comparison. We set the number of VNs (i.e., M) to be 2, 3, 4 and 5. Results are demonstrated in Table 6.6. The strengths of $SeqAS^M_{SAG}$ are underlined; in each group comparison, the strongest strength is highlighted in bold. We make the following observations.

First, $SeqAS^M_{SAG}$ is much stronger than $SynAS^M_{load}$ and $SynAS^M_{degree}$. Because, the metric, SAG, is specifically designed and more accurate than degree and load in finding multiple-node combinations that yield strong attacks.

Second, $SeqAS^M_{SAG}$ is mostly stronger than $SynAS^M_{RG}$, with a few exceptions. In Table 6.6, we can see that $SeqAS^M_{SAG}$ is weaker than $SynAS^M_{RG}$ only at $M = 2$ for IEEE 39 bus system and $M = 4$ for Polish transmission system. We explain this as follows. In Fig. 6.3, it is already shown that the strongest synchronous attack (according to x-axis) has similar strength to the strongest sequential attack (according to y-axis). Although, in an average sense the sequential attack is stronger the synchronous attack, the SeqAS does not guarantee to yield the strongest attack. This also indicates that $SeqAS^M_{SAG}$ can be further improved. For example, we allow that more than one nodes can be removed at the same time. That is, allow "equality" in the Equ. 6.3. This combination of sequential and synchronous attacks has a potential to yield strong attacks.

In summary, compared with the existing synchronous attack strategies, $SeqAS^M_{SAG}$ can surely yield larger damage and needs to be considered in designing defense approaches for power grids.

6.7.5 Complexity Analysis of Different Attack Strategies

In the current literature [3, 4, 26], the cascading failure in power grids is considered to be a complex process, and the close-form theoretical analysis the cascading failure is still unavailable. In this work, we use two CFSs, the sequential attack CFS and the synchronous attack CFS. Both are introduced in Section 6.4. We use O_{SeqCFS} to represent the computational complexity of the sequential attack CFS and O_{SynCFS} to represent the computational complexity of the synchronous attack CFS.

Although, theoretical complexities of O_{SeqCFS} and O_{SynCFS} are unavailable,

their numerical complexities can be obtained by simulations. On Window 7 OS with 4 GB memory and dual-core i5 CPU (2.4GHz each), we run the sequential attack CFS for 1000 times on each test benchmark, and obtain the average time as the numerical complexity of O_{SeqCFS}. Similarly, we can obtain the numerical complexity of O_{SynCFS}. In Table 6.7, numerical complexities are demonstrated. The unit is second (s). We have the following observations.

- Numerically, O_{SeqCFS} and O_{SynCFS} are almost the same on each test benchmark. Because, both CFSs use similar cascading procedures (discussed in Section 6.4).
- The numerical complexities increase dramatically as $N_{\mathcal{B}}$ increases. The scale of the power gird is an important factor to the computational complexity of both CFSs.

Table 6.7. Numerical complexity values.

	$N_{\mathcal{B}} = 39$	$N_{\mathcal{B}} = 300$	$N_{\mathcal{B}} = 2383$
O_{SeqCFS}	0.0107 (S)	0.0367 (S)	41.37 (S)
O_{SynCFS}	0.0108 (S)	0.0367 (S)	40.82 (S)

To compare different attack strategies on the same power grid, we use O_{SeqCFS} and O_{SynCFS} as the basic *unit* for complexity analysis. In other words, the complexity of an attack strategy is the number of times that this method needs to launch CFS before identifying its VNs. Compared with running once CFS, the complexity of other calculations is negligible. This philosophy of complexity analysis has been widely adopted in the existing works [4, 22, 32].

First, we calculate the complexity of $SeqAS^M_{ES}$, denoted by Ω^{ES}_{SeqAS}. $SeqAS^M_{ES}$ needs to search among $\binom{N_{\mathcal{B}}}{M} \times M!$ different removal orders. The complexity of $SeqAS^M_{ES}$ is,

$$\Omega^{ES}_{SeqAS} = \binom{N_{\mathcal{B}}}{M} \times M! \tag{6.5}$$

Second, we calculate the complexity of $SeqAS^M_{degree}$, denoted by Ω^{degree}_{SeqAS}. There are two steps to obtain Ω^{degree}_{SeqAS}. The first step is to obtain the metric, degree. This step dose not rely on CFS; the complexity is counted as 0. The second step is to determine VNs as well as the removal order. Determining VNs dose not rely on CFS; the complexity is counted as 0. Determining the removal order needs to run CFS twice, meaning the complexity is counted as 2. Therefore, the complexity of the second step is counted as 2. In summary, Ω^{degree}_{SeqAS} is counted as 2 (i.e., $0 + 2$).

In addition, let Ω^{degree}_{SynAS} denote the complexity of $SynAS^M_{degree}$. The calculation of Ω^{degree}_{SynAS} is similar to that of Ω^{degree}_{SeqAS}. The difference is that $SynAS^M_{degree}$ does not need to determine the removal order of VNs. Therefore, determining VNs for $SynAS^M_{degree}$ does not rely on CFS; Ω^{degree}_{SynAS} is counted as 0. The complexities of $SynAS^M_{degree}$ and $SeqAS^M_{degree}$ are,

$$\begin{aligned} \Omega^{degree}_{SynAS} &= 0 \\ \Omega^{degree}_{SeqAS} &= 2 \end{aligned} \tag{6.6}$$

Third, calculating the complexity of $SeqAS^M_{load}$, denoted by Ω^{load}_{SeqAS}, is similar to that of Ω^{degree}_{SeqAS}; calculating the complexity of $SynAS^M_{load}$, denoted by Ω^{load}_{SynAS}, is similar to that of Ω^{degree}_{SynAS}.

Finally, we calculate the complexity of $SeqAS^M_{SAG}$, denoted by Ω^{SAG}_{SeqAS}. There are two steps to obtain Ω^{SAG}_{SeqAS}. The first step is to obtain the metric, SAG, which includes searching for RRCS (discussed in Section 6.6.3) and constructing SAG (discussed in Section 6.6.3). Obtaining RRCS needs to run CFS in total $N_{\mathcal{B}} + P \times P \times (M-1)$ times; constructing SAG dose not rely on CFS. Therefore, the complexity of the first step is counted as $N_{\mathcal{B}} + P \times P \times (M-1)$. R and P are chosen to be less or equal to $N_{\mathcal{B}}$. At the worst case, when $R = P = N_{\mathcal{B}}$, the complexity of the first step is counted as $(M-1) \times (N_{\mathcal{B}})^2 + N_{\mathcal{B}}$, the same order to $M \times (N_{\mathcal{B}})^2$. The second step is to choose VNs and the removal order from SAG

Table 6.8. The complexity comparison among different attack strategies.

Attack Strategies	$SeqAS^M_{ES}$	$SeqAS^M_{SAG}$		$SynAS^M_{RG}$		$SynAS^M_{degree}$	$SynAS^M_{load}$	$SeqAS^M_{degree}$	$SeqAS^M_{load}$
Complexity	$\binom{N_{\mathcal{B}}}{M}\cdot M!$	Off-line	On-line	Off-line	On-line	0	0	2	2
		$M\times(N_{\mathcal{B}})^2$	0	$M\times(N_{\mathcal{B}})^2$	0				

(discussed in Section 6.6.3). This step does not rely on CFS; the complexity is counted as 0.

In practice, as long as attackers know the topology and electrical features of a power grid, they can construct SAG of the power grid in advance. This step can be done *off-line*. When conducting the attack, attackers may encounter different situations. If an attacker, for instance, has observed that node 31 in Fig. 6.5 is down for some reasons (e.g., nature disasters and previous attacks), he/she can quickly identify a sequential attack strategy by adding another VN, e.g. node 39, to the already-down node 31. Therefore, sequential attacks can be conducted *on-line* based on SAG.

From the above discussions, Ω^{SAG}_{SeqAS} consists of two parts as follows,

$$\Omega^{SAG}_{SeqAS} = \begin{cases} M\times(N_{\mathcal{B}})^2 & \text{Off-line} \\ 0 & \text{On-line} \end{cases} \tag{6.7}$$

The calculation of the complexity of $SynAS^M_{RG}$, denoted by Ω^{RG}_{SynAS}, is similar to that of Ω^{SAG}_{SeqAS}.

Generally speaking, other attack strategies in this work are conducted on-line. $SeqAS^M_{ES}$ is not a metric-based approach, and can only be conducted on-line. In addition, compared with simulating cascading failures, obtaining the metrics, degree and load, is fast, and does not need to be specifically calculated off-line. Therefore, the degree-based and load-based approaches can be conducted on-line.

In summary, complexity comparisons among different attack strategies in this work are given in Table 6.8. For the proposed SAG-based SeqAS, its on-line complexity is as low as that of the degree-based and load-based attack strategies,

and its off-line complexity is much lower than that of the exhaustive search SeqAS.

6.8 Conclusions and Future Works

In this work, we investigated the sequential attack against power grids. The sequential attack can discover new vulnerabilities of power grids. We specifically designed the metric SAG, and proposed the SAG-based SeqAS. Intensive experiments were conducted to study the features of the sequential attack, and to compare the proposed SAG-based SeqAS with the existing approaches.

There are several possible future directions along this topic. First, it is of importance to study the relation between the removal order of VNs and the performance. Are there better methods to determine the removal order besides searching all possible removal orders? Second, the proposed metric, SAG, demonstrates how nodes are related to each other in terms of sequential removals. This information can be exploited in terms of designing defense solutions against malicious attacks. Third, the construction of SAG on large-scale power grids, e.g., with thousands of nodes, is time-consuming, even computationally infeasible. Developing new strong SeqAS with lower complexity is needed. Finally, the visulization of sequential attacks and cascading process can help people better understand the triggers and propagation of cascading failures.

List of References

[1] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.

[2] The Guardian. "India blackouts leave 700 million without power." [Online]. Available: http://www.guardian.co.uk/

[3] R. Baldick et. al., "Initial review of methods for cascading failure analysis in electric power transmission systems," in *IEEE power engineering society general meeting*, Pittsburgh, PA, USA, July20-24 2008.

[4] M. Vaiman et. al., "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[5] "Attack ravages power grid." [Online]. Available: http://www.nytimes.com/

[6] X. Liu, K. Ren, Y. Yuan, Z. Li, and Q. Wang, "Optimal budget deployment strategy against power grid interdiction," in *Proceedings of IEEE INFOCOM*, Turin, Italy, Apr.14-19 2013.

[7] P. J. Hawrylak, M. Haney, M. Papa, and J. Hale, "Using hybrid attack graphs to model cyber-physical attacks in the smart grid," in *5th International Symposium on Resilient Control Systems*, Salt Lake City, UT, USA, Aug.14-16 2012.

[8] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *Eur. Phys. J. B*, vol. 46, pp. 101–107, 2005.

[9] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in U.S. power grid," in *Proceeding of IEEE Global Telecommunications Conference*, Houston, Texas, USA, Dec.5-9 2011.

[10] Y. Zhu, Y. Sun, and H. He, "Load distribution vector based attack strategies against power grid systems," in *Proceeding of IEEE Global Telecommunications Conference*, Anaheim, CA, USA, Dec.3-7 2012.

[11] Y. Zhu, J. Yan, Y. Sun, and H. He, "Risk-aware vulnerability analysis of electric grids from attacker's perspective," in *Proceeding of IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.

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

[13] J. E. David, "Double threat: US grid vulnerable on two fronts," Jan.5 2014. [Online]. Available: http://www.cnbc.com/

[14] "Platts." [Online]. Available: www.platts.com

[15] R. Lemos, "DHS video shows potential impact of cyberattack," Sept.27 2007. [Online]. Available: SecurityFocus.com

[16] P. K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "Network vulnerability to single, multiple, and probabilistic physical attacks," in *Military Communications Conference*, San Jose, CA, USA, Oct.31-Nov.3 2010.

[17] E. I. Bilis, W. Krger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 4, no. 7, pp. 854–865, Dec. 2013.

[18] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, pp. 1334–1340, July 2011.

[19] M. Khanabadi, H. Ghasemi, and M. Doostizadeh, "Optimal transmission switching considering voltage security and N-1 contingency analysis," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 0885–8950, Feb. 2013.

[20] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, June 2011.

[21] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, Sept. 2010.

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

[23] D. L. Pepyne, "Topology and cascading line outages in power grids," *Journal of Systems Science and Systems Engineering*, vol. 16, no. 2, pp. 202–221, June 2007.

[24] 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, Dec. 2009.

[25] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the north american power grid," *Phys. Rev. E*, vol. 69, no. 2, Feb. 2004.

[26] S. Mei, X. Zhang, and M. Cao, *Power Grid Complexity*. Beijing: Tsinghua University Press, Aug. 2011.

[27] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, *Power Generation, Operation and Control, 3rd Edition*. Wiley-Interscience, 2009.

[28] J. Yan, Y. Zhu, Y. Sun, and H. He, "Revealing temporal features of attacks against smart grid," in *IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.

[29] N. Fan, R. Chen, and J. Watson, "N-1-1 contingency-constrained optimal power flow by interdiction methods," in *IEEE Power and Energy Society General Meeting*, San Diego, CA, July22-26 2012.

[30] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, no. 5, May 2002.

[31] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, no. 4, Apr. 2004.

[32] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Transactions on Parallel and Distributed Systems*, 2014, in press.

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

[34] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, June 2011.

[35] J. Tollefson, "US electrical grid on the edge of failure," *Nature News and Comment*, Aug.25 2013.

CHAPTER 7

Summary

This dissertation is the study of *malicious attack strategies* against power grids. It investigated the vulnerability of power grids from the *attack* perspective. Different from the traditional contingency analysis, malicious attacks can be carefully designed by select substations, transmission lines, or both, as targets. In this dissertation, malicious attacks have been investigated from several perspectives.

- In manuscript 1, the details of failure propagation was demonstrated by a newly-designed platform. The proposed platform could visualize failure propagation in details, which was of great importance to help people understand such complicated phenomenon. In addition, by using the proposed platform to investigating single-substation failures, three different types of initial failures were discovered, which were *non-critical failures*, *rapid-and-critical failures*, and *propagative-and-critical failures*. These discoveries were meaningful to both attackers and defenders. For instance, from the attackers' perspective, propagative-and-critical failures provided a good direction to find stronger attacks. From the defenders' perspective, substations that yielded rapid-and-critical failures were very critical to the grid and needed to be protected from initial failures.

- In manuscript 2, it was assumed that attackers knew the topology of the target grid. Under this assumption, the efficiency model was used to mimic cascading failures. In particular, a new metric *load distribution vector* (LDV) was designed, and the LDV-based attack strategy was proposed. The load-based attack strategy was adopted as the comparison scheme, where the load

of a substation/transmission line was calculated as its betweenness. The simulation results showed that the LDV-based attack strategy could cause more damage than the comparison scheme in terms of reducing the grid network efficiency.

- In manuscript 3, it was assumed that the attackers would have some general information on the target grid, including the topology, the types of substations, and the admittance of transmission lines. With knowing of these information, the extended model was developed to mimic cascading failures. The extended model, obeying the Kirchoff's and Ohm's Laws, was more accurate than the efficiency model to reveal the power distribution in power systems. In particular, a novel metric *risk graph* was proposed to show the vulnerability relationship among critical substations/transmission lines. Based on the proposed metric, the riskgraph-based attack strategy was developed. The proposed attack strategy was compared with four other attack strategies in terms of attack performance and complexity analysis on three test benchmarks. The comparison results showed that the riskgraph-based attack strategy had strong performance and low complexity.

- In manuscript 4, it was assumed that attacks could occur on both substations and transmission, which was referred to as the joint-substation-transmission-line perspective. This assumption was a nature extension to the existing assumption that attacks/contingencies occurred on substations only or transmission lines only, which were referred to as the substation-only perspective and the transmission-line perspective. In this work, both the vulnerability analysis and the attack strategy were conducted from the joint-substation-transmission-line perspective. Specifically, there were many joint-substation-transmission-line combinations that could yield large attack strength. Such

combinations represented the joint-substation-transmission-line vulnerabilities, which were ignored by substation-only and transmission-line-only perspectives. In addition, three metrics, i.e., CIG, load and degree, were adopted to investigate joint-substation-transmission-line attack strategies. The metric CIG was newly-designed in this work; the other two were existing metrics. The comparison results showed that the CIG-based attack strategy had strong performance by balancing to choose substations and transmission lines as targets.

- In manuscript 5, the *sequential attack* was introduced to analyze the vulnerability and study the attack strategy of power grids. In the existing works, it was assumed that the attacks/contingencies occurred synchronously, referred to as the *synchronous attack*. Referring to malicious attacks, however, multiple attacks could be launched sequentially. The sequential attack was a new direction to conduct vulnerability analysis and develop attack strategy. In this work, it has been found that the sequential attack could discover many combinations of substation whose failures caused large attack strength. Previously, these combinations were ignored by the synchronous attack. In addition, a new metric, called the *sequential attack graph* (SAG), was proposed to reveal the relationship among substations/transmission lines. The SAG-based sequential attack strategy was developed from the attacker's perspective. Extensive simulations were conducted. Referring to simulation results and complexity analysis, the proposed SAG-based sequential attack strategy had strong performance and low complexity.