POWER SYSTEM VULNERABILITY ANALYSIS

A CENTRALITY BASED APPROACH UTILIZING LIMITED INFORMATION

By

TIMOTHY ALLEN ERNSTER

A thesis submitted in partial fulfillment of
the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

WASHINGTON STATE UNIVERSITY
School of Electrical Engineering and Computer Science

AUGUST 2012

To the Faculty of Washington State University:

The members of the Committee appointed to examine the thesis of TIMOTHY ALLEN ERNSTER find it satisfactory and recommend that it be accepted.

_____

Anurag K. Srivastava, Ph.D., Chair

_____

Anjan Bose, Ph.D.

_____

Carl H. Hauser, Ph.D.

ACKNOWLEDGMENTS

This research would not have been possible without the advice and support of my peers and the faculty at Washington State University. In particular, the efforts of Dr. Anurag Srivastava warrant special commendation. As my committee chair and advisor, Dr. Srivastava invested an extraordinary amount of time and effort in shaping the direction of this research. I am also grateful to the Department of Energy and Department of Homeland Security for their generous support of the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)[1] project. The financial resources TCIPG provided were crucial in sustaining my investigation into the cyber security challenges facing the electric power industry.

I would also like to extend my appreciation to the civilian and military leaders of the U.S. Army Corps of Engineers. The support of my superiors was in authorizing the extended leave of absence I needed to pursue full-time graduate studies in Pullman, WA. I am also grateful for all the encouragement and career guidance provided by those I served with in Baghdad during Operation Iraqi Freedom. Whether Iraqi or American, I like to think they would have been proud of me.

Finally, no acknowledgment would be complete without thanking my parents. They may not ever understand the contents of this thesis, but they endured the process with me nonetheless. I am fortunate to have been born to them, and am eternally grateful that sometimes family planning isn't quite so planned.

[1] The research presented in this thesis was funded under Department of Energy grant DE-OE0000097

POWER SYSTEM VULNERABILITY ANALYSIS

A CENTRALITY BASED APPROACH UTILIZING LIMITED INFORMATION

By Timothy Allen Ernster, M.S.
Washington State University
August 2012

Chair: Anurag K. Srivastava

Vulnerability assessments play a key role in determining appropriate mitigation strategies to counter credible cyber threats to a power system. Yet an assessment of the vulnerability of the electric grid to a cyber attack is dependent on the resources and capabilities of an attacker. Through an application of conventional principles of warfare to a potential cyberwar on the power grid, a framework for credible attack scenarios can be conceived. From such a framework, it is proposed that a severe threat of concern would involve a coordinated attack on specific power system cyber assets resulting in the malicious outage of multiple generators or lines throughout the power grid. It is further concluded that a coordinated attack scenario would likely involve selection of targets from a simplistic analysis based on limited information.

Since centrality measures only require system topology and branch impedance information to rank contingencies, they present the potential to aid attackers in targeting specific buses and lines that maximize the adverse reliability impact to the power grid. In order to establish the utility of centrality measures, a statistical comparison of contingency ranking schemes based on centrality measures with those of more conventional power flow based methods was performed. Such statistical tests indicate the strongest evidence in support of closeness and edge betweeness centrality as tools for N-1 contingency ranking schemes.

However, since a cyber attacker has the capability to cause multiple simultaneous contingencies, a novel approach to utilizing centrality measure for N-X contingency vulnerability assessments is developed and validated against a power flow based performance index. Since centrality based vulnerability assessments can serve as physical attack signatures, power system security may be enhanced through the creation of early detection and mitigation applications capable of thwarting an unfolding coordinated cyber attack.

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Reliable access to electricity is vital in supporting public safety and modern economic activities. Given the exposure of the electric power grid to cyber threats, the U.S. Department of Energy began facilitating the creation of roadmaps to develop, deploy, and maintain energy delivery systems capable of maintaining critical functions during a cyber assault [1]. A key focus of the U.S. government's efforts has been in assessing the risk of a coordinated cyber attack to the energy sector and generating proposals and policies aimed at minimizing the risk of a successful attack. Specifically, development of scenario-based analysis tools and credible attack exercises have been proposed to test the response preparedness of the electric sector to a coordinated cyber attack [2].

This thesis focuses on developing a topology based vulnerability assessment for power systems. Such a vulnerability assessment is needed to assess the threat of a coordinated cyber attack by an attacker that lacks complete information about the power system operating state. Generally, existing research into attack scenario modeling of a coordinated cyber attack assumes an attacker can perform conventional power flow based security studies to select targets. However, performing such vulnerability studies requires an attacker to acquire operational knowledge of a power system similar to authorized operators of the electric grid. This work relates to performing contingency analysis studies of the electric grid, which are based on information more readily available to an attacker attempting to plan a coordinated attack.

1.2 Overview of Electric Power Systems

A power system consists of a network of bus and branch components necessary to produce electric energy and transmit it to consumers. Facilities such as generators and capacitors that inject power

into a bus are referred to as energy sources. The load at a bus refers to the power demanded by customers. Branch components that permit the flow of power between buses are transmission lines, or transformers if power is required to be transmitted between two buses of different voltages. Other bus and branch components may include shunt or series reactors/capacitors and power electronics that are installed to improve performance and reliability characteristics. Figure 1.1 shows a simplified example of how power produced at a generation facility is transmitted to a customer. In order to reduce power losses during the transmission and distribution of electric energy, transformers located in substations raise voltage to transmit power efficiently over longer distances, and reduce voltage closer to customers so electric energy can be consumed safely.

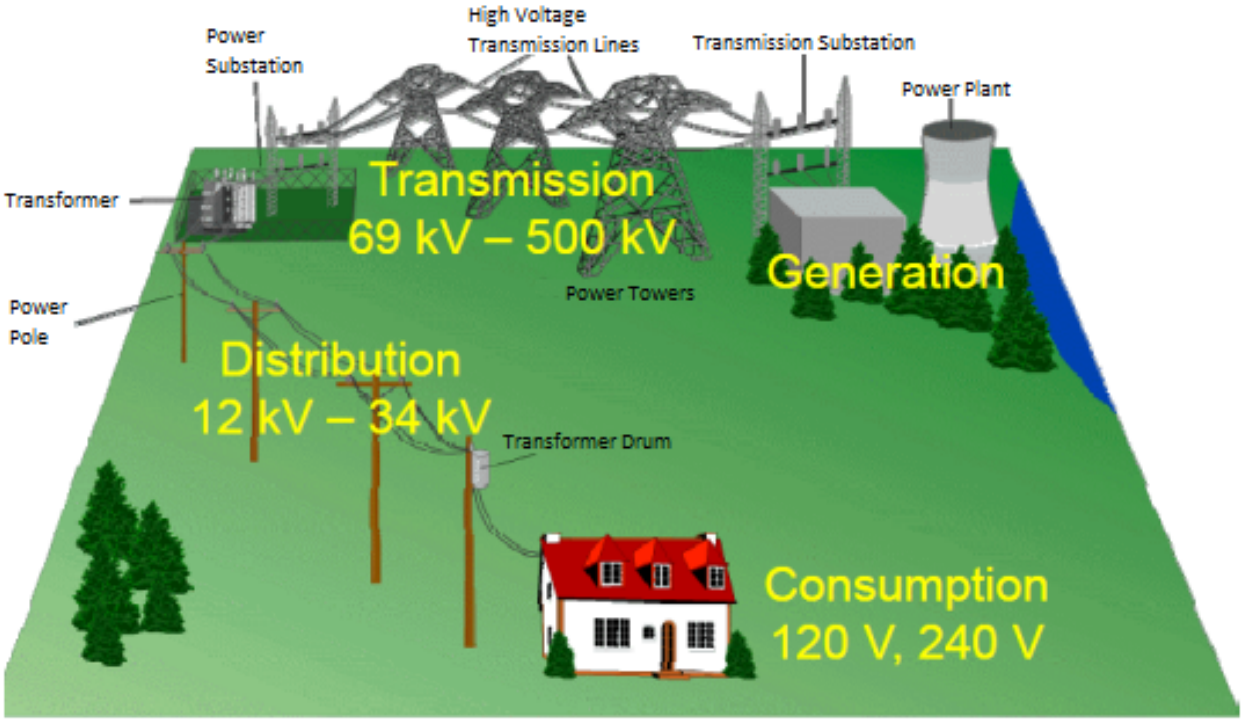

Figure 1.1: Overview of Electric Power Systems [3]

The primary objective of power systems is to maintain a high level of continuity of service, and to minimize the extent and time of an outage resulting from intolerable conditions [4]. In order to support this reliability objective, systems are installed throughout the electric grid that monitor the state of the grid, and take protective and control actions if intolerable conditions are detected. Additionally, there

exist control systems and operational procedures responsible for ensuring the power system is able to maintain reliability in the presence of component failures. While reliability is an important objective, it is also vital that power systems be operated economically. However, economic operation of power systems often conflicts with reliable operation of power systems. Reliability is achieved by ensuring there is system redundancy and excess capacity to respond to an emergency. Constructing redundant transmission facilities and maintaining excess generation on standby is expensive, so a balance between reliability and economic factors must be achieved.

The balance between reliable and economic operation of power systems is complicated by the fact that there are many interconnected utilities whose activities must be coordinated. In the United States alone, there are 3,273 traditional electric utilities [5] that must coordinate actions through balancing authorities to ensure reliable and economic operation of the electric grid. With few exceptions, energy is generated and transmitted as AC power. In order for utilities to remain interconnected, they must all be synchronized to a standard frequency, set at either 50Hz or 60Hz depending on the reliability region a utility operates in. In the United States, the North American Electric Reliability Corporation (NERC) is responsible for ensuring the reliability of the North American bulk power system, and is divided into eight regional entities that enforce standards and reliability compliance. While a non-governmental entity, the Federal Energy Regulatory Commission (FERC) had designated NERC the electric reliability organization for the United States, which effectively grants NERC legal authority to enforce energy standards in the U.S.

1.3 Overview of Power System Security and Vulnerability

Considering electric grids can consist of tens of thousands of branches and buses, it is not uncommon for components to fail from time to time. In order to maintain reliable operations, security measures are taken to reduce the likelihood that isolated disturbances degenerate into major incidents leading to disconnection of loads. Severe incidents include cases of frequency collapse that cause generators to disconnect from the grid, cascading thermal overloads that result in the disconnection of

multiple lines, voltage collapse scenarios deriving from a deficit of reactive power, and other transient instability issues [6]. Historically, when power engineers utilized the term 'security' they were referring to measures taken to assure system reliability in the presence of physical threats, such as severe weather events, equipment failures, or vandalism. However, with the integration of intelligent electronic devices into the power system, power system security must also account for cyber threats to the electric grid. Just as physical security incidents must be managed to prevent adverse reliability consequences, if an attacker compromises the monitoring, control, or protective cyber systems a severe incident can be maliciously inflicted on the physical electric grid [7]. In the proceeding subsections, physical and cyber vulnerabilities relevant to maintaining power system security will be reviewed to narrow the research focus of this thesis.

1.3.1 Physical Security & Vulnerability

Traditional physical security refers to the process of estimating the ability of a power system to meet all connected demand in the presence of limited failures without violating a reliability constraint. Security analysis involves formulating a list of possible credible contingencies, screening and evaluating the effects of each listed contingency, and suggesting preventive or corrective actions. Vulnerability analysis refers to evaluating possible sets of failures, and determining which can result in compromising the planned security of a power system to cause unreliable operation. In general, vulnerability analysis is often considered an extended contingency screening process. Due to the similar nature of the concepts with respect to cyber security, in this thesis the terms 'security' and 'vulnerability' will often be used interchangeably.

For steady state vulnerability analysis metrics, reliability violations occur when bus voltages exceed tolerance limits (typically outside the range of 0.95 to 1.05 per unit) or power transfers across branches exceed the rated capacity of the branch [8]. Dynamic wide-area vulnerability assessments also incorporate frequency violations into security studies [9]. Reliability violations are most likely to be caused by a fault in a power system. Faults are classified as either phase-to-ground, phase-to-phase, or

phase-open. Phase-to-ground faults occur when one, two, or all three phases come into contact with the earth. The causes of phase-to-ground faults are mostly weather related (i.e. a tree falls on a transmission line), although other insulation failures can also result in phase-to-ground faults. Phase-to-phase faults occur when two phases come into contact with one another. Common causes of phase-to-phase faults are severe winds forcing two conductors into contact, or instances involving birds and other animals coming into simultaneous contact with two phases. Phase-open faults occur when there is either one phase in service and two phases out of service, or two phases in service and one phase out of service. Phase-open faults are normally caused by circuit breaker or switch mechanical failures and misoperations. When relays throughout the power system detect a fault, a protective action will be taken to isolate the affected equipment from service [10]. The act of removing equipment from service to clear a fault causes the power system to transition from a normal operating state with all equipment in service to an alert or emergency operating state.

For security purposes, utilities need to operate power systems in such a way that reliability constraints are maintained in the presence of periodic failures. Operators often run a security constrained optimal power flow program to determine generator dispatch schedules so that reliability constraints are not violated if any one component is removed from service (termed an N-1 contingency analysis) [11]. In order to assess the impact of contingencies, tools also exist to take line flow and bus voltage information from an existing power system state, and report the possible future system changes resulting from various credible contingencies. On a basic level, DC power flow based sensitivity studies allow for a linear approximation of active power flows resulting from a contingency [12-14]. AC power flow based performance indices also exist that rank contingencies according to branch overloads and bus voltage changes caused by outages [15]. While on-line analysis of more than a single contingency (called N-X contingency analysis) is often difficult due to the computation time needed to assess multiple contingency cases, research activities into this topic are ongoing [16].

To a lesser extent contingency analysis tools have also been developed to assess the risk to an electric grid of intentional failures. While not common in the United States or other developed countries,

nations such as Colombia [17], Iraq [18], and the former Yugoslavia [19] have seen their electric grids targeted during hostilities. In cases of terrorism, vulnerability analysis algorithms use the solution to a power flow in conjunction with economic information concerning equipment destruction costs and inability to serve load. The risk of a power system due to loss of specific assets can then be established based on the total monetary loss a utility is expected to incur during the time needed to recover from the attack [20]. Alternatively, the severity of a terrorist attack on a power system can be assessed based on the amount of load not served following an incident [21]. In using a maximum network flow approach, a terrorist attack model has also been developed that envisions a coordinated attack scenario as a series of branch outages with the objective of disrupting the maximum power flow between energy sources and loads [22]. Contingency scenarios can also be understood through a min-max bilevel model, where both attacker and operator interacting actions can be simulated. In the bilevel model, attackers are assumed to have the objective of maximizing load shed by selecting which branch outages to intentionally cause, and the system operator reacts to minimize the load shed by redispatching generators and selecting which loads to sacrifice [23]. Even though these terrorism risk assessment and attack models may approach the topic of vulnerability assessments separately, the algorithms are primarily designed for planning studies and are not suited for on-line use.

1.3.2 Cyber Security & Vulnerability

Cyber security vulnerability assessment measures tend to come in two forms: those that assess the vulnerability of cyber assets in the power system to being compromised, and those that assess the consequences to the physical power system resulting from compromised cyber assets. However, since the electric grid is a cyber-physical system, the distinction between cyber vulnerabilities and the consequence to the physical system is often difficult to establish. For example, the existence of vulnerabilities in a cyber asset such as a control, protection, or monitoring device or system does not necessitate a severe reliability impact to the physical power system if the asset is compromised. However, if a cyber attacker

is able to utilize the vulnerability to cause an outage of physical power system components, it is possible for a power system to be thrust into an emergency state as a consequence of the cyber attack.

Power system cyber asset vulnerabilities are commonly understood through conventional information security principles. Successful cyber attacks will typically make use of some vulnerability in the communication protocol, routing, or authentication processes of a cyber asset to install malware, deny legitimate services, or directly intrude into an information system [24]. Successful cyber attacks can have a variety of consequences, but the most common are theft or corruption of information, unavailability of computing resources, and physical destruction of equipment [25].

The cyber assets and applications in a power system are uniquely susceptible to a variety of cyber attacks. By corrupting the information utilized by a state estimator, attackers have the potential to alter the state estimation solution to reflect a fictitious power system state while evading bad data detection routines [26]. Furthermore, if an attacker is able to inject false data into a state estimator they can alter the result of a security constrained optimal dispatch application, which can lead to generator redispatching that results in uneconomic operation of a system and/or an insecure operating state [27]. Research activities have been pursued in order to develop more robust bad data detection algorithms that can detect a state estimator false data injection attack [28].

Also of interest is the vulnerability of Supervisory Control and Data Acquisition (SCADA) systems to cyber attacks. While SCADA systems tend to be isolated from public communication networks, features such as remote vendor and engineering access into substation networks for legitimate purposes have created an attack surface from which a skilled attacker can obtain unauthorized entry into a SCADA system [29]. Once inside SCADA network, an attacker has the potential to cause outages and operational changes resulting in an adverse reliability impact to the physical power system. To address SCADA vulnerabilities, some research activities have investigated embedding security applications into firewall and password protocols to strengthen security at SCADA access points [30]. Additionally, activities at Idaho National Laboratory and other test beds have enabled security testing of SCADA systems to uncover and address vulnerabilities in a simulated environment [29-33].

1.4 Motivation for Research Work

In broadening traditional concepts of power system security to include cyber threats, there is a literature gap in understanding how a cyber attacker may target cyber systems to inflict a desired effect on the physical electric grid. Conventional physical contingency analysis tools rely on some version of the power flow problem, which requires calculating the solution to the following set of equations for all buses in the power system:

$$P_i = \sum_{j=1}^{n} V_i V_j Y_{ij} \cos\left(\delta_i - \delta_j - \theta_{ij}\right) \qquad (1.1)$$

$$Q_i = \sum_{j=1}^{n} V_i V_j Y_{ij} \sin\left(\delta_i - \delta_j - \theta_{ij}\right) \qquad (1.2)$$

where P_i and Q_i are the active and reactive power injection at bus i, $V_i \angle \delta_i$ is the voltage and phase angle at bus i (or bus j depending on the subscript), and Y_{ij} is the element of the bus admittance matrix defining the admittance between buses i and j [34]. While personnel within a utility may have knowledge of specific bus injections and voltage magnitudes needed to solve the power flow problem, it is not practical to assume that a cyber attacker will have the same knowledge of a power system state as a system operator. Additionally, physical security analysis is based on the assumption that failures occur in a probabilistic manner. A cyber attacker is an intelligent agent capable of coordinating attacks that result in deliberate component failures, which increases the risk of low probability high impact contingency scenarios.

Even though security researchers have shed light on specific vulnerabilities of the cyber assets within an electric grid, it remains unclear how an attacker in possession of limited information could know how to exploit cyber vulnerabilities to achieve an intended reliability impact. In order for a bad data injection attack on a state estimator to be successful, an attacker would need to perform on-line power flow studies. Based on these studies, determinations concerning how state estimation data should be corrupted can be made. Furthermore, bad data detection protocols would be able to identify false data injections if too significant an error existed between measurements and the estimated state [35]. Therefore, a detailed mathematical understanding of a bad data detection application would also be necessary so that corrupted measurements wouldn't result in too great an error between the estimated

state and measurement data. The bad data state estimation attack, if successful, would only then have the potential to project a desired false power system state without alerting a bad data detector. Yet the real-time information and resources required to perform such an attack would render such vulnerability exploits difficult to accomplish.

Similarly, compromising a SCADA system would first require an attacker to obtain confidential system design information for specific assets that would facilitate an attacker's objective. However, it would be impractical for an attacker to acquire the schematics needed at all substations, generation facilities, and control centers to determine which components in the power system should be targeted to cause a critical contingency. Rather, it would be more practical for an attacker to first choose targets based on available information, perform in-depth reconnaissance activities on the selected targets, then proceed with a cyber attack on systems related to the targets of interest. So while SCADA vulnerabilities may exist, a resource constrained attacker may find it impractical to determine how to exploit the vulnerabilities to cause a decisive critical contingency in the physical system.

Since the electric grid is already designed for reliability in the face of security challenges posed by severe weather events and other naturally occurring hazards, the addition of cyber threats may not initially appear alarming. After all, if the electrical grid can withstand an event such as a hurricane, the addition of cyber attacks may seem like just another threat in an already hazardous operating environment. However, the unique security challenges concerning reliability officials relate to responding to a coordinated threat that the electric grid is not prepared to face [36]. In order to respond to a coordinated attack, early identification of attack scenarios is required. Research into risk and attack modeling, risk mitigation, attack scenario detection, and integration of network traffic monitored at multiple substations is necessary in order to support early identification and prevention of a coordinated cyber attack [37].

1.5 Thesis Objective

In order to assist in developing tools that could be used for early identification of a cyber attack scenario, this thesis will develop an algorithm for use in a coordinated cyber attack model. The model will assume that an attacker seeks to cause a critical contingency on the physical power system, but does not possess knowledge of the operational state of the power system. Specific vulnerabilities of cyber assets within the electric grid will not be covered in detail. Rather, this thesis will focus on determining how a resource constrained attacker with incomplete system information may select attack targets so that cyber vulnerabilities may be exploited to cause a critical contingency. In pursuit of this goal, research activities will be directed in support of the following objectives:

1. Perform a conceptual review of issues related to cyber security for power systems, and develop a framework for cyber attack modeling based on a limited information vulnerability assessment of the physical power system.
2. Utilize existing contingency ranking tools to establish baseline metrics for comparison and evaluation of limited information vulnerability analysis algorithms.
3. Investigate whether there exists a statistically significant relation between graph theory based centrality measures and baseline metrics for N-1 contingency analysis studies.
4. Build an N-X contingency screening algorithm based on relevant centrality measures identified in objective 3, and assess the algorithm for a statistically significant relation compared to a baseline N-X contingency analysis algorithm.

1.6 Thesis Organization

This thesis is organized into six chapters. Chapter 1 contains an introduction to power systems and the security challenges faced by the electric energy industry. The motivation and objectives of this research are also covered in chapter 1. Chapter 2 discusses background information related to cyber security issues for the electric power grid. Topics such as the cyber assets in the electric grid, classifications of cyber attacks, profiles of cyber attackers, and conventional information security

objectives are discussed. The background material and literature review of essential cyber security concepts presented in chapter 2 forms a foundation that will serve to guide research activities in support of the thesis objectives. The principles of warfare needed to form credible attack and defense models are also included in chapter 2, along with the need for graph theory measures to model the physical effects of cyber attacks planned from limited information. Chapter 3 serves as a literature review of conventional power system security analysis tools. Both conventional DC power flow based sensitivity factors and AC power flow based performance index measures are discussed. The contingency ranking methods reviewed in chapter 3 will serve as baseline metrics for comparing the new limited information vulnerability assessment measures proposed in this thesis.

Chapter 4 constitutes a literature review of graph theory based centrality measures and how they can be applied to power systems. Since these measures will be used in the development of a limited information vulnerability assessment, the various graph theory measures are compared to the DC power flow based linear sensitivity factors. Based on the statistical results summarized in chapter 4, the suitability of the various centrality measures are evaluated for incorporation into an N-X centrality based power system vulnerability assessment algorithm. Chapter 5 serves to develop centrality based N-X algorithms that rank the vulnerability of the power system to various bus and branch contingencies. A unified N-X centrality based performance index is then proposed, and validated against the AC power flow based performance index and RTDS simulations of an N-3 attack scenario. Chapter 5 concludes with a discussion of defensive strategies that could be implemented based on the results of the centrality performance index. Chapter 6 discusses the contributions of this thesis and suggested directions for future work that can be performed to extend this research.

1.7 Summary

This chapter served to highlight security challenges to the electric grid posed by vulnerabilities to coordinated cyber attacks. A brief introduction to electric power systems was then provided, followed by a discussion of existing security and vulnerability analysis concepts relevant to the cyber-physical electric

grid. The objectives of this thesis are then outlined subsequent to an explaination of the motivations for performing vulnerability studies of electric grid using limited information. Finally, the thesis organization is summarized by briefly describing the content of the six chapters.

1.8 References

[1] Energy Sector Control Systems Working Group, “Roadmap to Achieve Energy Delivery Systems CyberSecurity,” Department of Energy, Sept. 2010. [Online]. Available: http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

[2] North American Electric Reliability Corporation (NERC) and U.S. Department of Energy (DOE), “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,” NERC and DOE, June 2010, http://www.nerc.com/files/HILF.pdf

[3] D. Whitehead, “Introduction to Power Systems,” presented at the *TCIPG Summer School on Cyber Security for Smart Energy Systems*, Urbana-Champagne, IL, 13-17 Jun. 2011.

[4] J. L. Blackburn and T. J. Domin, *Protective Relaying Principles and Applications*, ed. 3. CRC Press, 2007, p. 2.

[5] Rebecca Peterson, “Electric Power Industry Overview 2007,” U.S. Energy Information Administration, 2008. [Online]. Available: http://www.eia.gov/cneaf/electricity/page/prim2/toc2.html

[6] D. Kirschen, “Power System Security,” *Power Engineering Journal*, pp. 241-248, 2002.

[7] R. Schainker, J. Douglas, T. Kropp, "Electric utility responses to grid security issues," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 30-37, Mar.-Apr. 2006.

[8] Z. Hussain, Z. Chen, P. Thogersen, “Fast and Precise Method of Contingency Ranking in Modern Power Systems,” *2011 IEEE Jordan Conference on Applied Electrical Engineering Computing Technologies*,” pp. 1-7, 6-8 Dec. 2011.

[9] R.J. Marceau, J.C. Rizzi, R. Mailhot, "A frequency-domain transient stability criterion for normal contingencies," *IEEE Transactions on Power Systems*, vol. 10, no. 3, pp.1627-1634, Aug. 1995.

[10] N. Tleis, *Power System Modeling and Fault Analysis: Theory and Practice*, Oxford, UK: Elsevier Ltd., 2008, pp. 2-8

[11] A. Monticelli, M.V.F. Pereira, S. Granville, "Security-Constrained Optimal Power Flow with Post-Contingency Corrective Rescheduling," *IEEE Transactions on Power Systems*, vol. 2, no. 1, pp. 175-180, Feb. 1987.

[12] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. McGraw-Hill, 1994, pp. 626-628.

[13] T. Guler, G. Gross, M. Liu, "Generalized Line Outage Distribution Factors," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp.879-881, May 2007.

[14] J. Guo, Y. Fu, Z. Li, M. Shahidehpour, "Direct Calculation of Line Outage Distribution Factors," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp.1633-1634, Aug. 2009.

[15] A. J. Wood and B. F. Wollenberg, *Power Generation Operation and Control*, ed. 2. New York, NY: Wiley, 1996, pp. 427-432.

[16] Z, Huang, Y, Chen, F.L. Greitzer, R. Eubank, "Contingency Visualization for Real-Time Decision Support in Grid Operations," *IEEE 2011 Power and Energy Society General Meeting*, pp. 1-7, 27-29 July 2011.

[17] A. Torres and P. Santos, "Bayesian Networks and Monte Carlo Simulations in the Evaluation of Risk of Terrorism for the Colombian Electrical Infrastructure," *IEEE PES Power Systems Conference and Exposition*, pp. 1265-1271, 10-13 Oct. 2004.

[18] D. Lewis, "Iraq's Other Power Struggle," *Power Engineer*, vol. 20, no. 5, pp. 18-21, Oct.-Nov. 2006.

[19] Air Force Association, "The Kosovo Campaign: Airpower Made it Work," United States Air Force. [Online], retrieved 12 Dec. 2010. Available: http://www.afa.org/media/reports/campaign.asp

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

[21] M. Anjia, Y. Jiaxi, G. Zhizhong, "Electric Power Grid Structural Vulnerability Assessment," IEEE 2006 Power Engineering Society General Meeting, pp. 1-6, 18-22 June 2006.

[22] C.M. Rocco, J.E. Ramirez-Marquez, D.E. Salazar, C. Yajure, "Assessing the Vulnerability of a Power System Through a Multiple Objective Contingency Screening Approach," *IEEE Transactions on Reliability*, vol. 60, no. 2, pp. 394-403, June 2011.

[23] J.M. Arroyo, "Bilevel Programming Applied to Power System Vulnerability Analysis Under Multiple Contingencies," *IET Generation, Transmission & Distribution*, vol. 4, no. 2, pp. 178-190, Feb 2010.

[24] M. Govindarasu, A. Hann, P. Sauer, "Cyber-Physical Systems Security for Smart Grid," PSERC, Publication 12-02, Feb. 2012.

[25] C. Tranchita, N. Hadjsaid, A. Torres, "Overview of the power systems security with regard to cyberattacks," *Fourth International Conference on Critical Infrastructures*, pp.1-8, 27 Mar. 2009 – 30 Apr. 2009.

[26] O. Kosut, L. Jia, R.J. Thomas, L. Tong, "On Malicious Data Attacks on Power System State Estimation," *45th International Universities Power Engineering Conference*, pp. 1-6, 31 Aug. – 3 Sept. 2010.

[27] Y. Yuan, Z. Li, K. Ren, "Modeling Load Redistribution Attacks in Power Systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382-390, June 2011.

[28] O. Kosut, L. Jia, R.J. Thomas, L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," *First IEEE International Conference on Smart Grid Communications*, pp. 220-225, 4-6 Oct. 2010.

[29] C. Liu, C. Ten, M. Govindarasu, "Cybersecurity of SCADA Systems: Vulnerability Assessment and Mitigation," *IEEE 2009 Power Systems Conference and Exposition*, pp. 1-3, 15-18 Mar. 2009.

[30] C. Liu, C. Ten, M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[31] National SCADA Test Bed (NSTB), "Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program," Office of Electricity Delivery and Energy Reliability, Department of Energy, Report INL/EXT 08-13979, Nov. 2008. [Online]. Available: http://www.inl.gov/scada/publications/d/inl_nstb_common_vulnerabilities.pdf

[32] C.M. Davis, J.E. Tate, H. Okhravi, C. Grier, T.J. Overbye, D. Nicol, "SCADA Cyber Security Testbed Development," *38th North American Power Symposium*, pp. 483-488, 17-19 Sept. 2006.

[33] Y. Al-Nashif, D. Cox, T. Chadaga, S. Hariri, "A Testbed for Analyzing Security of SCADA Control Systems (TASSCS)," IEEE 2011 PES Innovative Smart Grid Technologies Conference, pp. 1-7, 17-19 Jan. 2011.

[34] Z. Yamayee, J. Bala, *Energy Devices and Power Systems*, John Wiley & Sons Inc., 1994, pp. 352-370.

[35] E. Handschin, F.C. Schweppe, J. Kohlas, A. Fiechter, "Bad Data Analysis for Power System State Estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 2, pp. 329-337, Mar 1975.

[36] North American Electric Reliability Corporation (NERC), "2011 NERC Grid Security Exercise: After Action Report," NERC, Mar. 2012. [Online]. Available: http://www.nerc.com/files/NERC_GridEx_AAR_16Mar2012_Final.pdf

[37] S. Sridhar, A. Hahn, M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012.

CHAPTER TWO

DEFINING THE CYBER THREAT TO AN ELECTRIC GRID

2.1 Introduction

This chapter consists of a conceptual discussion of cyber security issues affecting the electric power grid. In a historical context, from Sun-Tzu's *The Art of War* we can learn that "if you know the enemy and know yourself, you need not fear the result of a hundred battles [1]." So before delving too deeply into technical content, we first turn our attention to developing familiarity with the vulnerability of the electrical grid to cyber attacks and the adversaries with which a utility may come into conflict. Core concepts underlying cyber attack scenarios within the context of established principles of warfare will be presented in this chapter. Furthermore, since the electric grid is a cyber-physical system, a discussion of physical vulnerability based on varying levels of information is included to model a cyber attack.

2.2 Cyber Assets & Attack Surface

While the growing incorporation of information communication technologies into the power system has enabled enhancements to system reliability, proliferation of such technologies has also increased the attack surface from which cyber attacks may be launched. Since wide area control, monitoring, and protection systems require communications between control centers and geographically dispersed physical assets, of particular concern are the security implications of a skilled cyber attacker able to gain unauthorized access to the cyber systems interfacing with the physical system components.

In a power system, it is common for Supervisory Control and Data Acquisition (SCADA) communication systems to occur over dedicated or leased communication channels. SCADA systems include computer and communication devices installed in power plants, substations, energy control centers, company headquarters, regional operating offices, and large load sites. A SCADA system constantly gathers the latest status from remote terminal units (RTU) and intelligent electronic devices

(IED) throughout the power system, and sends the data to a SCADA control center. Data acquired by SCADA is utilized by energy management systems (EMS) and for other purposes, including real time control. Furthermore, utilities may have a separate communication infrastructure for collecting phasor measurement unit (PMU) data for wide area monitoring and control [2].

Even though the core of SCADA communications tends to occur over dedicated channels, the necessity of enterprise and engineering activities often requires communication with control centers, substations, and generation facilities over public communication channels such as the internet or telephone networks. Metering data acquired by SCADA systems is required in a corporate office for load forecasting and billing purposes, and engineers may update relay settings or acquire forensic data remotely without physically traveling to the site where the data is held. While there have been no confirmed incidents in public record of a cyber attack on a SCADA system within the United States, 53% of utilities have reported being victim of a cyber attack [3]. Such attacks are focused on the enterprise network of utilities subject to the same Trojan horse, worm, virus, denial of service, sabotage, and vandalism types of attacks as the enterprise network of any other industry. However, if an attacker is able to bypass the communication boundary between enterprise functions and SCADA or wide area protection cyber systems, the potential for physical consequences of a cyber attack emerges as a credible threat [4].

Intrusion points are considered anywhere the electric grid internal communication system interfaces with a public communication network, such as a modem or router within a substation that allows internet access. However, even dedicated communication channels such as point-to-point wireless communication links between substations, generation facilities, and control centers can be intrusion points if an attacker is able to intercept and modify transmitted data. Figure 2.1 depicts an overview of a power system communication network where potential intrusion points exist.

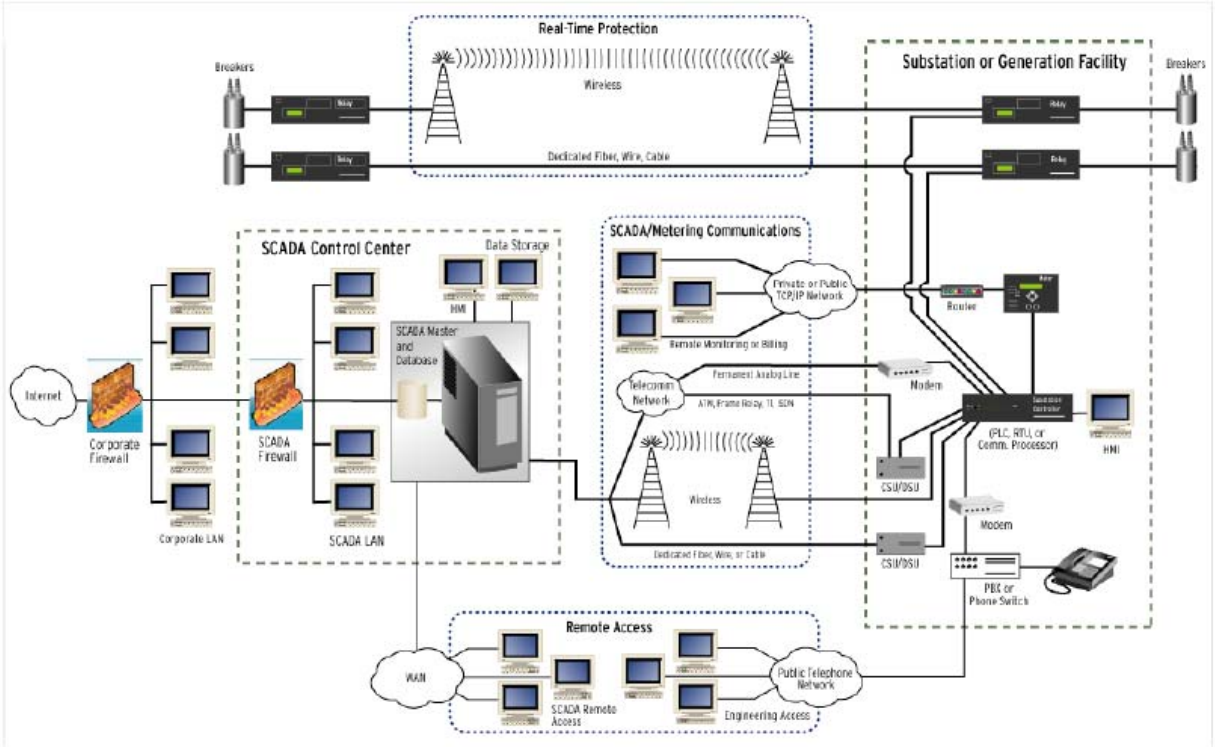

Figure 2.1: Overview of Electric Power Grid Control and Communication Systems [5]

2.3 Classification of Cyber Attacks

Formally, cyber attacks can be defined as those attacks that use electronic means to damage information and communication technologies on which the power system depends. Broadly speaking, cyber attacks on a power system are discussed in four categories or classes: theft of information, denial of service, corruption of information, and physical destruction [6]. Yet the four attack classes are not independent. As shown in figure 5.2, the attack classes can serve as precursors to one another. Attackers must steal information required to assess cyber and physical vulnerabilities before denial of service or corruption of information attacks can be executed on a cyber system. If the attack on a cyber system is able to cause damage to the physical system, then a physical destruction class of attack is realized. In the following subsections, these four broad classifications of attacks are discussed.

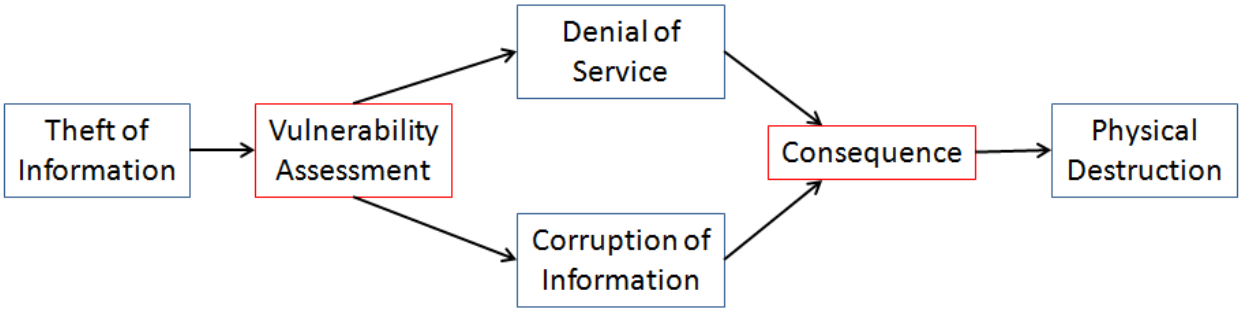

Figure 2.2: Relationship of Cyber Attack Classes

2.3.1 Theft of Information

Cyber attacks involving theft of information are considered those attacks where sensitive information is disclosed to unauthorized persons or systems. Theft of information attacks can be terminal if the objective of an attacker is to obtain financial information such as customer accounts and billing information. Alternatively, business competitors can steal trade secrets and intellectual property from rivals to expand access to markets. However, if an attacker has the objective of causing harm to the power system, theft of technical system design information can serve as a precursor to a more damaging attack [6]. It may be difficult to detect a theft of information attack while it is in progress, since attackers may be in possession of passwords and encryption keys that allow them to masquerade as normal users. Additionally, the effects of a theft of information attack tend to lack immediate consequences. Obtaining essential information about a target may only serve as an initial step in further exploiting cyber systems and establishing footholds that have more severe consequences.

2.3.2 Corruption of Information

If an attacker is successful in obtaining information required to exploit cyber vulnerabilities, information governing the operation of cyber assets may be corrupted. Corruption of information attacks occur when an attacker is able to improperly modify data on a computer or network [7]. If an attacker is able to corrupt data sent by RTUs or IEDs, SCADA systems can issue erroneous commands, display wrong state information, issue false alarms, etc. Alternatively, human operators of power systems may be

manipulated into taking unnecessary control actions if the data displayed in the control center reflects a false system state. Other corruption of information attack scenarios involve maliciously changing device settings. For example, if protective relay settings are altered to issue trip commands during normal system operating conditions, circuit breakers may erroneously isolate vital system components from service. Alternatively, if control systems are altered they could be utilized to force physical asset operations that thrust a power system from a secure operating state into an emergency state.

2.3.3 Denial of Service

The denial of service classification of attacks involves cases where resources of a network are used by unauthorized entities, preventing network resources from being utilized for legitimate purposes. Denial of service attacks are commonly achieved by flooding communication channels with miscellaneous information [8]. If denial of service attacks are performed on a utility's enterprise network, it can result in the same nuisance loss of information technology availability as experienced by other industries. However, if the communication channels of control and protection systems are rendered unavailable the consequences to the physical power system can be much more severe. Decisions made by IEDs in a power system are extremely time sensitive. If an emergency situation develops, control and protective decisions are often required within fractions of a second to prevent physical equipment from being destroyed or the system from sliding into instability. So a denial of service attack that impedes the flow of information to and from IEDs has the potential to render cyber assets in a power system unable to adequately maintain a secure operating state of the physical power system.

2.3.4 Physical Destruction

The final cyber attack classification relates to those resulting in physical destruction of components in the power system. Physical destruction can occur directly if cyber systems are hacked and directly manipulated to cause some enduring malfunction until the physical system is destroyed. Alternatively, physical destruction can be an indirect result of corruption of information or denial of

service attacks discussed in sections 2.3.2 and 2.3.3 [6]. Notable examples of physical destruction attacks are the Aurora Test attack simulation carried out by Idaho National Lab and the Stuxnet attack on the Natanz nuclear facility in Iran. However, physical destruction cyber attacks are rare and difficult to accomplish. Not only are control systems inherently complex and difficult to maliciously interface with [9], but physical assets are protected by multiple protective mechanisms that remove components from service if potentially damaging frequency, voltage, current, etc. operating states are detected. Additionally, backup protection schemes are coordinated to protect physical components in the event local protection fails. Due to the high impact physical destruction of assets poses to the power system, the Aurora and Stuxnet attacks will be reviewed to serve as examples of physical destruction cyber attacks.

In the Aurora attack, it was shown that if generator controls are compromised an attacker would be capable of issuing malicious open/close commands to generator breakers. Such an attack would result in dropping and reconnecting part of the system load to the generator in rapid succession, which would cause repetitive mechanical stress to the generator if the open/close operations were carefully timed so that the threshold of an out-of-step relay is not exceeded. The repetitive mechanical stress caused by an Aurora attack would eventually lead to physical destruction of a generator [10].

In the case of Stuxnet, physical destruction of industrial motors was achieved by changing the rotational speed of motors governed by a programmable logic controller (PLC) with variable frequency drives. Stuxnet would corrupt the settings of the PLC system, periodically increasing the motor frequency to 1410Hz, then dropping it down to 2Hz, and then returning it to the 1064Hz normal operating speed of the motors. These drastic rotational speed changes would eventually cause physical destruction to centrifuges being spun by the motors. Furthermore, Stuxnet was able to install software to corrupt the motor speed monitoring data, which concealed the true state of the motors from the SCADA monitoring system and prevented corrective actions from being taken before physical damage was realized [11].

2.4 Cyber Attacker Profiles

As a general security principle, understanding one's opponent is necessary in developing strategies to counter adversarial actions. Therefore, in this section general profiles of cyber attackers that the electric energy industry may face are discussed. Attackers are often divided into internal and external threats. Internal threats consist of disgruntled employees and vendors that are motivated to attack an organization to which they belong for reasons often associated with revenge or financial gain. Insider attackers often have detailed knowledge of a power system due to their insider access privileges and may not need extensive computer intrusion skills. While insider threats pose a unique and challenging threat, the focus of this research concerns how attackers may select targets for a cyber attack based on limited information. Therefore, this section will focus on external attacker profiles since external attackers possess only limited immediate knowledge of a given power system and must steal information without being detected [6,12].

At a basic level, external cyber attackers are often classified as hackers, criminal organizations, terrorists, or nation states. While the ultimate objectives of attackers may overlap, the motive, resources, and skills available to each class of attacker tend to diverge. In figure 2.3, the four attacker classifications are arranged hierarchically to reflect the resources available to each attacker to inflict damage on a power system through a cyber attack. In the subsequent subsections, profiles of these four attacker groups will be presented with an emphasis on the motivations and capabilities of each class of attacker.

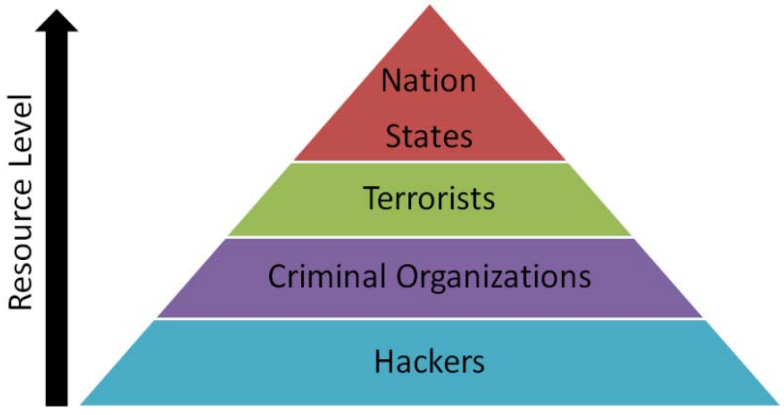

Figure 2.3: Resource Levels of Classifications of Cyber Attackers

2.4.1 Hackers

The hacker classification of cyber attackers contains a broad range of skill group categories, ranging from novice "script kiddies" who use existing software tools to break into systems to more technically skilled virus writers capable of assembling their own code and scripts. However, regardless of skill level, hackers are generally motivated by seeking the thrill of attacking cyber systems, attaining bragging rights that accompany successfully hacking a system, or by gaining revenge for some perceived slight [7]. Given the technical complexity of integrated control and protection systems, the majority of hackers are considered to lack the expertise and resources to threaten critical infrastructure targets. However, the considerable worldwide hacker population does raise the chances of an isolated or brief disruption caused by an attacker achieving serious damage to a power system [12]. Furthermore, hacker activist groups (termed "hacktivists") have been increasing in both skill and capabilities. It has been reported that General Keith Alexander, head of the National Security Agency, expects hacktivist groups such as Anonymous to be capable of achieving limited national power outages through cyber attacks by 2014 [13].

2.4.2 Criminal Groups

Criminal groups are defined based on their motivation to attack a digital network for monetary gain. Criminal groups often consist of highly trained and elusive technical experts [7] who will use spam, phishing, and spyware or malware to commit identity theft or fraud [12]. Operating independently, criminal groups are not considered to pose a serious direct threat to the physical power system. However, if hired by terrorist groups or nation states, criminal groups may be involved in cyber attacks on the power system with more damaging physical consequences to the electric grid. For example, a terrorist group or nation state may hire a criminal organization to steal sensitive design and other technical information on specific power system assets. In such a circumstance, a criminal group would be aiding and providing plausible deniability to a more threatening attacker capable of realizing a cyber attack with severe consequences to the power grid.

2.4.3 Terrorists

Terrorist groups are motivated by a desire to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken an economy, or damage public morale and confidence [12]. Support for terrorist entities usually comes from an extremist network, but can also derive from foreign intelligence agencies whose national security priorities are aligned with undermining the same nations terrorists seek to harm. With respect to the electrical energy sector in the United States, concerns exist over the increasingly sophisticated use of information technologies exhibited by terrorist organizations that have demonstrated intent to attack critical infrastructures [14]. An analysis of cyber attack data has shown energy industry companies are attacked twice as often as other industries, with a large amount of these attacks originating from the Middle East. Furthermore, surveillance of Al-Qaeda web traffic has indicated periods of increasing interest in SCADA systems [9]. While the consequences of a terrorist cyber attack range from minor to devastating, the threat of terrorist groups pose to critical infrastructures is considered severe enough that protection of critical infrastructures has generated substantial federal policy focus [15].

2.4.4 Nation States

The final cyber attacker profile concerns that of the nation state. It may not be entirely clear why nation states would be interested in attacking the civilian infrastructure of another nation. After all, transmission lines, power plants, and substations are far from weapons of war. Therefore, in order to explain precisely why the electrical sector is so vital to the defense strategies of nations, we will examine an analogous situation concerning Japanese merchant shipping during the 1940s. After the United States entered World War II, a vital component of the U.S. war strategy concerned attacking Japanese merchant vessels. While merchant ships were not explicit military targets, sinking cargo vessels was required to choke off enemy supply lines and deny the Japanese Empire the resources needed to sustain their war effort [16]. Such a high priority was placed on targeting merchant vessels that by the war's end, 2,346 Japanese merchant ships had been sunk compared to 686 Japanese naval vessels [17]. From this World

War II–era U.S. naval strategy, it becomes clear that the destruction of the commercial and industrial capacity of a nation is necessary to render its military ineffective.

With respect to the power grid, since reliable access to electricity is critical to modern economic activities, an attack against a power system could serve to undermine the war industries that support the military power of a nation. Given the vulnerabilities of the electric grid to cyber attacks, it is not surprising that military and intelligence services have been investigating the role of information warfare capabilities in attacking and defending critical infrastructures. So vital is the focus on cyberspace in national security strategies, that the traditional land, sea, air, and space domains of warfare are being expanded to include cyberspace as the fifth domain of warfare [18]. Yet cyberwarfare capabilities are not just limited to traditional global powers such as the United States, Great Britian, Russia, and China. Countries such as Israel, North Korea, and Iran have created organizations for cyber war. So as warfare expands to cyberspace, the resources of governments can be channeled into cyber weapons against electrical infrastructures in the conflict between nations.

2.5 Information Security

In the face of attackers that seek to undermine cyber systems, the three primary security objectives of cyber security systems deployed in response to cyber threats are confidentiality, integrity, and availability (CIA) [19]. Yet these three objectives (shown graphically in figure 2.4) are designed around cyber information systems and are not resolutely applicable to the cyber-physical nature of the electric grid. Nonetheless, an understanding of conventional cyber security objectives and systems are discussed in the subsequent sections in order to serve as a basis for the development of cyber security principles in relation to the cyber-physical electric grid. The firewall and intrusion detection systems employed to achieve operational security for information systems are then discussed to provide a conventional understanding of how cyber security objectives are realized.

Figure 2.4: Cyber Security Objectives [20]

2.5.1 Confidentiality

The security objective of confidentiality relates to preventing the unauthorized disclosure of information [21]. For information systems, confidentiality often relates to privacy and preventing unauthorized persons from obtaining sensitive financial and trade secrets. In a cyber-physical power system, the relevance of confidentiality as a security objective is that it counters the theft of information attacks discussed in section 2.3.1. However, with respect to SCADA and protection systems, confidentiality tends to be less feasible of a security concern. In order to ensure confidentiality, information systems invest computational resources in encrypting messages and authenticating users, which has a side effect of increasing delays in sending and receiving data. Furthermore, encryption of a packet adds to the amount of data that will be sent across a communication link. Due to economic constraints, power system communication channels may not be built with the capacity to transmit larger sized encrypted messages in a timely manner. So while confidentiality is feasible for the enterprise network of a utility, it may be an impractical objective for the control and protective cyber assets, especially taking into consideration the high amount of legacy systems remaining in existence throughout the electric grid [22].

2.5.2 Integrity

Integrity security objectives are concerned with averting the unauthorized modification or destruction of information [21]. Message integrity for electric grid cyber systems is similar to message

integrity for information systems. However, the potential impacts of information being modified or destroyed in a power system are especially severe given the integration of cyber systems with the operation of physical assets. Information integrity is vital to thwarting the corruption of information attacks discussed in section 2.3.2. Message integrity is achieved when receivers are able to successfully verify the origination of a message, and that the message has not been tampered with. In a power system this translates to ensuring data shared between cyber systems has not been falsified and that any device settings changes and control commands are only made by authorized systems and users. Conventional methods of ensuring integrity require message authentication codes (MAC) be appended to the end of messages, which can be decoded by a receiver with some manner of shared authentication key to validate integrity [23]. A MAC does not require an encryption algorithm if confidentiality issues are not of concern, so the resource burdens of building integrity into electric grid cyber systems is not as daunting as those faced with ensuring confidentiality.

2.5.3 Availability

Availability is the ability of a system to perform a function at some moment in time or over a defined period of time [21]. In information systems it is common for availability to be sacrificed in favor of increasing confidentiality and integrity. For applications such as web browsing, e-mail, or online banking, it is often considered better to incorrectly deny an authorized user access than accept a minor risk of an unauthorized user seeing or manipulating sensitive data. However, in the electric grid, cyber systems are required to make time-sensitive control and protective decisions. Therefore, power systems are less tolerant of losses in availability than most information systems. For example, modern high speed relays typically operate in less than five cycles (83 milliseconds) [24]. So if a denial of service attack such as that discussed in section 2.3.3 results in even a small loss in relay availability, vital equipment may be damaged during a fault due to unacceptable delays in breaker clearing times needed to isolate the contingency.

It is also worth mentioning the subject of availability with respect to the physical operation of generators in the power system. Since the total load on a power system fluctuates throughout the day, the generation-to-load balance in a system needs to be carefully monitored and controlled in order to ensure the system frequency remains at a nominal value (typically 50 or 60Hz). Automatic generation control (AGC) systems at an energy control center generally perform this function by controlling generator outputs [25]. So if a cyber attack were to deny availability of the communication system used for monitoring, processing, and control functions between remote assets and an energy control center, the AGC would have difficulty coordinating generator operations needed to maintain a stable system frequency. Additionally, if a cyber attack were to remove generators from service in a manner such as the physical destruction attacks described in section 2.3.4, generation units would be rendered unavailable until repaired. The loss of generating units available for dispatch would constrain the ability of an AGC to maintain system stability, so even if cyber assets remain available the consequences of a physical destruction cyber attack can still result in a loss of availability due to the cyber-physical relationship inherent to power systems.

2.5.4 Firewall

The first line of defense from a classical information security perspective is a network firewall. As shown in figure 2.5, a firewall is a combination of hardware and software that segregates an organization's network from the rest of the internet. Additionally, firewalls limit access to a network based on some set of rules. If a packet of information complies with the rules of the firewall, it will be allowed to pass through. Packets not complying with the firewall rules are blocked.

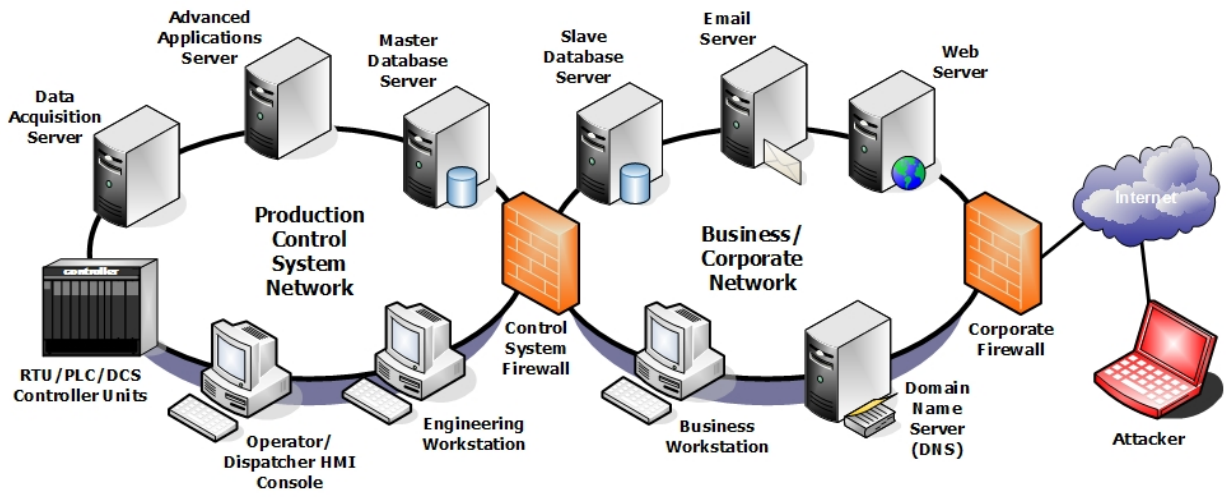

Figure 2.5: Example of a Firewall Network Architecture [26]

Traditional firewalls act as packet filters that examine all information packets entering and leaving the information network, and determine whether or not packets should be allowed to enter or leave the network. Examples of criteria on which a firewall may base a decision to authorize an information packet to enter or leave a network are IP source and destination address, protocol type, TCP or UDP source and destination port, TCP flag bits, ICMP message type, etc. Firewalls may also govern traffic to and from a network by implementing stateful filtering that tracks ongoing connections. Stateful filtering is useful in that it is able to check incoming packets against ongoing connections made within the network. If an external user attempts to establish a connection to an internal network protected by a firewall, a stateful filter would recognize the external traffic as not being part of a connection initiated by an internal user, and block the connection. The third type of firewall is an application gateway, which is an application-specific server from which all data unique to a specific application must pass. Such an application gateway serves to authenticate users, and acts as a server and client through which application specific data can be routed between users and a remote application server [23].

2.5.5 Intrusion Detection

Firewalls only check the header fields of information packets when deciding to allow or block traffic to and from a network. However, the payload of an information packet must also be examined to detect many types of attacks. The act of monitoring the entire contents of a packet for malicious activity is referred to as deep packet inspection, and systems that perform this function are referred to as intrusion detection systems (IDS). IDS systems can often be found at multiple points in an organization's network in order to diffuse the inspection burden placed on any one IDS.

There are two different classifications of IDS systems: signature based IDS and anomaly based IDS. A signature based IDS examines a packet against a database of known attack signatures. If content in an inspected packet matches a known attack signature, a packet is flagged as harmful and the IDS issues an alert to the network administrator or management system. Anomaly based IDS monitors the traffic profile of a network and looks for network traffic that statistically deviates from normal network behavior. Examples of anomalous traffic might be a sudden growth in port scans, a high proportion of packets using a certain protocol, or a high level of packet traffic related to a certain device in a network [23]. When either class of IDS system issues an intrusion alarm, an intrusion response system will take remedial actions such as quarantining suspect packets and compromised systems or severing suspicious communication connections [27].

2.6 Principles of Warfare

In the preceding sections, emphasis was placed on explaining the cyber vulnerabilities in the cyber-physical power system, the types of cyber attacks a power system may face, the potential effects of compromised cyber assets on the physical system, and the actors with the capability and motivation to execute a cyber attack on the electrical grid. Considerations for conventional cyber security objectives and systems were also discussed in addition to how they relate to cyber-physical systems. However, with over 10,000 power plants [28] and 167,000 miles of transmission lines (≥ 230kV) [29] in the United States alone, the sheer magnitude of potential targets could render it difficult to cause a system-wide

reliability impact from attacking a limited number of system components. After all, the power system is designed to be resilient in the face of a litany of natural disasters, such as earthquakes, hurricanes, and winter storms [12]. In order for a cyber attack to succeed in causing a system-wide reliability impact, an attacker would need to carefully coordinate cyber attacks against those assets that lead to exploitation of the inherent physical vulnerability of a power system. To formulate the underpinnings of a credible attack scenario on the power grid, the principles around which adversaries can be expected to define their actions must be understood.

While the issue at hand may be cyber terrorism, cyber crime, or cyber warfare on the smart grid, humanity has a long history of conflict. So even though the battlefield with respect to the power grid may occur in cyber space, an understanding of the core principles of warfare is required before seeking to develop specific cyber attack and defense models for the cyber-physical power grid. As a template for principles underlying attack and defense activities, we reference the U.S. Army's principles of war and operations from FM-03 [30]. FM-03 defines nine principles of warfare: objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity. Given a broad understanding of these nine principles as they relate to the cyber network of the electric grid, profiles of attack scenarios can be formulated and utilized as attack signatures for modeling defensive strategies.

2.6.1 Objective

The first principle of warfare concerns that of defining the objective. From a military perspective, operations should be directed toward a clearly defined, decisive, and attainable objective. As discussed in section 2.5, conventional classifications of cyber attacks typically group cyber attack operations as those resulting in loss of integrity, availability, or confidentiality of some cyber asset. However, in the case of a power system, networked intelligent electronic devices are heavily integrated into the control and protection of the power grid. Therefore, compromising a cyber asset and issuing commands that cause intentional malfunctions can lead to physical destruction of equipment on a local level, or if multiple devices are attacked in a coordinated fashion, the loss of enough key components can

give rise to a cascading failure resulting in a system-wide blackout. With respect to the physical consequences of a cyber attack, the attack models of paramount concern are those involving a cyber attacker whose objective is to interrupt the supply of electrical energy [25]. Naturally, defensive models would have the objective of preventing an interruption in the supply of electrical energy, or of minimizing the interruption if a cyber attack were successful.

2.6.2 Offensive

The principle of offensive relates to the ability of a force to seize, retain, and exploit the initiative. In the cyber realm, initiative is typically seized by bypassing the residual firewall and intrusion detection systems forming residual network security described in sections 2.5.4 and 2.5.5. An attacker would then exploit the initiative by maliciously interacting with a cyber asset to achieve the intended physical damage. Physical power systems are most vulnerable when the system load is at a peak, which reflects aggregate human behavioral habits and regularly occurs during specific hours of the day. An attacker planning to inflict physical harm on the electric grid to facilitate gaining the initiative may therefore plan for an attack to take place during peak hours. A utility would regain the initiative by responding to the intrusion, nominally by severing an attacker's communication tunnel into the network. However, from a utility's perspective, the difficulty in seizing the initiative from an attacker lies in detecting the system is under attack before the physical consequences of the attack reach such a critical state that the controllers and protective devices are unable to contain and respond to the physical effects of a cyber attack.

2.6.3 Mass

The concept of mass relates to concentration of power at a decisive place and time. Typically, attacks will either mass in space or mass in time. An attack that masses in space would seek to focus all resources in striking a decisive blow to a single power system asset, whereas massing in time seeks to overwhelm an adversary by spreading attack resources amongst multiple targets that could be compromised simultaneously. For example, Stuxnet would be an example of a cyber attack that massed

in space, as the sophisticated malicious code executed by the worm was geared towards physical destruction of centrifuge control systems at a specific Iranian nuclear facility [11]. An example of massing in time would be one in which an attacker was able to hack into multiple substations, change the protection settings of the devices, and cause a series of simultaneous line outages throughout a power system. Since NERC reliability criteria require operation of a power system to withstand loss of a single generator or transmission line (referred to as N-1 reliability criteria), attacks that threaten an entire power grid will typically mass in time on some level. Coordination of cyber security measures across generation, substation, and control center facilities will be required to adequately respond to a system-wide attack on the electric grid.

2.6.4 Economy of Force

The principle of economy of force relates to the need for both attackers and utilities to take calculated risks during an unfolding cyber attack and to allocate the minimum resources required to secondary objectives in order to preserve resources for achieving primary objectives. From a system topology standpoint, the transmission lines and buses of a power system are not all equally important in supplying power from generating units to loads within voltage and frequency tolerance limits. Despite possessing limited information, an attacker would need to focus on attacking as few key places as needed to achieve their objective. Conversely, a utility would need to know in advance what combinations of contingencies would likely result in critical vulnerabilities. During a cyber attack, if conventional information security firewalls and intrusion detection systems have been bypassed, the only indication of an ongoing cyber attack may be the physical contingencies being inflicted on the network. Defensive control actions and CIA tradeoffs must therefore be made while the attack is unfolding to prevent all targeted assets from being successfully attacked. If defensive systems take too long to process information and confront an emerging security threat, a critical combination of contingencies may have already emerged and defensive responses would come too late to save the power system.

2.6.5 Maneuver

The principle of maneuver relates to the ability of adversaries to place one another at a disadvantage through flexible application of their resources. The main application of this principle of warfare to cyber security would be in understanding attack vectors. Attackers can exploit vulnerabilities in a power system's cyber network via protocol attacks, routing attacks, direct intrusions, worms or other malware, or denial of service [31]. A utility capable of outmaneuvering a cyber attacker would posses some degree of attack resiliency in monitoring systems, protection, and controllers, so systems could function to some degree even if an attacker successfully exploited an attack vector.

2.6.6 Unity of Command

The principle of unity of command relates to the need for there to be a single responsible commander for every objective. The purpose of unity of command is to mitigate coordination conflicts that hinder the achievement of an objective. This is a significant problem for the energy sector in the United States, where there are over 3,273 traditional electric utilities and 1,738 nonutility power producers separately operating grid systems [32] to maximize their profitability and supplying reliable power to customers. While regional coordinating councils do have a limited role in coordinating reliable operating activities amongst grid entities, the fact remains that attackers have a significant advantage in being able to exploit the boundaries between grid entities where a coordinated response to a cyber incident becomes more difficult. Additionally, many protective devices throughout the power system automatically respond to local conditions, which can result in competing responses to system-level attacks unless attack-resilient wide-area protection schemes are developed [33].

2.6.7 Security

Broadly speaking, the principle of security relates to never allowing an adversary to gain an unexpected advantage. Security from a utility perspective can be understood through conventional firewall and intrusion detection network security applications. Each of the geographically disparate

generators, substations, and control centers within the grid contain cyber components that lie within their respective electronic perimeter, the security of which is subject to compliance with CIP-005 [34]. As discussed in section 2.5.4, firewalls are placed at the access points to an electronic perimeter so that they block unauthorized communication traffic by filtering packets according to allowable protocols, port numbers, source addresses, etc. In the event an attacker is able to bypass a firewall and enter the electronic perimeter of a utility, there exist applications discussed in section 2.5.5 that look for statistically anomalous network activities and check packets for known attack patterns. If an intrusion is detected, an intrusion response procedure or application will act to remove an attacker from the network [35]. Cyber attackers will naturally seek to maintain security by concealing their information-gathering activities and attack vector so that they are able to establish footholds within a system to attain their objective while avoiding detection [7].

2.6.8 Surprise

Surprise is the ability to strike an adversary at a time and place for which they are unprepared. Surprise and security are inherently related, as a successful cyber attack or defense is dependent on relying on one's own security to avoid being surprised and on overcoming the security of an opponent to achieve surprise. However, since power systems form a cyber-physical system, the principle of surprise extends beyond the realm of traditional cyber security concepts to the physical power system. Reliability criteria necessitate a degree of fault tolerance so that a power system can continue normal operations through a single contingency, nominally referred to as N-1 contingency constraint. Normally, the contingencies studied concern the loss of a transmission line or generating unit. For practical economic reasons, power systems are generally not built with the excess redundancy needed to maintain reliability criteria during cases of more than one contingency. Therefore, if a cyber attack were able to result in multiple coordinated physical contingencies (referred to as an N-X contingency), the attacker would be capable of achieving the element of surprise, thrusting a grid entity into an emergency situation to which personnel may be ill prepared to respond. However, not all N-X contingencies will produce a critical

adverse reliability impact [36]. An attacker with limited resources would find it difficult to know the exact state of a power system needed to determine the precise combination of contingencies required to achieve a certain number of physical voltage violations, line overloads, etc. needed to realize an adverse reliability objective.

2.6.9 Simplicity

From the perspective of a utility, the principle of simplicity generally refers to the idea that plans executed on time are better than detailed plans executed late. When utilities run contingency screening applications, the number of contingency cases to study grows exponentially beyond the N-1 cases, so it is computationally infeasible to plan for what will happen beyond the N-1 case before the power system changes. Therefore, when conceptualizing the N-X scenarios, more simplistic methods are required to address the physical implications of a cyber attack in a timely manner. For an attacker, simplicity means being able to plan a successful attack based on limited information. Conventional contingency screening procedures take voltage, generation, and load data being acquired at buses throughout the power system, and use this information to predict the changes the system will experience during an abrupt disturbance [37]. However, since the state of a power system constantly changes, an attacker that meticulously selects attack targets, gathers design information on the selected targets, and then exploits vulnerabilities based on the power system operating state at a certain moment in time will likely find their plan invalidated at a future moment in time when the attack occurs. The only feature in a power system not subject to drastic changes is the location of generators and loads and the system of transmission lines that connects them, referred to as the system topology. Granted, it is normal for a system topology to change during planned maintenance outages or during emergency conditions, requiring removal of a component from service. However, outside maintenance and emergency operating conditions, system topology tends to remain considerably more static. Permanently changing the topology requires physical construction or demolition activities that are capital intensive and subject to publically disclosed regulatory approval. Under normal operating conditions, the only way to physically alter the topology of a power system is to

decommission or construct buses or power lines; these are projects that tend to occur gradually from year-to-year. Therefore, a resource constrained attacker will need to plan attack scenarios based on the static system topology and take advantage of sensitivities of a power system to topology changes in order to ensure the greatest chance a malicious objective is met.

2.7 Attack and Defense Modeling

Given these nine principles of war, attacker profiles can be formulated into a credible, coordinated attack scenario on an electrical grid. First, an adversary launching a coordinated attack on a power grid will need to cause a loss of load to achieve a decisive reliability impact. While attacks that do not result in a cascading failure may be a nuisance to a utility, or perhaps costly if isolated components are physically damaged, the grid as a whole would ultimately be resilient to an attack without a decisive adverse reliability objective. Since power systems are operated to be resilient through an N-1 contingency, an attacker would be required to mass in time, dividing their resources so that multiple targets could be hit simultaneously.

2.7.1 Attack with Complete Information

As will be discussed later in chapter 3, utilities use both DC and AC power flow based performance indices to screen for contingencies meriting concern. However, these contingency screening algorithms typically rely on solving the power flow equations, which requires knowledge of real power injection (P), reactive power injection (Q), bus voltage magnitude (V), bus angle (δ), and elements Y and θ from the system Ybus matrix. AC power flow based contingency screening methods use this information to iteratively converge to the power flow equations and assess the changes in bus voltage magnitude and branch MVA flows. DC power flow based contingency analysis neglects reactive power injections and assumes bus voltage magnitudes are held constant at unity per unit in order to give a linear approximation of branch flows.

Naturally, if an attacker were in possession of real-time state information of a system, they would be able to rank contingencies in the same manner as a power system operator. However, it is important to note that had an attacker intruded into a utility's information network and begun acquiring volumes of technical planning data, the risk to the attacker of a network intrusion detection scheme recognizing such activity as statistically anomalous would be high. An attacker would be exposed to a lesser risk of detection if the intrusion footprint were limited to specific information concerning targets predetermined from a more limited body of information.

2.7.2 Attack with Incomplete Information

From the power flow equations, we know the only variables not subject to change under normal operating conditions are the terms of the bus admittance matrix. So in order to limit the information gathering footprint needed by an attacker, attack targets could be selected based on limited topology system information. Such a strategy would assist with achieving success in a planned offensive by allowing an attacker to increase their security by minimizing chances of detection. However, attacks planned from incomplete information also risk selecting targets that, due to the specific operating state of the power system at the time of attack, turn out to be non-critical targets. As such, an economy of force decision to plan an attack based on incomplete information would require taking a calculated risk favoring the benefits of detection avoidance over certainty in the impact of a given N-X contingency. In chapter 4, graph theory based centrality measures will be investigated as a means to assess the vulnerability of a power system topology to contingencies.

2.8 Summary

The initial sections of this chapter focused on identifying the cyber assets within a power system and describing various manners in which these cyber systems may be attacked. In order to gain familiarity with the motivations and capabilities of potential adversaries, attacker profiles were also discussed. An emphasis was subsequently placed on the challenges posed in applying conventional cyber

security objectives and solutions to the cyber-physical power system. The second part of this chapter centered around the research gap in combining the cyber and physical vulnerabilities of a power system when modeling a coordinated cyber attack. To address this gap, principles of warfare were applied in reference to power grid cyber conflicts in an attempt to generate a foundational knowledge of attack scenario characteristics. Finally, considerations for attack and defense models were introduced based on practical informational awareness limitations attackers face concerning access to power system technical and operations data.

2.9 References

[1] S. Tzú and L. Giles (translator), *The Art of War*. Berkeley, CA: Ulysses Press, 2007, pp.27-34.

[2] F. Wu, K. Moslehi, A. Bose, "Power System Control Centers: Past, Present, and Future," *Proceedings of the IEEE* , vol. 93, no. 11, pp. 1890-1908, Nov. 2005.

[3] R. Rantala, "Cybercrime against Businesses, 2005," Bureau of Justice Statistics, U.S. Department of Justice, Washington, DC, Report NCJ-221943, Sep. 2008.

[4] C. Ten; G. Manimaran; C. Liu; , "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, no. 4, pp. 853-865, Jul. 2010.

[5] D. Whitehead, "Introduction to Power Systems," presented at the *TCIPG Summer School on Cyber Security for Smart Energy Systems*, Urbana-Champagne, IL, 13-17 Jun. 2011.

[6] C. Tranchita, N. Hadjsaid, A. Torres, "Overview of the power systems security with regard to cyberattacks," *Fourth International Conference on Critical Infrastructures*, pp.1-8, 27 Mar. 2009 – 30 Apr. 2009.

[7] S. Liu, B. Cheng, "Cyberattacks: Why, What, Who, and How," *IT Professional*, vol. 11, no. 3, pp. 14-21, May-June 2009.

[8] A. Piskozub, "Denial of service and distributed denial of service attacks," *Proceedings of the International Conference* on *Modern Problems of Radio Engineering, Telecommunications and Computer Science*, pp. 303-304, 2002.

[9] D. Shea, “Critical Infrastructure: Control Systems and the Terrorist Threat,” Congressional Research Service, Library of Congress, Washington, DC, Report RL31534, 21 Feb. 2003.

[10] A. Yazdani, J. Holbach, F. Katiraei, “RTDS (Real Time Digital Simulator) Testing on Aurora Event Hardware Mitigating Devices,” *QT e-News*, vol.2, no. 2, pp. 1-4, Spring 2011.

[11] N. Falliere, L. O. Murchu, and E. Chien, “W32.Stuxnet Dossier,” v1.4, Symantec, Cupertino, CA, 14 Feb. 2011. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[12] R. Schainker, J. Douglas, T. Kropp, "Electric utility responses to grid security issues," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 30-37, Mar.-Apr. 2006.

[13] G. Smith, “Hacking group Anonymous could shut down the entire U.S. power grid, head of national security warns,” *MailOnline*, 22 Feb. 2012. [Online]. Available: http://www.dailymail.co.uk/news/index.html

[14] *DCSINT Handbook No. 1.02 Critical Infrastructure: Threats and Terrorism*. Fort Leavenworth, KS: US Army Training and Doctrine Command, pp. I:1-3, 10 Aug. 2006.

[15] *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: Department of Homeland Security, 17 Dec. 2003. [Online]. Available: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

[16] E. Whitman, “Rising to Victory: The Pacific Submarine Strategy in World War II Part II,” *UNDERSEA WARFARE*, vol. 3, no. 3, Spring 2001. [Online]. Available: http://www.navy.mil/navydata/cno/n87/usw/issue_11/rising_victory.html

[17] The Joint Army-Navy Assessment Committee, “Japanese Naval and Merchant Shipping Losses During World War II by All Causes,” Naval History & Heritage Command, U.S. Department of the Navy, Report NAVEXOS P 468, Feb. 1947. [Online]. Available: http://www.history.navy.mil/library/online/japaneseshiploss.htm

[18] M. Murphy, “War in the Fifth Domain,” *The Economist*, 1 Jul. 2010. [Online]. Available: http://www.economist.com/node/16478792

[19] *Standards for Security Categorization of Federal Information and Information Systems*, National Institute of Standards and Technology, Standard FIPS PUB 199, Feb. 2004.

[20] E. Carabott, “Taking Security Seriously,” *TalkTechToMe*, 15 Jun. 2009. [Online] Available: http://www.gfi.com/blog/taking-security-seriously/

[21] K. S. Trivedi, D. S. Kim, A. Roy, D. Medhi, "Dependability and security models," *7th International Workshop on Design of Reliable Communication Networks*, pp. 11-20, 25-28 Oct. 2009.

[22] INL Critical Protection/Resilience Center, “Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues,” Office of Electricity Delivery and Energy Reliability, Department of Energy, Idaho Falls, ID, Report INL/EXT-09-15500, Apr. 2009.

[23] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*, ed. 5. Boston, MA: Pearson Education Inc., 2010, pp. 704-709 & 747-759.

[24] J. L. Blackburn and T. J. Domin, *Protective Relaying Principles and Applications*, ed. 3. CRC Press, 2007, p. 21.

[25] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. McGraw-Hill, 1994, pp. 532 & 562.

[26] U.S. Computer Emergency Readiness Team, "Control Systems Security Program: Overview of Cyber Vulnerabilities," Department of Homeland Security. [Online]. Available: http://www.us-cert.gov/control_systems/csvuls.html

[27] N. Stakhanova, S. Basu, J. Wong, "A Taxonomy of Intrusion Response Systems," *International Jounal on Information and Computer Security*, vol. 1, no. 1/2, 2007, pp. 169-184.

[28] "What is the electric power grid, and what are some challenges it faces?," U.S. Energy Information Administration, 27 Apr. 2012. [Online]. Available: http://205.254.135.7/energy_in_brief/power_grid.cfm

[29] M. Kaplan, "Electric Power Transmission: Background and Policy Issues," Congressional Research Service, Library of Congress, Washington, DC, Report R40511, 14 Apr. 2009.

[30] *Operations*, U.S. Army Field Manual FM 3-0, 2001, pp. 4:11-15.

[31] M. Govindarasu, A. Hann, P. Sauer, "Cyber-Physical Systems Security for Smart Grid," PSERC, Publication 12-02, Feb. 2012.

[32] Rebecca Peterson, "Electric Power Industry Overview 2007," U.S. Energy Information Administration, 2008. [Online]. Available: http://www.eia.gov/cneaf/electricity/page/prim2/toc2.html

[33] D. Kirschen, "Power System Security," *Power Engineering Journal*, pp. 241-248, 2002.

[34] *Cyber Security – Electronic Security Perimeter(s)*, NERC Reliability Standards for the Bulk Electric Systems of North America, Standard CIP-005-2, May 2009.

[35] N. B. Anuar, M. Papadaki, S. Furnell, N. Clarke, "An investigation and survey of response options for Intrusion Response Systems (IRSs)," *Information Security for South Africa*, pp. 1-8, 2-4 Aug. 2010.

[36] T. S. Sidhu, L. Cui, "Contingency screening for steady-state security analysis by using FFT and artificial neural networks," *IEEE Transactions on Power Systems*, vol. 15, no. 1, pp. 421-426, Feb. 2000.

[37] A. J. Wood and B. F. Wollenberg, *Power Generation Operation and Control,* ed. 2. New York, NY: Wiley, 1996, pp. 410-432.

CHAPTER THREE

POWER SYSTEM PHYSICAL VULNERABILITY ANALYSIS

3.1 Introduction

This chapter discusses some of the core concepts related to vulnerability analysis for the physical power system. Since power systems are cyber-physical systems, a cyber attack has the potential to physically impact the electric grid. Therefore, an understanding of the fundamentals of conventional power system security analysis is needed to assess the physical vulnerability impact of a coordinated cyber attack. Concepts important to ranking contingencies are also presented, and the relevance of conventional contingency ranking schemes in validating various attack models based on limited information is highlighted. This chapter then concludes with a more technically detailed presentation of DC power flow based contingency analysis measures and an AC power flow based performance index ranking method.

3.2 Power System Security Analysis

Regardless of the cyber threats discussed in chapter 2, maintaining physical system security has long been a factor in operation of power systems. However, the term 'security' in power systems is usually defined as the ability to supply customers with uninterrupted power in the presence of unexpected failures throughout the grid [1]. As described in section 1.3.1, there are generally two types of failures that can occur within a power system: i) short circuit faults and ii) open circuit faults. Short circuit faults are normally the result of some form of insulation failure. Any time phases in a power system come into contact with one another or the earth, an energized part of the power system fails to be insulated from its ambient surroundings. Such conditions are usually caused by extreme weather events, unmanaged vegetation, or equipment failures, and can result in dangerously high short-circuit conditions. The second failure type is classified as a cessation of current flow that results in an open-circuit fault. Normally,

open-circuit faults occur when circuit breakers or switches fail to open and close correctly, so that phases are unintentionally in or out of service [2].

In order to mitigate the shock to a power system caused by failure, protection systems are installed throughout the electric grid. These protection systems are designed to isolate problem areas quickly while leaving the rest of the power system intact. The devices that monitor power system conditions and initiate appropriate control actions if abnormal or dangerous situations develop are called protective relays [3]. However, other systems and procedures related to how a power system is operated are also encompassed in power system security [4].

In current practice, electric grids are designed for limited resiliency in the face of naturally occurring security challenges such as tornadoes, hurricanes, ice storms, and earthquakes. In times of emergency, utility personnel can often respond quickly to perform repairs and restore systems isolated by protection systems due to enduring failures [5]. So given that the power system has already been designed for resiliency in the face of a hostile natural environment, it may not seem that cyber security challenges pose much of an added threat beyond those already present and protected against. After all, if a cyber attack were to cause a problem in the physical system, protective relays should be able to take sufficient control actions to isolate the problem just as they would in any other emergency condition. Even if a certain protective relay or system is compromised by a cyber attack, power system protective schemes include remote and local back-up protection that can isolate problem areas in the event primary protection fails [3]. However, it is not economically feasible for power systems to be built with enough redundancy to be 100% reliable. The redundancy built into power systems is designed so that the system can be operated in a manner by which the probability of dropping service to customers due to an unanticipated failure is relatively small [4]. If a cyber attacker were to cause equipment failures in a random manner, it may be possible to state a cyber attack is no more of a threat than bad weather. However, as intelligent human beings cyber attackers are not bound to abide by statistical failure probability models. Just like utility engineers, a cyber attacker with sufficient information could perform a vulnerability analysis on a power system and identify coordinated failures that would result in

catastrophic conditions in the electric grid. Therefore, security or vulnerabilities studies of the physical power system are closely related to cyber security challenges posed by an attacker who coordinates targeted attacks on specific cyber systems, leading to harmful conditions within the electric grid.

3.3 Contingency Ranking

Regardless of the purpose and intent behind a security or vulnerability study, both forms of analysis involve ranking studied contingencies according to severity of the adverse reliability impact. Yet implicit in the notion of a coordinated attack on a power system is that an attacker has the ability to rank possible contingencies and attack those cyber systems which result in the highest adverse reliability impact. This raises further questions concerning what constitutes an adverse reliability impact. Furthermore, ranking contingencies requires some methodology to assess the condition of a power system and to integrate the various system properties into a single index number that reflects the overall impact to system reliability. Physical components (generators, lines, transformers, etc.) constituting a power system have certain capacity ratings for which they are designed to be operated safely within. Since it would be dangerous for equipment to be operated outside rated performance specifications, contingency ranking algorithms favor cases resulting in conditions that exceed component design ratings. Commonly studied violations include branch flow overloads and bus voltages being under or over rated limits. Contingency screening can also include performance indices based on stability studies utilizing dynamic characteristics of components [6]. Here we will limit our ranking discussions to the more simplistic steady state contingency analyses.

As will be discussed in greater detail in section 3.4, DC power flow based assessments can be used to calculate approximate changes in line flow resulting from loss of a branch or power injection at a bus. More detailed AC power flow based studies such as those discussed in section 3.5 can determine changes in line flows and bus voltages resulting from a branch and bus injection outages. The only problem with conventional AC/DC power flow ranking schemes from a cyber attacker's perspective is they require some knowledge of the power system operating state, which an attacker may not possess.

However, as a precursor to modeling a coordinated cyber attack, it is first necessary to understand how utilities in possession of complete system information conventionally assess and rank the performance impact of a contingency. Such conventional contingency ranking techniques serve as a baseline for assessing the actual adverse reliability impact of various contingency scenarios. With a conventional assessment of the physical consequences of contingencies established, the utility of nonconventional contingency ranking algorithms based on more limited information available to attackers can be validated.

3.4 DC Power Flow Based Ranking

DC power flow based linear sensitivity factors (LSF) are commonly used to quickly compute approximate changes in line MW flows resulting from possible outages or a given change in bus injection. The two principle LSF measures utilized to screen for likely line overloads are the generation shift factor (GSF) and the line outage distribution factor (LODF) methods. However, it is important to note that LSF methods are only approximate. Since the DC power flow neglects both MVAR flows and bus voltage magnitudes, the calculated MW flows have an error of approximately 5% compared to the actual values [4]. The main disadvantage of LSF contingency ranking methods is that they cannot incorporate voltage violations when assessing contingencies. AC power flow calculations are required to calculate bus voltage violations resulting from a contingency.

3.4.1 Generation Shift Factors

In order to provide a linear estimate of the proportionate effect a change in power injection at a bus i will have on a line l of the power system, the GSF is defined as follows:

$$a_{li} = \frac{\Delta f_l}{\Delta P_i} \tag{3.1}$$

where Δf_l is the change in MW power flow on line l when a change in generation or load ΔP_i occurs at bus i [4]. However, for the purposes of this research we will generalize the GSF equation to let i equal all system buses rather than just those where a generator is present. In this manner, the sensitivity factor a_{li}

indicates how sensitive a line l is to a change in generation or load at bus i. Accordingly, we will now refer to a_{li} as the bus injection shift factor (BISF)

The results of the BISF method are reported as a matrix with n columns representing the number of buses in the power system, and m rows corresponding to the number of branches in the system. However, it is often useful to assign each bus in the power system a single value indicating its relative importance rather than the sensitivity of each branch flow to the change in bus injection. Therefore, the BISF matrix will be consolidated into a single column reflecting how significant an impact a change in bus power has on the power system as a whole. In other words, we need to extract a measure from the BISF matrix indicating the total change in MW flows along lines caused by a change in bus power or loss of a line. Using principles of matrix norms that provide an assessment of linear vector system sensitivities we use the BISF matrix to generate a bus injection impact factor (BIIF) a_i defined as:

$$a_i = \sum_l |a_{li}| \tag{3.2}$$

for each non-swing bus i representing the total magnitude of the factors a_{li} attributable to bus i, or the L_1 norm [7] of each column of a_{li}. In this manner, the importance of each bus is determined by the degree to which the change in power at the bus causes changes in line flows throughout the power system.

The BISF factor can also be generalized to approximate changes in line flows due to multiple changes in bus injections. If we define k as a set of numbers relating to those buses where there are changes in bus injections, we can define $\Delta f_{l,k}$ as the resulting change in MW flow along line l from the simultaneous change of injections at buses included in k as:

$$\Delta f_{l,k} = \sum_{i \in k} a_{li} \Delta P_i \tag{3.3}$$

However, this complicates the generation of a multiple bus injection impact factor (MBIIF), since the linear combination of BIIF terms are weighted according to the change in bus injection ΔP_i at multiple buses, and given two buses a and b it is not necessarily true that $\Delta P_a = \Delta P_b$. Yet for purposes of achieving some MBIIF number we need only ensure similar assumptions apply consistently to all

contingency cases. Therefore, for a power system with a set of buses N, we can define the MBIIF as a_k, where $k \subset N$, as:

$$a_k = \sum_l \left| \sum_{i \in k} a_{li} \right| \tag{3.4}$$

In this case, it is effectively being assumed that $\Delta P_a \approx \Delta P_b$ for all $a, b \subset N$ and $a \neq b$. While this could be a poor assumption for a specific contingency case involving multiple changes in bus injection, the utility of the measure is realized when comparing the sensitivity of the power system to higher order contingencies.

3.4.2 Line Outage Distribution Factors

Similar to the BISF linear sensitivity method, the LODF provides a linear estimate of the proportionate effect a loss of a line k has on the MW flow on line l of the power system, and is defined as follows:

$$d_{l,k} = \frac{\Delta f_l}{f_k^0} \tag{3.5}$$

where Δf_l is defined the same as shown in section 3.4.1, and f_k^0 is the pre-outage MW flow on line k. The resulting sensitivity factor $d_{l,k}$ provides an indication as to how sensitive a line l is to a loss of line k, and is commonly used to screen for potential overloads if a transmission line outage occurs [4].

Similar to the GSF, the results of the LODF method are reported as a matrix. However, there are m columns and m rows in the LODF matrix representing the number of branches in the power system. The diagonal entries of the LODF matrix are empty as there is no power flow along an outaged line. In order to consolidate the impact the loss of a single line has on changes in branch flows, a line outage impact factor (LOIF) d_k can be generated for each line k from the L_1 norm of the LODF matrix columns, and is defined as:

$$d_k = \sum_l \left| d_{l,k} \right| \tag{3.6}$$

Here, the importance of a line k is determined by the collective proportionate change in line flows resulting from the outage of line k.

Generalization of the LODF procedure to cases involving more than one line outage can be accomplished by following the detailed procedures described in [8] and [9] to produce a multiple line outage distribution factor (MLODF) matrix. However, for general awareness purposes the concept behind calculation of the MLODF will be explained in brief. Generation of a MLODF matrix for a contingency involving x line outages requires computation of x LODF matrices. Each of the x LODF matrices is generated from a unique subsystem created from the base case power system by removing $x - 1$ lines. For example, if we wanted to generate the MLODF matrix for a contingency case involving the outage of lines k_1, k_2, and k_3 we would write the sum of three separate LODF expressions:

$$\Delta f_l = \left(d_{l,k\in S-k2-k3}\right)f_{k1}^0 + \left(d_{l,k\in S-k1-k3}\right)f_{k2}^0 + \left(d_{l,k\in S-k1-k2}\right)f_{k3}^0$$

Combining these summations into matrix-vector multiplication yields:

$$\Delta f_l = \begin{bmatrix} d_{l,k\in S-k2-k3} & d_{l,k\in S-k1-k3} & d_{l,k\in S-k1-k2} \end{bmatrix} \begin{bmatrix} f_{k1}^0 \\ f_{k2}^0 \\ f_{k3}^0 \end{bmatrix} = MLODF_{l,\{k1\ k2\ k3\}} \begin{bmatrix} f_{k1}^0 \\ f_{k2}^0 \\ f_{k3}^0 \end{bmatrix} \tag{3.7}$$

So we can define then MLODF factor of a line l for contingencies involving the outage of lines k_1, k_2, and k_3 as the augmentation of three LODF matrices, expressed as:

$$MLODF_{l,\{k1\ k2\ k3\}} = \begin{bmatrix} d_{l,k\in S-k2-k3} & d_{l,k\in S-k1-k3} & d_{l,k\in S-k1-k2} \end{bmatrix} \tag{3.8}$$

Similar to the MBIIF complication, there is a problem in generating multiple line outage impact factor (MLOIF) values since the change in preoutage flows f_k^0 is not equal for all possible values of k. However, a MLOIF value for each line l for a contingency set c can be found by assuming all LODF matrices augmented to form the MLODF have equally weighted f_k^0 factors in order to apply consistent assumptions for relating contingency cases. In this manner, the MLOIF can be defined for a power system S with line outage contingency case c as:

$$MLOIF_c = \sum_l \left| \sum_{i=1}^{x} d_{l,k\in S-c/i} \right| \tag{3.9}$$

While this MLOIF measure would be a poor assessment of determining the change in specific line flows for a given contingency, it does provide a rough manner in which to assess the sensitivity of line flows to multiple line outages that will prove useful later in chapter 5.

3.5 AC Power Flow Based Performance Index Ranking

For contingency studies where accuracy is more important than the speed at which solutions can be computed, AC power flow based studies are required. Unlike the DC power flow based studies discussed in section 3.4, reactive power is not neglected when computing an AC power flow based solution. Therefore, AC power flow based contingency studies not only allow analysis of steady state MVA line flows, but bus voltages can be determined and checked for under/over voltage conditions. With the information available from an AC power flow, it is often desirable to form an assessment of how much a certain outage may affect the entire power system compared to other outage conditions. Naturally, such a need gives rise to the concept of a performance index for a power system during a contingency state. Such a performance index would integrate all calculated line flows and bus voltages into a single index number reflecting the estimated physical security of a power system. The performance index would also need to take into consideration the MVA limits of all branches in the power system, as well as tolerable voltage variations at each system bus.

When evaluating the performance of a power system against branch overloads, the overload performance index PI_{OL} is defined as:

$$PI_{OL} = \sum_{\substack{all\ branches \\ i}} \left(\frac{P_{flow\ l}}{P_l^{max}} \right)^{2n} \tag{3.10}$$

Here, $P_{flow\ l}$ is the calculated MVA flow on line l from the power flow solution. The MVA capacity of line l is P_l^{max}, and n is just a design constant. If n is large, then $P_{flow\ l}/P_l^{max}$ will be near zero if the MVA flow on line l is less than the MVA capacity of line l, but will approach infinity if the flow on line l exceeds the MVA capacity of line l. While values of n can theoretically be as large or small as desired,

in practice n is a finite number. This results in branches that are not overloaded contributing some number less than one to the performance index, and overloaded lines adding some finite value greater than one assuming $n \geq 1/2$. So it is not always the case where the contingency resulting in the most overloads is given the highest performance index. Depending on the severity of overloads and how near the capacity limit overloaded branches are operating, the performance index ranking of a contingency will change for different values of n set in accordance with the needs of the designer.

Since bus voltages are also determined from the AC power flow solutions, it is possible to create a bus voltage variation performance index PI_{VV} defined as:

$$PI_{VV} = \sum_{\substack{all\ buses \\ i}} \left(\frac{\Delta|E_i|}{\Delta|E|^{max}} \right)^{2m} \tag{3.11}$$

The variable $\Delta|E|^{max}$ reflects the maximum allowable change in bus voltage, which can be based on utility engineer settings, reliability standards, or other criterion. The change in bus voltage $\Delta|E_i|$ is found by taking the magnitude of the difference between bus voltage magnitudes from a solved power flow with no outages and the power flow solution with outages. Similar to the variable n from the overload performance index, m is just a design constant that affects the emphasis given in the performance index to bus voltage variations within tolerance limits compared to those exceeding the maximum specified voltage variation.

The voltage violation and overload performance indices can now be combined into a unified AC power flow performance PI_{ACPF} [4] given as:

$$PI_{ACPF} = \sum_{\substack{all\ branches \\ i}} \left(\frac{P_{flow\ l}}{P_l^{max}} \right)^{2n} + \sum_{\substack{all\ buses \\ i}} \left(\frac{\Delta|E_i|}{\Delta|E|^{max}} \right)^{2m} \tag{3.12}$$

Once PI_{ACPF} values are calculated for all contingencies of concern, the resulting list of performance indices can be sorted such that the largest PI_{ACPF} is at the top of the list. In this manner, utility engineers can study remedial action schemes for those credible contingences with severe performance impacts as identified by a highly ranked PI_{ACPF} value. In the event a contingency with a critical performance impact

actually occurs, a response can be implemented by a system operator or remedial action scheme [10] to change the operation of a power system for purposes of mitigating the reliability impact of outages.

3.6 Summary

Since the cyber assets within an electric grid control the physical operation of the power system, this chapter delved into security analysis concepts that have relevance in assessing the physical consequences of a coordinated cyber attack for vulnerability analysis purposes. It was explained that, to an extent, the power system is designed for resiliency in the face of naturally occurring failure events. However, a unique challenge resulting from cyber threats to the electric grid is that an attacker can target assets for attack that result in the emergence of a dangerous, low probability contingency scenario. So even a system designed, protected, and operated for resiliency in the face of random component failures may be ill prepared to defend against deliberate failures coordinated by a cyber attacker. The importance of contingency ranking methods was also discussed since a coordinated cyber attack would ultimately have the objective of inflicting a highly ranked contingency on the power grid. This chapter then elaborated on the DC and AC power flow based contingency analysis methods in order to establish a baseline for evaluating the adverse reliability impact of possible contingency scenarios.

3.7 References

[1] D. Kirschen, “Power System Security,” *Power Engineering Journal*, pp. 241-248, 2002.

[2] N. Tleis, *Power System Modeling and Fault Analysis: Theory and Practice*, Oxford, UK: Elsevier Ltd., 2008, pp. 4-6.

[3] J. L. Blackburn and T. J. Domin, *Protective Relaying Principles and Applications*, ed. 3. CRC Press, 2007, pp. 1-5, 168-169.

[4] A. J. Wood and B. F. Wollenberg, *Power Generation Operation and Control,* ed. 2. New York, NY: Wiley, 1996, pp. 414-432.

[5] R. Schainker, J. Douglas, T. Kropp, "Electric utility responses to grid security issues," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 30-37, Mar.-Apr. 2006.

[6] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. McGraw-Hill, 1994, pp. 695-746.

[7] L. N. Trefethen and D. Bau, *Numerical Linear Algebra*. Philadelphia, PA: Society for Industrial and Allied Mathematics, 1997, pp. 17-18.

[8] J. Guo, Y. Fu, Z. Li, M. Shahidehpour, "Direct Calculation of Line Outage Distribution Factors," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp.1633-1634, Aug. 2009.

[9] T. Guler, G. Gross, M. Liu, "Generalized Line Outage Distribution Factors," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp.879-881, May 2007.

[10] S. Wang, G. Rodriguez, "Smart RAS (Remedial Action Scheme)," *2010 Innovative Smart Grid Technologies (ISGT) Conference*, pp. 1-6, 19-21 Jan. 2010.

CHAPTER FOUR

APPLICATION OF GRAPH THEORY TO POWER SYSTEM VULNERABILITY

4.1 Introduction

This chapter pertains to the fundamentals of graph theory (also referred to as network theory). The necessary concepts leading up to the definition of centrality measures are explained; centrality measures are then utilized to rank the relative importance of buses and lines in a power system for vulnerability analysis purposes. Subsequently, centrality measures are compared to conventional DC power flow based sensitivity factors for a number of single contingency test cases. Based on the results of statistical correlations and Wilcoxon signed rank tests, conclusions are then drawn concerning the potential utility of centrality for power system vulnerability studies.

4.2 Definition of a Graph

In a formal sense, a graph $G = \{V, E\}$ consists of an ordered pair of vertices V and edges E. The finite nonempty vertex set of the graph G with n verticies is expressed as $V(G) = \{v_1, v_2, \dots, v_n\}$. A graph G with m edges joining the vertices in V has an edge set defined as $E(G) = \{e_1, e_2, \dots, e_m\}$. Edges and vertices are related in that any given edge e is a two-element subset of two adjacent vertices u and v [1]. Simply stated, vertices can be thought of as points, and edges thought of as the lines connecting pairs of points. Relating these graph theory (also referred to as network theory) terms to a power system, we can consider the buses in a power system as the set of vertices V, and the transmission lines and transformers connecting the buses in a power system as the edges E [2]. Figure 4.1 shows a simple case for how the buses and branches of an example six bus power system may be graphically converted into an equivalent graph model of the same power system.

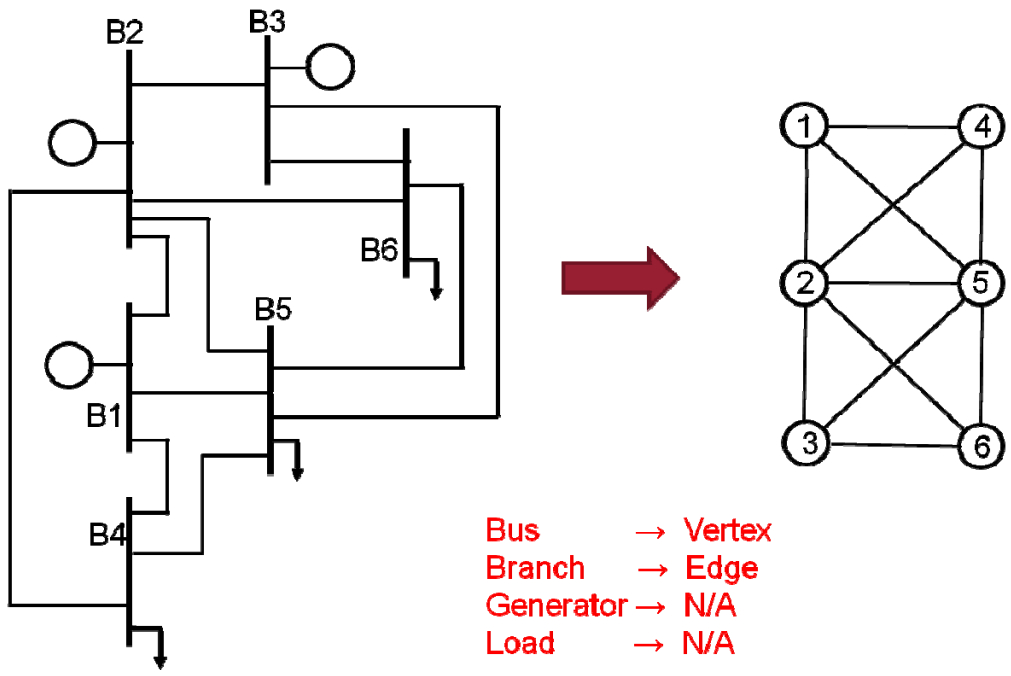

Figure 4.1: Visual Representation of the Conversion of a 6-Bus Power System into a Graph

However, since the branches in a power system have different impedances based on conductor length, circular area, and configuration it would be inappropriate to treat all edges equally in modeling a power system as a graph. Therefore, we assign weights $w(e)$ to each edge in the graph model of a power system based on the estimated impedance of corresponding power system branch. Yet the branch impedance Z of a transmission line or transformer is a complex number, where the real component is a resistance R and the imaginary component is the reactance X, such that $Z = R + jX$. Since graph theory is only suited to weighting edges with scalar quantities, approximating the complex branch impedances by scalar quantities is required. The existing body of published research concerning graph theory and power systems has resolved this scalar edge weighting in one of two ways [3]:

1) Utilize the magnitude of a branch impedance as the edge weight such that $w(e) = |Z|$.
2) Since the reactive component of a branch impedance is usually much greater than the resistive component (i.e. $X \gg R$), simply use the reactance of a branch as the edge weight such that $w(e) = X$.

For purposes of simplicity, we will elect to define edge weights in the manner described in the second option. As will be described in the next section, the value of edge weights for our purposes is to reflect the electrical distance between buses in a power system. In cases where buses are not directly adjacent, utilizing $w(e) = |Z|$ will result in a path distance that reflects the sum of magnitudes of complex numbers, which is not a conventional mathematical operation. By defining $w(e) = X$, we can reasonably reflect the electrical distance between two buses without complicating the shortest path algorithms forming the foundation of the centrality measures in which we are interested.

Given a graph model of a power system consisting of vertices V corresponding to system buses, edges E representing the system branches, and edge weights $w(e)$ reflecting the branch impedances, we can now represent the relations between buses as an adjacency matrix. For a graph of order n, where the order of a graph is defined as the total number of vertices, we can represent the graph G as an $n \times n$ adjacency matrix A [4], where the entry a_{ij} in the i^{th} row and j^{th} column of A is defined as:

$$a_{ij} = \begin{cases} w(e_{ij}) & \text{if } v_i \text{ is adjacent to } v_j \in E \\ 0 & \text{otherwise} \end{cases}$$

Formulation of the adjacency matrix is similar in nature to formulation of the Y_{bus} [5] matrix. However, nonzero off diagonal terms in A reflect the branch impendence instead of the admittance, and diagonal terms in A are zero rather than the nonzero bus coupling terms found in the diagonal elements of the Y_{bus}.

4.3 Shortest Path Problem

Some analytical techniques used to rank the importance of vertices and edges in a graph rely on being able to determine the shortest path between a pair of vertices. Namely, the closeness centrality measure discussed in section 4.4.3 and the betweeness centrality measures discussed in sections 4.4.4 and 4.4.5 require determination of the shortest path between pairs of vertices. Fundamentally, shortest path algorithms seek to determine the minimum distance required to traverse from some vertex v_i to another vertex v_j. Since in our study we are defining edge weights as the branch reactances, the shortest path

between two vertices will effectively be the minimum sum of branch reactances required to form a $v_i v_j$ path.

There are a number of algorithms for determining the shortest path between all pairs of vertices in a graph. Here, we will focus on the relatively simple Floyd-Warshall algorithm [6][7]. However, if the adjacency matrix of a graph is sparse Johnson's algorithm [8] will be more computationally efficient, and the Bellman-Ford algorithm [9][10] can be utilized in cases where edge weights are allowed to be negative.

The Floyd-Warshall algorithm starts with an initialized distance matrix D^0 with entries $d^0(i,j)$. The initial distance matrix is merely the adjacency matrix with infinity entries in the off diagonal terms where an edge does not exist, defined as:

$$d^0(i,j) = \begin{cases} 0, & i = j \\ w(e_{ij}), & v_i \text{ is adjacent to } v_j \\ \infty, & \text{otherwise} \end{cases}$$

For a graph with n vertices, the Floyd-Warshall algorithm will require n^3 iterations to completely cycle through the three nested loops to yield a shortest path distance matrix D, whose entries $d(i,j)$ correspond to the length of the shortest path between vertices v_i and v_j is the manner shown below:

$$\begin{aligned} &Initialize: D = D^0 \\ &\quad for\ k = 1:n \\ &\quad\quad for\ i = 1:n \\ &\quad\quad\quad for\ j = 1:n \\ &\quad\quad\quad\quad d(i,j) = min[d(i,j), d(i,k) + d(k,j)] \end{aligned}$$

For each iteration, the Floyd-Warshall algorithm checks each entry $d(i,j)$ of D in search of a shorter path from vertex v_i to vertex v_j passing through vertex v_k. If the sum $d(i,k) + d(k,j)$ is less than the current entry of $d(i,j)$, then the Floyd-Warshall algorithm will replace the entry $d(i,j)$ with $d(i,j) = d(i,k) + d(k,j)$. In this manner, the computational performance complexity of the Floyd-Warshall algorithm is $O(n^3)$, or the process requires an amount of work proportional to n^3. The space complexity of the Floyd-

Warshall algorithm is $O(n^2)$, meaning the amount of memory needed to store the result of the Floyd-Warshall algorithm is of order n^2.

4.4 Centrality Measures

In this study, the rationale behind studying graph theory applications to power systems is based on potential insight into how an attacker in possession of limited information may target components of a power system such that the adverse reliability impact of a coordinated cyber attack is maximized. So when modeling a physical power system as a graph, the goal is to use the graph model to determine how important the various edges (branches such as transmission lines, transformers) and vertices (buses) are in relation to one another in a given system. While the precise definition of an 'important' power system bus or branch relates to reliability criteria in the physical system, in a graph theory sense a number of centrality measures have been developed to assign a ranking coefficient to each vertex or edge in a graph. While these ranking coefficients have little meaning independently, their relative values can provide some insight as to the importance of vertices and edges compared to each other. In the following subsections, the degree, eigenvector, closeness, and vertex betweeness centrality measures are examined for purposes of ranking the vertices of a graph, as well as the edge betweeness centrality measure for ranking the importance of graph edges [3].

4.4.1 Degree Centrality

One of the more simplistic centrality measures for assigning a relative importance to each vertex of a graph is the degree centrality measure, defined as:

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

Here, the degree centrality of vertex v is simply the degree of vertex v divided by the normalizing constant $n-1$. Since the maximum degree of a vertex is one less than the total number of vertices, the $n-1$ normalizing constant effectively ensures that the degree centrality remains bounded in the interval

$[0,1]$. The underlying concept behind degree centrality is that a given vertex v in graph G will have the greatest capacity to influence some other vertex $u \neq v \in V(G)$ if u and v are adjacent, i.e. there is an edge $= (u, v) \in E(G)$. Therefore, if the maximal degree of G is $\Delta(G)$ and the minimal degree of G is $\delta(G)$, then a vertex v will have the greatest capacity to influence other vertices in G if $deg(v) = \Delta(G)$, and v will have minimal influence if $deg(v) = \delta(G)$. However, if $\delta(G) \leq deg(v) \leq \Delta(G)$ then v has some relative influence proportional to the value of $deg(v)$ within the integer interval $[\delta(G) \ldots \Delta(G)]$.

4.4.2 Eigenvector Centrality

The eigenvector centrality method defines the importance of a bus in the power system based on the coupling of the bus to high-ranking neighboring buses. This is found by finding the maximum eigenvalue λ_{max} and eigenvectors x_j of the adjacency matrix A_{ij} of a power system. For this particular centrality measure, branch admittances are utilized for the edge weights of nonzero terms in the adjacency matrix since the branch admittances scale directly with the coupling of a bus to a given neighboring bus. Expressed as an equation, the eigenvector centrality for each bus i of an n bus power system is defined as:

$$C_E(i) = \frac{1}{|\lambda_{max}|} \sum_{j=1}^{n} |A_{ij} x_j|$$

Here, it can be seen that the eigenvector centrality of each bus is proportional to the sum of the centralities of all connected buses. It is also worth noting that the eigenvector centrality measure is often related to the degree centrality measure in that a bus with high eigenvector centrality will typically be adjacent to buses with high degree centrality.

4.4.3 Closeness Centrality

In utilizing the Floyd-Warshall or alternate shortest path algorithm, we can develop a more sophisticated centrality measure for determining the importance of a vertex. The closeness centrality

measure defines the importance of a vertex $v \in V(G)$ as the mean geodesic distance from the vertex v to all other vertices in $V(G)$ in the manner shown below:

$$C_C(v_i) = \frac{\sum_{j \in V \setminus i} d(i,j)}{n-1}$$

Here, the $d(i,j)$ term consists of the entries of the shortest path distance matrix D, denoting the length of the shortest path between vertices v_i and v_j. The $n-1$ divisor is attributed to the $n-1$ vertices reachable from some vertex v (for a connected graph with n vertices). However, since the above version of closeness centrality would result in vertices having a large mean geodesic distance to all other vertices having a greater closeness centrality value than vertices that are actually "closer" in the sense of there being a smaller mean geodesic distance to all other vertices, the closeness centrality measure can alternatively appear as:

$$C_C(v_i) = \frac{n-1}{\sum_{j \in V \setminus i} d(i,j)}$$

which is merely the inversion of the initial closeness centrality measure for a given vertex v_i. In this inverted form, a vertex with a smaller relative mean geodesic distance to all other vertices will have a larger closeness centrality value.

4.4.4 Vertex Betweeness Centrality

While the closeness centrality measure is well suited to identifying centrally located vertices, in many applications it is often desirable to attribute the importance of a vertex according to its influence on the shortest path of flow between vertices. This is particularly relevant in applications such as the internet, where routers tend to direct information packets through a network in order to minimize the time delay between a source of information and the end host. Therefore, the betweeness centrality measure introduces a quantity $\sigma_{jk}(i)$, defined as follows:

$$\sigma_{jk}(i) = \begin{cases} 1, & \text{if vertex } v_i \neq v_j \neq v_k \text{ lies on the shortest path between } v_j \text{ and } v_k \\ 0, & \text{otherwise} \end{cases}$$

However, it is possible for there to be multiple parallel paths between pairs of vertices of equal distance, so we introduce the term σ_{jk} defined as:

$$\sigma_{jk} = \text{total number of unique shortest paths between } v_j \text{ and } v_k$$

Given these definitions for $\sigma_{jk}(i)$ and σ_{jk} we can now express the betweeness centrality for a vertex v_i as:

$$\mathrm{C_{Bv}}(v_i) = \sum_{j \neq i \neq k \in V} \frac{\sigma_{jk}(i)}{\sigma_{jk}}$$

It is important to note that a modified version of the shortest path algorithm is required to keep track of the vertices on each shortest path (or paths if more than one shortest path exists) between pairs of vertices. Given a complete set of shortest paths between all pairs of vertices, the betweeness centrality algorithm essentially awards points to a given vertex for being on a shortest path between pairs of vertices (or fractional points if more than one shortest path exists). The final vertex betweeness centrality values then give an indication as to relative importance of a given vertex to the flow between all vertices in a graph.

4.4.5 Edge Betweeness Centrality

In the act of tracking the vertices encountered along shortest paths, it is also possible to develop a betweeness centrality measure of the edges in a graph, defined as:

$$C_{Be}(e_i) = \sum_{j \neq k \in V} \frac{\sigma_{jk}(i)}{\sigma_{jk}}$$

Here, the definition of σ_{jk} remains the same, but now $\sigma_{jk}(i)$ can be defined as:

$$\sigma_{jk}(i) = \begin{cases} 1, & \text{if edge } e_i \text{ lies on the shortest path between } v_j \text{ and } v_k \\ 0, & \text{otherwise} \end{cases}$$

In this manner, we now have an edge betweeness centrality measure for the edges in a graph indicating the relative importance of each edge to the efficient flow between all vertices in a graph.

4.5 Correlation of Centrality Measures to Linear Sensitivity Factors

With the five centrality measure definitions described in section 4.4, the questions remains concerning whether any graph theory centrality measures reflect a conventional method of understanding the impact of a given contingency. In order to quickly screen a centrality measure for potential utility, we correlate the DC power flow based impact factors defined in section 3.4 with the corresponding vertex and edge centrality measures for a series of test systems. In this manner, the bus injection impact factor (BIIF) will serve as a baseline for determining a critical loss of generation or load at a bus, and the degree, eigenvector, closeness, and vertex betweeness centrality measures will be considered promising candidates for further study if the centrality measure correlates well with the BIIF. Likewise, the line outage impact factor (LOIF) for assessing the reliability consequences for the loss of a branch will be correlated with the edge betweeness centrality measure to assess whether or not edge betweeness warrants further investigation concerning a limited information contingency analysis technique.

By performing these correlations, we attempt to validate whether any centrality measures have a consistent, statistically significant similarity with the DC power flow based sensitivity methods. When correlating the BIIF with a vertex centrality measure, or the LOIF with an edge centrality measure, a correlation coefficient R ranging from -1 to 1 will reflect the degree of similarity between the two measures [11]. For instance, an R coefficient of 1 would indicate the measures are perfectly identical, a -1 would indicate the measures are perfectly opposite from one another, and an R coefficient of 0 would mean there is no relationship between the two measures. These correlations were performed for the smaller IEEE test systems: IEEE-14 bus system, IEEE-30 bus system, IEEE-57 bus system, and IEE-118 bus system [12] as well as a larger Polish 2383 bus winter peak test system from the 1999-2000 year, Polish 2736 bus summer peak system from the year 2004, Polish 2737 bus summer off-peak system from the year 2004, Polish 2746 winter peak system from the year 2003-2004, Polish 2746 winter off-peak system from the year 2003-2004 [13].

Both small and large test systems were chosen for analysis in order to provide some indication as to the consistency of results across a variety of power system topologies and operating conditions.

Correlation coefficients for each simulation are shown in tables 4.1 and 4.2 below along with the p-value level of significance test statistics [14] (note that any test statistic less than 10^{-308} will register as zero due to underflow restrictions inherent to performing double-precision floating point arithmetic [15]).

Table 4.1: Vertex Centrality Measures Correlated with the N-1 Bus Injection Impact Index

Test System	Correlation, $R(C_D, a_i)$		Correlation, $R(C_E, a_i)$		Correlation, $R(C_C, a_i)$		Correlation, $R(C_{Bv}, a_i)$	
	R coeff	p-value	R coeff	p-value	R coeff	p-value	R coeff	p-value
IEEE-14	-0.7681	1.01×10^{-3}	-0.8816	1.14×10^{-6}	-0.5699	2.83×10^{-3}	-0.3770	1.69×10^{-2}
IEEE-30	-0.4885	1.56×10^{-12}	0.1680	1.74×10^{-16}	-0.6923	4.36×10^{-11}	-0.3152	2.49×10^{-4}
IEEE-57	-0.4218	6.42×10^{-25}	0.0442	9.60×10^{-28}	-0.6580	2.01×10^{-21}	-0.2598	7.54×10^{-8}
IEEE-118	-0.2992	3.20×10^{-59}	-0.3473	3.34×10^{-65}	-0.6409	9.67×10^{-46}	-0.4156	2.40×10^{-7}
Polish-2383	-0.0956	0	-0.0594	0	-0.6354	0	-0.3565	3.31×10^{-39}
Polish-2736sp	-0.2372	0	-0.1471	0	-0.3647	0	-0.3387	2.22×10^{-53}
Polish-2737sop	-0.2343	0	-0.1229	0	-0.3712	0	-0.3390	2.30×10^{-53}
Polish-2746wp	-0.2470	0	-0.0798	0	-0.3714	0	-0.3416	1.91×10^{-53}
Polish-2746wop	-0.2416	0	-0.0813	0	-0.3902	0	-0.3421	2.13×10^{-53}

Table 4.2: Edge Centrality Measure Correlated with the N-1 Line Outage Impact Factor

Test System	Correlation, $R(C_{Be}, d_k)$	
	$R(C_{Be}, d_k)$	p-value
IEEE-14	0.5179	1.39×10^{-4}
IEEE-30	0.5679	2.10×10^{-9}
IEEE-57	0.6609	3.79×10^{-12}
IEEE-118	0.5519	4.91×10^{-12}
Polish-2383wp	0.6012	6.83×10^{-68}
Polish-2736sp	0.5332	8.82×10^{-86}
Polish-2737sop	0.5373	9.34×10^{-86}
Polish-2746wp	0.5344	1.50×10^{-85}
Polish-2746wop	0.5357	1.87×10^{-85}

The results of the correlation simulations highlight several important relationships. It is notable that the eigenvector centrality measure does not consistently correlate with the BIIF, as the correlation coefficients range from strongly negative to weakly positive. However, the remaining centrality measures do appear to have some consistent correlation with their corresponding BIIF and LOIF metrics. The closeness centrality measure appears to have a weak to moderately strong negative linear relationship with the BIIF index across all nine test systems, and the degree and vertex betweeness centrality measures have a seemingly consistently weak negative correlation with the BIIF index. In order to further analyze the vertex centrality measures correlated with the BIIF index, scatter plots of the correlations such as

those shown in figure 4.2 for the IEEE 57 bus system and Polish 2383 bus system were reviewed. This was necessary to assure a linear relationship between the two indices and an ability to rank contingencies (i.e., there is not an excessive number of components that share a top rank).

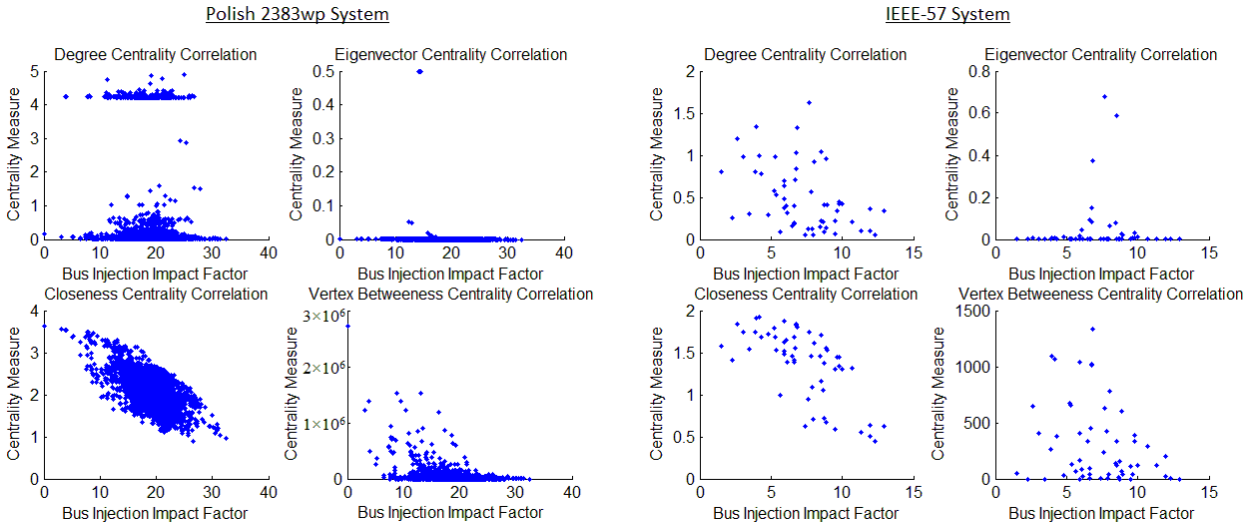

Figure 4.2: Degree, Eigenvector, Closeness, and Vertex Betweeness Centrality Correlations with the Bus Injection Impact Factor (BIIF) for the Polish-2383wp (Left) and IEEE-57 (Right) Systems.

From the correlation plots in figure 4.2, it appears that the only vertex centrality index resulting in a fairly linear trend is the closeness centrality measure. While there may be a somewhat linear appearance in the vertex betweeness centrality correlation plots, the negative trend in the correlation coupled with the number of buses having zero vertex betweeness centrality yields a series of top contingencies that are unrankable. For example, in the larger Polish 2383 bus winter peak system there are 560 buses with zero centrality. Essentially, this means that there are far too many top ranked contingencies identified by the vertex centrality method sharing a number one ranking for the measure to be useful. However, the smaller coefficients for the correlation of closeness centrality with the BIIF for the Polish-2736sp, Polish- 2737sop, Polish-2746wp, and Polish-2746wop is of note, as it provides some evidence indicating the closeness centrality measure is not consistent. Since these four Polish test systems are topologically similar, we would expect the correlation coefficients to be approximately equal.

Yet a closer examination of figure 4.3 indicates that the weak correlation of the four Polish test systems is primarily due to a cluster of outliers shared by all four plots. While the existence of outlier data points does not necessarily rule out the closeness centrality measure in being considered for vulnerability analysis purposes, it does suggest some caution in trusting the measure to reliably rank critical contingencies.

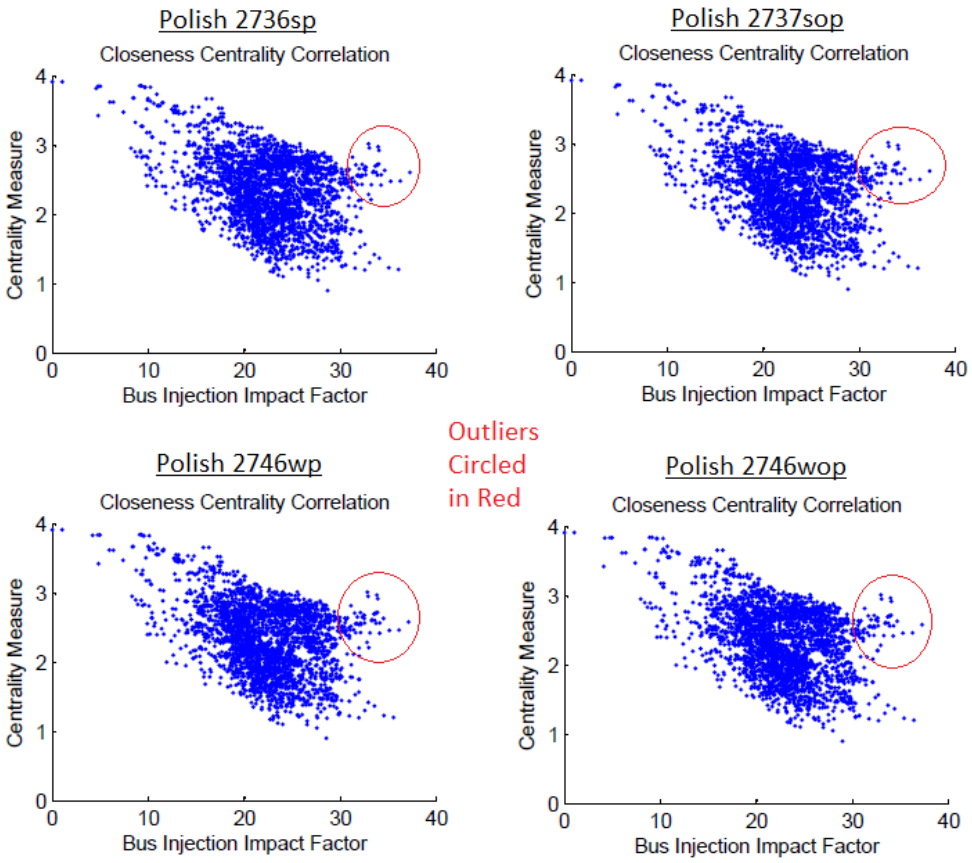

Figure 4.3: Closeness Centrality Correlations with the Bus Injection Impact Factor (BIIF) for the Polish-2736wp (Left) and Polish-2746wop (Right) Systems.

Scatter plots were also analyzed for the correlations involving the edge betweeness centrality and LOIF measures. As observed in figure 4.4 for the IEEE 57 bus system and Polish 2383 bus system, the relationship between the two line vulnerability indices (C_{be} and d_k) appears linear. Since the correlation coefficients ranged from approximately 0.52 to 0.66, additional plots are not shown to investigate

inconsistencies in correlation coefficients across test systems. For the purposes of this screening of centrality measures, the edge betweeness centrality and LOIF correlations yielded consistently strong results.

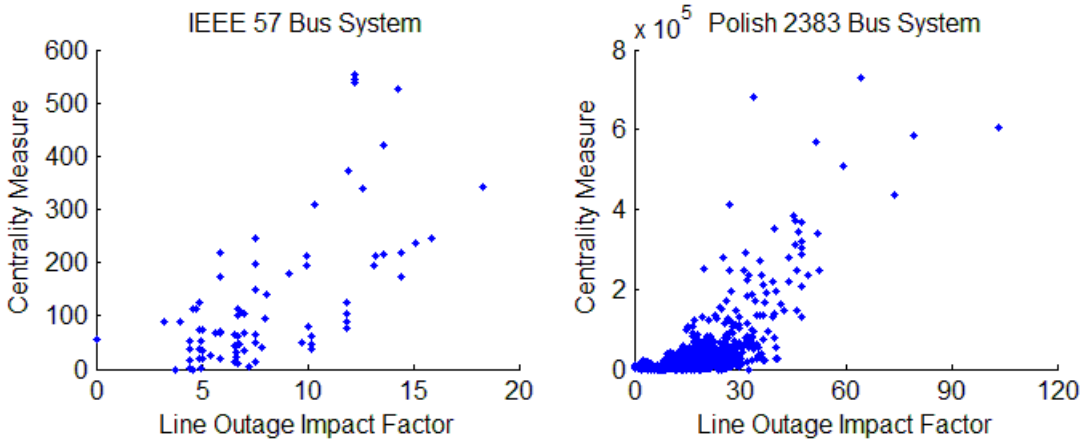

Figure 4.4: Edge Betweeness Centrality Correlation with the Line Outage Impact Factor (LOIF) for the IEEE-57 (Left) and Polish-2383wp (Right) Systems.

4.6 Statistical Comparison of Centrality and Linear Sensitivity for N-1 Contingencies

While correlating entire data sets for the centrality and linear sensitivity factor based vulnerability indices provides useful information concerning how a specific centrality measure may be used to rank the relative importance of contingencies, such an analysis does not wholly reveal the utility of a centrality measure with respect to planning a cyber attack. A cyber attacker would only be interested in using a vulnerability index to identify a subset of highly ranked targets that, if successfully attacked, are likely to result in a reasonably high impact adverse reliability scenario. Therefore, to assess the usefulness of a centrality technique, we perform a more in-depth statistical analysis of the top ten contingencies indicated by a given centrality technique compared to the corresponding rank of the component as indicated by relevant LSF based index. Since we are comparing matched pairs of line or bus vulnerability rankings, the Wilcoxon signed rank test [16] was utilized to estimate the median difference between the two rankings for purposes of providing some indication as to the level of difference between ranking systems. For each case a Wilcoxon signed rank test was performed to test the following null hypothesis:

H0: There is not a difference between the DC power flow based index and the centrality based index being tested.

In the event that the lower bound and upper bound of the estimated median difference between ranking indices encompass the zero median difference, the null hypothesis would fail to be rejected (i.e. the two indices are statistically identical for the stated confidence interval). Conversely, if the lower bound and upper bound of the estimated median difference between ranking indices does not encompass the zero median difference, the null hypothesis would be rejected (i.e., the two indices are statistically different for the stated confidence interval) [17]. An example of the matched pair difference data generated for use with the Wilcoxon signed rank test and the resulting statistical results is shown in table 4.3 for the edge betweeness and LOIF based indices. In hypothesis testing, the confidence interval sets the range of values expected to encompass the true median a certain percentage of the time. Here, statistical results were calculated using Minitab [18], which sets a default confidence level of 95% commonly used in statistical studies. However, depending on the sample size it is not always possible to achieve a confidence level of exactly 95%. Rather, a confidence level near 95% is achieved, resulting in the 94.7% confidence level observed in table 4.3 for the comparisons of ten quantities from each of the two ranking systems.

Table 4.3: Matched Pair Data from the Polish-2383wp System, Edge Betweeness Centrality and LOIF

Line	Centrality Rank	LOIF Rank	Matched Pair Difference
15-165	1	4	3
18-76	2	56	54
20-18	3	1	-2
67-20	4	2	-2
159-165	5	8	3
18-15	6	5	-1
138-67	7	3	-4
159-176	8	126	118
176-158	9	21	12
8-18	10	19	9
	Estimated Median Difference		5.0
	94.7% Confidence Interval		-1.5 to 58.0
	Conclusion		Fail to Reject H0

While only the closeness and edge betweeness centrality methods were identified as adequate candidates for a top 10 ranking analysis, the degree centrality rankings compared to the corresponding BIIF ranks were also analyzed in order to provide some basis for comprehending the severity of differences between rankings that do not linearly correlate well. As is shown in table 4.4, the median difference between the top ten degree centrality bus rankings matched to the BIIF based bus index rankings tends to drastically scale upwards with the size of the test system. Additionally, the 94.7% confidence interval bounds of the estimated median difference between the degree centrality and BIIF based rankings expand as the subset of top ten buses becomes a smaller portion of the total number of system buses to such an extent that one would expect similar results from comparing two measures assigning bus ranks at random.

Table 4.4: Wilcoxon Signed Rank Test for Top 10 Vulnerabilities – Degree Centrality Matched to the BIIF Index

Test System	N	Estimated Median	Lower Bound	Upper Bound	Achieved Confidence
IEEE-14	10	0.5	-1.5	3.0	94.7%
IEEE-30	10	3.5	-1.5	8.0	94.7%
IEEE-57	10	12.5	3.5	22.5	94.7%
IEEE-118	10	35.5	11.5	63.5	94.7%
Polish-2383wp	10	1104	319	1925	94.7%
Polish-2736sp	10	1385	807	1937	94.7%
Polish-2737sop	10	1381	768	1970	94.7%
Polish-2746wp	10	1496	924	2055	94.7%
Polish-2746wop	10	1371	799	1976	94.7%

The estimated median differences between the closeness centrality top 10 bus rankings matched to the BIIF bus rankings are shown in table 4.5 along with the 94.7% confidence interval bounds. The results indicate the estimated median differences remain closer to zero as the number of test system buses increase compared to the degree centrality method. However, an increase in the range of values encompassed in the 94.7% confidence interval for larger test systems indicates that the closeness centrality method will prove unreliable at correctly identifying the top 10% of high impact buses. As such, it is concluded that the Closeness Centrality measure fails to provide a reasonable estimate for the top ten sensitive buses as indicated by the BIIF based index.

Table 4.5: Wilcoxon Signed Rank Test for Top 10 Vulnerabilities – Closeness Centrality Matched to the BIIF Index

Test System	N	Estimated Median	Lower Bound	Upper Bound	Achieved Confidence
IEEE-14	10	1.0	-1.0	4.5	94.7%
IEEE-30	10	3.0	0.0	6.5	94.7%
IEEE-57	10	4.5	-1.0	11.5	94.7%
IEEE-118	10	-19.5	-37.0	-12.0	94.7%
Polish-2383wp	10	80	20	404	94.7%
Polish-2736sp	10	676	275	1060	94.7%
Polish-2737sop	10	652	275	1006	94.7%
Polish-2746wp	10	690	318	999	94.7%
Polish-2746wop	10	669	353	959	94.7%

While the vertex centrality based top 10 bus ranking may have matched poorly with the BIIF based bus rankings, the results shown in table 4.6 indicate that the edge betweeness line rankings match well to the paired LOIF based line ranks. For each test system, the 94.7% confidence interval encompasses the zero median (a zero median indicates no statistical difference in the top ten lines identified by the edge betweeness centrality and LOIF based indices). Furthermore, the confidence interval appears to remain fairly constricted around the estimated median difference, even for large test systems. Such results provide evidence in support of the edge betweeness centrality measure to reliably rank critical contingencies.

Table 4.6: Wilcoxon Signed Rank Test for Top 10 Vulnerabilities – Edge Betweeness Centrality Matched to the LOIF Index

Test System	N	Estimated Median	Lower Bound	Upper Bound	Achieved Confidence
IEEE-14	10	3.0	-1.5	7.0	94.7%
IEEE-30	10	5.0	-2.0	11.5	94.7%
IEEE-57	10	6.0	-1.5	10.0	94.7%
IEEE-118	10	4.5	-1.0	10.5	94.7%
Polish-2383wp	10	5.0	-1.5	58.0	94.7%
Polish-2736sp	10	6.0	-1.0	23.0	94.7%
Polish-2737sop	10	7.5	-1.0	20.0	94.7%
Polish-2746wp	10	7.5	-1.0	23.5	94.7%
Polish-2746wop	10	10	-2.0	28.5	94.7%

4.7 Summary

In this chapter, the necessary theoretical background for applying graph theory to a power system was presented. Graph theory based centrality measures were then applied to the power system to rank N-1 generator/load and line outage contingencies. These graph theory based rankings were compared to DC power flow based linear contingency screening methods for assessing the sensitivity of power system line flows to bus injection and line outage contingencies. Correlation and non-parametric statistical tests indicated the closeness centrality measure was most suited to identifying high impact bus injection contingencies, and the edge betweeness centrality measure posed a promising measure for identifying high impact line outage contingencies. As a result of these studies, it is concluded that the closeness centrality and edge betweeness centrality measures are the most promising candidates for use in developing an N-X graph theory based vulnerability assessment algorithm.

4.8 References

[1] G. Chartrand and P. Zhang, *Introduction to Graph Theory*. New York, NY: McGraw-Hill, 2005, pp. 1-17.

[2] P. Hines, S. Blumsack, E. Cotilla Sanchez, C. Barrows, "The Topological and Electrical Structure of Power Grids," presented at the *43rd Hawaii International Conference on System Sciences*, 5-8 Jan. 2010.

[3] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical Centrality Measures for Electric Power Grid Vulnerability Analysis," presented at the *49th IEEE Conference on Decision and Control*, pp.5792-5797, 15-17 Dec. 2010.

[4] N. Deo, *Graph Theory with Applications to Engineering and Computer Science*. New Delhi, India: Prentice Hall, 1974, pp. 157-161.

[5] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. McGraw-Hill, 1994, pp. 238-255.

[6] R. W. Floyd, "Algorithm 97: Shortest Path," *Communications of the ACM*, vol. 5, p. 345, Jun. 1962.

[7] S. Warshall, "A Theorem on Boolean Matrices." *Journal of the ACM*, vol. 9, pp. 11-12, Jan. 1962.

[8] D. Johnson, "Johnson's Algorithm for Sparse Graphs," Journal of the ACM, vol. 24, pp. 1-13, Jan. 1977.

[9] R. Bellman, "On a Routing Problem," *Quarterly of Applied Mathematics*, vol. 16, pp. 87-90, 1958.

[10] L. R. Ford and D. R. Fulkerson, "Maximal Flow Through a Network," *Canadian Journal of Mathematics*, vol. 8, pp. 399-404, 1956.

[11] D. J. Best and D. E. Roberts, "Algorithm AS 89: The Upper Tail Probabilities of Spearman's Rho," *Journal of the Royal Statistical Society Series C*, vol. 24, no. 2, pp. 377-379, 1975.

[12] Power Systems Test Case Archive, University of Washington Department of Electrical Engineering. Available: http://www.ee.washington.edu/research/pstca/.

[13] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. 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.

[14] R. Lyman Ott and M. Longnecker, *An Introduction to Statistical Methods and Data Analysis*, ed. 6. Belmont, CA: Brooks/Cole CENGAGE Learning, 2010, pp. 246-249.

[15] D. Watkins, *Fundamentals of Matrix Computations*, ed. 3. Hoboken, NJ: Wiley, 2010, p. 141.

[16] R. Rumsey, *Statistics II for Dummies*. Indianapolis, IN: Wiley, 2009, pp. 296-301.

[17] R. Lyman Ott and M. Longnecker, *An Introduction to Statistical Methods and Data Analysis*, ed. 6. Belmont, CA: Brooks/Cole CENGAGE Learning, 2010, pp. 265-270.

[18] Minitab 16.1.1 (software). State College, PA: Minitab Inc, 2010.

CHAPTER FIVE

TOPOLOGY ATTACK SCENARIOS AND SIMULATION STUDIES

5.1 Introduction

In chapter 4, statistical evidence was presented indicating a significant relationship between the closeness and edge betweeness centrality measures and the analogous linear sensitivity factors for the N-1 contingency case. In an effort to build upon the chapter 4 results, the focus of this chapter will be on generalizing the closeness and edge betweeness centrality measures for use in N-X contingency analysis studies. Here, the objective of ranking contingencies using limited information remains the same as the chapter 4 single contingency studies. Only now the goal is development of a centrality based tool capable of ranking at least three concurrent contingencies such that the top five percent of ranked N-X contingences have a higher than average mean AC power flow (ACPF) based performance index. This goal is realized by proposing separate N-X graph theory based bus and branch vulnerability analysis measures. Subsequent statistical comparisons are then made between the graph theory measures compared to the corresponding DC power flow based N-X linear sensitivity measures. In an attempt to develop a unified centrality performance index for ranking N-X contingencies, a method to combine the two closeness and edge betweeness based N-X contingency algorithms is proposed. This unified centrality performance index is then compared to a conventional ACPF based performance index. The statistical results of the centrality and ACPF performance index comparisons provide evidence in support of the centrality based performance index to select branch and generator outage contingencies that statistically have a higher expected ACPF performance index value than contingencies selected at random. A presentation of how vulnerability assessments based on centrality performance indices can be validated within a test bed environment is also included, along with contingency performance assessments using direct measurements from a real time power system simulator. While the purpose of this research is chiefly to develop background knowledge concerning coordinated attack models based on limited

information, at the end of this chapter prospective defensive applications of topology based performance indices are discussed in order to offer guidance for future research activities.

5.2 Selectivity Considerations

Before delving into an N-X topology based vulnerability algorithm, it is first important to note that an attacker has the option to select targets for attack based on screening measures used by operators to generate a short list of contingencies warranting further analysis. Given the size and computations involved in studying contingencies, system operators often select only a short list consisting of those contingencies most likely to result in a line overload or bus voltage violation to study. By examining a short list of likely cases of concern, the amount of time needed to execute a contingency analysis program can be quick enough that potential operational security constraint issues can be addressed within a reasonable amount of time. A common selectivity filtering assumption is to neglect analyzing contingencies involving losses of lines below a certain power transfer (such as 100MW) [1]. Additionally, under NERC critical infrastructure protection standard CIP-002-4 [2] general criteria are established designating assets as critical despite the operational state of the power system at a specific moment in time. Examples of critical asset criteria from CIP-002-4 include those generation facilities exceeding 1500MW or 1000MVAR and transmission facilities exceeding 500kV. While capacity and operational based selection filtering assumptions have their uses, there is often a speed/accuracy tradeoff associated with skipping potentially critical cases or being overwhelmed with information to analyze. For example, taking more conservative threshold limits tends to result in a short list that is too large to analyze in a timely manner. Conversely, a smaller short list may be quicker to analyze, but some contingencies left off the short list may in fact be critical and warrant further analysis.

By using topology based methods for contingency analysis rather than focusing on the capacity, bus voltage, power injection, or power transfer of a specific asset, we instead utilize the location of a bus or line in the power system as the primary selectivity concern. This approach has the benefit of utilizing information more readily available to an attacker, while also taking into account relevant system level

relationships between buses and branches that go beyond capacity based assessments. However, in order to accomplish such a topology based selectivity study, the closeness centrality and edge betweeness centrality concepts presented in section 4.4 must be integrated into a unified measure with the ability to rank simultaneous bus injection and line outage contingencies resulting from a coordinated attack on a power system.

5.3 Development of a Graph Theory Based N-X Contingency Analysis Algorithm

Given the significant statistical relation of closeness centrality and edge betweeness centrality to conventional measures for N-1 bus injection and line outage contingencies respectively, algorithms are developed in this section that generalize centrality measures presented in section 4.4.3 and 4.4.5 to the N-X case. However, existing centrality measures have not been developed for assessing the importance of multiple elements taken simultaneously. Therefore, algorithms presented in this section are designed to be as analogous as feasible to DC power flow based multiple contingency screening methodologies [3-4].

5.3.1 Closeness Centrality

The statistical analysis concerning the utility of vertex centrality measures performed in sections 4.5 and 4.6 indicated a lack of suitability of the four vertex centrality measures in relation to generation or load outage contingencies. However, since closeness centrality proved the strongest vertex centrality candidate, in this section we will generalize the closeness centrality algorithm to identify high impact N-X generator or load contingencies. Modeling an N-X outage through graph theory is not straightforward. Generator and load outages only result in loss of power injection at a bus, so from a topology standpoint the graph $G = (V, E)$ remains unchanged since the contingency does not result in loss of buses or lines in the power system. Therefore, even in the presence of a bus injection contingency, the closeness centrality measure for each vertex will remain unchanged. Accordingly, assessing an N-X contingency can only be based on combining closeness centrality terms from the base case $C_C\big(V(G)\big)$.

To extend the closeness centrality concept to the general case involving N-X bus injection outages, we first note that for an N bus power system being modeled as a graph G, the set of vertices $V \in \mathbb{R}^N$ correspond to the power system buses. Now we define some $N - X$ contingency case $k \in \mathbb{R}^X$, where $k \subset V$. A new closeness centrality impact measure CI_C can then be introduced reflecting a collective topology assessment of multiple generator outages, defined as:

$$CI_C(k) = \sum_{i \in k} |C_C(v_i)| \tag{5.1}$$

In effect, the closeness centrality impact factor (CCIF) is just the sum of the closeness centrality of the vertices relating to the X vertices resulting in a loss of bus injection.

5.3.2 Edge Betweeness Centrality

From sections 4.5 and 4.6, evidence was provided in support of the edge betweeness centrality measure as a strong candidate for selecting high impact line outage contingencies. However, when transitioning from the N-1 to N-X case a complication occurs in that there does not exist a method of assessing the edge betweeness of multiple edges taken at the same time. Since we are assessing edge betweeness for purposes of line outages in a power system, removal of X edges in G will result in a subgraph $H = G - X$. The resulting edge betweeness centrality $C_{Be}\big(E(H)\big)$ of the edges in $E(H)$ is fundamentally different from that exhibited in $C_{Be}\big(E(G)\big)$, so direct addition of $C_{Be}\big(E(G)\big)$ terms cannot be performed in the manner similar to section 5.3.1.

A procedure similar to that performed in an MLODF analysis is therefore proposed for combining edge betweeness centralities to determine a cumulative edge betweeness impact factor CI_{Be} for an N-X line outage contingency $k \in \mathbb{R}^X$. Here, we determine all combinations of edges in a N-X contingency case k taken $X - 1$ at a time, expressed as C_X^{X-1} in combinatoric notation. We define the list $E' \in \mathbb{R}^{X \times (X-1)}$ as having unique row entries containing all but one of the of the edges $E(k)$. Within a row c of E', the edge $e_{o,c}$ from contingency k not appearing in $E'(c)$ will be defined as $e_{o,c} = (e \in k) \notin E'(c)$.

We now define a subgraph $H_c = G - E'(c)$. The edge betweeness of $e_{o,c}$ can be now be taken from $C_{Be}\big(E(H_c)\big)$. The collective edge betweeness impact for contingency k is therefore:

$$CI_{Be}(k) = \sum_{c=1}^{X} C_{Be}\big(e_{o,c}\big) \tag{5.2}$$

In this manner, the edge betweeness centrality impact factor (EBCIF) for an N-X contingency is basically the sum of the edge betweeness centralities for each individual outage edge, where the edge betweeness centrality of an outage edge is calculated from a subgraph formed by removing the other X-1 outage edges. A flow chart of this procedure is included as figure 5.1.

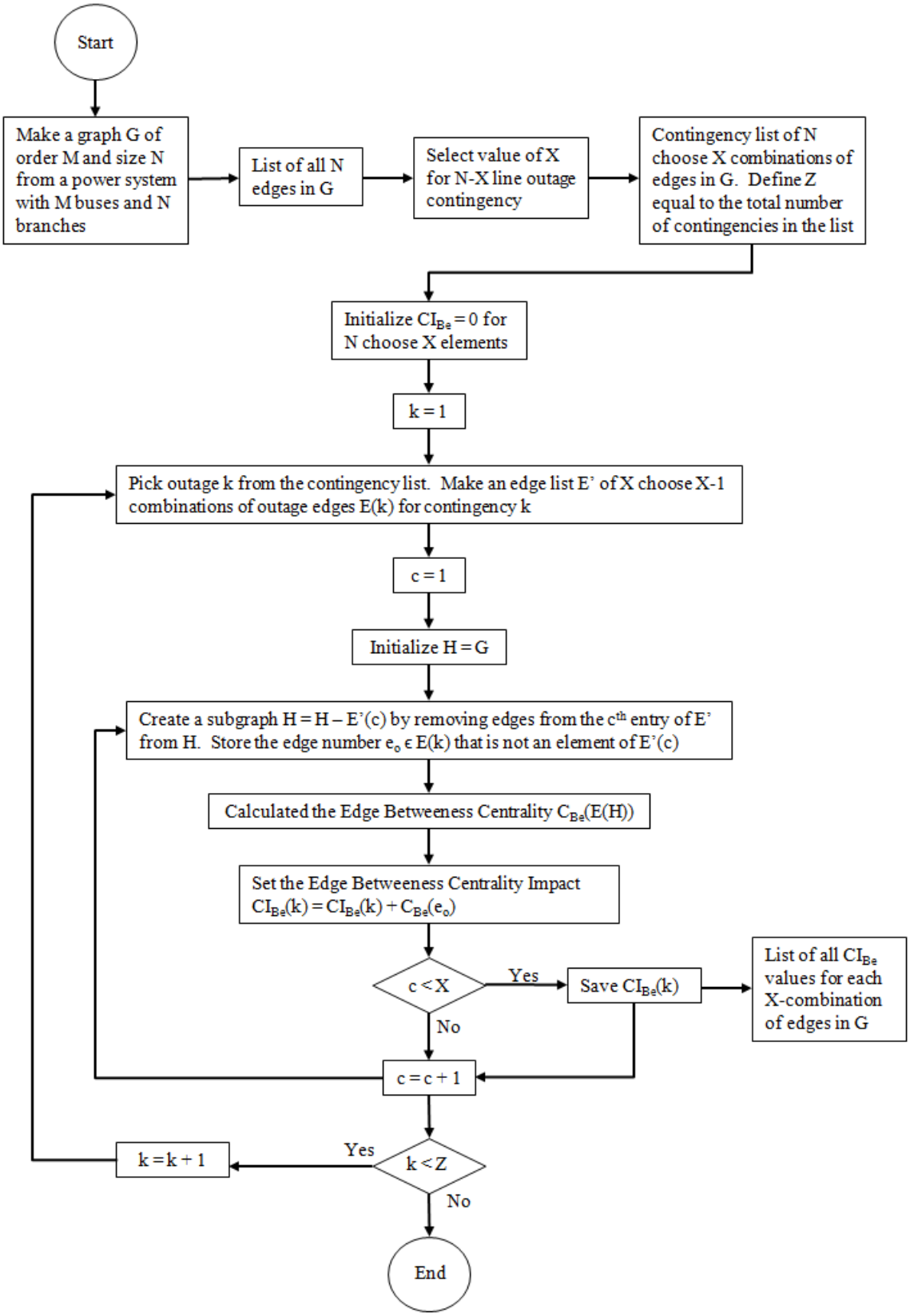

Figure 5.1: N-X Edge Betweeness Centrality Impact Algorithm

5.4 Statistical Comparison of Centrality and Linear Sensitivity for N-X Contingencies

With closeness and edge betweeness centrality algorithms established for N-X contingencies, it is now imperative to determine whether these N-X contingency graph theory based algorithms relate at all to the respective Multiple Line Outage Impact Factor (MLOIF) or Multiple Bus Injection Impact Factor (MBIIF). The conclusions drawn in sections 4.5 and 4.6 were specific to the N-1 case, so it must be verified whether or not closeness and edge betweeness centrality vulnerability measures can be accurately generalized to the N-X case. Therefore, in this section correlations and Wilcoxon signed rank tests will be performed relating the closeness centrality impact measure to the DC power flow based multiple bus injection impact factor, and the edge betweeness impact factor will be related to the MLOIF. These statistical tests were performed for both N-2 and N-3 results on the IEEE-14, IEEE-30, IEEE-57 bus systems, and for N-2 contingencies on the IEEE-118 bus system. Larger systems or higher-order contingencies were not analyzed given the computational efficiency issues resulting from analyzing and comparing ranking systems based on an exponentially growing data set.

5.4.1 Losses of Multiple Bus Injections

The correlation results for the closeness centrality impact factor measure and multiple bus injection impact factor are presented in table 5.1. From the case studies, the moderately strong negative correlation between the graph theory based closeness centrality measure and DC power flow based bus injection shift factors observed in the N-1 case holds consistent even for the generalized N-X case. Of particular importance is how little the correlation coefficient varied amongst the N-1, N-2, and N-3 comparisons within a specific test system. For a given test system, the difference in correlation coefficients for the N-1, N-2, and N-3 cases varied by as little as 0.009 (IEEE-30 bus system) to as much as 0.042 (IEEE-118 bus system).

Table 5.1: Closeness Centrality Impact Correlated with the N-X Multiple Bus Injection Impact Factor

Test System	N-2		N-3	
	R coeff	p-value	R coeff	p-value
IEEE-14	-0.5503	1.7916×10^{-7}	-0.5495	5.7545×10^{-24}
IEEE-30	-0.6920	3.7530×10^{-59}	-0.6831	0
IEEE-57	-0.6682	9.4216×10^{-200}	-0.6679	0
IEEE-118	-0.5981	0	-----	-----

Sample plots relating the graph theory based CCIF and DC power flow based MBIIF are provided in figure 5.2. From these plots, it is confirmed that there are no outliers leading to arbitrarily high correlation coefficients and that the two measures do, in fact, relate linearly. Since the CCIF and MBIIF are related by a moderately strong correlation coefficient and the correlation plots do not expose any errant data set issues, the evidence provided supports the utility of the CCIF measure in determining the sensitivity of a power system to N-X bus injection contingencies.

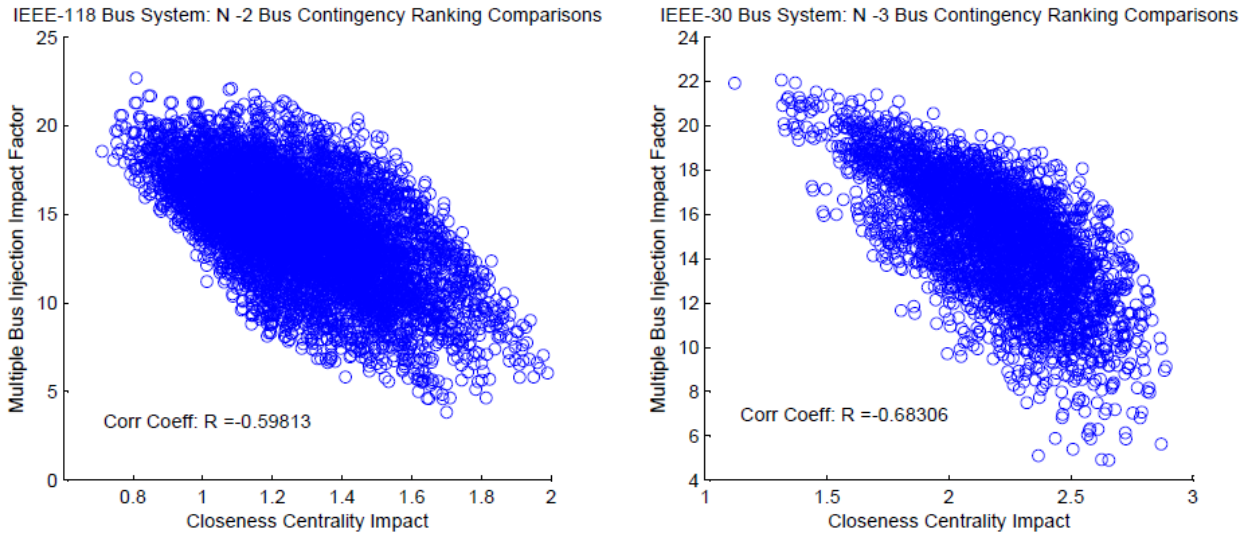

Figure 5.2: Closeness Centrality Impact Correlations with the Multiple Bus Injection Impact Factor for the N-2 Case of the IEEE-118 (Left) System and N-3 Case of the IEEE-30 (Right) System

Similar to the discussion in section 4.6, we now also perform a nonparametric Wilcoxon signed rank test on the highly ranked contingencies identified by the CCIF measure matched to the ranking of the same contingency identified by the MBIIF. However, unlike in section 4.6, the purpose of this statistical test is not to reject or fail to reject a specific null hypothesis. Rather, we are using the Wilcoxon signed

rank test to garner a statistical assessment of similarity between the graph theory and DC power flow based contingency ranking schemes. Furthermore, since N-X contingency cases produce N choose X combinations of contingencies to analyze, where N is the number of buses in the test system and X is the number of simultaneous bus injection contingencies, it is no longer appropriate to only evaluate the ranking similarity of the top 10 contingencies. Since a single branch appears in multiple contingency cases, selecting too small a sample size risks over-biasing the results to a specific high-impact bus that frequently appears in high outages contingency cases. Therefore, we select the top 5% of contingencies identified by the CCIF and compare these ranks to the corresponding MBIIF rank for the contingency. For the smaller N-2 case of the IEEE-14 bus system, the sample size is fixed at 10 to maintain a statistically relevant sample size, even though 5% of all contingency cases are actually less than 10. The Wilcoxon signed rank tests for N-2 and N-3 contingency cases are summarized in tables 5.2 and 5.3. Tables 5.2 and 5.3 are similar in format to tables 4.5 and 4.6. However, tables 5.2 and 5.3 also include information concerning the total number of test system contingency cases and the estimated median percent difference between the two compared ranking systems.

Table 5.2: Wilcoxon Signed Rank Test for Top N-2 Vulnerabilities – Closeness Centrality Impact Matched to the Multiple Bus Injection Impact Factor

Test System	Cases	Sample Size	Estimated Median	Lower Bound	Upper Bound	Achieved Confidence	Ranking % Difference
IEEE-14	78	10	15.0	1.0	30.0	94.7%	19.2%
IEEE-30	406	20	8.5	2.0	19.5	95.0%	2.1%
IEEE-57	1540	77	163	108	223	95.0%	5.0%
IEEE-118	6786	339	766	681	852	95.0%	11.3%

Table 5.3: Wilcoxon Signed Rank Test for Top N-3 Vulnerabilities – Closeness Centrality Impact Matched to the Multiple Bus Injection Impact Factor

Test System	Cases	Sample Size	Estimated Median	Lower Bound	Upper Bound	Achieved Confidence	Ranking % Difference
IEEE-14	286	14	50.0	11.5	90.0	94.8%	17.5%
IEEE-30	3654	183	111.0	78.5	154.0	95.0%	5.0%
IEEE-57	27,720	1386	1731	1570	1896	95.0%	5.0%

The principal conclusion that the statistical evidence presented in tables 4.8 and 4.9 supports is that the top 5% of contingencies identified via the CCIF appear to reflect (in the worst case) the top 20% of contingencies ranked according to the MBIIF. The two ranking systems cannot be considered statistically identical since the lower and upper bound of the median difference does not encompass the zero estimated median. However, from a statistical perspective these results provide an indication that if a cyber attacker were to examine the top 5% of bus injection contingencies produced from a CCIF vulnerability assessment, it is estimated that the list of targets at which the attacker would be looking typically reflect the top 20% of multiple bus injection contingencies to which line flows are sensitive.

5.4.2 Multiple Line Outages

Correlation results for the edge betweeness centrality impact factor and multiple line outage impact factor are presented in table 5.4. In order to simplify analysis of the results, for cases in which line outages caused an islanding situation (i.e., where one or more buses were disconnected from the rest of the power system) the case was neglected. Unlike the N-1 case, these case studies indicate an extremely weak positive correlation between the graph theory based edge betweeness centrality measure and DC power flow based line outage impact factors. This indicates that generalization of the N-1 betweeness centrality measure to the N-X case did not preserve the consistency of results. While it is possible that some other edge betweeness centrality based algorithm may yield stronger correlation with the MLOIF, since the EBCIF algorithm developed in section 4.7.2 was modeled closely after conventionally accepted MLODF algorithm procedure, the prospects of edge betweeness centrality reflecting some conventional N-X contingency screening measure are not promising.

Table 5.4: Edge Betweeness Centrality Impact Correlated with the N-X Multiple Line Outage Impact Factor

Test System	N-2		N-3	
	R coeff	p-value	R coeff	p-value
IEEE-14	0.2838	2.4163e-004	0.2685	4.6602e-015
IEEE-30	0.1817	1.9418e-006	0.1993	4.5385e-068
IEEE-57	0.0461	0.0114	0.0394	7.4171e-027
IEEE-118	0.2693	9.3170e-256	-----	-----

Despite the weak correlation coefficients, sample plots relating the graph theory based EBCIF and DC power flow based MLOIF are provided in figure 5.3. It is interesting to note that while there are quite a few errant data points obscuring a clear trend, the higher ranked EBCIF contingencies do vaguely appear to result in higher MLOIF values (hence the weakly positive correlation coefficient). While it would not be accurate to conclusively state a decisive trend, it would also not be accurate to conclude the MLOIF and EBCIF for two completely random, unrelated data sets. Therefore, a closer examination of the Wilcoxon signed rank test results is required to give an indication as to the matching between graph theory and DC power flow based line outage contingency ranking methods in agreeing upon highly ranked contingencies.

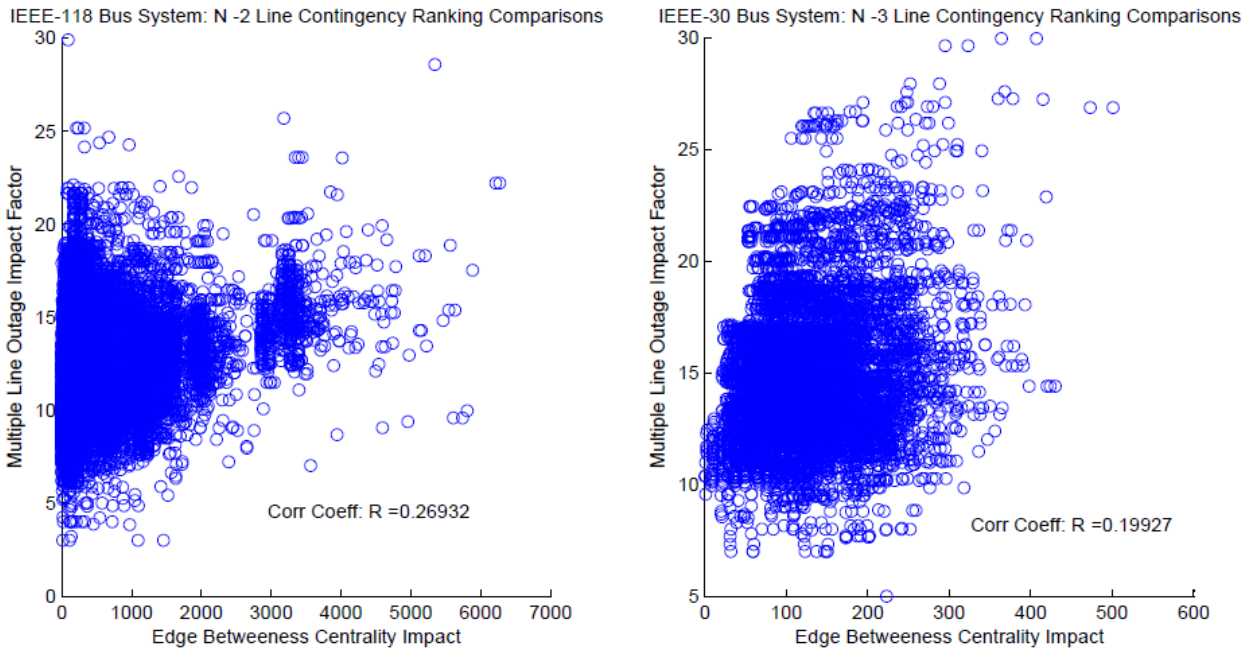

Figure 5.3: Edge Betweeness Centrality Impact Correlations with the Multiple Line Outage Impact Factor for the N-2 Case of the IEEE-118 (Left) System and N-3 Case of the IEEE-30 (Right) System

As was mentioned in section 5.4.1, the purpose of performing the nonparametric Wilcoxon signed rank test on the highly ranked contingencies identified by the EBCIF measure matched to the ranking of the same contingencies identified by the MLOIF is not to reject or fail to reject a specific null hypothesis. The degree of similarity between the graph theory and DC power flow based line outage contingency ranking measures is the focus of interest here. Wilcoxon signed rank tests for N-2 and N-3 contingency cases are summarized in tables 5.5 and 5.6.

Table 5.5: Wilcoxon Signed Rank Test for Top N-2 Vulnerabilities – Edge Betweeness Centrality Impact Matched to the Multiple Line Outage Impact Factor

Test System	Cases	Sample Size	Estimated Median	Lower Bound	Upper Bound	Achieved Confidence	Ranking % Difference
IEEE-14	163	10	50.5	22.5	85.5	94.7%	31.0%
IEEE-30	677	34	314	241	407	95.0%	46.4%
IEEE-57	3,014	151	1285	1132	1427	95.0%	42.6%
IEEE-118	15,500	775	2546	2381	2717	95.0%	16.4%

Table 5.6: Wilcoxon Signed Rank Test for Top N-3 Vulnerabilities – Edge Betweeness Centrality Impact Matched to the Multiple Line Outage Impact Factor

Test System	Cases	Sample Size	Estimated Median	Lower Bound	Upper Bound	Achieved Confidence	Ranking % Difference
IEEE-14	823	41	283	188	388	95.0%	34.4%
IEEE-30	7,504	375	2497	2238	2751	95.0%	33.3%
IEEE-57	73,930	3697	32628	31906	33342	95.0%	44.1%

Of particular interest from tables 5.5 and 5.6 is the ranking percent difference column. Here, statistical evidence is presented indicating that the top 5% of contingencies identified via the EBCIF appear to be ranked differently from those identified through the MLOIF by some estimated median difference in the range of 16% to 44%. Such results seem to provide further evidence in support of the marginal utility of the EBCIF in determining the sensitivity of changes in line flows to some N-X line outage contingency. However, in the absence of information concerning the operational state of a power

system, the marginal utility of the EBCIF may prove better than nothing when selecting targets for a coordinated cyber attack resulting in multiple line outages.

5.5 Combining Graph Theory Bus Injection and Line Outage Measures

In section 5.3, N-X contingency ranking methods based on closeness centrality and edge betweeness centrality were proposed. However, for a graph theory based contingency ranking technique to be broadly applicable, the centrality measures must be combined such that bus and branch ranking techniques can be evaluated simultaneously. In order to perform this function, we draw from the ACPF based performance index [5] defined in section 3.5, reiterated here as follows:

$$PI_{ACPF}(k) = \sum_{\substack{all\ branches \\ i}} \left(\frac{P_{flow\ l}}{P_l^{max}}\right)^{2n} + \sum_{\substack{all\ buses \\ i}} \left(\frac{\Delta|E_i|}{\Delta|E|^{max}}\right)^{2m} \tag{5.3}$$

Here, line flows and bus voltages make up the two constituent terms of the ACPF performance index. While not directly analogous, the closeness centrality impact assigns a bus ranking to a contingency based on topology rather than on changes in bus voltage. Similarly, the edge betweeness centrality measure assesses the importance of a line based on edge topology rather than on how near line flows are to an overload limit.

By relating the closeness centrality impact to the bus voltage performance index term we can examine analogous relationships of:

$$\sum_{\substack{all\ buses \\ i}} \left(\frac{\Delta|E_i|}{\Delta|E|^{max}}\right)^{2m} \rightarrow \sum_{i \in k} \left(\frac{C_C(v_i)^{-1}}{C_C^{min}}\right)^{2m} \tag{5.4}$$

Similar to how $\Delta|E|^{max}$ sets a maximum permissible voltage variation at a bus, C_C^{min} can be a design constant indicating some threshold closeness centrality value of interest for a given contingency k. Depending on the values of the design constants m and C_C^{min}, the proportionate weight assigned to a contingency bus can be altered to reflect the intent and needs specific to the circumstances required.

Also, note the closeness centrality terms are raised to a negative exponent to account for the inverse relation closeness centrality exhibited with the bus injection shift factors.

For the edge betweeness centrality impact, we can study the following analogous relation with the branch from performance index terms:

$$\sum_{\substack{all\ branches \\ i}} \left(\frac{P_{flow\ l}}{P_l^{max}}\right)^{2n} \rightarrow \sum_{c \in k} \left(\frac{C_{Be}(e_{o,c})}{C_{Be}^{max}}\right)^{2n} \tag{5.5}$$

Here, similar to how P_l^{max} reflects the power transfer capacity limit of a branch in the power system, C_{Be}^{max} is a design constant reflecting some edge betweeness threshold of interest for outaged edge $e_{o,c}$ in the set of outaged lines k. Again, to reflect the intended requirements of a user, the design constants n and C_{Be}^{max} can be tailored to affect the weights assigned to line outage cases necessary to emulate the situational conditions of interest.

Putting the closeness and edge betweeness centrality impact measures together, we now have a centrality based performance index for ranking bus injection and line outage contingencies, expressed as:

$$PI_{CENT}(k) = \sum_{c \in k} \left(\frac{C_{Be}(e_{o,c})}{C_{Be}^{max}}\right)^{2n} + \sum_{i \in k} \left(\frac{C_C(v_i)^{-1}}{C_C^{min}}\right)^{2m} \tag{5.6}$$

This centrality performance index is structurally similar to the ACPF performance index. However, since it is based on the branch and bus structural topology of a power system, the resulting ranking of line and bus injection contingencies is unlikely to reflect the ACPF performance index in all cases. Though if a topological contingency in a power system is able to cause the underlying conditions needed for the genesis of a serious operational failure, it is expected the centrality performance index will share some highly ranked contingencies with the ACPF performance index.

5.6 Comparison of Topology and Power Flow Based Performance Indices

Despite the fundamental differences between the centrality performance index presented in section 5.5 and the conventional ACPF performance index, we compare the measures for a modified

IEEE-14 bus system (see appendix A for the bus and branch data) in order to provide some basis for analyzing how a topology based performance index relates to ACPF based performance indices. Since there is not a direct mathematical derivation relating the power flow and centrality analyses, the comparisons performed in this section are statistical in nature. We are effectively attempting to validate whether or not there is evidence in support of the centrality based performance index in selecting higher ranked critical contingencies as identified through an ACPF performance index. Investigation of this issue is examined by performing statistical comparisons for an N-3 contingency analysis on a modified IEEE-14 bus system. Larger test systems were not studied since the results presented in this section will be utilized for RTDS simulations in sections 5.7 and 5.8. Given computational hardware limitations of the available test bed, larger test systems are not possible to simulate in RTDS. A modification made to the IEEE-14 bus system was setting the four PV buses to generate 55MW each in order to convert the three synchronous condensers to generators, thereby expanding potential non-swing generator targets from one to four. Additionally, the IEEE-14 bus system did not specify MVA ratings for branches, so it was assumed that all lines were at 75% capacity (rounded up to the nearest whole number) during the base case with all components in service. Since the IEEE-14 bus system is relatively small, contingency cases of order higher than the N-3 case were not studied. Simulated N-3 contingency cases involved all combinations of one generator outage and two line outages, with cases resulting in an islanding condition neglected in order to simplify the analysis. Under such conditions, 652 contingency cases on the modified IEEE-14 bus system were generated for analysis.

In order to calculate performance indices, several design constants had to be set in the performance index equations. The exponential constants were set to be $m = 1/2$ and $n = 1/2$ in order to ensure a linear comparison of index terms and preserve consistency with the analysis methodologies performed thus far. Further, setting $\Delta|E|^{max} = 0.1$ was assumed since WECC reliability standards limit post transient bus voltage variations to 10% for N-2 contingencies, and permissible threshold limits are not specified for contingencies higher than the N-2 case [6]. The P_l^{max} values from each line are just the assumed MVA capacities of each line in the IEEE-14 bus system. Design constants for the centrality

performance index were set to give equal weight to the generator outage and two line outages. Since the lowest generator centrality value occurred at bus 8, we let C_C^{min} equal the centrality value at bus 8. The value of C_{Be}^{max} was set to be the maximum edge betweeness centrality impact value for two lines taken simultaneously.

Performing ACPFs on all 652 contingency cases resulted in seven cases where the ACPF diverged. Since no power flow solution exists on a divergent case, indicating a possible voltage collapse scenario, it is standard to assign divergent power flow cases the highest ranking of all contingencies [7]. However, the lack of a power flow solution means a performance index cannot be directly calculated. In order to preserve the ranking importance of divergent power flow cases, the performance index for the seven divergent cases was set to be 10% higher than the largest performance index value for all 645 of the convergent indices. Histograms showing the distribution of ACPF and centrality performance indices are shown in figure 5.4.

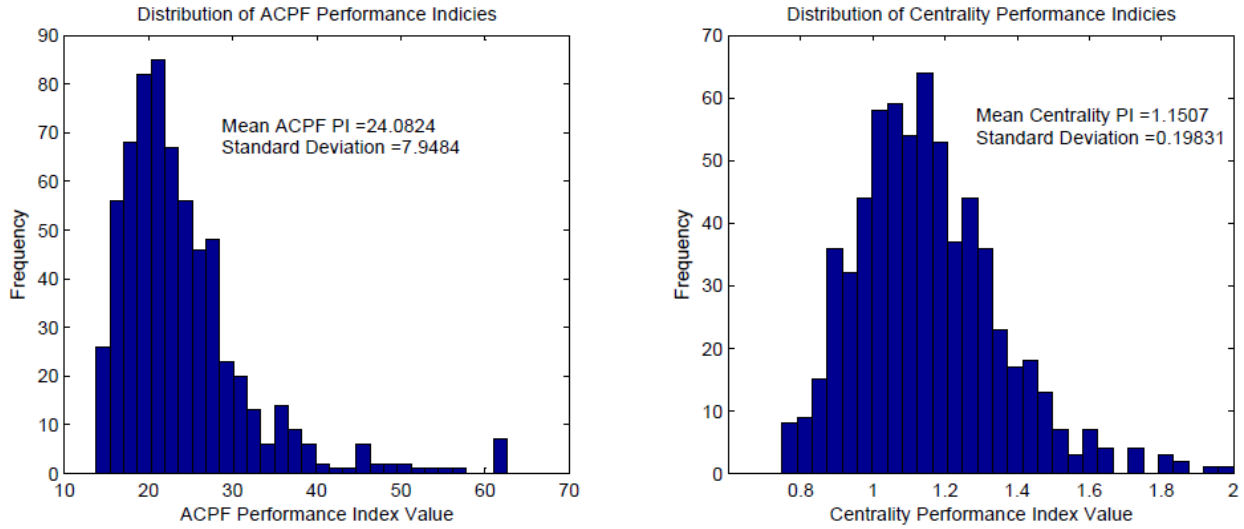

Figure 5.4: Distribution of ACPF (Left) and Centrality (Right) Performance Index Values for N-3 Contingency Cases (1 Generator Outage, 2 Line Outages) on the Modified IEEE-14 Bus System

From the histograms in figure 5.4, it is noticed that for both centrality and ACPF performance indices the distribution of performance indices is normal. Therefore, we can utilize parametric statistical

analysis techniques when relating the two performance indices [8]. In order to assess whether the top contingencies identified by the centrality performance index are actually more critical than N-3 contingencies selected at random, we test the following null hypothesis:

H0: The top 5% of contingencies identified by the centrality performance index have a mean ACPF performance index that is indistinct from the mean ACPF performance index for all N-3 contingencies studied.

As an intermediary process in determining whether or not the null hypothesis can be rejected, the top 5% of contingencies identified through the centrality performance index must be matched to the corresponding ACPF performance index. While the top 5% of contingencies totals 33 cases, the first 15 cases are presented in table 5.7 for reference to give an indication of the data sets being compared.

Table 5.7: Summary of Centrality and ACPF Performance Indices for the Modified IEEE-14 Bus System

Centrality PI Rank	ACPF PI Rank	Gen Bus Outage	Branch 1 Out	Branch 2 Out	Centrality PI	ACPF PI
1	122	8	5 – 6	7 – 9	2.00	28.36
2	340	8	5 – 6	9 – 10	1.92	21.89
3	83	3	5 – 6	7 – 9	1.87	31.31
4	114	8	4 – 7	5 – 6	1.84	28.68
5	133	2	5 – 6	7 – 9	1.82	27.84
6	245	8	5 – 6	10 – 11	1.79	24.11
7	478	3	5 – 6	9 – 10	1.79	19.26
8	610	2	5 – 6	9 – 10	1.74	16.05
9	1**	6	5 – 6	7 – 9	1.73	62.61*
10	39	8	4 – 7	6 – 11	1.71	36.88
11	206	3	4 – 7	5 – 6	1.71	25.56
12	390	3	5 – 6	10 – 11	1.67	21.01
13	327	2	4 – 7	5 – 6	1.66	22.11
14	65	8	4 – 7	10 – 11	1.66	33.00
15	1**	6	5 – 6	9 – 10	1.64	62.61*

* Power flow diverged, ACPF PI set to 10% higher than the largest convergent ACPF PI
** All cases where the power flow diverged share a #1 rank

Since the data set is suited to parametric statistical techniques, we utilize a T-test [9] to test the null hypothesis. Basically, the mean ACPF performance index is calculated for the top 5% of N-3

contingencies identified by the centrality performance index, and the mean is compared to the mean ACPF performance index of all N-3 contingencies. The T-test will give an indication on whether the two means are distinct, and provide a statistical basis for assessing the difference between means if the means are indistinct. The T-test results for the N-3 contingencies performed on the modified IEEE-14 bus system are presented in table 5.8.

Table 5.8: Statistical Comparison of Highly Ranked Centrality PI Contingencies with the ACPF PI

	Sample Size	Sample Mean	Standard Deviation	Standard Error on Mean
ACPF Performance Index for All Cases	652	24.08	7.95	0.31
ACPF Performance Index for the Top 5% of Contingencies Ranked by the Centrality Performance Index	33	30.60	13.0	2.3
Estimate for Difference Between Means	6.52			
95% Confidence Interval for Difference Between Means	1.88 to 11.16			
T-Test for Equal Means vs. Different Means	T-Value 2.86 P-Value 0.007			

From the results in table 5.8, evidence is presented in support of a conclusion to reject the null hypothesis. The threshold for concluding means to be distinct is commonly drawn for a p-value less than 0.05 [10], and since the p-value in this study was 0.007, there is a relatively high confidence that the centrality performance index identifies contingencies ranked highly by the ACPF performance index. Additionally, a rudimentary comparison of means for this scenario indicates that the top 5% of contingencies identified by the centrality performance index have approximately a 27% higher expected ACPF performance index than if contingency targets were selected random. It is also important to note that future studies will be needed to provide validation of the centrality performance index for larger systems.

5.7 RTDS Simulation of an N-3 Attack Scenario

While comparisons of the ACPF performance index and centrality performance index within MATLAB allow for a rapid screening and statistical comparison of ranking methodologies, the utility of the graph theory measures with respect to attack modeling necessitates validation within a test bed environment. Therefore, the modified IEEE-14 bus system was simulated and analyzed within a power system Real-Time Digital Simulator (RTDS) that is designed to study electromagnetic transient phenomena in real-time [11]. However, since the analytical framework of this research has focused on steady state analyses the dynamic modeling features will not be fully utilized. Rather, the chief purpose of this section is to provide some foundational basis from which a graph theory based contingency ranking measure can be applied to modeling a coordinated attack on an actual power system. It is expected that the ACPF performance index calculated from the Newton-Raphson solution is similar to the same performance index calculated directly from actual system measurements of the RTDS model at steady state. Since RTDS uses more detailed models of transmission lines, transformers, generators, and loads (in addition to real-time simulator output based on electromagnetic numerical equations), discrepancies do exist. Steady state measurements of the IEEE-14 bus system are therefore likely to match the ACPF results only roughly, not exactly. However, if the highly ranked contingencies based on the centrality performance index have similar ACPF and measured performance index quantities, we can translate an attack scenario planned from a centrality based contingency analysis to a real power system.

The pre-contingency case for the modified IEEE-14 bus system was modeled using the RSCAD software that interfaces with the RTDS hardware. The draft layout shown in figure 5.5 uses default transmission line, transformer, dynamic load, and source models with specified component characteristics as given in the bus and branch data for the modified IEEE-14 bus system. Since RTDS models can include actual hardware in the loop, the system-wide effects of compromising an actual cyber asset in the power system can be observed in a test bed environment. However, given the foundational nature of this research, actual cyber attacks were not performed on the modified IEEE-14 bus system. Performing an actual cyber attack on a power system is intended to be encompassed in future work. Only the physical

consequences of a coordinated cyber attack are simulated here by removing generator and branch components from the model, as could result from a coordinated attack plan based on the centrality performance index.

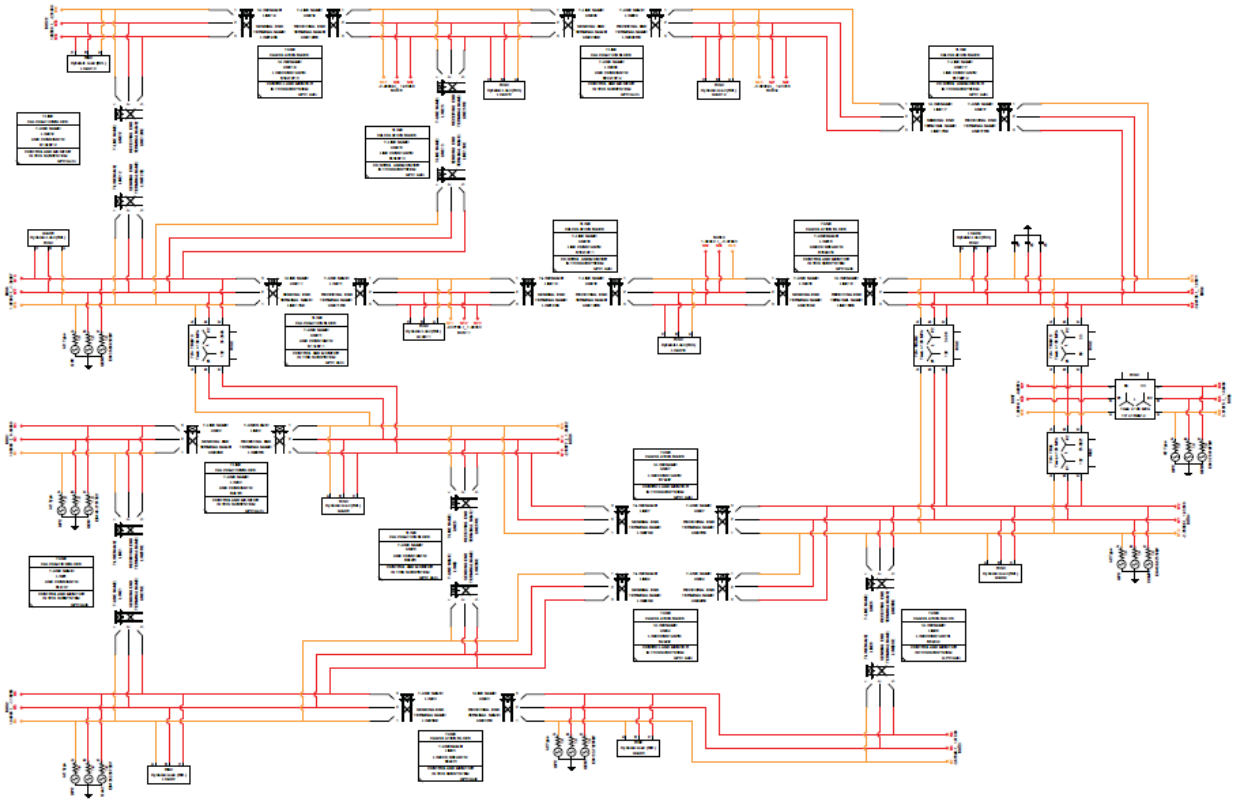

Figure 5.5: Schematic Diagram Generated in RSCAD of the Modified IEEE-14 Bus System Modeled in RTDS

For the purposes of this simulation, we assume that a cyber attacker is able to exploit some vulnerability in a power system cyber asset resulting in an N-3 contingency on the modified IEEE-14 bus system. The top five N-3 contingencies identified by the centrality performance index measure (presented in table 5.7) are carried out in RTDS, and the ACPF performance index is calculated directly from the RTDS measurements to assess the physical consequences of the cyber attack scenario. In table 5.9, RTDS measured performance index results are compared to the power flow results calculated in MATPOWER for the top five contingencies ranked by the centrality performance index. From table 5.9

we can see that the impact of an N-3 contingency modeled in the test bed is similar to what was expected from the power flow solution, as the difference between models does not exceed 7%.

Table 5.9: ACPF Performance Index Results Calculated Directly from RTDS Measurements Compared to the Corresponding Values Calculated in MATPOWER

Gen Bus Outage	Branch 1 Out	Branch 2 Out	ACPF PI (RTDS)	ACPF PI (MATPOWER)	% Difference
8	5 – 6	7 – 9	30.11	28.36	6.2%
8	5 – 6	9 – 10	23.24	21.89	6.2%
3	5 – 6	7 – 9	33.24	31.31	6.2%
8	4 – 7	5 – 6	30.02	28.68	4.7%
2	5 – 6	7 – 9	29.71	27.84	6.7%

Disparities between performance indices are likely due to fundamental differences between the Newton-Raphson power flow solution and the dynamic RTDS model. The values obtained from RTDS were obtained by measuring the power system after the transient conditions settled to some steady state condition. However, the component models in RTDS are considerably more complex than the common data format input used in a MATPOWER power flow solution. The detailed component properties taken into account in the RTDS model are approximated by a more simplistic equivalent impedance for the Newton-Raphson power flow model. However, the performance index disparities are subtle enough that we can assume attacks planned from a centrality based vulnerability assessment do, in fact, reflect the consequences observed in an actual power system. Accordingly, the statistical comparisons made throughout this research provide a basis for assessing the relative observed performance impact a coordinated attack planned by centrality measures can achieve on an actual power system.

5.8 Defensive Strategies

Given an understanding of the performance impact of highly ranked contingencies identified by centrality measures, a subsequent question is raised concerning how to prevent a coordinated attack from fully materializing. In section 2.5, conventional information security tools were discussed. Of particular note here is the concept of a signature based intrusion detection systems. Now that it is assumed that

cyber security defenses fail, we are interested in how the physical consequences of a coordinated cyber attack can be monitored to determine the likelihood of an unfolding attack. Since computation of the centrality performance index is independent of specific power system operating states, it is possible to identify in advance those branches and generators that are systemically critical to system reliability from a topology standpoint. Furthermore, by monitoring information being collected by the topology processor in a power system operations center, a centrality performance index application can rapidly determine the topological severity of additional contingencies. So if a certain contingency develops in a power system, a blocking scheme could either prevent relay operation or protection element setting changes at other locations within the power system that would appear critical in the event a contingency is the result of a cyber attack rather than some naturally occurring event.

One of the basic objectives of power system protection schemes involves that of selectivity, or ensuring relays only operate within a specified timeframe within their zones of protection [12]. Since contingencies occurring in a power system are infrequent, the likelihood of multiple contingencies occurring simultaneously in different protection zones would be rare. It would be even more unlikely for multiple systemically critical branches or generators to be removed from the power system simultaneously. As an example of how centrality performance indices may be developed to look for physical attack signatures, we examine the top ranked N-3 contingency from table 5.7 and simulate within RTDS performance index improvements resulting from preventing the full N-3 contingency from materializing. Shown in figure 5.6 is the modified IEEE-14 bus system one-line. The components included in the top ranked N-3 contingency involving the loss of branches 5-6 and 7-9 in addition to an outage of the generator on bus 8 are highlighted in red for emphasis.

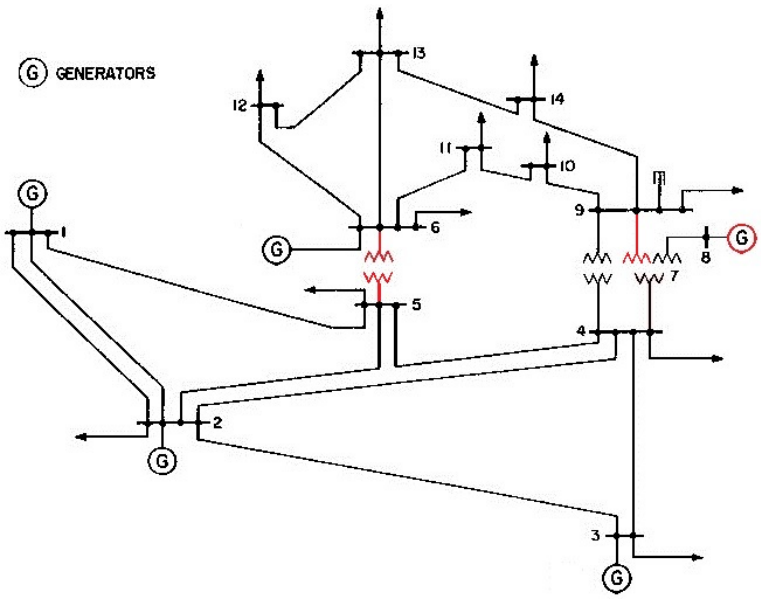

Figure 5.6: Modified IEEE-14 Bus System with Components Highlighted in Red Indicating the Highest Ranked N-3 Contingency

In figure 5.6, we can see that the bus 8 generator and the branch 7-9 are only separated by a single bus. Therefore, backup protection schemes would likely place the two components within one another's backup overreach area of protection, and we may risk preventing a legitimate protection action by blocking protection of generation on bus 8 if line 7-9 is lost. However, we would not expect contingency conditions and protection decisions involving branch 5-6 and branch 7-9 or bus 8 to be related since there are intermediary components that would be expected to have more directly associated protective relationships and contingencies only have a limited geographical effect [13]. In table 5.10 the results of the RTDS N-1 and N-2 contingencies involving generator 8 and branches 5-6 and 7-9 are shown. Results in this table show adverse impact avoided in terms of performance index savings if a blocking action taken after the N-1 or N-2 case prevents the N-3 contingency from materializing. It is important to note that a blocking action assumes the N-3 attack results in sequential outages. If all three outages occur simultaneously, the time period between outages needed for reactionary blocking would not exist.

Table 5.10: Performance Index Calculated from RTDS Measurements for Contingencies Involving Generation on Bus 8, and Branches 5-6 and 7-9

X	Gen Bus Outage	Branch 1 Out	Branch 2 Out	ACPF PI (RTDS)	% PI Difference from N-3 Case
1	8	-----	-----	24.42	-18.89%
1	-----	5 – 6	-----	16.18	-46.26%
1	-----	-----	7 – 9	27.07	-10.10%
2	8	5 – 6	-----	23.35	-22.46%
2	8	-----	7 – 9	29.31	-2.67%
2	-----	5 – 6	7 – 9	27.79	-7.71%

From table 5.4, we can see that most of the performance index impact is realized subsequent to the loss of a single component, which cannot be prevented from a physical signature security assessment without risking blocking legitimate N-1 protection actions. However, some performance improvements can still be achieved by preventing the N-3 and N-2 cases from materializing. Based on the geographical proximity argument, assessment of the physical attack signature would lead to blocking not only the N-3 contingency, but the N-2 contingencies involving generation on bus 8 and branch 5-6, as well as the case of simultaneous outages of branches 5-6 and 7-9. If an attacker targeting generation on bus 8, branch 5-6, and branch 7-9 inflicts a contingency on branch 5-6 first, the performance index of the attack could be limited to approximately 54% of the N-3 based on geographical proximity blocking. However, other scenarios permitting geographical blocking would limit the performance index savings to less than 20% depending on the sequence of attack events, with negligible savings achieved if blocking a malicious trip of branch 5-6 were to occur after attacks resulting in the outage of branch 7-9 and generation at bus 8.

While the potential for geographical proximity blocking of protection actions would require significantly more study to determine if the preventive action yields a net benefit to power system security, the purpose of this discussion is principally to highlight how centrality performance indices may be used in interdicting an unfolding cyber attack in the event information security measures fail. By modeling how an attacker may target assets for a coordinated attack and the resulting power system performance impact, we can begin to understand attack models and the benefits of potential responses. Yet if the tradeoffs associated in merging cyber security defensive measures with power system control

and protection decisions present too great a risk in reacting to false positives, centrality measures could be limited to a risk assessment index that offers operators an assessment of the degree to which a contingency situation aligns with a coordinated attack signature profile based on topological vulnerabilities.

5.9 Summary

In this chapter, novel algorithms were proposed for generalizing the closeness and edge betweeness centrality measures to cases involving N-X contingencies. Statistical comparisons with an N-X DC power flow sensitivity measure for assessing loss of bus injection indicated a close relationship with the developed closeness centrality N-X algorithm. However, the edge betweeness centrality N-X algorithm was only weakly related to the respective DC power flow based measure for assessing multiple line outages. It is therefore concluded that the proposed closeness centrality impact factor method for identifying high impact bus injection outages is the most promising topology based vulnerability assessment tool for assessing the physical vulnerability of a power system to a coordinated attack based on limited information. This chapter also proposed a unified centrality performance index, and statistical evidence was provided in support of the centrality performance index to select N-X contingencies that are expected to have a higher adverse impact compared to contingencies selected at random. However, the results also indicate limitations in the ability of centrality based indices to capture top contingencies. Furthermore, additional studies involving large system simulations and variable operating conditions are needed to more definitively ascertain the utility of the centrality performance index. In order to lay some foundational groundwork for the application of centrality performance index measures to modeling a coordinated attack on an actual power system, a modified IEEE-14 bus system was built in RTDS for use in attack scenario modeling. Using RTDS, the performance impact of highly ranked contingencies identified by the centrality performance index was confirmed using simulator measurements. Additionally, the adverse impact avoided based on performance index savings associated with blocking a coordinated cyber attack from fully materializing were studied in brief. It was then postulated that graph

theory can assist in thwarting cyber attacks by assessing changes in the topology state of a power system for physical attack signatures that have the potential for leading to a high impact contingency.

5.10 References

[1] C. M. Davis, T. J. Overbye, "Multiple Element Contingency Screening," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp.1294-1301, Aug. 2011.

[2] NERC, North American Electric Reliability Corporation. Critical Infrastructure Protection (CIP) NERC Standards CIP-002-4. Available: http://www.nerc.com/page.php?cid=2|20

[3] T. Guler, G. Gross, M. Liu, "Generalized Line Outage Distribution Factors," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp.879-881, May 2007.

[4] J. Guo, Y. Fu, Z. Li, M. Shahidehpour, "Direct Calculation of Line Outage Distribution Factors," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp.1633-1634, Aug. 2009.

[5] A. J. Wood and B. F. Wollenberg, *Power Generation Operation and Control,* ed. 2. New York, NY: Wiley, 1996, pp. 430-432.

[6] WECC, Western Electricity Coordinating Council. Reliability Standards and Criterion. Available: http://www.wecc.biz.

[7] H. Liu, A. Bose, V. Venkatasubramanian, "A Fast Voltage Security Assessment Method Using Adaptive Bounding ," *IEEE Transactions on Power Systems*, vol. 15, no. 3, pp.1137-1141, Aug 2000.

[8] R. Rumsey, *Statistics II for Dummies*. Indianapolis, IN: Wiley, 2009, pp. 275-279.

[9] R. Lyman Ott and M. Longnecker, *An Introduction to Statistical Methods and Data Analysis*, ed. 6. Belmont, CA: Brooks/Cole CENGAGE Learning, 2010, pp. 293-305.

[10] E. Kreyszig, *Advanced Engineering Mathematics*, ed. 4. New York, NY: Wiley, 1979, pp. 909-917.

[11] *Real-Time Digital Simulator Tutorial Manual*, RTDS Technologies Inc., May 2006.

[12] J. L. Blackburn and T. J. Domin, *Protective Relaying Principles and Applications*, ed. 3. CRC Press, 2007, p. 20.

[13] J. Zaborsky, K. W. Whang, K. Prasad, "Fast Contingency Evaluation Using Concentric Relaxation," *IEEE Transactions on Power Apparatus and Systems*, vol. 99, pp. 28-36, Jan. 1980.

CHAPTER SIX

CONCLUSIONS AND FUTURE WORK

6.1 Introduction

The integration of cyber assets into the modern electric grid has exposed associated control, communication, and monitoring systems to cyber threats. One of the most concerning cyber threats is the potential for a coordinated cyber attack. A study of coordinated cyber attack scenarios is important for understanding the threat to the electric power industry, so that appropriate countermeasures can be developed. This chapter summarizes the research presented in this thesis to develop an attack model of a coordinated cyber attack. Of particular interest is conceiving how an attacker in possession of limited system information could select targets to attack. In order to develop intrusion detection and response applications, potential future research activities building upon the work presented in this thesis are also suggested in this chapter.

6.2 Research Conclusions

The objective of this thesis is to contribute toward developing tools that enable identification of a coordinated cyber attack. To this end, attack models were explored to conceive of how the physical vulnerability of a power system may be assessed by attackers using readily available but limited topology information. With such an attack model, an understanding of how attackers may perform a power system vulnerability assessment is advanced. Since understanding a threat is a necessary precursor to developing defensive countermeasures, the conclusions of this research assist in enhancing power system security in the presence of the threat of a coordinated cyber attack. The following list contains the conclusions drawn by this research in support of the original thesis objectives:

1. A conceptual review of issues related to cyber security for power systems was performed, and principles of warfare were applied to power system cyber security. Through this framework, it

was concluded that cyber attackers would likely plan a cyber attack based on limited information. Graph theory was proposed as a potential tool to model coordinated attacks based on a limited information vulnerability assessment.

2. In order to establish a baseline for comparing graph theory based vulnerability assessment tools, the DC power flow based line outage impact factor and bus injection impact factor were proposed for analyzing N-1 and N-X contingencies. Additionally, the AC power flow based performance index was presented as another baseline metric for ranking the reliability impact of a contingency on an electric grid.
3. Correlation and Wilcoxon signed rank statistical tests were performed between centrality measures and DC power flow baseline metrics for N-1 contingencies. With correlation coefficients of approximately 0.6, it was concluded that the closeness centrality and edge betweeness centrality measures were the strongest candidates for ranking the sensitivity of a power system to bus injection and branch outages. No evidence was found in support of the degree, eigenvector, and vertex betweeness centrality measures as effective contingency ranking tools.
4. An N-X centrality based performance index was proposed. This centrality based performance index utilized the closeness and edge betweeness centrality measures in a comprehensive algorithm to rank multiple bus and branch outages. Simulations performed indicated the expected reliability impact (established by the AC power flow performance index) of an N-3 coordinated attack on a modified IEEE 14 bus test system was 27% higher if targets were selected amongst the top 5% of contingencies ranked by the centrality performance index than if targets were selected at random.

6.3 Specific Contributions

The following contributions towards advancing research in cyber-physical security for the electric power grid were made in this thesis:

1. A critical analysis of coordinated cyber attacks on the electric grid was advanced by framing the threat through established principles of warfare.
2. Progress concerning the suitability of graph theory based power system vulnerability assessments was made through the development of centrality tools to rank the impact of cyber attacks resulting in various N-1 and N-X physical outage scenarios.
3. The presented DC and AC power flow based contingency ranking frameworks contributed toward creation of a method to validate proposed topology vulnerability assessment tools.
4. Development of metrics to analyze vulnerability assessment results was advanced through the establishment of statistical methodologies.
5. An assessment of the benefits of early detection of a coordinated cyber attack was established with a preliminary analysis of performance impact savings achieved by possible corrective actions.

6.4 Future Work

In the future electric power grid, communication and data delivery systems will be more flexible and sophisticated to meet the needs of control centers, distributed applications, and sensors collecting increasing amounts of data [1]. A data delivery framework like GridStat will enable information from sensors throughout the power system to be published to individual applications at a specific quality of service [2]. With a flexible demand based data delivery architecture such as GridStat, a centrality based topological vulnerability analysis application requiring more data at the time of an outage is possible. In the event the information security systems of an electric grid communication system are compromised or fail, an analysis of the physical signature of coordinated cyber attacks may still allow for detection of an ongoing cyber attack. To be useful, detection of a coordinated attack signature must occur in time for

security response provisions to prevent a coordinated attack from fully succeeding. To realize such a goal, cyber security systems within a control center will be required to analyze data acquired throughout the electric grid and to look for signatures or patterns of an ongoing contingency scenario that appear unlikely to occur naturally. Since a successful cyber attack may corrupt the system state data being sent to the control system, the physical security of a power system will need to be assessed by multiple applications. A cyber attack detection system may then determine the likelihood that an emerging contingency situation is the result of a coordinated attack or the result of alternate causes. If a contingency event has a high enough likelihood of resulting from a coordinated attack, an intrusion response system can assume appropriate defensive measures. This process is shown graphically in figure 6.1 and includes a centrality based vulnerability analysis application that could fit into the security architecture of the future cyber-physical power grid.

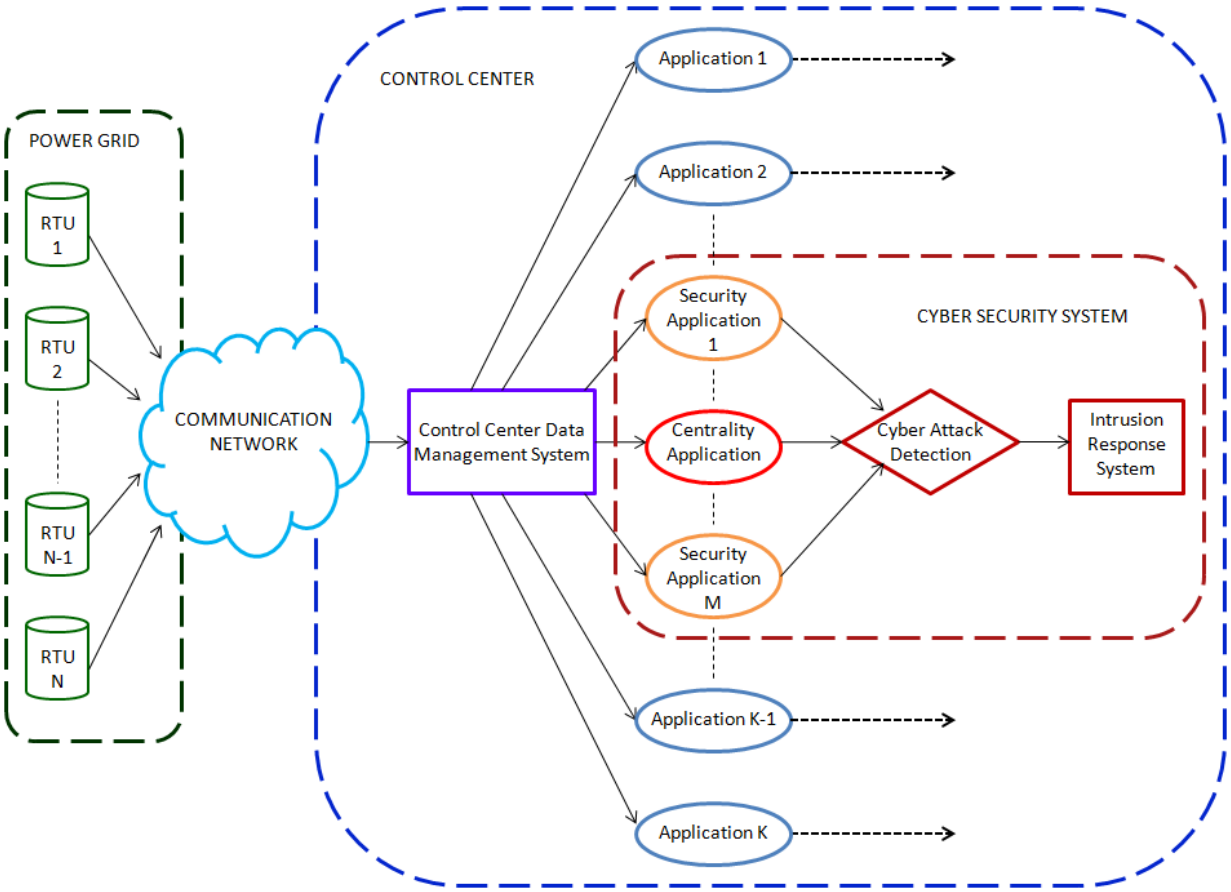

Figure 6.1: Role of Centrality Applications in Electric Grid Operations

To support such a centrality application within the security architecture of the power grid, the research performed in this thesis serves as a foundational exploration of how the power system topology data can be assessed to draw conclusions concerning power system vulnerability to bus and branch outages. Future research activities will be directed toward validating whether the statistical conclusions of the centrality based performance index can be scaled to multiple larger systems across a broad set of operating conditions. Additional modifications of the centrality performance index will likely be required to improve statistical agreement with the AC power flow based contingency ranking tool. Other topology characteristics, such as the capacity of various substations and generators, may also be incorporated into the centrality performance index to weight various bus component ranking coefficients. Alternate approaches to vulnerability analysis utilizing limited information should also be investigated for potential to yield results of greater significance. Finally, an application utilizing data published by a power system topology processor should be developed. Such an application will output a status variable indicating the topology security state of the electric grid to be utilized in higher level system security applications.

6.4 Summary

A centrality based performance index for electric power grids is developed in this thesis. Such a graph theory based performance index enables a reliability impact assessment of higher order contingencies using limited topology information. Within this chapter, conclusions and fundamental contributions of research activities performed in support of the thesis objectives are outlined. Additionally, directions of future research work needed to improve the centrality performance index are suggested. It is further proposed that research activities be taken to develop a topology security assessment application capable of integrating into a future cyber security intrusion detection and response system.

6.5 References

[1] F.F. Wu, K. Moslehi, A. Bose, “Power System Control Centers: Past, Present, and Future,” *Proceedings of the IEEE,* vol. 93, No. 11, pp. 1890-1908, Nov 2005.

[2] K. Tomsovic, D. Bakken, V. Venkatasubramanian, A. Bose, “Designing the Next Generation of Real-Time Control, Communication and Computations for Large Power Systems,” *Proceedings of the IEEE,* vol. 93, no. 5, pp. 965-979, May 2005.

APPENDIX A

MODIFIED IEEE-14 BUS SYSTEM CASE DATA

BUS DATA

Bus No.	Bus Type	Final Voltage (per unit)	Final Angle (degrees)	Load (MW)	Load (MVAR)	Gen (MW)	Gen (MVAR)	Shunt G (per unit)	Shunt B (per unit)
1	3	1.060	0.0	0.0	0.0	40.9	22.0	0.0	0.0
2	2	1.045	-0.570	21.7	12.7	55.0	2.9	0.0	0.0
3	2	1.010	-3.148	94.2	19.0	55.0	-2.6	0.0	0.0
4	0	1.032	-2.248	47.8	-3.9	0.0	0.0	0.0	0.0
5	0	1.034	-1.623	7.6	1.6	0.0	0.0	0.0	0.0
6	2	1.070	-0.903	11.2	7.5	55.0	1.1	0.0	0.0
7	0	1.064	-0.446	0.0	0.0	0.0	0.0	0.0	0.0
8	2	1.090	4.339	0.0	0.0	55.0	17.5	0.0	0.0
9	0	1.059	-2.575	29.5	16.6	0.0	0.0	0.0	0.19
10	0	1.053	-2.568	9.0	5.8	0.0	0.0	0.0	0.0
11	0	1.058	-1.876	3.5	1.8	0.0	0.0	0.0	0.0
12	0	1.056	-1.822	6.1	1.6	0.0	0.0	0.0	0.0
13	0	1.051	-1.974	13.5	5.8	0.0	0.0	0.0	0.0
14	0	1.037	-3.313	14.9	5.0	0.0	0.0	0.0	0.0

BRANCH DATA

From Bus	To Bus	Resistance (per unit)	Reactance (per unit)	Line Charging B (per unit)	Line Rating (MVA)	Transformer Turns Ratio
1	2	0.01938	0.05917	0.0528	40	0.0
1	5	0.05403	0.22304	0.0492	23	0.0
2	3	0.04699	0.19797	0.0438	39	0.0
2	4	0.05811	0.17632	0.034	25	0.0
2	5	0.05695	0.17388	0.0346	17	0.0
3	4	0.06701	0.17103	0.0128	21	0.0
4	5	0.01335	0.04211	0.0	36	0.0
4	7	0.0	0.20912	0.0	24	0.978
4	9	0.0	0.55618	0.0	3	0.969
5	6	0.0	0.25202	0.0	25	0.932
6	11	0.09498	0.1989	0.0	15	0.0
6	12	0.12291	0.25581	0.0	12	0.0
6	13	0.06615	0.13027	0.0	28	0.0
7	8	0.0	0.17615	0.0	76	0.0
7	9	0.0	0.11001	0.0	52	0.0
9	10	0.03181	0.0845	0.0	9	0.0
9	14	0.12711	0.27038	0.0	13	0.0
10	11	0.08205	0.19207	0.0	10	0.0
12	13	0.22092	0.19988	0.0	3	0.0
13	14	0.17093	0.34802	0.0	11	0.0

APPENDIX B

LIST OF SOFTWARE APPLICATIONS USED

The following list serves to provide record of the software applications used for specific purposes throughout the course of this research:

1. MATLAB, version R2010a, developed by The MathWorks. Served as the primary programming environment from which graph theory and power flow contingency analysis code was written. The MATPOWER and MATLAB_BGL open source m-file libraries were used extensively within the code written to execute the simulations described within this thesis.
2. RSCAD, version 2.0.23, developed by RTDS Technologies. Use described in detail in sections 5.7 and 5.8. Was used to generate data for performance index calculations under simulated outages in the modified IEEE-14 bus system.
3. PSSE, version 32.0.5, developed by Siemens Energy Inc. Software was utilized to validate code written in MATLAB to determine branch flows and bus voltages resulting from various N-X contingencies.
4. Minitab, version 16.1.1, developed by Minitab Inc. Minitab was the primary statistical analysis software utilized to perform Wilcoxon signed rank tests and T-test on data sets.