VULNERABILITY ASSESSMENT AND RESILIENCE ENHANCEMENT OF CRITICAL INFRASTRUCTURE NETWORKS

VULNERABILITY ASSESSMENT AND RESILIENCE ENHANCEMENT OF CRITICAL INFRASTRUCTURE NETWORKS

By

Mohamed Gamal Aboelkasem Salama

BSc., M.Sc.

A Thesis Submitted to the School of Graduate Studies in Partial Fulfillment of the Requirements for the Degree

Doctor of Philosophy

Doctor of Philosophy (2022) (Civil Engineering)	McMaster University Hamilton, Ontario
TITLE:	Vulnerability Assessment and Resilience Enhancement of Critical Infrastructure Networks
AUTHOR:	Mohamed Gamal Aboelkasem Salama BSc., MSc. (Cairo University)
SUPERVISORS:	Dr. Wael El-Dakhakhni Dr. Michael Tait
NUMBER OF PAGES:	xxiv, 214

Dedications

To

My Father & Mother,

My Wife: Aliaa, My siblings: Esraa, Ahmed & Fatma

Abstract

Modern societies are fully dependent on critical infrastructures networks to support the economy, security, and prosperity. Energy infrastructure network is of paramount importance to our societies. As a pillar of the economy, it is necessary that energy infrastructure networks continue to operate safely and be resilient to provide reliable power to other critical infrastructure networks. Nonetheless, frequent large-scale blackouts in recent years have highlighted the vulnerability in the power grids, where disruptions can trigger cascading failures causing a catastrophic regional-level blackout. Such catastrophic blackouts call for a systemic risk assessment approach whereby the entire network/system is assessed against such failures considering the dynamic power flow within. However, the lack of detailed data combining both topological and functional information, and the computational resources typically required for large-scale modelling, considering also operational corrective actions, have impeded large-scale resilience studies.

In this respect, the research in the present dissertation focuses on investigating, analyzing, and evaluating the vulnerability of power grid infrastructure networks in an effort to enhance their resilience. Through a Complex Network Theory (CNT) lens, the power grid robustness has been evaluated against random and targeted attacks through evaluating a family of centrality measures. The results shows that CNT models provide a quick and potential indication to identify key network components, which support regulators and operators in making informed decisions to maintain and upgrade the network, constrained by the tolerable risk and allocated financial resources.

Furthermore, a dynamic Cascade Failure Model (CFM) has been employed to develop a Physical Flow-Based Model (PFBM). The CFM considers the operational corrective actions in case of failure to rebalance the supply and demand (i.e., dispatch and load shedding). The CFM was subsequently utilized to construct a grid vulnerability map function of the Link Vulnerability Index (LVI), which can

be used to rank the line maintenance priority. In addition, a Node Importance Index (NII) has been developed for power substations ranking according to the resulting cascade failure size. The results from CNT and CFM approaches were compared to address the impact of considering the physical behavior of the power grid. The comparison results indicate that relying solely on CNT topology-based model could result in erroneous conclusions pertaining to the grid behavior. Moving forward, a systemic risk mitigation strategy based on the Intentional Controlled Islanding (ICI) approach has been introduced to suppress the failure propagation. The proposed mitigation strategy integrated the operation- with structure-guided strategies has shown excellent capabilities in terms of enhancing the network robustness and minimizing the possibility of catastrophic large-scale blackouts. This research demonstrates the model application on a real large-scale network with data ranging from low to high voltage. In the future, the CFM model can be integrated with other critical infrastructure network systems to establish a network-of-networks interaction model for assessing the systemic risk throughout and between multiple network layers. Understanding the interdependence between different networks will provide stakeholders with insight on enhancing resilience and support policymakers in making informed decisions pertaining to the tolerable systemic risk level to take reliable actions under abnormal conditions.

Acknowledgement

I would like to express my sincere appreciation to Dr. Wael El-Dakhakhni, Dr. Michael Tait, Dr. Chi Tang, Dr. Zoe Li, Dr. Mohamed Ezzeldin, and Dr. Ahmed Siam for their continuous help and guidance throughout my study. A very special thanks to Dr. El-Dakhakhni for his continuous support and encouragement through my research.

I would like to thank the Canadian Nuclear Energy Infrastructure Resilience under Systemic Risk (CaNRisk) – Collaborative Research and Training Experience (CREATE) program of the Natural Science and Engineering Research Council (NSERC) of Canada, INTERFACE Institute, and the INViSiONLab of McMaster University for the financial support of the research.

Many thanks are due to my brothers, before being friends, in McMaster: Yassien Salaheldin, Mohamed Elsefy, Mahmoud Madany, Mohamed Elganzory, Ahmed Yassin, Ahmed Yosri, Ahmed El-Sayed, and Maysara Ghaith.

I am thankful to my colleagues, in Bruce Power, Tetra Tech, and Next Structural Integrity: Fouad Kelada, Waleed Mekky, Ahmed Ashour, Nader Aly, Revi Kizhatil, Mohammed Albutainy, Mohamed Hamda, Mohamed Saifelislam, Mostafa Siam, Taher Abu Seer, and Mohamed Elmorsy.

I also owe special gratitude to my family: Gamal Salama, Nadia Ibrahim, Esraa Salama, Ahmed Salama, Fatma Salama, Atyat Rashad, Kamal Hamam, Sabreen Ahmed, Wael Abdelhamid, Noray Wael, Oday Wael, Retaj Ahmed, Alaaeldin Hamam, Retaj Hamam, and Amr Hamam. They have always been generous with their love and encouragement despite the long distance between us. I am forever indebted to my parents for giving me the opportunities and experiences that have made me who I am. They selflessly encouraged me to explore new

directions in life and to shape my destiny. This journey would not have been possible if not for them, and I dedicate this milestone to them.

Finally, I can find no words to express my sincere gratitude to my lovely and wonderful wife: Aliaa Hamam for her unparalleled love and unconditional support. I am utterly grateful to her for always being there for me.

Acronym List

AC	Alternating Current
CIN	Critical Infrastructure Networks
CNT	Complex Network Theory
CFM	Cascade Failure Model
CSC	Constrained Spectral Clustering
CaNRisk	Canadian Nuclear Energy Infrastructure Resilience under Systemic Risk
CREATE	Collaborative Research and Training Experience
DC	Direct Current
LVI	Link Vulnerability Index
ICI	Intentional Controlled Islanding
IESO	Independent Electricity System Operator
NII	Node Importance Index
NIAC	National Infrastructure Advisory Council
NERC	North American Electric Reliability Corporation
NSERC	Natural Science and Engineering Research Council
PSSE	Power System Simulator for Engineering software
PFBM	Physical Flow-Based Model

Table of Contents

List of Figures

List of Tables

Declaration of Academic Achievement

This dissertation was prepared following the guidelines set by the school of graduate studies at McMaster University for the sandwich thesis format. This dissertation presents the work carried out solely by Mohamed Salama, where technical advice and guidance were provided for the whole thesis by Drs. Wael El-Dakhakhni, Michael Tait, Chi Tang, Zoe Li, and Mohamed Ezzeldin. Four papers were prepared in this dissertation and presented in chapters 2, 3, 4, and 5. The research paper presented in Chapters 2 and 3 are two journal articles already published in the *Journal of Sustainable and Resilient Infrastructure*, whereas Chapters 4, and 5 have been submitted for publication also as journal articles. The original contributions of the author to each paper (Chapter) in this dissertation are outlined below:

Chapter 2: Mohamed Salama, Mohamed Ezzeldin, Wael El-Dakhakhni, and Michael Tait. 2020 "**Temporal Networks: A Review and Opportunities for Infrastructure Simulation**" Journal of Sustainable and Resilient Infrastructure, https://doi.org/10.1080/23789689.2019.1708175.

Mohamed Salama planned the article, conducted the literature review and prepared the manuscript. The manuscript was further conceptualized, reviewed and edited by Drs. Mohamed Ezzeldin, Wael El-Dakhakhni, and Michael Tait.

Chapter 3: Mohamed Salama, Wael El-Dakhakhni, and Michael Tait. 2021 "**Mixed Strategy for Resilience Enhancement of Power Grid under**

Cyberattack" Journal of Sustainable and Resilient Infrastructure, https://doi.org/10.1080/23789689.2021.1974675.

Mohamed Salama envisioned the study and developed a complex network model to simulate the power grid to identify and rank key network components. The manuscript was further conceptualized, reviewed and edited by Drs. Wael El-Dakhakhni and Michael Tait.

Chapter 4: Mohamed Salama, Wael El Dakhakhni, Michael Tait, and Chi Tang. 2022 "**Dynamic Network Flow Model for Power Grid Systemic Risk Assessment and Resilience Enhancement**" Forthcoming, Journal of Infrastructure Systems, https://doi.org/10.1061/(ASCE)IS.1943-555X.0000677.

Mohamed Salama developed the dynamic complex network theoretic-physical power flow model described in this article and prepared the manuscript. The manuscript was further conceptualized, reviewed and edited by Drs. Wael El Dakhakhni, Michael Tait, and Chi Tang.

Chapter 5: Mohamed Salama, Wael El Dakhakhni, and Michael Tait. "**Intentional Controlled Islanding and Flow Rebalance for Power Grid Systemic Risk Mitigation**" Submitted to the Journal of Energy Engineering in January 2022.

Mohamed Salama developed a systemic risk mitigation strategy based on intentional controlled islanding by applying constrained spectral algorithm in the cascade failure model. Mohamed Salama prepared the manuscript that was further conceptualized, reviewed and edited by Drs. Wael El Dakhakhni and Michael Tait.

Chapter 1 : INTRODUCTION

1.1. BACKGROUND AND MOTIVATION

Virtually all pivotal economic and societal functions rely on the secure, resilient, and reliable operation of energy, water, transportation, communication, and other critical infrastructure networks (CINs) (Rome et al. 2014). These critical infrastructure networks are necessary for public safety and the people's well-being. However, with expanded benefits came expanded risks. This is because such CINs are not isolated but interdependent in different ways. Although these interdependencies enhance the overall *network-of-networks* efficiencies, interdependences also increase CIN vulnerabilities, where a disruption in one network can propagate from a local (intra-dependence) to a global (inter-dependence) scale, leading to large scale cascading failures. As a result, simulating infrastructure networks has attracted the interest of researchers from different domains to enhance the latter's performance through comprehensive decision support systems. In particular, energy infrastructure networks are at the forefront of CINs for modern societies (Panteli and Mancarella 2017) as the ramifications of energy infrastructure network failure extend to the communication, transportation, water, banking and finance, and other CINs that have become increasingly dependent on power grids to energize and control their operations (Amin 2001). In this respect, power grids are one of the most critical, challenging, and interesting complex networks to study (Gasser et al. 2019).

The occurrence of several worldwide catastrophic events, such as the 2003 North American outage, 2004 Atlantic hurricane season, 2011 Japan earthquakes, and 2012 hurricane Sandy events have directed the spotlight on the vulnerability of CINs (Ouyang 2014). Notably, power grids are exposed to damage from numerous weather/ climate events. For example, extreme weather events have wreaked havoc on the distribution and transmission lines across Canada's coasts (Lemmen 2016). power transfer and transmission infrastructure components extend for thousands of kilometers and making them vulnerable to a multitude of natural hazards, such as lightning strikes, avalanches, storm surge, and hurricanes. In addition to climate-induced hazards, the ageing of power grid components coupled with increased energy demands exacerbate the risk of failure and poses a severe threat to grid operations. Furthermore, anthropogenic hazard (e.g., cyber-attacks) presents additional challenges and thus necessitates the need to investigate, analyze, and evaluate the vulnerability of these networks to enhance their resilience.

Although power grids are intended to be robust, previous events have shown that a disruption in key network components may lead to overload on other components and thus a possible initiation of a chain of cascading failures, which propagate throughout the network causing catastrophic system-level cascade failure—*systemic risks* (Ezzeldin and El-Dakhakhni 2019). The most recent example of such failures is the 2021 Pakistan blackout that plunged all of Pakistan's major cities into darkness, including the capital, and affected about 200 million people (90% of the country's population). Another example is the Northeast

blackout in 2003, which started with a local failure that propagated to most of the power grid and affected approximately 55 million people in Ontario and eight U.S. states (Andersson et al. 2005). In addition to the above examples, there are numerous other major blackout examples worldwide that have affected millions of people, including those in Indonesia 2019 (120 million), Argentina 2019 (48 million), Venezuela 2019 (30 million), Pakistan 2015 (140 million), Bangladesh 2014 (150 million), India 2010 (120 million), Brazil 2009 (60 million), Indonesia 2005 (100 million), and Italy 2003 (56 million) (Schäfer and Yalcin 2019).

Consequently, understanding the nature of power grid systemic risks supports decision-makers in making better choices regarding the degree of risk and financial resources. Identifying the critical power grid components is particularly crucial to evaluate network robustness and subsequently enhance the grid resilience against random and targeted/cyberattacks. Traditionally, Complex Network Theory (CNT) has been used to construct a topology-based model for simulating infrastructure networks based solely on their topological and connectivity properties. Such models disregard flows and physical properties of/within the network, and instead represent the underlying network in an abstract manner, as a set of nodes and links (i.e., *static*). Although abstract in nature, such topology-based models can nonetheless provide indications of network behavior and vulnerability, albeit while lacking the ability to draw a complete picture of the real infrastructure behavior since all infrastructure networks are governed by the laws of physics and are subjected to constraints pertaining to demand and supply (Hines et al. 2010a;

Salama et al. 2021). As such, a *dynamic* cascade failure physical flow-based model is preferable to consider actual power flow, component capacities, as well as dynamic power flow redistribution. Furthermore, to maintain the acceptable level of electricity that is necessary for basic safety during crises, there is a critical need to provide effective mitigation strategies to suppress the failure propagation and reduce the network failure, thus enhance grid resilience by reducing the restoration time.

1.2. RESILIENCE OF ENERGY INFRASTRUCTURE NETWORK

The concept of resilience emerged possibly for the first time from materials science in the early nineteenth century, while the word itself comes from Latin word *resilire*, which means bounce back (Alexander 2013). Several studies have attempted to define energy infrastructure network resilience (Panteli and Mancarella 2017). The National Infrastructure Advisory Council, USA (Berkeley III et al. 2010), provide the following definition for resilience: "*Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event*". Therefore, energy infrastructure network resilience can be assessed based on four main attributes: *Resist*, *Restabilize*, *Rebuilt*, and *Reconfigure* (Ezzeldin and El-Dakhakhni 2019; Gasser et al. 2019). These latter attributes form the core of resilience engineering that focuses on "draw-down" and "draw-up"

behaviours (Heinimann and Hatfield 2017). The resist and re-stabilize attributes represent the "draw-down" phase, which focus on the network ability to handle a disruptive event. The "draw-down" phases can be evaluated by vulnerability analysis and modelling of failure propagation to quantify the network robustness. The recovery behaviours in the "draw-up" phase represent both the rebuilt and reconfigure resilience attributes. Therefore, the smaller performance loss "draw-down" and the faster the bounce back "draw-up" of the network after a disruptive event, the higher its resilience is (Gasser et al. 2019). The main resilience attributes can be further explained as:

- Resist (*robustness*): The ability to withstand and keep operating in the face of (or the insensitivity to) disruptive events. Robustness requires redundancy or substitute systems that can replace the damaged or non-functioning component.
- Re-stabilize (*resourcefulness*): The capacity to provide enough resources to adsorb and effectively manage damage to ensure critical system functionality survives. Resourcefulness includes identifying options and priority as to what should be implemented to control and mitigate damage.
- Rebuild (*recovery*): The ability to restore the system back to its normal operation condition rapidly. It includes contingency plans, emergency operations, and getting the right resources and people to the right places.
- Reconfigure (*adaptability*): The ability to learn and apply new lessons from catastrophes by modifying plans, revising procedures, and developing and deploying new technologies to improve robustness, resourcefulness, and recovery abilities in the face of future anticipated disruptions.

1.3. METHODS AND APPROACHES

The current research focuses on the "draw-down" phase of power grid infrastructure to enhance network resilience by increasing its ability to withstand disruptive events (i.e., robustness). First, CNT topological network characteristics, network metrics, and several centrality measures are reviewed. After describing different classes of infrastructure network-based models, the infrastructure network simulation opportunities based on network models are discussed. It is concluded that using CNT models present a promising framework to simulate and reveal CIN characteristics, evaluate their interdependence, quantify their resilience, and mitigate their systemic risks. In addition, findings indicate that energy infrastructure networks are at the leading of critical infrastructure networks as the operations of most other CINs such as water, communication, transportation, finance, and other CINs depend on an adequate and reliable power supply. Therefore, providing a resilient power grid supports modern societies by reducing the potential consequences to other CINs.

Secondly, the CNT topology centrality measures have been integrated with the grid operating conditions (i.e., power flow) to recognize the relative importance of network components. The considered grid robustness to random and targeted attack scenarios based on the centrality measures are evaluated. By knowing these critical components, a mixed strategy that aims to systematically isolate the critical system components from attacks can be implemented. As such, an improvement in

network robustness by applying the proposed mixed strategy to limit attacks is identified. Afterwards, it is recommended to incorporate physics governing the behavior of the considered network to yield high-fidelity models.

Thirdly, the dynamic Cascade Failure Model (CFM) is developed through adopting a Direct Current (DC) power flow model to establish a Physical Flow-Based Model (PFBM) to evaluate the network performance in case of contingencies. The CFM considers the actual power flow, transmission line electrical properties, and generator supply and capacity limits. This model has been used to calculate two vulnerability indices, the Link Vulnerability Index (LVI) and the Node Importance Index (NII). As such, the LVI is used to construct a transmission line vulnerability map of the power grid. Furthermore, the NII is used to present the consequences of (sub)station failure in the whole network behavior, NII outputs are compared to classic topology measures of network centrality to address the adequacy of using CNT solely in identifying the critical network components.

Finally, a risk mitigation strategy to improve network robustness by suppressing the cascade failures and reducing the vulnerability is proposed. By integrating operation- and structure-guided strategies, the work focuses on mitigating the risk of such cascade failure (i.e., systemic-risk) to minimize the possibility of catastrophic large-scale blackouts. The operation-guided strategy was implemented through dispatch and load shedding to rebalance demand and supply after disruptive events. On the other hand, the structure-guided strategy adopted an

Intentional Controlled Islanding (ICI) approach by employing a Constrained Spectral Clustering (CSC) algorithm. Overall, the research helps to better understand the vulnerability of power grids and highlights the criticality of different network components, which provides some clues toward constructing a more resilient power grid.

The following subsections present a brief introduction pertaining to the main used approaches.

1.3.1. COMPLEX NETWORK THEORY

Recent advances in complex network theory have provided powerful tools to simulate several complex networks, from the world wide web to biological and infrastructure networks. In addition, the significant development in CNT measures (Barabási and Pósfai 2016; Newman 2010b) has led to the ability to model more complex and diverse sets of networks. Within the context of CNT, the core components of any network are its corresponding nodes and links (Newman 2010b). More specifically, the nodes simulate the main elements comprising the network (i.e., substations in power grids), while the links represent the interdependency between these nodes within the same network (i.e., transmission lines in power grids). This simulation facilitates a better understanding of the interdependency between the nodes comprising the network. Subsequently, the analysis of this network does not only demonstrate its topological characteristics, but also identifies its most influential nodes and links (Barabási and Pósfai 2016;

Tang et al. 2010b). In addition, more complex characteristics, such as network resilience, can be evaluated by subjecting the network to progressive damage (Motter and Lai 2002; Wang and Rong 2009, 2011). Moreover, systemic risk, optimization, and multiple other processes related to complex networks depend on the network topology/structure (Motter 2004; Stergiopoulos et al. 2015; Wang 2013a, 2013b). Therefore, utilizing complex network analysis to model the power grids will provide fundamental insight into these networks, reveal their critical points and help developing effective risk mitigation strategies to suppress the cascading failures and reduce the vulnerability of such networks.

1.3.2. CASCADE FAILURE MODEL

Unlike CNT models based solely on topology, high-fidelity cascade failure models of power grid should take into consideration the real power flow, the transmission lines electrical properties, and the generation actual supply and capacity limits (Ouyang 2014; Pagani and Aiello 2013b). Despite the recent advance in conceptual modelling of cascade failure propagation (Ju 2018; Li et al. 2018; Yan et al. 2015; Zhao et al. 2018), a major obstacle still remains due to the lack of high-resolution data, which is typically restricted for security reasons. In the absence of such data, it is very unlikely a realistic network vulnerability analysis can be provided to ensure the reliability and resilience of power grids. Such cascade failure physical flow-based models usually require significant computational time and more data to simulate the functionality of network components, compared to their topology-

based model counterparts. In particular, infrastructure network resilience analysis based on CFM is more realistic when considering physical flow within such complex networks (i.e., PFBM). In this respect, the current research has been extended to simulate the cascade failure propagation based on dynamic CFM, which considers actual power flow, demand, supply, components capacities, and power flow redistribution. Furthermore, the results for the CFM have been compared with the previous results from CNT models to indicate to what extent the CNT models can be used to assess power grid vulnerability.

1.3.3. INTENTIONAL CONTROLLED ISLANDING

ICI is a corrective control action for a grid under a severe contingency (i.e., loss/failure of power grid components, such as transmission lines, generators, or transformers) to prevent the cascade failure propagation. ICI essentially splits the grid into several isolated sub-grids. This technique is key following instabilities as it can supress the grid from becoming uncontrollable (Ding et al. 2018). In this respect, the CSC algorithm has been employed as a mitigation strategy based on ICI approach for the power grid to determine a set of transmission lines to be disconnected across the network to create stable functioning sub-grids (islands). A high-fidelity CFM of the power grid that was previously developed has been used to evaluate the effectiveness of the proposed mitigation strategy through the cascade failure model on a realistic large-scale network.

1.4. RESEARCH OBJECTIVES

This research aims at utilizing the latest developments in complex network theory and physical flow-based modeling approaches to simulate CINs, especially, the power grid infrastructure networks. The research objectives can be summarized in the following:

- Review the advances in CNT, with a focus on network-based models and approaches of CINs.
- Model the power grid based on CNT. This model takes advantage of the complex network centralities measures to provide the fundamental insight into the networks including revealing its vulnerabilities and key components. By knowing these critical components, a mixed strategy approach can be implemented to improve network robustness against cyberattacks.
- Model the cascade failure propagation in power grid by using a dynamic CFM through physical flow-based network model. The dynamic CFM is subsequently used to evaluate the performance in case of contingencies by providing two vulnerability indices, namely the link vulnerability index, and the node importance index.
- Introduce an effective systemic risk mitigation strategy to suppress the cascade failures, enhance the robustness, and reduce the vulnerability in a power grid.

This research will also open the gate for further investigations under the theme of *Intelligent Energy Systems* within the Department of Civil Engineering at McMaster University.

1.5. THESIS ORGANIZATION

This section summarizes the content of each of the six chapters in this dissertation.

Chapter 1 provides research background, concepts pertaining to the resilience of energy infrastructure, an overview of CNT, CFM, ICI, research objectives, and a description of the thesis organization.

Chapter 2 provides a review of complex network theory characteristics and modelling approaches. Specifically, fundamental network topological characteristics (i.e., reachability, length, distance) are presented. In addition, the chapter reviews the different centrality measures (i.e., degree, closeness, betweenness) that can be utilized to identify the most critical nodes and links in a networks. Furthermore, different graphical representation techniques of networks are summarized. This chapter describes different classes of infrastructure network-based models, which can be classified into three groups: topology-based-, flow-based-, and physics-based models. Moreover, opportunities and applications in transportation, power, and water infrastructure networks simulations are presented.

Chapter 3 focuses on the "draw-down" phase of power grid resilience considering different centrality measures to evaluate the robustness of power grids against cyberattacks. At the network-level, this chapter considers two network

representations for the grid based on the network's topological/connectivity (i.e., unweighted network) and the network's power flow information (i.e., weighted network). At the nodal-level, various centrality measures are considered to identify and rank key network components. This chapter includes modeling large power grids by integrating both their topology and their operating (i.e., power flow) conditions to identify the relative importance of network components and evaluate their impact on network robustness. Next, the considered grid robustness is evaluated to random and targeted cyberattack scenarios based on the centrality measures. Subsequently, by knowing these critical components, implementing the proposed mixed strategy that aims to isolate critical system components from cyberattack impacts.

Chapter 4 assesses the power grid vulnerability and robustness through simulating cascade failure propagations using a dynamic CFM. The CFM model adopts a DC power flow model to redistribute power through network after disruptions by considering the real network component properties. As such, the proposed CFM is a physical flow-based model that simulates the cascade failure under different initial failure scenarios and evaluates the network robustness based on its topological and functional characteristics. This chapter develops and demonstrates the utility of a LVI for constructing power transmission line vulnerability maps; as well as a NII for power (sub)stations ranking according to the resulting cascade failure size. Furthermore, the results of NII from the cascade failure model are compared to those of the CNT model discussed in **Chapter 3.**

Chapter 5 focuses on mitigating the risk of such cascade failure to minimize the possibility of catastrophic large-scale blackouts by integrating operation- with structure-guided strategies. The operation-guided strategy is implemented through dispatch and load shedding, while the structure-guided strategy adopts a ICI approach by employing a CSC algorithm. To evaluate the effectiveness of the proposed mitigation strategy, a real power scale grid was modelled under different cascade failure scenarios to compare the cascade failure size with and without the proposed algorithm for different sub-grid numbers.

Chapter 6 provides a reflective summary of the research, draws out the overall implications of the research and key findings, and offers dynamic recommendations for the possibility of future work.

1.6. REFERENCES

Alexander, D. E. 2013. "Resilience and disaster risk reduction: an etymological journey." Natural hazards and earth system sciences, 13(11): 2707–2716.

Amin, M. 2001. "Toward self-healing energy infrastructure systems." IEEE Computer Applications in Power, 14(1): 20–28.

Andersson, G., P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal. 2005. "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance." IEEE Trans. Power Syst., 20(4):

1922–1928. https://doi.org/10.1109/TPWRS.2005.857942.

Barabási, A.-L., and M. Pósfai. 2016. Network science, Cambridge United Kingdom: Cambridge University Press.

Berkeley III, A. R., W. Mike, and C. Constellation. 2010. "A framework for establishing critical infrastructure resilience goals.", Final Report and Recommendations by the Council, National Infrastructure Advisory Council.

Ding, L., Y. Guo, P. Wall, K. Sun, and V. Terzija. 2018. "Identifying the Timing of Controlled Islanding Using a Controlling UEP Based Method." IEEE Trans. Power Syst., 33(6): 5913–5922. https://doi.org/10.1109/TPWRS.2018.2842709.

Ezzeldin, M., and W. E. El-Dakhakhni. 2019. "Robustness of Ontario power network under systemic risks." Sustainable and Resilient Infrastructure: 1–20. https://doi.org/10.1080/23789689.2019.1666340.

Gasser, P., P. Lustenberger, M. Cinelli, W. Kim, M. Spada, P. Burgherr, S. Hirschberg, B. Stojadinovic, and T. Y. Sun. 2019. "A review on resilience assessment of energy systems." Sustainable and Resilient Infrastructure: 1–27. https://doi.org/10.1080/23789689.2019.1610600.

Heinimann, H. R., and K. Hatfield. 2017. "Infrastructure resilience assessment, management and governance–state and perspectives." In Resilience and risk: 147–187: Springer.

Hines, P., E. Cotilla-Sanchez, and S. Blumsack. 2010. "Do topological models provide good information about electricity infrastructure vulnerability?" Chaos: An Interdisciplinary Journal of Nonlinear Science, 20(3): 33122.

Ju, W. 2018. "Modeling, Simulation, and Analysis of Cascading Outages in Power Systems.".

Lemmen, D. S. 2016. Canada's marine coasts in a changing climate, [Ottawa, Ontario]: Natural Resources Canada.

Li, J., C. Shi, C. Chen, and L. Dueñas-Osorio. 2018. "A cascading failure model based on AC optimal power flow: Case study." Physica A: Statistical Mechanics and its Applications, 508: 313–323. https://doi.org/10.1016/j.physa.2018.05.081.

Motter, A. E. 2004. "Cascade control and defense in complex networks." Physical review letters, 93(9): 98701. https://doi.org/10.1103/PhysRevLett.93.098701.

Motter, A. E., and Y.-C. Lai. 2002. "Cascade-based attacks on complex networks." Physical review. E, Statistical, nonlinear, and soft matter physics, 66(6 Pt 2): 65102. https://doi.org/10.1103/PhysRevE.66.065102.

Newman, M. E. J. 2010. Networks: An introduction / M.E.J. Newman, Oxford: Oxford University Press.

Ouyang, M. 2014. "Review on modeling and simulation of interdependent critical infrastructure systems." Reliability Engineering & System Safety, 121: 43–

60. https://doi.org/10.1016/j.ress.2013.06.040.

Pagani, G. A., and M. Aiello. 2013. "The power grid as a complex network: a survey." Physica A: Statistical Mechanics and its Applications, 392(11): 2688–2700. https://doi.org/10.1016/j.physa.2013.01.023.

Panteli, M., and P. Mancarella. 2017. "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events." IEEE Systems Journal, 11(3): 1733–1742. https://doi.org/10.1109/JSYST.2015.2389272.

Rome, E., P. Langeslag, and A. Usov. 2014. "Federated modelling and simulation for critical infrastructure protection." In Networks of networks: the last frontier of complexity: 225–253: Springer.

Salama, M., W. El-Dakhakhni, and M. Tait. 2021. "Mixed Strategy for Resilience Enhancement of Power Grid under Cyberattack." Sustainable and Resilient Infrastructure. https://doi.org/10.1080/23789689.2021.1974675.

Schäfer, B., and G. C. Yalcin. 2019. "Dynamical modeling of cascading failures in the Turkish power grid." Chaos: An Interdisciplinary Journal of Nonlinear Science, 29(9): 93134. https://doi.org/10.1063/1.5110974.

Stergiopoulos, G., P. Kotzanikolaou, M. Theocharidou, and D. Gritzalis. 2015. "Risk mitigation strategies for critical infrastructures based on graph centrality analysis." International Journal of Critical Infrastructure

Protection, 10: 34–44. https://doi.org/10.1016/j.ijcip.2015.05.003.

Tang, J., M. Musolesi, C. Mascolo, V. Latora, and V. Nicosia. 2010. "Analysing information flows and key mediators through temporal centrality metrics." In Proc., the 3rd Workshop, edited by E. Yoneki, E. Bursztein, and T. Stein: 1–6, New York, New York, USA. https://doi.org/10.1145/1852658.1852661.

Wang, J. 2013a. "Mitigation strategies on scale-free networks against cascading failures." Physica A: Statistical Mechanics and its Applications, 392(9): 2257–2264. https://doi.org/10.1016/j.physa.2013.01.013.

Wang, J. 2013b. "Robustness of complex networks with the local protection strategy against cascading failures." Safety Science, 53: 219–225. https://doi.org/10.1016/j.ssci.2012.09.011.

Wang, J.-W., and L.-L. Rong. 2009. "Cascade-based attack vulnerability on the US power grid." Safety Science, 47(10): 1332–1336. https://doi.org/10.1016/j.ssci.2009.02.002.

Wang, J.-W., and L.-L. Rong. 2011. "Robustness of the western United States power grid under edge attack strategies due to cascading failures." Safety Science, 49(6): 807–812. https://doi.org/10.1016/j.ssci.2010.10.003.

Yan, J., Y. Tang, H. He, and Y. Sun. 2015. "Cascading failure analysis with DC power flow model and transient stability analysis." IEEE Trans. Power Syst., 30(1): 285–297. https://doi.org/10.1109/TPWRS.2014.2322082.

Zhao, K., C. Ma, J. Sun, B. Zhang, L. Ma, and L. Wang, eds. 2018. A New Simulation Method for Complicated Successive Power System Faults in Extreme Weather: IEEE. https://doi.org/10.1109/CIEEC.2018.8745920.

Chapter 2 : Temporal Networks: A Review and Opportunities for Infrastructure Simulation

ABSTRACT

Complex network theory (CNT) has been providing the platform to simulate, analyze, and visualize different complex interconnected networks, from the world wide web to biological and infrastructure networks. Despite the successes of simulating and analyzing infrastructure networks based on their static topological characteristics using CNT, there remain some challenges pertaining to considering the temporal variation within such networks. This is an important aspect, especially that most infrastructure (e.g., ¬transportation and power) networks are dynamic (i.e., evolve over time) and vary not only spatially but also temporally. Therefore, neglecting the time dimension of such networks may result in misleading interpretation of network behaviors. In this respect, the current study focuses on first presenting a review of temporal network characteristics and modeling approaches. Specifically, key temporal network topological characteristics (e.g., temporal scale and path length) are presented and discussed. In addition, the study reviews the different centrality measures that can be utilized to identify the most critical nodes and links in temporal networks. The different graphical representation techniques of temporal networks are also summarized and compared to their static counterparts. Finally, the study highlights the fact that considering the time

dimension in simulating complex networks is a relatively new research field that presents new research frontiers for breakthrough opportunities in simulating complex interdependent infrastructure networks.

Keywords: complex network theory, dynamic network, infrastructure networks, temporal network, time-varying graphs, temporal centrality.

2.1. INTRODUCTION

The use of complex network theory (CNT) analysis techniques has extended to a wide spectrum of applications in different fields (Costa et al. 2011). Within the context of CNT (Newman 2010a), the main components of the network are simulated by nodes (e.g., bus stops in transit networks and substations in power networks), whereas links represent the interdependencies between these nodes within such a network (e.g., bus routes in transit networks and transmission lines in power networks). In other words, links mimic the relational connections among the nodes (Ouyang 2014). Such links can be related to physical, cyber, geographical location, or logical interdependencies between nodes (Rinaldi et al. 2001). For example, the link may indicate a physical connection between two nodes, or that two nodes sharing the same resources or are managed/controlled by the same entities.

Such an elegant simulation approach facilitates the quantification of the interdependency between the components comprising such networks. CNT analyses also facilitate the identification of the underlying network topological characteristics, and its most influential nodes and links (Tang et al. 2010c; Wang et al. 2017b). In addition, other characteristics, such as network robustness, can be evaluated by subjecting the underlying network to dynamic stress tests (Barabási and Pósfai 2016; Wang et al. 2010b; Wang and Rong 2009), within which, the

systemic risk (e.g., domino-type cascade failure possibility) would mainly depend on the network topology (Wang 2013a).

Most published research studies have focused on simulating and analyzing networks using static approaches. Such approaches assume that the network nodes and links remain unchanged over time (Barabási et al. 2000; Guimerà et al. 2005; Latora and Marchiori 2002; Sen et al. 2003). However, most real networks evolve over time, where their links can emerge and decline over time. This can be exemplified by the temporal nature of social media (Sanlı and Lambiotte 2015), phone call (Saramäki and Moro 2015), email (Eckmann et al. 2004), biology (Holme 2016) and infrastructure networks (Borgnat et al. 2013; Rocha 2017). For all such networks, the links may only be present for a small duration (i.e., according to the corresponding application), and their statuses always fluctuate (Holme and Saramäki 2012). As such, neglecting the time dimension in studying such networks may result in erroneous interpretations of network behaviors (Pan and Saramäki 2011; Tang et al. 2013; Wu et al. 2014). Accordingly, several recent studies have focused on extending static network approaches to simulate the dynamic network behavior.

Such studies however generated multiple nomenclatures and evaluation approaches for similar network characteristics. To name but one example, the term *temporal networks* have been used interchangeably with *dynamic networks* (Caceres et al. 2011), *time-varying graphs* (Nicosia et al. 2012; Tang et al. 2010d),

temporal graphs (Wu et al. 2014), *dynamic graphs* (Kim and Anderson 2012), or *evolving graphs* (Xuan et al. 2003).

The current study thus focuses on reviewing temporal network metrics, simulation approaches and applications in infrastructure by adopting the following structure subsequent to this introduction section: Section 2.2 reviews several critical topological temporal network characteristics; Section 2.3 introduces and analyzes temporal centrality measures reported in literature; Section 2.4 outlines the different graphical representations of temporal networks; Section 2.5 describes different classes of infrastructure network-based models; Section 2.6 highlights infrastructure networks simulation opportunities; and, finally, the study summary and overall conclusions are provided in Section 2.7.

2.2. TOPOLOGY AND CHARACTERISTICS OF TEMPORAL NETWORKS

The analysis of static networks mainly relies on specific characteristics pertaining to the network topology. In the current chapter, the authors give specific attention to various characteristics and performance measures of temporal networks, as applied to infrastructure systems. For example, most infrastructure systems such as power grid or transportation networks can be modeled by nodes and links, networks within that continuously evolve over time (Borgnat et al. 2013; Rocha 2017), regardless of the underlying applications (Holme 2015; Holme and Saramäki 2012).

In addition, centrality measures, as will be shown in the next section, highlight the role played by certain key nodes in networks, while, the significance of this role is translated according to the corresponding application (Nicosia et al. 2013; Tang et al. 2010c). As such, this section presents the extension of such network characteristics from their static simulation approach to considering the time dimension within the temporal simulation approach.

2.2.1. TIME WINDOW AND TEMPORAL SCALE

A temporal network can be simulated as a sequence of static network *snapshots*. Each snapshot represents the network nodes and links within a specific time interval referred to as the *time window* (Tang et al. 2010a). The selection of the time window is key when simulating temporal networks. For example, if a network is analyzed using an overly coarse resolution (i.e., too large a time window), the temporal variations of the nodes and links may not be properly identified. Nonetheless, the use of too fine a resolution (i.e., too small a time window) may result in only a very few changes within the selected time window (Caceres et al. 2011; Caceres and Berger-Wolf 2013). Accordingly, the appropriate time window is based on the underlying application, the availability of data, and the required level of the study (Holme 2015; Li et al. 2017). For example, Borgnat et al. (2013) selected a time window of two hours in studying the temporal behavior of a France shared bicycle system to detect communities in the network and evaluate their weekly dynamical

behavior. In case of evaluating the system performance at failure propagation or restoration process, the time window needs to be short enough (e.g., seconds or minutes) to capture the accelerated dynamic of network topology. In particular, studying power grid outages involves various dynamics with different timescales. Line tripping due to overload or the load shedding usually last a few seconds, whereas, the overhead lines outages due to vegetation contact or overheat usually last for a few minutes (Yao et al. 2015).

The main criterion for selecting an optimal time window to analyze temporal networks is to maintain the balance between the degree of resolution and the target outputs. For this reason, several studies have proposed different approaches to select the optimal time window of the networks based on their underlying applications. For example, Tang et al. (2013) selected the time window according to the maximum available resolution of the data. This approach can be appropriate for some networks, where their dynamic (flow) data are collected at intervals coincident with the corresponding interactions between the nodes. However, substantial recent advances in data collection and storage have resulted in high-resolution dynamic information that requires optimizing the framework considered to select the appropriate time window. Moreover, the study by Sulo et al. (2010) revealed that there are various appropriate temporal scales, each scale demonstrates distinct measure for the same network.

2.2.2. REACHABILITY

Reachability is also key for simulating the structure of any static or temporal network. In general, reachability describes the connectivity between any two nodes. For example, node F is *directly reachable* from node A, if and only if there is one direct link, without any bridge nodes, between nodes F and A. If node F is connected to node A through other bridge nodes, then node F is *indirectly reachable* to node A (Nicosia et al. 2013).

The time dimension significantly influences the reachability between nodes, when the status of links (i.e., emergent or declining over time) is considered (Holme and Saramäki 2012; Nicosia et al. 2013). This is a key aspect in simulating temporal networks that is typically not considered in their static counterparts (Grindrod et al. 2011). As shown in Figure 1(a), node A is not connected to node F due to the time order of the links; however, the same two nodes appear connected if the focus is only on the aggregated static network, as shown in Figure 1(b). This explains the potential overestimate of the reachability when only the static state of a network is considered.

2.2.3. TEMPORAL PATH, LENGTH, AND DISTANCE

The definition of reachability is geared towards the notion of *path*. In static networks, the path represents the set of links traversed to reach from one node to another. The length of such a path is evaluated as the number of traversed links. Thus, the temporal path can be defined as the sequence of links that exist in an

ascending time order (Göbel et al. 1991; Kempe et al. 2002; Nicosia et al. 2013).

The temporal path length can be described through two different approaches (Nicosia et al. 2013). First, similar to the definition of the path length in static networks, the *topological length* is the number of links in the path between any pairs of nodes. From a static network perspective, the shortest path is the one that contains the minimum number of links (i.e., minimum topological length). However, in many temporal networks, the time taken to transfer from one node to another becomes more critical than the minimum number of links between these nodes (i.e., how quick a bus can move from one station to another throughout the transportation network). Second, the *temporal length* can be evaluated as the duration of the path in terms of the number of time windows, w. For example, in Figure 1(a), there are several temporal paths from node A to node E (A-B-E, A-D-C-E, A-B-D-C-E). The first path A-B-E has the smallest topological length (i.e., two links), while its temporal length is equal to $4w$. The second path A-D-C-E has the smallest temporal length (i.e., $2w$), while its topological length is equal to three links.

Several definitions for the shortest/minimum temporal path have been introduced based on the underlying applications (Nicosia et al. 2013; Pan and Saramäki 2011; Tang et al. 2009, 2010a; Wu et al. 2014; Xuan et al. 2003). For example, Xuan et al. (2003) presented three definitions of a *minimum journey* (i.e., path): 1) shortest journey (minimum hop count); 2) foremost journey (earliest

arrival date); and 3) fastest journey (minimum duration). The same authors termed temporal graphs as a sequence of subgraphs (i.e., timed snapshots) and provided algorithms to evaluate temporal paths. Other research studies (Pan and Saramäki 2011; Tang et al. 2009, 2010a) defined the shortest temporal path between two nodes as the temporal path with the minimum duration (e.g., path A-D-C-E between nodes A and E in Figure 2.1). More recently, Wu et al. (2014) investigated four different measures to evaluate the temporal path: 1) shortest path (minimum distance); 2) fastest path (minimum duration); 3) earliest-arrival path; and 4) latest-departure path. Unlike the work of Xuan et al. (2003) that only considered the hop count, the latter four measures take into consideration the traversal time (e.g., phone call duration or flight duration) in quantifying the shortest path.

Hence, the *temporal distance* or *latency*, d_{ij}, is the duration for the shortest temporal path between nodes *i* and *j* (Nicosia et al. 2013; Pan and Saramäki 2011). Subsequently, the average temporal distance between all pair of nodes can be expressed by calculating the *characteristic temporal path length* (Tang et al. 2009) in the network as:

$$L = \frac{1}{N\,(N-1)} \sum_{i \neq j} d_{ij} \qquad (1)$$

where, N is the total number of nodes in the network.

According to Eq. 1, if two nodes are disconnected, their temporal distance is infinity. Such infinite value influences the characteristic temporal path length quantification and subsequently yields unrealistic results. To address this issue, the definition of *temporal global efficiency*, as shown in Eq. 2 is the inverse of temporal distance, becomes more practical (Tang et al. 2010d).

$$\varepsilon = \frac{1}{N\,(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \qquad (2)$$

As a summary, Table 2.1 lists previous research studies that presented definitions of the shortest/minimum temporal path.

2.3. TEMPORAL CENTRALITY MEASURES

CNT is not only concerned with evaluating the complex interdependence between nodes through links, but also with revealing the influences of different nodes on the overall network behavior. For this reason, several network centrality measures have been widely utilized in different applications to identify critical nodes in the relevant networks. Such applications range from identifying influential individuals in social networks (Kempe et al. 2003) to bottlenecks in transportation networks (Hossain and Alam 2017; Zhao et al. 2017). As such, several studies recently extended the different static centrality measures to temporal networks and subsequently compared their correlation to static network applications (Pan and Saramäki 2011; Tang et al. 2010c; Taylor et al. 2017). This section summarizes the

most common centrality measures within both static and temporal networks.

For notational consistency, the temporal network measures discussed next are based on a set of nodes, *N*, connected by a set of links, *L*, where links change over time. This network also has a finite time interval that starts and ends at t_{start} and t_{end}, respectively. The temporal network can be represented by a set of static graphs [$G_1, G_2, \ldots G_m$], where each graph captures some network information for specific duration of time, referred to as the time window size, *w*. The number of the time intervals or the number of the snapshots, *m*, equals to the integer value of the quotient $((t_{end} - t_{start}) / w)$.

2.3.1. DEGREE CENTRALITY

For static networks, the degree centrality of a node is the total number of links connected directly to this node normalized (divided) by the maximum number of links that can be connected to the same node (Freeman 1978), as presented in Eq. 3. In directed networks, there are two types of degrees: an *in*-degree and an *out*-degree. According to the degree centrality, the node with the highest degree is the most central node (i.e., hub) (Barabási and Pósfai 2016).

$$D_{C_S}(i) = \frac{1}{(N-1)} \sum_j \mathrm{L}_{ij} \qquad (3)$$

where, L_{ij} = 1 if, and only if, there is a link between nodes *i* and *j*, and L_{ij} = 0 otherwise.

To extend the degree centrality measure to temporal networks, Kim and Anderson (2012) developed a time-ordered graph that facilitates evaluating the centrality measure for such networks. The time-ordered graph simulates the temporal network topology as a static network with directed flows, as shown in Figure 2.2. Accordingly, the temporal degree centrality of a node can be evaluated first from this graph as the sum of all the *in* and *out* links connected to this node in a time interval (i.e., from t_{start} to t_{end}). Subsequently, this summation is normalized through dividing by $2m(N-1)$, as presented in Eq.4. In other words, the temporal degree centrality of a node is the average value of its *in*- and *out*-degrees over a set of the snapshots, *m*.

$$D_{C_I}(i) = \frac{1}{2m\,(N-1)} \sum_{t} (\mathrm{K}_{in} + \mathrm{K}_{out}) \qquad (4)$$

where, K_{in} and K_{out} are the number of *in* and *out* links connected to the node, respectively.

2.3.2. CLOSENESS CENTRALITY

The closeness centrality measures how close a node is to other nodes in the same network. In static networks, the closeness centrality of a node is evaluated as the inverse of the average static distances from this node to all other nodes (Freeman 1978), as expressed in Eq. 5. Where the static distance S_{ij} is the minimum number of the links that connects nodes *i* and *j*.

$$C_{C_S}(i) = \frac{1}{N-1}\sum_{j}\frac{1}{S_{ij}} \quad (5)$$

Tang et al. (2010c) extended the concept of closeness centrality to temporal networks by replacing the static by the temporal distance. Therefore, the temporal closeness centrality can be expressed in terms of the average of the total shortest temporal distances from a given node to all other nodes:

$$C_{C_I}(i) = \frac{1}{m\,(N-1)}\sum_{j} d_{ij} \quad (6)$$

Again, having disconnected nodes in the network would lead to an infinite temporal distance value, and therefore, the closeness centrality can be defined as (Pan and Saramäki 2011):

$$C_{C_{II}}(i) = \frac{1}{m\,(N-1)}\sum_{j}\frac{1}{d_{ij}} \quad (7)$$

Tang et al. (2010c) demonstrated that the closeness centrality of a node is useful to identify the most influential *spreaders* throughout the network. For example, an infected individual (node) with high a closeness centrality value (compared to other exposed individuals) is potentially the most effective distributor for spreading virus or cascade systemic risks throughout the network. In the case of infrastructure networks, closeness centrality provides a potential indicator to the critical nodes that are, for example, responsible for blackouts in power networks or

traffic jams in transportation networks. In addition, Pan et al. (2011) emphasized that some nodes might appear too close in a static network; however, considering the temporal dimension, such nodes might actually not be even connected or have a long temporal path. Therefore, in a temporal network, some nodes might possess low closeness centrality values relative to their counterparts when the same network is evaluated as a static network.

Moreover, Kim and Anderson (2012) proposed a formula to calculate the closeness centrality of a node by considering the shortest temporal path distance for all time intervals from t to t_{end} (i.e., $t_{start} \leq t < t_{end}$), as presented in Eq. 8. This definition differs from that presented in Eq. 7 that focused only on the overall time interval (i.e., from t_{start} to t_{end}).

$$C_{C_{III}}(i) = \frac{1}{m\,(N-1)} \sum_{t} \sum_{j} \frac{1}{d_{ij}[t, t_{end}]} \qquad (8)$$

where $d_{ij}[t, t_{end}]$ is the shortest temporal distance between nodes i and j within a time interval from t to t_{end}.

Table 2.2 presents the closeness centrality values calculated according to Eqs. 7 and 8 (Kim and Anderson 2012; Pan and Saramäki 2011) to facilitate a direct comparison. As can be seen in Table 2.2, nodes B, C, D, and E have the same closeness centrality value according to Eq. 7 suggested by Pan et al. (2011). Conversely, according to Eq. 8 proposed by Kim and Anderson (2012), node C

possesses a unique large value over nodes B, D, and E. This difference in closeness centrality values is mainly attributed to the variation of temporal paths as the time increases. More specifically, according to Eq. 7, the temporal centrality is governed by the shortest temporal path within the overall time interval [t_{start}, t_{end}] and all other interactions are ignored. While, according to Eq. 8, all possible time intervals [t, t_{end}] are considered to include the dynamics of temporal paths between nodes.

2.3.3. BETWEENNESS CENTRALITY

The betweenness centrality measure identifies nodes that play a central role between other nodes in the network (Lazega et al. 1995). In a static network (Freeman 1977), this measure is calculated as:

$$C_{B_S}(i) = \frac{\sum_{i \neq j \neq k} \sigma_{jk}(i)}{\sum_{i \neq j \neq k} \sigma_{jk}} \qquad (9)$$

where $\sigma_{jk}(i)$ is the total number of shortest paths between nodes *j* and *k* that passes through node *i*, while σ_{jk} is the total number of shortest paths between nodes *j* and *k*.

The definition in Eq. 9 can be extended to temporal networks by considering the temporal paths in lieu of the static paths (Tang et al. 2010c). In a similar way, the temporal betweenness centrality of node *i* can be defined as the ratio between the number of shortest temporal paths between all pairs of nodes that pass through node (*i*) and the total number of the shortest temporal paths between all nodes in

the network. Tang et al. (2010c) proposed an expression to calculate the temporal betweenness centrality to consider the waiting time (e.g., the difference between arrival and departure time at the bus station in a transit network). In this respect, the betweenness centrality of node *i* at time *t* can be expressed as:

$$C_B\,(i,t) = \frac{1}{(N-2)(N-1)} \sum_{j \neq i} \sum_{\substack{k \neq i \\ k \neq j}} \frac{u\,(i,t,j,k)}{\sigma_{jk}} \qquad (10)$$

where, $u\,(i,t,j,k)$ is the number of the temporal shortest paths between nodes *j* and *k* that passes through node *i* at a time equals to or less than *t*. Hence, the betweenness centrality of node *i* over all time intervals is defined as:

$$C_{B_I}\,(i) = \frac{1}{m} \sum_{t} C_B\,(i,t) \qquad (11)$$

2.4. GRAPHICAL REPRESENTATION OF TEMPORAL NETWORKS

Graphical representation of temporal networks is a critical aspect to visualize the network structure. This section provides a review of the different representation techniques proposed in previous studies to visualize temporal network data (e.g., links time, links order and duration).

2.4.1. TIME-LABELED GRAPH

A simple technique to represent a temporal network is by using a *time-labeled graph* (Kempe et al. 2002), in which each link is labeled with the time of contact

between its pair of nodes, as shown in Figure 2.3. Therefore, the temporal path is strictly committed to follow an ascending order through these labels (Kempe et al. 2002). Such a graph is also referred to as *contact sequences* (Holme 2005) or *time series of contacts* (Holme 2015). Holme (2005) used this graph to illustrate the spreading processes in directed temporal networks. This representation technique illustrates the temporal data in a single graph, thus taking advantage of the static network layouts.

2.4.2. SEQUENCE OF STATIC GRAPHS

Another technique to represent temporal networks is to show the evolving network over time by a set of subgraphs, where each subgraph captures the network information at a specific time (Ferreira 2004; Tang et al. 2009), as shown in Figure 2.1(a). Such a graph also termed *graph sequences* (Holme 2015) or *time-varying graph* (Nicosia et al. 2012; Nicosia et al. 2013). Such a representation depends mainly on the selected time window, as discussed earlier. One drawback of using this technique lies in its inability to consider the time spent to transfer the information (i.e., contact duration) within the same time window. For example, in Figure 2.1(a), node B can connect to node E in one-time step through nodes D and C without any consideration to the time needed to reach from one node to another.

2.4.3. TIME-ORDERED GRAPH

Another powerful technique to represent temporal networks is the time-ordered

graph introduced by (Kim and Anderson 2012). This graph has also been termed *directed acyclic graph* (Speidel et al. 2015; Takaguchi et al. 2016), *time-unfolded network* (Pfitzner et al. 2013), *static expansion* (Michail 2016), or *time-node graphs* (Holme 2015). The concept behind this graph is to represent the temporal network by a single static network with directed links, as shown in Figure 2.2. This facilitates analyzing and visualizing any large temporal network using a simple organized equivalent static network (Kim and Anderson 2012). This technique considers the contact duration, where no more than one interaction can occur at one-time step for each path.

2.4.4. TIMELINE GRAPH

Timeline graph is an effective technique to illustrate the link status/evolution over time, where one axis represents the time and the other represents the nodes of the network, as shown in Figure 2.4 (Holme 2015). This technique provides a distinct visualization of the network, where the temporal path can be followed. However, the technique is limited to small networks as the graph can become too complex for networks with a large number of nodes.

2.4.5. GRAPHING/VISUALIZATION TOOLS

It is difficult to utilize the aforementioned visualization techniques for large networks without practical/efficient tools. The difficulty stems from the fact that the corresponding network graphs would become very dense and, subsequently, it

would be challenging to visualize the temporal nature of the underlying networks. To address this matter, there are several temporal network visualization tools that are either stand-alone software packages, or available within different programming languages such as C/C++, R, and Python. Table 2.3 lists some of the several software packages and libraries for temporal network analysis.

2.5. INFRASTRUCTURE NETWORK-BASED MODEL CLASSES

After highlighting the main differences in the previous sections between static and temporal networks, it is important to relate these two network models to different infrastructure network simulation applications. In general, studies that focused on evaluating infrastructure system performance, resilience and robustness can be broadly classified into three groups: topology-based-, flow-based-, and physics-based models (LaRocca et al. 2015; Ouyang 2014).

2.5.1. TOPOLOGY-BASED MODELS

Topology-based models would simulate an infrastructure network based only on the former's topology and connectivity properties. Such models disregard flows and physical properties of/within the network, and instead represent the underlying network in an abstract manner, as a set of nodes and links, without differentiation between the component physical functions/roles within the network (LaRocca et al. 2015; Ouyang 2014). For example, when modeling a power grid, key stations would be treated simply as nodes with no distinction between generation-,

distribution-, or sub-stations (Rosato et al. 2007). Some studies however adopted topology-based models with additional consideration for node heterogeneity (e.g., the different functions between network components) (Albert et al. 2004). Another example is the work of Kaluza et al. (2010) that investigated the global maritime transportation network, where ports were represented by nodes that were linked by ship paths.

Although abstract in nature, topology-based models can provide a general indication of network behavior and vulnerability, albeit such models lack the ability to give a complete picture of infrastructure behavior. This is because all infrastructure networks are governed by the law of physics and subjected to constraints pertaining to their supply and demand capacities (Hines et al. 2010b).

2.5.2. FLOW-BASED MODELS

Unlike network models based solely on topology, flow-based models consider also the flow or service delivered through the infrastructure network (Ouyang 2014). In other words, such models combine the network topology with network flow models to represent loads, demands, and capacities within the network. However, these models do not incorporate real dynamic flow modeling (e.g., power flow analysis in power grid or hydraulic flow model in water network). For example, many network flow models proposed to consider power load and capacity according to shortest paths or centrality measures in studying power grid vulnerability and

resilience (Ezzeldin and El-Dakhakhni 2019; Fang et al. 2014; Motter and Lai 2002; Wang and Rong 2009, 2011).

Based on this concept, some studies focused on infrastructure networks and their interdependencies provided a more realistic simulation approach. For example, Lee and Wallace (2007) utilized a mathematical representation of network flow to model interdependence within infrastructure networks. Although such modeling approach considered different types of interdependencies to analyze and simulate network post-disruption and restoration processes, it only focused on a single level of the decision-making (i.e., the selection of components to repair or install to restore the network service). Such mathematical models can be integrated with optimization algorithms to incorporates the restoration planning and scheduling decisions (Cavdaroglu et al. 2013; Nurre et al. 2012). Nonetheless, high-fidelity models have to consider real system components properties, dynamics physical flow, and capacities especially for modeling the dynamics of cascade failure (Pagani and Aiello 2013a), systemic risk mitigation strategies, and resilience of infrastructure networks.

2.5.3. PHYSICS-BASED MODELS

The two network-based models described above do not fully captured the realistic dynamics physical flow within infrastructure systems (LaRocca et al. 2015). For example, a high-fidelity model of power grid should take into consideration the real

power flow, the transmission lines electrical properties, and the generations supply and capacity (Bernstein et al. 2014a; Li et al. 2018; Yang et al. 2017). Such physics-based models usually require significant computational time and required more data to simulate the functionality of network components, compared to their topology- and flow-based model counterparts. In particular, infrastructure network resilience analysis based on physics-based models is more realistic when considering the dynamic behavior of such complex networks. In real-life, infrastructure networks continuously evolve due to the changing of service demand, topological adjustments, the growth of the interdependencies, in addition to the post-event improvements such as enhancements of component capacities, implementation of the new standards, the increase of situational awareness, and the integration with the new technologies (Goldbeck et al. 2019; Ouyang and Dueñas-Osorio 2012).

In this respect, Ouyang and Dueñas-Osorio (2012) evaluated the resilience assessment processes of power infrastructure networks when the networks' future evolving processes are considered. Moreover, González et al. (2016) provided a simulation-optimization framework to optimize the resource allocation and recovery strategy in the restoration planning for interdependent infrastructure networks. Furthermore, other studies focused on evaluating interdependent infrastructure networks resilience, through a dynamic network flow model (Goldbeck et al. 2019) or a multi-objective restoration model (Almoghathawi et al. 2019), to maximize the network resilience while minimizing the total cost

associated. In summary, the integration between temporal network models with physics-based models yields more realistic analysis results, especially when simulating the dynamics of cascade failure, developing systemic risk mitigation strategies, and enhancing the resilience of infrastructure networks.

In closure, real infrastructure networks experience temporal variations of their topologies as well as the flow or service provided through them (Goldbeck et al. 2019; Rocha 2017). Dynamics of network topology can be readily observed when evaluating failure propagation, recovery, systemic risk mitigation, as well as restoration and reconfiguration processes, whereas, the dynamics of flow are represented through the demand, supply, load, or service fluctuation through the network components (Hines et al. 2010b; Ouyang 2014). For example, in power grids or transportation networks, the network topology continuously varies due to maintenance scheduling of transmission lines or roads, closing roads or bridges due to accident or disruptive event, and/or failure propagation. Therefore, the temporal network approach provides a promising direction to model the dynamics of network topology. This approach can be also extended by an integration with physics-based models to also account for the dynamic of flow (Ouyang and Dueñas-Osorio 2012; Yang et al. 2017).

2.6. OPPORTUNITIES FOR INFRASTRUCTURE NETWORKS SIMULATION

Modern societies are fully dependent on physical- and cyberinfrastructure networks, that do not operate in isolation, but are instead interdependent on multiple levels (Ouyang 2014). In fact, it can be argued that our prosperity and security rely on our future ability to understand and analyze not only the *intra*-dependence within each of such infrastructure networks but also their overall *inter*-dependence (Min et al. 2007). Although interdependence improves network efficiencies, it also increases their interdependence –induced vulnerability, which gives rise to systemic risk and may thus result in severe loss of functionality and recovery capability (Monsalve and de la Llera, Juan Carlos 2019). In reality, multiple independent, possibly noncooperative, decision-makers are responsible for managing infrastructure networks (Smith et al. 2017). Furthermore, various layers of complexity play a role related to operating, maintenance, and recovery of infrastructure networks especially in case of catastrophic failure.

Another layer of complexity that needs to be tackled relates to the socio-technical aspects— the interface between the social networks with the underlying physical infrastructure networks. Specially, infrastructure networks are not only affected by physical components but also by human behavior, regulatory agencies, stakeholders, and government/private enterprise (Barrett et al. 2004). Recently, the work of Guidotti et al. (2019) highlighted the consequences of neglecting such interdependence between the social systems and physical infrastructure networks. It was concluded that disregarding the information from human response models

may result in misleading conclusions including lower estimate of population dislocation; higher estimates demands on physical network components; and slower recovery process. Therefore, it is imperative to consider decentralized decision making in modeling and simulation interdependent infrastructure networks. Moreover, it is quiet challenging to develop informative and computationally high-fidelity modeling, especially with consideration of both time dynamics and interdependencies.

Another promising research area involves data-driven and game theory applications, especially for large scale network analysis. For instance, Dueñas-Osorio and Kwasinki (2012) used the historical restoration curves through a time series method to quantify coupling strength and interdependencies between infrastructure networks. Furthermore, Monsalve and Juan Carlos (2019) presented a data-driven model to simulate the restoration process of interdependent infrastructure networks after a disruptive event. Some studies proposed data-driven models to generate a linear recovery operator from numerous disaster and failure scenarios (González et al. 2017). This operator can be used later to provide the optimal recovery strategies associated with any damage scenario. For consideration of multiple independent, utility network controllers, and decisionmakers, game theoretic approaches have been used to resolve such crossed interactions between numerous players. Smith et al. (2017) proposed a game theoretic recovery model to address the decentralized related to infrastructure networks decisionmakers.

The following subsections highlight temporal network modeling research efforts in and potential opportunities in transportation-, power-, and water distribution infrastructure networks. Overall extensive research is needed to simulate and analyze the infrastructure networks based on the temporal variation within the networks, rather than only the static topological characteristics. Especially when assessing infrastructure resilience, where the network topologies are evolving due to increase of service demand, retrofit, reconfiguration, and restoration processes (Goldbeck et al. 2019; Ouyang and Dueñas-Osorio 2012).

2.6.1. TRANSPORTATION NETWORKS

Transportation networks possess one of the most vivid temporal behavior in infrastructure networks. Recent computational advances coupled with the availability of detailed data that describes real-time interactions have also boosted the field of transportation network dynamical behavior research (Gallotti and Barthelemy 2015). For example, the data collected by smart card systems can include accurate information about the corresponding time and space domains. A shared bicycle/car system is also a common example of a temporal network constructed using data from smart cards (Borgnat et al. 2013).

Air traffic networks present another mode of transportation that strongly evolves over time. Rocha (2017) provided a review of air traffic networks, where airports were represented by nodes and flights were represented by links between

each pair of nodes. Studying such networks from a temporal perspective can demonstrate how flight delays propagate. This can be subsequently used to enhance network efficiency and connectivity by reducing the total travel time, optimizing resources, and maximizing profits. Moreover, Sun et al. (2015) studied the temporal evolution of air traffic networks within the European context. In their study, different network centrality measures have been analyzed over time to identify the hub nodes. It was found that these air traffic networks are dominated by seasonal (time) variation. Such results would assist stakeholders in managing and enhancing the performance of their air traffic networks.

Additional studies focused on other modes of transportation. For instance, Ducruet and Notteboom (2012) investigated the network structure for vessel movement data covering about all of the world's container fleets in 1996 and 2006. The study also analyzed the relative position of ports (i.e., centrality) in the global network with mapping the changing of ports centrality through time. In addition, Williams and Musolesi (2016) investigated the performance of four transport networks in the time and space dimensions. The same authors evaluated the behavior of these networks under random failures and targeted attacks.

In term of specific opportunities considering that, transportation networks usually encompass multi modes that require different types of nodes and/or links, there remains a significant lack of understanding of multilayer temporal transportation networks. Multilayer (multiplex) networks include multiple layers

representing the connectivity and the types of interactions between nodes. A comprehensive review pertaining to static multilayer networks have been discussed by Domenico et al. (2013) and Kivela et al. (2014). Furthermore, it is worth mentioning that one way to reveal more complexity and provide a deep understanding of transportation infrastructure networks is to combine different concepts in simulation. For example, spatio-temporal networks typically integrate both space and time dimensions. These networks can develop a more accurate representation of several infrastructure networks, especially when multi-modal transit systems are analyzed (George and Kim 2013; Goforth et al. 2019). Another example, adaptive dynamic networks combine the dynamics of nodes and/or links and their influences on the temporal network topology, where, links shift adaptively according to the network status. This leads to a dynamical interplay (Gross and Sayama 2009) between the topology and the operation state of the transit network, especially in disaster situations and emergency traffic management.

2.6.2. POWER NETWORKS

The temporal behavior of power networks can be easily observed in two aspects. First, power networks are typically subjected to load balancing between supply and demand. The supply may change frequently due to the fluctuation of renewable energy sources such as wind. In addition, power storage infrastructure has only limited capacities to store electric power, thus, any overproduced electric power

must be transferred and consumed within the large power network (grid). Moreover, the demand for electricity continuously varies throughout the day (Nardelli et al. 2014) and based on numerous factors including weather conditions. Subsequently, the electric loads on power stations and transmission lines vary continuously over time. Second, a blackout is a typical example of the dynamic nature of power networks (Carreras et al. 2001). A blackout can be initiated by several causes including those attributed to weather conditions, network component failures, or human errors. It should also be noted that a small disruption in some key components may lead to overload on other components and start a chain of cascade failures, which can spread throughout the network (Bernstein et al. 2014a; Costa et al. 2011).

Several studies have investigated cascade failures by simulating failure propagation on power networks (Crucitti et al. 2005; Fang et al. 2014; Kinney et al. 2005; Motter and Lai 2002; Pagani and Aiello 2013a; Sun et al. 2008; Wang et al. 2010b; Wang and Rong 2009, 2011). For example, Motter et al. (2002) studied the cascade failures due to targeted attacks on several real undirected networks, including power networks. It was concluded that power networks have high robustness to random attacks, but once a node with high load fails, network-level cascade failures may be triggered, affecting the performance of the entire network. In addition, Rosato et al. (2007) analyzed power networks of Spain, Italy, and France to identify their critical links (i.e., transmitting lines) and improve the

network connectivity (e.g., robustness and redundancy) by adding new links. Moreover, Wang et al. (2009) studied the vulnerability of the US power network. Different attack scenarios have been applied through the removal of nodes in ascending or descending orders (in terms of their loads). The initial load of a node was assumed by integrating a node *degree* and its neighbors' degrees. After a node is successfully attacked and thus removed, the load is redistributed to that node's neighbors according to their initial loads. Although this research work contributed to the understanding the US power network behavior and evaluating its robustness under different attack scenarios, the model in the study by Wang and Rong (2009) did not consider actual power distribution, where the initial load of a node was assumed according to its corresponding degree. In addition, the model did not account for the overload on the links. Bernstein et al. (2014a) modeled the cascade failure for US western interconnected with considering power flow distribution to identify the most vulnerable locations in the grid. Recently, Yang et al. (2017) provided a large-scale model for the US – South Canada power network to investigate network vulnerability. The model was characterized by its large scale, the physical properties of power flow and a large amount of temporal data representing a wide range of system conditions over time.

Most previous research studies have focused only on cascade modeling, while a limited number of studies developed risk mitigation and resilience enhancement strategies. For example, Motter (2004) proposed a cascade control

method based on minimal alterations to the network structure. These alterations consisted of removing a few selected nodes or links after the initial attack and prior to the propagation of cascade failures (e.g., similar to the function of the circuit breakers). Another risk mitigation strategy has been introduced by Wang (2013a) to suppress the cascade propagation through load redistribution from the overloaded nodes to other neighboring nodes. This redistribution maintains the overloaded nodes' normal and efficient function.

Overall, there is an opportunity for temporal/dynamic behavior of power networks to be adopted in simulating changes in both network topology (i.e., cascade failures) and network flow. Such an approach would facilitate better understanding of network behavior and developing real-time defense and risk mitigation strategies of actions prior to and during cascade failures.

2.6.3. WATER DISTRIBUTION NETWORKS

A limited number of studies has been conducted on water networks using CNT. For example, Xu et al. (2008) utilized different network topological characteristics (e.g., betweenness centrality and path distance) to identify the key nodes within a water distribution network. These key nodes can be used to accommodate sensors to detect contamination locations within the network. Furthermore, the same authors used the concept of *reachability* to formulate the receivability, which indicates the set of nodes that has paths to a certain node in a directed network. The

receivability measure is useful to simulate the different risk scenarios and the corresponding mitigation strategies following any contamination events. Dueñas et al. (2007) also investigated the water distribution networks, where tanks and pipelines were represented by nodes and links, respectively. Their work illustrated the network topology to evaluate the network vulnerability under both targeted and random disruptions. However, the network has been studied as an undirected network without any consideration to the flow direction. Furthermore, Yazdani and Jeffrey (2011) investigate four water distribution networks using several measurements to quantify the network's vulnerability and robustness. Finally, Perelman and Ostfeld (2011) used the network topology and connectivity analysis to study strongly- and weakly-connected clusters in directed water distribution networks.

In closure, water distribution networks are becoming more complex with the introduction of large-scale infrastructure components such as tanks, pumping stations, hydrants, valves, and pipelines. It is thus challenging to predict the network performance in case of failure scenarios or provide an efficient contaminant spread risk mitigation strategy (Perelman and Ostfeld 2011). However, the use of temporal network modeling approaches might facilitate tackling such challenges. For example, temporal centrality could help enhancing water security by detecting contamination sources and highlighting critical locations to place sensors.

2.7. DISCUSSION AND CONCLUSION

The recent revolution in collecting network-type data has boosted CNT studies and applications. In addition, current available datasets collected for example by mobile devices, sensors, or smart cards, include many details about the temporal (i.e., dynamic) behavior of the underlying network. In this respect, the current study provided a review and a fundamental background of the temporal simulation approach of complex networks. The static network topological characteristic extensions to temporal networks were also outlined. In addition, several temporal centrality measures and graphical representation techniques were discussed and investigated. Finally, opportunities and applications of infrastructure networks simulation using CNT were presented.

Previous studies demonstrated that temporal measures provide more realistic and accurate results compared to static measures. Therefore, the temporal network simulation approach can be considered a more appropriate framework to simulate and analyze infrastructure networks. However, there remains several gaps that need to be addressed. For example, the current review showed that, to date, there is no consensus among researchers about the definition of some temporal metrics, with previous studies providing several definitions to the same measure (e.g., the shortest temporal path). It is also clear that the temporal closeness centrality measure can be evaluated by two different approaches: one that considers only the overall time interval, while the other considers all possible time intervals. The results of the two approaches were significantly different for the same nodes.

Although there is a significant amount of literature related to the robustness of infrastructure networks from a static perspective, a limited number of studies has been conducted considering the temporal nature of these networks. Furthermore, despite the significant progress in modeling cascade failures, there is still a lack of large-scale models for infrastructure networks that consider the dynamical changes in the network topology. For example, most previous studies consider power networks merely as undirected networks without any physical or electrical properties of actual infrastructure network. In addition, most of the proposed models do not account for the actual loads on the nodes and links (i.e., the power pass-through stations and transmitting lines), and the subsequent real load redistribution when any component fails. Developing such model remains an intriguing research area.

Overall, the current study indicates that using the temporal network as a simulating approach for infrastructure complex networks presents a promising framework to simulate and reveal complex infrastructure network characteristics, evaluate their interdependence, quantify their resilience, and mitigate their systemic risks.

2.8. ACKNOWLEDGMENT

This research was supported by NSERC through the Canadian Nuclear Energy Infrastructure Resilience under Systemic Risk (CaNRisk) – Collaborative Research

and Training Experience (CREATE) program of the Natural Science and Engineering Research Council (NSERC) of Canada.

2.9. REFERENCE

Albert, R., I. Albert, and G. L. Nakarado. 2004. "Structural vulnerability of the North American power grid." Physical review. E, Statistical, nonlinear, and soft matter physics, 69(2 Pt 2): 25103. https://doi.org/10.1103/PhysRevE.69.025103.

Almoghathawi, Y., K. Barker, and L. A. Albert. 2019. "Resilience-driven restoration model for interdependent infrastructure networks." Reliability Engineering & System Safety, 185: 12–23. https://doi.org/10.1016/j.ress.2018.12.006.

Barabási, A.-L., R. Albert, and H. Jeong. 2000. "Scale-free characteristics of random networks: The topology of the world-wide web." Physica A: Statistical Mechanics and its Applications, 281(1-4): 69–77. https://doi.org/10.1016/S0378-4371(00)00018-2.

Barabási, A.-L., and M. Pósfai. 2016. Network science, Cambridge United Kingdom: Cambridge University Press.

Barrett, C., S. Eubank, V. A. Kumar, and M. V. Marathe. 2004. "Understanding large scale social and infrastructure networks: a simulation based approach." SIAM news, 37(4): 1–5.

Bernstein, A., D. Bienstock, D. Hay, G. Uzunoglu, and M. Zussman, eds. 2014. Power grid vulnerability to geographically correlated failures — Analysis and control implications, IEEE INFOCOM 2014 - IEEE Conference on Computer Communications. https://doi.org/10.1109/INFOCOM.2014.6848211.

Borgnat, P., C. Robardet, P. Abry, P. Flandrin, J.-B. Rouquier, and N. Tremblay. 2013. "A Dynamical Network View of Lyon's Vélo'v Shared Bicycle System." In Dynamics On and Of Complex Networks, Volume 2, edited by A. Mukherjee, M. Choudhury, F. Peruani, N. Ganguly, and B. Mitra: 267–284, New York, NY: Springer New York. https://doi.org/10.1007/978-1-4614-6729-8_13.

Caceres, R. S., and T. Berger-Wolf. 2013. "Temporal Scale of Dynamic Networks." In Temporal Networks, edited by P. Holme, and J. Saramäki: 65–94, Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-36461-7_4.

Caceres, R. S., T. Berger-Wolf, and R. Grossman. 2011. "Temporal Scale of Processes in Dynamic Networks." In Proc., 2011 IEEE International Conference on Data Mining Workshops (ICDMW): 925–932. https://doi.org/10.1109/ICDMW.2011.165.

Carreras, B. A., V. E. Lynch, M. L. Sachtjen, I. Dobson, and D. E. Newman, eds. 2001. Modeling blackout dynamics in power transmission networks with simple structure: IEEE. https://doi.org/10.1109/HICSS.2001.926275.

Cavdaroglu, B., E. Hammel, J. E. Mitchell, T. C. Sharkey, and W. A. Wallace. 2013. "Integrating restoration and scheduling decisions for disrupted interdependent infrastructure systems." Annals of Operations Research, 203(1): 279–294. https://doi.org/10.1007/s10479-011-0959-3.

Costa, L. d. F., O. N. Oliveira, G. Travieso, F. A. Rodrigues, P. R. Villas Boas, L. Antiqueira, M. P. Viana, and L. E. Correa Rocha. 2011. "Analyzing and modeling real-world phenomena with complex networks: A survey of applications." Advances in Physics, 60(3): 329–412. https://doi.org/10.1080/00018732.2011.572452.

Crucitti, P., V. Latora, and M. Marchiori. 2005. "Locating critical lines in high-voltage electrical power grids." Fluct. Noise Lett., 05(02): L201-L208. https://doi.org/10.1142/S0219477505002562.

Domenico, M. de, A. Solé-Ribalta, E. Cozzo, M. Kivelä, Y. Moreno, M. A. Porter, S. Gómez, and A. Arenas. 2013. "Mathematical Formulation of Multilayer Networks." Phys. Rev. X, 3(4): 1082. https://doi.org/10.1103/PhysRevX.3.041022.

Ducruet, C., and T. Notteboom. 2012. "The worldwide maritime network of container shipping: spatial structure and regional dynamics." Global Networks, 12(3): 395–423. https://doi.org/10.1111/j.1471-0374.2011.00355.x.

Dueñas-Osorio, L., J. I. Craig, B. J. Goodno, and A. Bostrom. 2007. "Interdependent Response of Networked Systems." J. Infrastruct. Syst., 13(3): 185–194. https://doi.org/10.1061/(ASCE)1076-0342(2007)13:3(185).

Dueñas-Osorio, L., and A. Kwasinski. 2012. "Quantification of lifeline system interdependencies after the 27 February 2010 Mw 8.8 offshore Maule, Chile, earthquake." Earthquake Spectra, 28(S1): S581-S603. https://doi.org/10.1193/1.4000054.

Eckmann, J.-P., E. Moses, and D. Sergi. 2004. "Entropy of dialogues creates coherent structures in e-mail traffic." Proceedings of the National Academy of Sciences of the United States of America, 101(40): 14333–14337. https://doi.org/10.1073/pnas.0405728101.

Ezzeldin, M., and W. E. El-Dakhakhni. 2019. "Robustness of Ontario power network under systemic risks." Sustainable and Resilient Infrastructure: 1–20. https://doi.org/10.1080/23789689.2019.1666340.

Fang, X., Q. Yang, and W. Yan. 2014. "Modeling and analysis of cascading failure in directed complex networks." Safety Science, 65: 1–9. https://doi.org/10.1016/j.ssci.2013.12.015.

Ferreira, A. 2004. "Building a reference combinatorial model for MANETs." IEEE Network, 18(5): 24–29. https://doi.org/10.1109/MNET.2004.1337732.

Freeman, L. C. 1977. "A Set of Measures of Centrality Based on Betweenness." Sociometry, 40(1): 35. https://doi.org/10.2307/3033543.

Freeman, L. C. 1978. "Centrality in social networks conceptual clarification." Social Networks, 1(3): 215–239. https://doi.org/10.1016/0378-8733(78)90021-7.

Gallotti, R., and M. Barthelemy. 2015. "The multilayer temporal network of public transport in Great Britain." Scientific data, 2: 140056. https://doi.org/10.1038/sdata.2014.56.

George, B., and S. Kim. 2013. Spatio-temporal networks: Modeling and algorithms, New York, NY [u.a.]: Springer. https://doi.org/10.1007/978-1-4614-4918-8.

Göbel, F., J.O. Cerdeira, and H. J. Veldman. 1991. "Label-connected graphs and the gossip problem." Discrete Mathematics, 87(1): 29–40. https://doi.org/10.1016/0012-365X(91)90068-D.

Goforth, E., M. Ezzeldin, W. El-Dakhakhni, L. Wiebe, and M. Mohamed. 2019. "Network-of-Networks Framework for Multi-modal Hazmat Transportation: Application to Used Nuclear Fuel in Canada." ASCE Journal of Hazardous, Toxic, and Radioactive Waste. https://doi.org/10.1061/(ASCE)HZ.2153-5515.0000493.

Goldbeck, N., P. Angeloudis, and W. Y. Ochieng. 2019. "Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models."

Reliability Engineering & System Safety, 188: 62–79. https://doi.org/10.1016/j.ress.2019.03.007.

González, A. D., A. Chapman, L. Dueñas-Osorio, M. Mesbahi, and R. M. D'Souza. 2017. "Efficient infrastructure restoration strategies using the recovery operator." Computer-Aided Civil and Infrastructure Engineering, 32(12): 991–1006. https://doi.org/10.1111/mice.12314.

González, A. D., L. Dueñas-Osorio, M. Sánchez-Silva, and A. L. Medaglia. 2016. "The interdependent network design problem for optimal infrastructure system restoration." Computer-Aided Civil and Infrastructure Engineering, 31(5): 334–350. https://doi.org/10.1111/mice.12171.

Grindrod, P., M. C. Parsons, D. J. Higham, and E. Estrada. 2011. "Communicability across evolving networks." Physical review. E, Statistical, nonlinear, and soft matter physics, 83(4 Pt 2): 46120. https://doi.org/10.1103/PhysRevE.83.046120.

Gross, T., and H. Sayama. 2009. Adaptive Networks, Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-01284-6.

Guidotti, R., P. Gardoni, and N. Rosenheim. 2019. "Integration of physical infrastructure and social systems in communities' reliability and resilience analysis." Reliability Engineering & System Safety, 185: 476–492. https://doi.org/10.1016/j.ress.2019.01.008.

Guimerà, R., S. Mossa, A. Turtschi, and L. A. N. Amaral. 2005. "The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles." Proceedings of the National Academy of Sciences of the United States of America, 102(22): 7794–7799. https://doi.org/10.1073/pnas.0407994102.

Hines, P., E. Cotilla-Sanchez, and S. Blumsack. 2010. "Do topological models provide good information about electricity infrastructure vulnerability?" Chaos: An Interdisciplinary Journal of Nonlinear Science, 20(3): 33122.

Holme, P. 2005. "Network reachability of real-world contact sequences." Physical review. E, Statistical, nonlinear, and soft matter physics, 71(4 Pt 2): 46119. https://doi.org/10.1103/PhysRevE.71.046119.

Holme, P. 2015. "Modern temporal network theory: A colloquium." Eur. Phys. J. B, 88(9): 558. https://doi.org/10.1140/epjb/e2015-60657-4.

Holme, P. 2016. "Temporal network structures controlling disease spreading." Physical review. E, 94(2-1): 22305. https://doi.org/10.1103/PhysRevE.94.022305.

Holme, P., and J. Saramäki. 2012. "Temporal Networks." Physics Reports, 519(3): 97–125. https://doi.org/10.1016/j.physrep.2012.03.001.

Hossain, M. M., and S. Alam. 2017. "A complex network approach towards modeling and analysis of the Australian Airport Network." Journal of Air Transport Management, 60: 1–9. https://doi.org/10.1016/j.jairtraman.2016.12.008.

Kempe, D., J. Kleinberg, and A. Kumar. 2002. "Connectivity and Inference Problems for Temporal Networks." Journal of Computer and System Sciences, 64(4): 820–842. https://doi.org/10.1006/jcss.2002.1829.

Kempe, D., J. Kleinberg, and É. Tardos. 2003. "Maximizing the spread of influence through a social network." In Proc., the ninth ACM SIGKDD international conference, edited by T. Senator, P. Domingos, C. Faloutsos, and L. Getoor: 137, New York, New York, USA. https://doi.org/10.1145/956750.956769.

Kim, H., and R. Anderson. 2012. "Temporal node centrality in complex networks." Physical review. E, Statistical, nonlinear, and soft matter physics, 85(2 Pt 2): 26107. https://doi.org/10.1103/PhysRevE.85.026107.

Kinney, R., P. Crucitti, R. Albert, and V. Latora. 2005. "Modeling cascading failures in the North American power grid." Eur. Phys. J. B, 46(1): 101–107. https://doi.org/10.1140/epjb/e2005-00237-9.

Kivela, M., A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter. 2014. "Multilayer networks." Journal of Complex Networks, 2(3): 203–271. https://doi.org/10.1093/comnet/cnu016.

LaRocca, S., J. Johansson, H. Hassel, and S. Guikema. 2015. "Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems." Risk Analysis, 35(4): 608–623. https://doi.org/10.1111/risa.12281.

Latora, V., and M. Marchiori. 2002. "Is the Boston subway a small-world network?" Physica A: Statistical Mechanics and its Applications, 314(1-4): 109–113. https://doi.org/10.1016/S0378-4371(02)01089-0.

Lazega, E., S. Wasserman, and K. Faust. 1995. "Social Network Analysis: Methods and Applications." Revue Française de Sociologie, 36(4): 781. https://doi.org/10.2307/3322457.

Lee II, E. E., J. E. Mitchell, and W. A. Wallace. 2007. "Restoration of services in interdependent infrastructure systems: A network flows approach." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(6): 1303–1317. https://doi.org/10.1109/TSMCC.2007.905859.

Li, A., S. P. Cornelius, Y.-Y. Liu, L. Wang, and A.-L. Barabási. 2017. "The fundamental advantages of temporal networks." Science, 358(6366): 1042–1046. https://doi.org/10.1126/science.aai7488.

Li, J., C. Shi, C. Chen, and L. Dueñas-Osorio. 2018. "A cascading failure model based on AC optimal power flow: Case study." Physica A: Statistical Mechanics and its Applications, 508: 313–323. https://doi.org/10.1016/j.physa.2018.05.081.

Michail, O. 2016. "An introduction to temporal graphs: An algorithmic perspective." Internet Mathematics, 12(4): 239–280. https://doi.org/10.1080/15427951.2016.1177801.

Min, H.-S. J., W. Beyeler, T. Brown, Y. J. Son, and A. T. Jones. 2007. "Toward modeling and simulation of critical national infrastructure interdependencies." IIE Transactions, 39(1): 57–71. https://doi.org/10.1080/07408170600940005.

Monsalve, M., and de la Llera, Juan Carlos. 2019. "Data-driven estimation of interdependencies and restoration of infrastructure systems." Reliability Engineering & System Safety, 181: 167–180. https://doi.org/10.1016/j.ress.2018.10.005.

Motter, A. E. 2004. "Cascade control and defense in complex networks." Physical review letters, 93(9): 98701. https://doi.org/10.1103/PhysRevLett.93.098701.

Motter, A. E., and Y.-C. Lai. 2002. "Cascade-based attacks on complex networks." Physical review. E, Statistical, nonlinear, and soft matter physics, 66(6 Pt 2): 65102. https://doi.org/10.1103/PhysRevE.66.065102.

Nardelli, P. H.J., N. Rubido, C. Wang, M. S. Baptista, C. Pomalaza-Raez, P. Cardieri, and M. Latva-aho. 2014. "Models for the modern power grid." Eur. Phys. J. Spec. Top., 223(12): 2423–2437. https://doi.org/10.1140/epjst/e2014-02219-6.

Newman, M., ed. 2010. Networks: an introduction: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199206650.001.0001.

Nicosia, V., J. Tang, C. Mascolo, M. Musolesi, G. Russo, and V. Latora. 2013. "Graph Metrics for Temporal Networks." In Temporal networks, edited by P.

Holme, and J. Saramäki: 15–40, New York: Springer. https://doi.org/10.1007/978-3-642-36461-7_2.

Nicosia, V., J. Tang, M. Musolesi, G. Russo, C. Mascolo, and V. Latora. 2012. "Components in time-varying graphs." Chaos (Woodbury, N.Y.), 22(2): 23101. https://doi.org/10.1063/1.3697996.

Nurre, S. G., B. Cavdaroglu, J. E. Mitchell, T. C. Sharkey, and W. A. Wallace. 2012. "Restoring infrastructure systems: An integrated network design and scheduling (INDS) problem." European Journal of Operational Research, 223(3): 794–806. https://doi.org/10.1016/j.ejor.2012.07.010.

Ouyang, M. 2014. "Review on modeling and simulation of interdependent critical infrastructure systems." Reliability Engineering & System Safety, 121: 43–60. https://doi.org/10.1016/j.ress.2013.06.040.

Ouyang, M., and L. Dueñas-Osorio. 2012. "Time-dependent resilience assessment and improvement of urban infrastructure systems." Chaos: An Interdisciplinary Journal of Nonlinear Science, 22(3): 33122. https://doi.org/10.1063/1.4737204.

Pagani, G. A., and M. Aiello. 2013. "The Power Grid as a complex network: A survey." Physica A: Statistical Mechanics and its Applications, 392(11): 2688–2700. https://doi.org/10.1016/j.physa.2013.01.023.

Pan, R. K., and J. Saramäki. 2011. "Path lengths, correlations, and centrality in temporal networks." Physical review. E, Statistical, nonlinear, and soft matter physics, 84(1 Pt 2): 16105. https://doi.org/10.1103/PhysRevE.84.016105.

Perelman, L., and A. Ostfeld. 2011. "Topological clustering for water distribution systems analysis." Environmental Modelling & Software, 26(7): 969–972. https://doi.org/10.1016/j.envsoft.2011.01.006.

Pfitzner, R., I. Scholtes, A. Garas, C. J. Tessone, and F. Schweitzer. 2013. "Betweenness preference: Quantifying correlations in the topological dynamics of temporal networks." Physical review letters, 110(19): 198701. https://doi.org/10.1103/PhysRevLett.110.198701.

Rinaldi, S. M., J. P. Peerenboom, and T. K. Kelly. 2001. "Identifying, understanding, and analyzing critical infrastructure interdependencies." IEEE control systems magazine, 21(6): 11–25. https://doi.org/10.1109/37.969131.

Rocha, L. E.C. 2017. "Dynamics of air transport networks: A review from a complex systems perspective." Chinese Journal of Aeronautics, 30(2): 469–478. https://doi.org/10.1016/j.cja.2016.12.029.

Rosato, V., S. Bologna, and F. Tiriticco. 2007. "Topological properties of high-voltage electrical transmission networks." Electric Power Systems Research, 77(2): 99–105. https://doi.org/10.1016/j.epsr.2005.05.013.

Sanlı, C., and R. Lambiotte. 2015. "Temporal Pattern of Communication Spike Trains in Twitter: How Often, Who Interacts with Whom?" arXiv, 1508.00540.

Saramäki, J., and E. Moro. 2015. "From seconds to months: An overview of multi-scale dynamics of mobile telephone calls." Eur. Phys. J. B, 88(6): 721. https://doi.org/10.1140/epjb/e2015-60106-6.

Sen, P., S. Dasgupta, A. Chatterjee, P. A. Sreeram, G. Mukherjee, and S. S. Manna. 2003. "Small-world properties of the Indian railway network." Physical review. E, Statistical, nonlinear, and soft matter physics, 67(3 Pt 2): 36106. https://doi.org/10.1103/PhysRevE.67.036106.

Smith, A. M., A. D. González, L. Dueñas-Osorio, and R. M. D'Souza. 2017. "Interdependent network recovery games." Risk Analysis. https://doi.org/10.1111/risa.12923.

Speidel, L., T. Takaguchi, and N. Masuda. 2015. "Community detection in directed acyclic graphs." Eur. Phys. J. B, 88(8): 97. https://doi.org/10.1140/epjb/e2015-60226-y.

Sulo, R., T. Berger-Wolf, and R. Grossman. 2010. "Meaningful selection of temporal resolution for dynamic networks." In Proc., the Eighth Workshop, edited by U. Brefeld, L. Getoor, and S. A. Macskassy, ACM conference proceedings series: 127–136, New York, N.Y. https://doi.org/10.1145/1830252.1830269.

Sun, H. J., H. Zhao, and J. J. Wu. 2008. "A robust matching model of capacity to defense cascading failure on complex networks." Physica A: Statistical Mechanics and its Applications, 387(25): 6431–6435. https://doi.org/10.1016/j.physa.2008.07.028.

Sun, X., S. Wandelt, and F. Linke. 2015. "Temporal evolution analysis of the European air transportation system: Air navigation route network and airport network." Transportmetrica B: Transport Dynamics, 3(2): 153–168. https://doi.org/10.1080/21680566.2014.960504.

Takaguchi, T., Y. Yano, and Y. Yoshida. 2016. "Coverage centralities for temporal networks." Eur. Phys. J. B, 89(2): 47. https://doi.org/10.1140/epjb/e2016-60498-7.

Tang, J., I. Leontiadis, S. Scellato, V. Nicosia, C. Mascolo, M. Musolesi, and V. Latora. 2013. "Applications of Temporal Graph Metrics to Real-World Networks." Temporal Networks. Springer, Berlin, Heidelberg: 135–159. https://doi.org/10.1007/978-3-642-36461-7_7.

Tang, J., M. Musolesi, C. Mascolo, and V. Latora. 2009. "Temporal distance metrics for social network analysis." In Proc., the 2nd ACM workshop, edited by J. Crowcroft, and B. Krishnamurthy: 31, New York, New York, USA. https://doi.org/10.1145/1592665.1592674.

Tang, J., M. Musolesi, C. Mascolo, and V. Latora. 2010a. "Characterising temporal distance and reachability in mobile and online social networks." SIGCOMM Comput. Commun. Rev., 40(1): 118. https://doi.org/10.1145/1672308.1672329.

Tang, J., M. Musolesi, C. Mascolo, V. Latora, and V. Nicosia. 2010b. "Analysing information flows and key mediators through temporal centrality metrics." In Proc., the 3rd Workshop, edited by E. Yoneki, E. Bursztein, and T. Stein: 1–6, New York, New York, USA. https://doi.org/10.1145/1852658.1852661.

Tang, J., S. Scellato, M. Musolesi, C. Mascolo, and V. Latora. 2010c. "Small-world behavior in time-varying graphs." Physical review. E, Statistical, nonlinear, and soft matter physics, 81(5 Pt 2): 55101. https://doi.org/10.1103/PhysRevE.81.055101.

Taylor, D., S. A. Myers, A. Clauset, M. A. Porter, and P. J. Mucha. 2017. Eigenvector-Based Centrality Measures for Temporal Networks <http://arxiv.org/pdf/1507.01266v3>.

Wang, J. 2013. "Mitigation strategies on scale-free networks against cascading failures." Physica A: Statistical Mechanics and its Applications, 392(9): 2257–2264. https://doi.org/10.1016/j.physa.2013.01.013.

Wang, J.-W., and L.-L. Rong. 2009. "Cascade-based attack vulnerability on the US power grid." Safety Science, 47(10): 1332–1336. https://doi.org/10.1016/j.ssci.2009.02.002.

Wang, J.-W., and L.-L. Rong. 2011. "Robustness of the western United States power grid under edge attack strategies due to cascading failures." Safety Science, 49(6): 807–812. https://doi.org/10.1016/j.ssci.2010.10.003.

Wang, Z., A. Scaglione, and R. J. Thomas. 2010. "The Node Degree Distribution in Power Grid and Its Topology Robustness under Random and Selective Node Removals." In Proc., 2010 International Conference On Communications Workshops: 1–5. https://doi.org/10.1109/ICCW.2010.5503926.

Wang, Z.-Y., J.-T. Han, and J. Zhao. 2017. "Identifying node spreading influence for tunable clustering coefficient networks." Physica A: Statistical Mechanics and its Applications, 486: 242–250. https://doi.org/10.1016/j.physa.2017.05.037.

Williams, M. J., and M. Musolesi. 2016. "Spatio-temporal networks: Reachability, centrality and robustness." Royal Society open science, 3(6): 160196. https://doi.org/10.1098/rsos.160196.

Wu, H., J. Cheng, S. Huang, Y. Ke, Y. Lu, and Y. Xu. 2014. "Path problems in temporal graphs." Proc. VLDB Endow., 7(9): 721–732. https://doi.org/10.14778/2732939.2732945.

Xu Jianhua, Fischbeck Paul S., Small Mitchell J., VanBriesen Jeanne M., and Casman Elizabeth. 2008. "Identifying Sets of Key Nodes for Placing Sensors in Dynamic Water Distribution Networks." Journal of Water Resources Planning and

Management, 134(4): 378–385. https://doi.org/10.1061/(ASCE)0733-9496(2008)134:4(378).

Xuan, B. B., A. Ferreira, and A. Jarry. 2003. "Computing shortest, fastest, and foremost journeys in dynamic networks." Int. J. Found. Comput. Sci., 14(02): 267–285. https://doi.org/10.1142/S0129054103001728.

Yang, Y., T. Nishikawa, and A. E. Motter. 2017. "Small vulnerable sets determine large network cascades in power grids." Science (New York, N.Y.), 358(6365). https://doi.org/10.1126/science.aan3184.

Yao, R., S. Huang, K. Sun, F. Liu, X. Zhang, and S. Mei. 2015. "A multi-timescale quasi-dynamic model for simulation of cascading outages." IEEE Transactions on Power Systems, 31(4): 3189–3201.

Yazdani, A., and P. Jeffrey. 2011. "Complex network analysis of water distribution systems." Chaos (Woodbury, N.Y.), 21(1): 16111. https://doi.org/10.1063/1.3540339.

Zhao, S., P. Zhao, and Y. Cui. 2017. "A network centrality measure framework for analyzing urban traffic flow: A case study of Wuhan, China." Physica A: Statistical Mechanics and its Applications, 478: 143–157. https://doi.org/10.1016/j.physa.2017.02.069.

2.10. TABLES

Table 2.1: Temporal path definition according to different studies.

Ref.	Temporal path	Definition	Application
Xuan. et al. (Xuan et al. 2003)	-Shortest journey -Foremost journey -Fastest journey	- Minimum hop count. - Earliest arrival time. - Minimum duration.	- Non specific
Tang et al. (Tang et al. 2009) Pan et al. (Pan and Saramäki 2011)	-Shortest path	- Minimum duration.	- Mobile and email networks
Wu. et al. (Wu et al. 2014)	-Shortest path -Fastest path -Earliest-arrival path -Latest-departure path	- Minimum distance. - Minimum duration. - Earliest arrival time. - Latest departure time.	- Applied to twelve real temporal networks

Table 2.2: Comparison between different approaches to calculate Closeness centrality.

Ref.	Node A	B	C	D	E	F
Pan and Saramaki (Pan and Saramäki 2011)	0.150	0.200	0.200	0.200	0.200	0.125
Kim and Anderson (Kim and Anderson 2012)	0.221	0.196	0.371	0.363	0.325	0.175

Table 2.3: Software packages for network analysis.

Software	Stand-alone software	Software package used	Features		Web-address
			Visualization	Analysis	
Cytoscape	✓		✓	✓	http://www.cytoscape.org
Gephi	✓		✓	✓	https://gephi.org
Graphviz	✓		✓		http://www.graphviz.org
Igraph		Python, R, C/C++	✓	✓	http://igraph.org
NetworKit		Python	✓	✓	https://networkit.iti.kit.edu
Networkx		Python	✓	✓	http://networkx.github.io
NodeXL		Microsoft Excel, Python	✓	✓	https://archive.codeplex.com
SNAP					http://snap.stanford.edu
Pajek	✓		✓	✓	http://mrvar.fdv.uni-lj.si/pajek/
SOCNETV	✓		✓	✓	http://socnetv.org

2.11. FIGURES

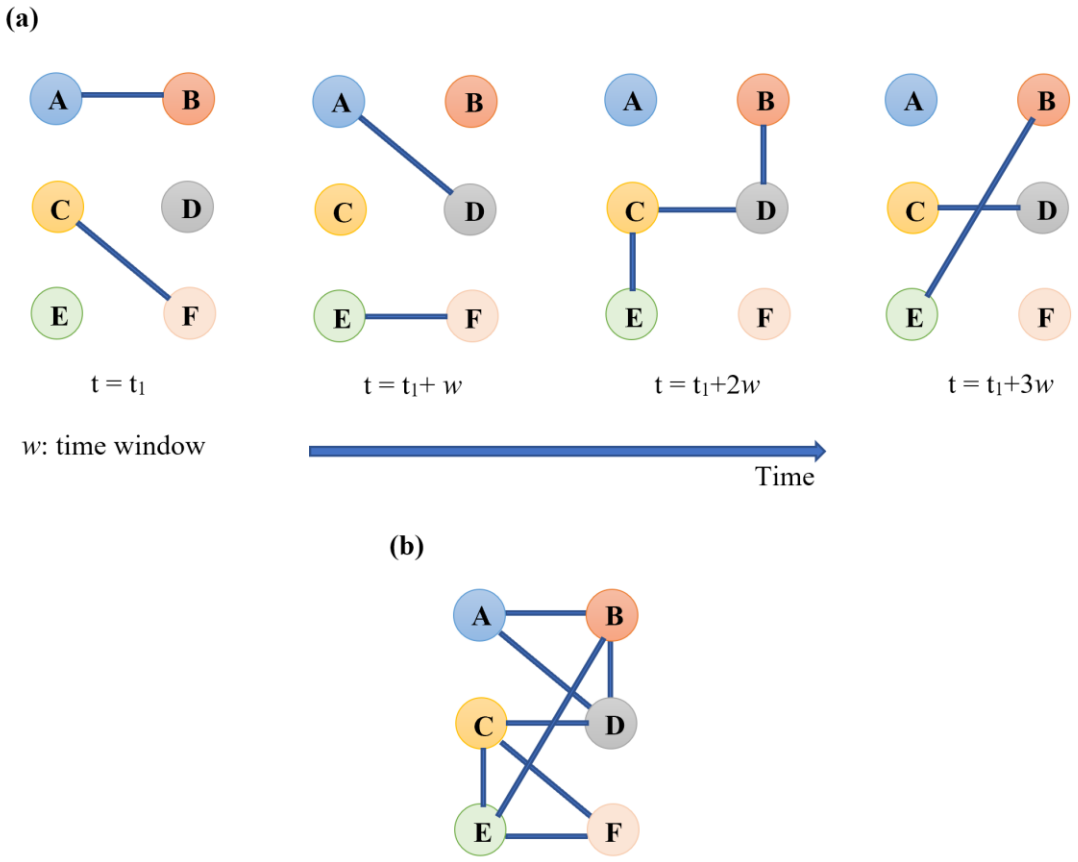

Figure 2.1: A network consists of six nodes: (a) temporal network presentation with four snapshots; and (b) static network presentation with one graph.

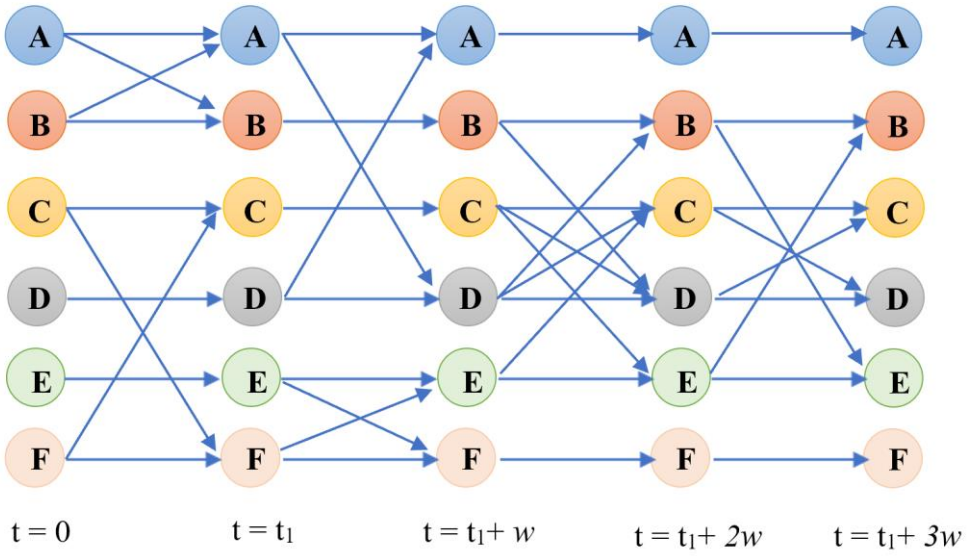

Figure 2.2: The time-ordered graph of the network presented in Figure 2.1.

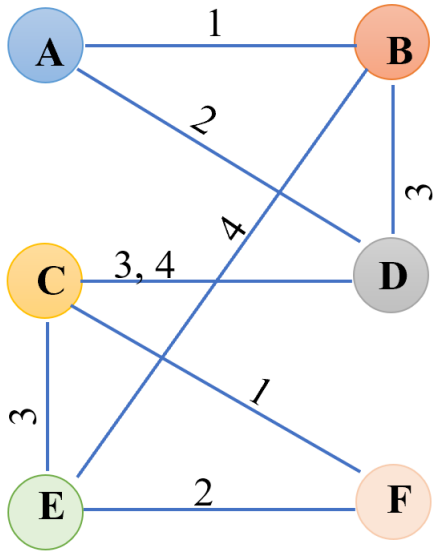

Figure 2.3: The time-labeled graph of the network presented in Figure 2.1.

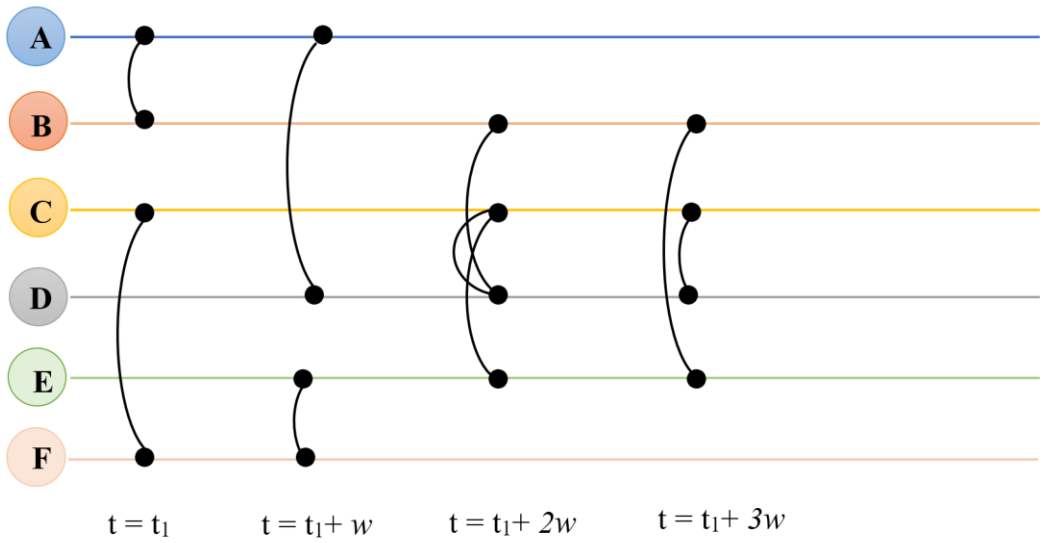

Figure 2.4: The timeline graph of the network presented in Figure 2.1.

Chapter 3 : Mixed Strategy for Resilience Enhancement of Power Grid under Cyberattack

ABSTRACT

Power infrastructure networks continue to be at risk under natural and anthropogenic hazard events. Minor disruption in key network components may lead to overloading others and subsequently triggering network-level cascade failures. Cyberattacks targeting power grids aim at magnifying the impacts of such attacks through damage propagation to other dependent infrastructure network. As such, there is a growing push to adopt 'retro' technologies (i.e., replacing some automated systems with low-tech redundancies) as a defensive strategy against cyberattacks. Such mixed (automation plus manual control) strategies seek to thwart sophisticated cyber-adversaries by strategically protecting key network components to mitigate cascade, systemic, risks. In this respect, through a complex network theoretic lens, the current study focuses on the "draw-down" phase of power infrastructure network resilience considering different centrality measures to evaluate the robustness of power grids against cyberattacks. At the network-level, the study considers two network representations for the grid based on the network's topological/connectivity (i.e., unweighted network) and the network's power flow information (i.e., weighted network). At the nodal-level, various centrality measures are considered to identify and rank key network components. In addition,

the closeness and betweenness centralities, respectively calculated based on both the shortest paths and the electric current flow, were evaluated. Finally, the study utilizes the evaluated measures to improve network robustness under cyberattacks, through considering (or not) the mixed strategy. In general, simulated cyberattacks led to the dysfunctionality of the network components that in turn led to rapid diminishing of the functional network size. Based on the analyses, network-level vulnerability is quantified considering five different scenarios (i.e., guided by either the degree, Eigenvector, PageRank, betweenness, or the closeness centralities) through evaluating two key performance metrics—Topology and Functionality indices. Subsequently, the considered grid was found to be highly vulnerable to targeted cyberattacks especially if the attackers targeted the hubs based on the current flow betweenness centrality. Nonetheless, applying the proposed mixed strategy to limit the hacker's access to the network hubs would boost the overall grid robustness.

Keywords: Centrality measures, Complex network theory, Cyberattacks, Mixed strategy, Robustness, Vulnerability analysis.

3.1. INTRODUCTION

In March 2019, hackers exploited firewall vulnerabilities to cause periodic "blind spots" for grid operators in the western US for approximately 10 hours (NERC 2019), where firewalls were facing consecutive rebooting leading to cut communication between control centers and generation sites (Sussman 2019). Subsequently, the U.S. government announced a surprise move to secure power grids through considering "retro" technologies (O'Flaherty 2019). These technologies are to limit hackers' attacks and to make it more strenuous, by adopting a mixed strategy through replacing some automated systems with low-tech redundancies (e.g., analogue and manual control technologies). As the risk of targeted cyberattacks on the critical power grid components poses a severe threat to grid operations and may cause a large-scale blackout, identifying critical power grid components is crucial to evaluate grid robustness and enhance grid resilience.

The previous studies of power infrastructure network resilience described resilience using four functions: resist, re-stabilize, rebuild, and reconfigure (Gasser et al. 2019). These functions form the core of physical resilience engineering that focuses on "draw-down" and "draw-up" behaviors (Heinimann and Hatfield 2017), as shown in Figure 3.1. The resist and re-stabilize function represent the "draw-down" phase, which focuses on the network's ability to handle the disruptive event. The "draw-down" phases can be evaluated using vulnerability analysis and

modelling of failure propagation to quantify the network robustness. On the other hand, the recovery behavior in the “draw-up” phase represents both the rebuild and reconfigure resilience functions.

The current study focuses on the "draw-down" phase of power infrastructure network by using a family of complex network theory centrality measures to evaluate the robustness of power grids against random and targeted cyberattacks, starting by identifying critical substations which have the highest impact on the network performance. Overall, the study facilitates better understanding of power grid vulnerability and provides guidance to enhance the overall grid resilience under cyberattacks using a mixed strategy.

Complex network theoretic (CNT) strategies have been providing powerful tools to understand the behavior of different real complex networks. Within a CNT context, the core components of any network are its corresponding nodes and links (Newman 2010a), whereas the nodes simulate the main components comprising the network (e.g., substations in power grid), and the links represent the interdependency between these network nodes (e.g., transmission lines in power grid). Some substations, based on their position and operation conditions, are more essential for grid operation than others, which in turn makes their continued functionality and security more imperative. In this respect, *vulnerability analysis* refers to identifying key substations and assessment of their role in the robustness of the power grid (Shahpari et al. 2019). Simulation of power grids based on CNT

strategies facilitates a better understanding of the interdependence between the components comprising this network. Subsequently, network analysis does not only demonstrate the network's topological characteristics, but should also identify its most influential nodes and links (Barabási and Pósfai 2016). Subsequently, more complex characteristics such as network robustness can be evaluated by subjecting the network to different targeted attack and random failure scenarios (Motter and Lai 2002; Wang and Rong 2009, 2011).

Several research studies have adopted CNT in analyzing power grid vulnerability (Pagani and Aiello 2013b) . A significant part of these studies focused on only the topological characteristics and the basic measures of a network, which typically ignore the directions and the magnitude of the real power flow (Albert et al. 2004; Ezzeldin and El-Dakhakhni 2019; Motter and Lai 2002; Rosato et al. 2007). Specifically, the two essential aspects of power grid vulnerability analysis are (i) the network topology: substations and their interconnections through the transmission lines; (ii) the operating conditions: governed by supply and demand distributions (Cetinay et al. 2018). Network topology is typically static in power grids, whereas network operation condition is usually dynamic and depends on how power flow is distributed over the grid (Shahpari et al. 2019). Topology-based measures could provide a potential indication of network behavior and vulnerability, albeit with such models incapable of fully simulating infrastructure behavior as governed by laws of physics and subjected to constraints pertaining to

their supply and demand capacities. Consequently, models based solely on topology could result in misleading conclusions that may not reflect the real physical behaviors of the network (Hines et al. 2010c; Salama et al. 2020).

Based on the above, the current study focuses on modeling large power grids by integrating both their topology and their operating (power flow) conditions to identify the relative importance of network components and evaluate their impact on network robustness. Next, the study evaluates the considered grid robustness to random and targeted cyberattack scenarios based on the centrality measures. Subsequently, by knowing these critical components, implementing the proposed mixed strategy aims to introduce new manual devices to isolate critical system components from cyberattack impacts. This mixed strategy was inspired from the 2015 cyberattack on Ukraine's power grid, which left most of the country without power. Ukraine's grid operators were able to quickly bypass its compromised controls by switching to manual controllers. In fact, the consequences of this attack could have been much worse if the grid has been entirely reliant on automatic control (Lee et al. 2016).

Following this Introductory section, Section 3.2 presents the considered power grid both as a simple network and a weighted network; Section 3.3 introduces different centrality measures and their extensions for the weighted network; Section 3.4 presents the distribution and correlation between the five centrality measures; Section 3.5 evaluates the network robustness to random and

targeted cyberattack scenarios based on the centrality measures; and, finally, the study summary and overall conclusions are provided in Section 3.6.

3.2. NETWORK REPRESENTATIONS OF A POWER GRID

In order to demonstrate the application of the proposed approach, the power grid supplying the Canadian province of Ontario will be considered hereafter. The Ontario power grid delivers the power to 14 million customers by coordinating about 160 TWh of annual demand and supply across 51 cities within the Province of Ontario (Ezzeldin and El-Dakhakhni 2019). This section describes the representations of the grid as a simple network and weighted network.

Table 3.1 summarizes most of the previous studies on power grid vulnerability analysis based on CNT. From these studies, it can be concluded that each power grid has its unique topology that results in a significant effect on its robustness, which requires a particular vulnerability analysis for each distinct network. Additionally, it can be observed that most published studies focused on the USA, the European, or synthetics power grids (Fang et al. 2016; Pagani and Aiello 2011; Pu and Wu 2019; Xu et al. 2014), whereas only a single study, Ezzeldin and El-Dakhakhni (2019), focused on the Ontario power grid. Nonetheless, the study by Ezzeldin and El-Dakhakhni (2019) provided only potential indications of network behavior and vulnerability, as the corresponding network model did not consider power flow data within all transmission lines

represented as unweighted undirected links. In contrast, the enhanced model in the current study simulates the power grid as a weighted network with each link is assigned with a weight and a direction according to the power flow value and direction. In addition to the unweighted and weighted centrality measures, the current flow centrality measures have been computed as explained in section 3.3. Furthermore, the Ontario power grid in the current study includes the network from low to high voltage, in contrast to the simplified model by Ezzeldin and El-Dakhakhni (2019) that considered only the high voltage transmission network (i.e., 118 to 500 kV). Furthermore, the current study develops a network robustness band against random cyberattacks, without and with mixed strategy to track the improvement in network robustness with transfer from fully automatic control to a mixed strategy.

3.2.1. POWER GRID AS A SIMPLE NETWORK

A power grid network model with undirected and unweighted links is based only on the grid topology and connectivity properties. Such simplified models does not consider the flows and physical properties of/within the network, and instead represent the underlying network in an abstract manner (Rosato et al. 2007). The power grid is simulated as a network $G(N, L)$ that consists of N nodes (e.g., substations in power networks) and L links represent the interdependencies between these nodes within such a network (e.g., transmission lines in power networks). The interconnection pattern of the network can be summarized on $N\ x\ N$ adjacency

matrix A, where $a_{ij} = 1$ if, and only if, there is a link between nodes i and j, and $a_{ij} = 0$ otherwise. The Ontario power grid was modeled as 3,653 nodes and 4,503 links, as shown in Figure 3.2.

For clarity, only the high voltage transmission network (i.e., the substations and transmission lines with a base voltage equal to 220 and 500 kV) are shown in Figure 3.3. As expected, a large cluster of stations is in proximity to the highly populated regions (e.g., the cities of Toronto and Ottawa) in the South-East of Ontario. In contrast, the Northern parts of Ontario, which is less populated, have a much fewer number of substations, as shown in Figure 3.3.

3.2.2. POWER GRID AS A WEIGHTED NETWORK

In contrast to a simple network model, the grid can also be simulated as a weighted network where to each link a weight and a direction according to the power flow value and direction are assigned. This hypothesis assumes that transmission lines that carry more flow have more influence than the lines that carry the smaller flow. It should be noted that the node connectivity in the power grid with other nodes is not only related to how many links connected to it but also related to the connection strength of each link (Wang et al. 2010a); and the power flow of each link reflects this strength. In addition, the network considers node heterogeneity where the nodes have been classified into three groups, namely: supply-station nodes “generator”, demand-station nodes “load”, and switching-station nodes “junction”, as shown in

Figure 3.4. The transmission lines have been classified into three groups: AC lines, and two- and three winding transformers. AC lines connected to two stations at the same voltage, while two and three winding transformers connected with two or three stations different voltage. In the current network, the three winding transformers are visualized as three links intersecting at one junction node, as shown in Figure 3.4.

The power flow was calculated using the Direct Current power flow model (DC power model). The DC power model is widely used as an approximation method for the Alternating Current (AC power model) to simplify power flow analysis in power networks (Bernstein et al. 2014b; Pahwa et al. 2014; Yan et al. 2015). The DC power model is used wherever repetitive and fast load flow estimations are required, whereas this method is non-iterative and absolutely convergent. The Power System Simulator for Engineering (PSSE) software (Siemens PTI 2015) has been used to compute the transmission lines power flow.

In DC power model, nonlinear equations of AC power model are simplified to a linear form based on the following assumptions (Pahwa et al. 2014):

- Line resistance is negligible compared to line reactance ($R_{ij} \ll x_{ij}$).
- The voltage profile is flat (i.e., Magnitudes of node voltages are set to 1.0 per unit).
- Voltage angle differences between nodes are small (i.e., $\sin(\delta_{ij}) = \delta_{ij}$ and $\cos(\delta_{ij}) = 1$).

As such, based on the above assumptions, the power at each node f_i is equal to all the "in" and the "out" power flows, as:

$$f_i = \sum f_{ij} = \begin{cases} S_i , & Generation\ nodes \\ -D_i , & Load\ nodes \\ 0 , & junction\ nodes \end{cases} \quad (1)$$

where, f_{ij} is the power flow for the link from node i to node j, S_i and D_i is the given power at generator and load nodes, respectively.

To calculate the power flow, the following equations are applied from Pahwa et al. (2014).

$$f_{ij} = \frac{\delta_{ij}}{x_{ij}} \quad (2)$$

where, $\delta_{ij} = (\theta_i - \theta_j)$ is the difference in the phase angle between node i and node j, and x_{ij} is the transmission line reactance. The phase angle difference δ_{ij} of a line is the phase shift between the voltage of the start node i and the end node j. The transmission line reactance is the opposition to the power flow.

Therefore, the value and direction of power flow for each transmission line f_{ij} have been assigned to the link that represent this transmission line in the network.

3.3. CENTRALITY MEASURES

Centrality measures reveal the influences of different nodes on the overall network behavior. This section presents a family of centrality measures adopted to rank the

importance of nodes. The most commonly used CNT centrality measures were examined to provide a comprehensive comparison and to cover all different centrality measures employed in previous studies, as shown in Table 3.1. Although the classical centrality measures are based solely on topological information (i.e., simple network), it is beneficial to extend these measures by including the link weight information and the power flow calculations (i.e., simulating a weighted network). This section summarizes five topological centrality measures and explains their extensions to consider the power flow.

3.3.1. DEGREE CENTRALITY

One of the key measures to identify node importance is its degree centrality. The degree centrality of a node is the total number of links connected directly to this node, as shown in Eq. 3.

$$D(i) = \sum_{j}^{N} a_{ij} \qquad (3)$$

According to the degree centrality, the node with the highest degree is the most central node (i.e., hub) (Barabási and Pósfai 2016). Figure 3.5 illustrates the degree centrality distribution of the Ontario power grid, where the $D(i)$ values vary between $D(i) = 1$ and $D(i) = 22$, which are the degree centrality of the least and most connected nodes, respectively. Most of the network nodes (≈92%) have low

degree centrality values (i.e., ≤ 3), while the few remaining nodes are the degree hubs (i.e., high degree nodes).

The degree centrality has been extended to sum the weights of links connected directly to the node (Opsahl et al. 2010), as presented in Eq. 4. Therefore, a large value of weighted degree centrality $D(i)^w$ corresponds to larger values of power flow reaching node, which indicates a good connection between node and its neighboring nodes.

$$D(i)^w = \sum_{j}^{N} f_{ij} * a_{ij} \qquad (4)$$

3.3.2. EIGENVECTOR CENTRALITY

Based on the idea that a node is more central if it is connected with other central nodes (Ruhnau 2000), the Eigenvector centrality of a node not only depends on the number of its adjacent nodes, but also on the centrality of the adjacent nodes. Therefore, Bonacich (1987) defines the Eigenvector centrality $E(i)$ of a node i as positive multiple of the sum of adjacent centralities, as shown in Eq. 5.

$$E(i) = \frac{1}{\lambda_{max}} \sum_{j}^{N} a_{ij}\ E(j) \qquad (5)$$

This equation can be written in matrix form as $A\,E = \lambda\,E$. Accordingly, the E is equal to the eigenvector of the maximal eigenvalue λ_{max} of the adjacency matrix A.

The weighted Eigenvector centrality is influenced by the power flow of all transmission lines connected to its neighbors, their neighbors and so on. Therefore, the weighted Eigenvector centrality $E(i)^W$ is equal to the i^{th} component of the eigenvector corresponding to the largest eigenvalue λ_{max_w} of the weighted adjacency matrix A_w , as shown in Eq. 6.

$$E(i)^W = \frac{1}{\lambda_{max_w}} \sum_{j}^{N} a_{ij_w} \; E(j)^w \qquad (6)$$

3.3.3. PAGERANK CENTRALITY

The PageRank centrality is an algorithm used originally by the Google search system to rank web pages (Brin and Page 1998). The essence of the PageRank algorithm is that the rank of a node is high if this node is linked from a high-ranked node. Li et al. (2014) provided a method to evaluate the importance of power grid nodes based on the PageRank algorithm by comparing the similarities between the internet and power grid topology. In the power grid, PageRank centrality estimated the importance of each (sub)station given the importance of substations connected to it and their output lines. The iterative formula of the PageRank algorithm is defined as follows:

$$PR(i) = (1 - d) + d \sum_{j \in N_i} \frac{PR(j)}{L(j)} \qquad (7)$$

where, d is a damping factor which can be set between 0 and 1. It is usually set to

0.85 (Li et al. 2014). $L(j)$ is defined as the number of out links from node j. N_i are set of nodes that have at least one directed link to node i.

For the weight PageRank $PR(i)^W$, the number of out links $L(j)$ in the formula will be altered by the total out power flow f_{jout} from node j.

$$PR(i)^W = (1-d) + d \sum_{j \in N_i} \frac{PR(j)^W}{f_{jout}} \qquad (8)$$

3.3.4. BETWEENNESS CENTRALITY

The betweenness centrality measure is one of the most widely used measures to indicate the node importance. This measure identifies nodes that play a central role between other nodes in the network (Opsahl et al. 2010). The betweenness centrality measure of node i is calculated as the number of shortest paths between pairs of other nodes that pass through node i (Freeman 1977; Opsahl et al. 2010), as presented in Eq. 9.

To extend the definition of betweenness centrality to nodes in a weighted power grid network, the formula has been modified by considering the weighted shortest path (i.e., each link weight by $1/f_{ij}$), as presented in Eq. 10. This hypothesis assumed that the shortest path is not only related to the number of links but also how much power flow is passing through that path.

$$B(i) = \frac{\sum_{i \neq j \neq k} \sigma_{jk}(i)}{\sum_{i \neq j \neq k} \sigma_{jk}} \quad (9)$$

$$B(i)^W = \frac{\sum_{i \neq j \neq k} \sigma_{jk}(i)^W}{\sum_{i \neq j \neq k} \sigma_{jk}{}^W} \quad (10)$$

where, $\sigma_{jk}(i)$ is the total number of shortest paths between nodes *j* and *k* that passes through node *i*; σ_{jk} is the total number of shortest paths between nodes *j* and *k*; and $\sigma_{jk}(i)^W$ and $\sigma_{jk}{}^W$ are calculated considering the weighted shortest paths.

In general, unweighted and weighted betweenness centralities assume that the power flow passes through the nodes via the unweighted and weighted shortest paths, respectively. Nonetheless, these shortest paths-based centrality measures ignore the power flow splitting among different paths when the current flow transfer from supply to demand node. In this respect, the *"current flow betweenness centrality"* addresses the node importance by considering Kirchhoff's and Ohm's laws (Brandes and Daniel 2005; Cetinay et al. 2018). The current flow betweenness centrality $B(i)^{CF}$ can be evaluated as total flow passing through a node when a unit current flow transfers from a supply node to a demand node over all possible supply-demand pairs, as shown in Eq.11.

$$B(i)^{CF} = \frac{\sum_{s \neq d} f_i^{(s \to d)}}{0.5\,(N-1)\,(N-2)} \qquad for\ all\ (s \to d) \in N \qquad (11)$$

where, $f_i^{(s \to d)}$ is the power flow passing through node i when a unit current flow is injected at a supply node s and extracted from a demand node d. And, N is the total number of network nodes.

3.3.5. CLOSENESS CENTRALITY

The closeness centrality measures how close a node is to other nodes in the same network. The closeness centrality of a node is evaluated as the inverse of the average distances from this node to all other nodes (Freeman 1978), can be expressed as

$$C(i) = \frac{1}{N-1}\sum_{j}^{N}\frac{1}{S_{ij}} \qquad (12)$$

where the distance S_{ij} is the number of links in the shortest path that connects nodes *i* and *j*. To adapt the definition of closeness centrality to nodes in a weighted power grid, the weighted distance ${S_{ij}}^{W}$ is defined as the sum of links weight (i.e., each link weight by $1/f_{ij}$) in the weighted shortest path that connects nodes *i* and *j*. The weighted distance depends not only on the shortest path, but also on how much power flows through this path. Therefore, the corresponding weighted closeness centrality can be calculated as follows:

$$C(i)^W = \frac{1}{N-1}\sum_{j}^{N}\frac{1}{S_{ij}{}^W} \quad (13)$$

The two previous closeness centrality measures are calculated based on the shortest path (considering unweighted or weighted links). However, the current flow closeness centrality is calculated using alternative distances based on the effective resistance (Brandes and Daniel 2005; Cetinay et al. 2016), defined as the voltage difference between node i and node j, when the power is injected at node i and extracted from node j. The effective resistance were calculated by the algorithm proposed in Brandes and Daniel (2005). Therefore, the current flow closeness centrality $C(i)^{CF}$ of node i is calculated as the reciprocal of the summation of effective resistance from node *i* to all other nodes in the network, as shown in Eq.14.

$$C(i)^{CF} = \frac{N-1}{\sum_j V_i{}^{(i\to j)} - V_j{}^{(i\to j)}} \quad (14)$$

where, $V_i{}^{(i\to j)}$ is the voltage of node i when the power is injected at node i and extracted from node j.

Finally, Table 3.2 summarizes the different centrality measures used in the current study for both cases: simple and weighted network model.

3.4. GRID COMPONENT CENTRALITY-BASED RANKING

Different centrality measures have been used to rank the relative importance of stations in the power grid. For better comparison, all the mentioned centrality

measures in the previous section are normalized to ensure that the largest value equals to 1, while the smallest value equals to 0, as presented in Eq. 15.

$$Normalized\ Centrality(i) = \frac{Centrality(i) - Min\ Centrality}{Max\ Centrality - Min\ Centrality} \qquad (15)$$

Figure 3.6 and Figure 3.7 present the distribution and correlation between the five centrality measures in both cases: unweighted and weighted network. It can be observed that for most centrality distributions, the majority of nodes have low centrality values whereas only a few nodes (i.e., the hubs) have high values—potentially impacting network performance the most (Barabási and Pósfai 2016). Conversely, failure of nodes with low centrality values may cause negligible reduction to the network due to the limited node failure extent (cascade) following the former's failures. It should however be noted that, closeness and current flow closeness centralities have different distribution patterns from that of the remaining centralities. This discrepancy is attributed to the fundamental difference between the closeness and other centralities measures, whereas the closeness centrality ranks each node based on its relationship to all other nodes in the network (i.e., distance from the node to all network nodes), while other centralities rank each node based on its relation to its neighbor nodes (i.e., directly connected nodes) (Golbeck 2013). As such, the difference between the highest closeness centrality nodes and average closeness centrality nodes reflects the distance from the node to its nearest higher closeness centrality. For example, in Figure 3.8, node 1 has higher closeness

centrality than that of node 2, however, the main difference between the two nodes in calculating the closeness centrality is the distance from node 2 to node 1. Subsequently, the node closeness centrality values will be in close to each other and this in turn will result in the distribution pattern in Figure 3.6 and Figure 3.7.

In addition, a weak, and sometimes even a negative correlation between different centrality measures can be observed, whereas each measure ranks the network nodes depending on different approaches, as explained in the previous section. For example, a node with a high degree centrality may not necessarily possess a high closeness, betweenness, or eigenvector centrality. Nonetheless, there is a good correlation between the degree and PageRank centrality as shown in Figure 3.6. This can be explained by examining the formula of the PageRank centrality presented in section 3.3. The PageRank node centrality considers three factors: (i) the number of the adjacent nodes connected to the node; (ii) the link propensity of the adjacent nodes; and (iii) the centrality of the adjacent nodes (Hansen et al. 2020). The first factor reflects the fact that the more links a node attracts, the more important it is perceived. The second factor indicates that the value of the link depreciates proportionally to the number of links given out by the adjacent nodes (i.e., the links coming from low degree nodes are worthier than those emanated by high degree ones). Finally, the third factor reflects that fact that links from central nodes are more valuable than those from peripheral ones. The first factor is directly related to the node degree centrality which resulted in the high

correlation between the degree and PageRank centralities. However, in the case of weighted network, there is a poor correlation between these two centralities. This is because the degree weighted centrality depends on how much flow reaches a node, whereas PageRank depends on the number of the adjacent nodes connected to the node and the total power flowing out of the adjacent nodes.

In addition, it can be observed in Figure 3.9 that nodes with high unweighted betweenness centrality value $B(i)$ are not the same nodes with high weighted betweenness centrality value $B(i)^w$. Therefore, the two measures are uncorrelated, which indicates the sensitivity of the centrality measures to the weight and direction of the links. To quantify centrality, which represents the most critical nodes in the network, the network is *stress tested* by removing the nodes by descending order according to different centrality measures (i.e., targeted cyberattacks based on nodes centrality).

3.5. ROBUSTNESS ASSESSMENT

The network robustness against cyberattacks can be assessed through the performance of the network due to the failure of some nodes randomly (i.e., random cyberattack) or systematically (i.e., targeted cyberattack) (Cetinay et al. 2018). In this section, first, two performance indices have been introduced to quantify both the topology and service loss as a result of components removal. Second, a comparison between the effect of different targeted cyberattack scenarios based on

the previously described centrality measures has been discussed.

3.5.1. PERFORMANCE INDICES

The removal of critical nodes from the network can split the grid into isolated islands (i.e., disconnected sub-grids). The size and the total power flow of the giant component are the two performance indices that have been used to evaluate both the topological and functional characterization of the network. The giant component is the connected component that contains the largest set of nodes (Barabási and Pósfai 2016).

3.5.1.1 TOPOLOGY INDEX

Performance index based on the topology P_t can be calculated as the percentage of the number of the nodes in the giant component N_G with respect to the total number of nodes N, as presented in Eq.16.

$$P_t = \frac{N_G}{N} \tag{16}$$

A network with high P_t value indicates that most of its nodes are fully connected through a giant component, where the failure of some components does not result in a major impact on the network performance. In contrast, a low value of P_t indicates that the failure of some components divided the network into separate sub-grids and impacted the entire network performance.

3.5.1.2 FUNCTIONALITY INDEX

Performance index based on the functionality P_f can be calculated as the ratio between the summation of the power flow carried by links to the giant component and the summation of the power flow of the network at the initial status (i.e., the stability of the power grid prior to failure), as presented in Eq. 17. Therefore, this performance index not only considers the size of the giant component but also the power flow which indicates the grid demands and supplies.

$$P_f = \frac{\sum_{l \in L_G} f_l}{\sum_{l \in L} f_l} \quad (17)$$

where, f is the power flow of link l, L is the set of network links at the initial status, and L_G is the set of links in the giant component.

3.5.2. RANDOM CYBERATTACKS

The random cyberattacks failure represents the hackers' random attacks to the stations in the grid. This scenario has been used to evaluate the improvement in network robustness with transfer from being under full automatic control (i.e., random cyberattack for any nodes in the network) to being only partially automatically controlled (i.e., excluded some nodes from random cyberattack selection set). The second case represents the grid with the mixed strategy adopted to systematically isolate the critical stations to limit hackers' access.

Four random sample sizes have been used to compute the average random failure scenario (i.e., run the random failure for 10, 20, 50, and 100 scenarios).

Figure 3.10 presents the average result of the four random sample sizes. The Kolmogorov-Smirnov Test (KS Test) (Conover 1998) was used to compare between the average result of the four sample sizes to select the appropriate one. KS Test computes the max of difference between the cumulative distribution function of two sample sizes, as presented in Eq. 18.

$$D_{n,m} = max|F(x) - G(x)| \quad (18)$$

where, the first sample has size m with a cumulative distribution function of $F(x)$ and that the second sample has size n with a cumulative distribution function of $G(x)$. The null hypothesis is rejected at level 0.05 if $D_{n,m} > D_{n,m,\propto}$. The null hypothesis is that the curves of the two samples are similar.

$$D_{n,m,\propto} = 1.36 * \sqrt{\frac{m+n}{mn}} \quad (19)$$

Table 3.3 summaries the KS test results. The average results of sample size 10, 20, and 50 have been compared to average result of sample size 100 (i.e., n = 10,50, or 50 while m = 100). The null hypothesis is accepted for same size 20 where $P - value > 0.05$ and $D_{n,m} < D_{n,m,\propto}$. It was concluded that that there is no significant difference between the average results of sample size 20, 50, and 100 (i.e., the difference is less than 5%). Therefore, the average of 20 random failure scenarios was found to be statistically adequate to provide a good representation for the random failure behavior of the grid. Subsequently, a total of 20 random

attacks were considered and the average value is used hereafter to compare network robustness considering (or not) the mixed strategy.

3.5.2.1 RANDOM CYBERATTACKS WITHOUT MIXED STRATEGY

Figure 3.11 shows the performance indices of the grid under random failure based on 20 different scenarios. It can be noticed that following random removal of about 25% of the nodes, the grid is divided into numerous isolated islands and almost lost its functionality. As shown in these figures, to account for the variability, the network robustness can be represented as a *band*. For example, after removing 15% of the network nodes, the topology index P_t ranges from 0.05 to 0.60 with an average value of 0.33, while the functionality index P_f is in the range from 0.63 to 0.17 with an average value of 0.45.

3.5.2.2 RANDOM CYBERATTACKS CONSIDERING MIXED STRATEGY

The grid robustness can be significantly enhanced by protecting the critical network components against random cyberattacks. In this respect, the simulation of the grid under the random cyberattacks has been modified by excluding some key nodes from the random removal set. These excepted nodes represent the substations protected from random cyberattacks by systemic isolation from automatic control (i.e., mixed strategy). The protected nodes have been selected based on their

centrality values (i.e., the highest weighted degree or current flow betweenness centrality). These two centrality measures have been chosen because they are the most effective centralities to identify the key network nodes for the grid as would explain in the discussion section later.

Figure 3.12 presents the grid robustness against random cyberattacks considering (or not) the mixed strategy. The figure tracks the improvement in network robustness through systemic isolation of the critical network substations from automatic control. It can be inferred that there is a significant enhancement to the grid robustness especially in terms of protecting the top 20 current flow betweenness hubs. Furthermore, Figure 3.12 (right) illustrates the enhancement of network robustness measured by the topology index based on the current flow centralities with different numbers of protected nodes Np. As expected, with increased Np, the network robustness continues to be enhanced. For example, after removing 15% of the network nodes, the topology index P_t rises from 0.33 in case of random failure without any protected nodes to 0.48, 0.53, and 0.57 for cases of protected the top 20, 50, and 100 current flow betweenness hubs, respectively. Regarding the functionality index, it can be observed from Figure 3.13 that there is a similar improvement in grid robustness when considering node protection based on the current flow betweenness hubs; however, there is no signification change considering the top 20 weighted degree hub protections. Overall, protecting the

network hubs from random attacks has a considerable effect in boosting the grid robustness.

Random Cyberattacks Robustness Algorithm:

Input: Network N nodes, L links, f_l Link weight
Output: Fraction of the removed nodes k, Topology index P_t, Functionality index P_f

Start
Build Network: $G(N, L)$
Calculate the sum of weight links: $Int.F = \sum_{l \in L} f_l$
  While ($P_t > 0$ & $P_f > 0$)
    $N_i \in N$; N_i Randomly select Node i
    Delete the selected node: G = delete_vertices (G, N_i)
    Calculate the network clusters: G.components = clusters (G)
    Select the Giant connected component: Cluster that contains the largest set of nodes
    Calculate the number of nodes in Giant component
    Calculate the Topology index: $P_t(k) = \frac{N_G}{N}$ (Eqn.16)
    Calculate the sum of weight links in the Giant component: $Step.F = \sum_{l \in L_G} f_l$
    Calculate the Functionality index: $P_f(k) = \frac{Step.F}{Int.F} = \frac{\sum_{l \in L_G} f_l}{\sum_{l \in L} f_l}$ (Eqn.17)
    $k = (k+1)/N$
  End While
Return $P_t(k)$; $P_f(k)$
End

3.5.3. TARGETED CYBERATTACKS

A targeted cyberattack represents the hacker's intentional attacks to the high centrality stations in the grid. Different cyberattack scenarios have been used to assess the network robustness and provide a comparison between different centrality measures. Both unweighted and weighted centrality measures have been applied as node attack scenarios for the power grid. For each centrality measure,

the network has been exposed to a stress test by sequentially removing the nodes according to the descending order of their centrality value. After each node removal, the two performance indices have been calculated to evaluate the grid robustness. The current study focuses on the instant impact of node removal on the topology and function of the grid without consideration of the cascade failure effect (i.e., the failure of overloaded transmission lines due to power flow redistribution).

Figure 3.14 and Figure 3.15 present the robustness of the network with sequentially removing the nodes (i.e., targeting nodes with the highest centrality measure). It is observed that the Eigenvector centrality in both the weighted and unweighted network cases is the least effective attack scenarios. In other words, targeted cyberattacks according to eigenvector centrality disrupts the network slower than the other attack scenarios. Conversely, the network is vulnerable to the targeted cyberattacks based on the degree, PageRank or betweenness centrality, which can maximize the network separation into isolated islands and disrupt its functioning. For example, in Figure 3.14 (left), after removing 1% of the network nodes, the topology performance index P_t is 0.85, 0.20, 0.16, and 0.25 for targeted cyberattacks based on eigenvector $E(i)$, degree $D(i)$, PageRank $PR(i)$, and betweenness $B(i)$ centrality, respectively. Also, in Figure 3.14 (right), after removing 1% of the network nodes, the topology performance index P_t is 0.73, 0.30, 0.05, and 0.24 for targeted cyberattacks based on weighted eigenvector $E(i)^w$, weighted degree $D(i)^w$, weighted PageRank $PR(i)^w$, and betweenness

$B(i)^w$ centrality, respectively. Furthermore, it is worth to mention that the current flow betweenness centrality is the most effective cyberattack scenario. As can be inferred from Figure 3.14 and Figure 3.15, cyberattacks based on the current flow betweenness centrality is the first attack scenario that results in zero topology and functional index. In other words, by only removing 1% of the network nodes, based on their current flow betweenness centrality, the network is fully disrupted.

In addition, from Figure 3.14 and Figure 3.15, it can be observed that the three targeted cyberattack scenarios (degree, PageRank, and betweenness) are analogical in the case of the unweighted network, while they are distinguished in the case of the weighted network. The simplification considering unweighted network (i.e., neglection the link weight and direction) may result in misleading interpretation of network behaviors. Furthermore, the trend similarity between the attacks based on the degree and PageRank centrality is attributed to the high correlation between these both centralities in case of unweighted network. For the target cyberattacks based on the closeness centrality, it can be observed that the network is slightly robust when removing fewer nodes, but suddenly the robustness diminished rapidly with the increase of the nodes removals. For example, the topology performance index P_t dropped from 0.99 to 0.5 when the fraction of the removed nodes changes from 0.47% to 0.49% in the case of the unweighted network, and dropped from 0.77 to 0.55 when the fraction of the removed nodes changes from 0.9% to 1.0% in the case of the weighted network. These performance

drops indicate how a node -even if not the highest centrality node- becomes critical and highly effective in network performance, since its failure impacts almost the entire network. Identifying these critical nodes in real-time is quite an important task to avoid the failure propagation through the network.

Targeted Cyberattacks Robustness Algorithm:

Input: Network N nodes, L links, f_l Link weight
Output: Fraction of the removed nodes k, Topology index P_t, Functionality index P_f

Start
Build Network: $G(N, L)$
Calculate the sum of weight links: $Int.F = \sum_{l \in L} f_l$
Calculate the centrality based on equations in section 3.3.
  While ($P_t > 0$ & $P_f > 0$)
    $N_i \in N$; N_i select Node i with the highest centrality value
    Delete the selected node: G = delete_vertices (G, N_i)
    Calculate the network clusters: G.components = clusters (G)
    Select the Giant connected component: Cluster that contains the largest set of nodes
    Calculate the number of nodes in Giant component
    Calculate the Topology index: $P_t(k) = \frac{N_G}{N}$ (Eqn.16)
    Calculate the sum of weight links in the Giant component: $Step.F = \sum_{l \in L_G} f_l$
    Calculate the Functionality index: $P_f(k) = \frac{Step.F}{Int.F} = \frac{\sum_{l \in L_G} f_l}{\sum_{l \in L} f_l}$ (Eqn.17)
    $k = (k+1)/N$
  End While
Return $P_t(k)$; $P_f(k)$
End

3.5.4. DISCUSSION

In order to present a clear comparison between the different targeted cyberattack scenarios, the average of the topology and the functional performance indices have been calculated by normalizing the sum of the size and the flow of the giant component over successive targeted cyberattacks. Therefore, the average topology performance index $P_t{}'$ can be calculated as follows:

$$P_t{}' = \frac{\sum_M P_t(M)}{M} \qquad (20)$$

where, $P_t(M)$ is the topology performance index after M successive attacks. Similarly, the average functional performance index $P_f{}'$ can be calculated as follows:

$$P_f{}' = \frac{\sum_M P_f(M)}{M} \qquad (21)$$

Therefore, the average topology $P_t{}'$ and functional $P_f{}'$ performance indices are estimated between 0 and 1. High robust networks, where its robustness to the targeted cyberattacks and the node removals have a slight effect on its performance, show values close to 1. On the other side, a low average performance value indicates a destructive cyberattack scenario, whereas, after a few successive node removals, the network performance is highly negatively affected. Figure 3.16 presents the average topology and functional performance indices for the grid following five cyberattack scenarios for the unweighted and weighted network. It

can be observed that the targeted cyberattacks based on degree and current flow betweenness centrality are the most destructive attack scenarios which destroy the network faster than other cyberattack scenarios. Furthermore, Figure 3.16 shows the attack scenario based on the current flow betweenness have the lowest average topology index and second least average functional index.

The main observations from evaluating the grid robustness to targeted cyberattack scenarios, based on considered different centrality measures, can be summarized as follows:

- The node degree centrality focuses directly on the local connectivity with its neighboring nodes, with the weighted degree centrality extending it by considering the coupled strength of the links. Nonetheless, these centralities reflect the local network topology, removing degree hubs nodes have a large global effect in the overall network performance. For example, the results of the grid robustness analysis illustrated that targeting nodes based on the degree and weighted degree are one of the most destructive cyberattack scenarios.
- The Eigenvector centrality in both unweighted and weighted network is not successful to identify the key nodes in comparison with the other four presented centrality measures. On the other hand, the targeted cyberattacks based on the Eigenvector centrality and the weighted eigenvector centrality are the least destructive cyberattack scenarios.

- The PageRank centrality and the betweenness centrality measures generally come at the second place after degree centrality and current flow betweenness centrality to identify the most critical nodes in the grid, and thus, removing nodes based on these centralities seems to destroy the network faster than targeted cyberattack scenarios based on closeness or Eigenvector centrality measures.
- Depending on the number of hops, the betweenness and the closeness centralities rank node importance. The number of hops may not discriminate the peripherical nodes, or nodes with high load but with low number of shortest paths. However, in case of weighted network, these centralities consider the weighted shortest path according to power flow not the minimum hops, which reflects the physical properties of the network.
- The current flow betweenness calculated the importance of the node based on the power flow passing through it. Therefore, it addressed the limitations related the shortest paths-based centrality such as ignoring the power flow splitting among different paths and not discriminating the peripherical nodes. The results concluded that targeted cyberattack based on the current flow betweenness centrality is the most destructive attack scenarios which destroy the network faster than other cyberattack scenarios.

Overall, the centrality measures provide an effective and quick indication to rank the importance of the substations. Subsequently, identifying the critical

substations in advance can support the power grid operator to improve the grid robustness by upgrading, protecting, and monitoring the vulnerable substations and applying the mixed strategy to limit the hacker's access to key network substations.

3.6. CONCLUSION

The study focused on using complex network theory to analyze the robustness and evaluate the vulnerability of the considered grid to different cyberattack scenarios. In this respect, two different network models have been presented: a simple and weighted network. Subsequently, based on these network models, a family of centrality measures has been calculated to recognize the key network components. The basic centrality measures focused only on the topology, while the weighted centrality measures consider the operating conditions of the grid such as the power flow allocation for each transmission line according to the DC power flow model. Therefore, two performance indices have been introduced to quantify the grid robustness by removing the nodes sequentially based on their centrality values. The robustness of the grid has been evaluated for both random and targeted cyberattacks. For random cyberattacks, it can be noticed that applying the proposed mixed strategy by limit the hacker's access to only 20 current flow betweenness hubs boost the grid robustness about one and half time compared to random cyberattacks without mixed strategy. For targeted cyberattacks, it can be concluded that the grid considered is highly vulnerable to targeted cyberattacks, whereas in

the current simulation, the topology and the functional performance indices are almost zeros (i.e., the network is completely disrupted) by removing 1% of the network nodes according to their current flow betweenness centrality value. Overall, understanding the criticality of different network components will provide insights to design and maintain a resilient power network against cyberattacks, and support policymakers and regulators in making informed decisions pertaining to the tolerable degree of risk and constrained by allocated financial resources.

Future studies would extend the current study to include the cascade failure propagation due to power overload by considering the power flow redistributions and the components capacity. Therefore, building a high-fidelity physics-based cascade failure model which considers the actual power flow, the transmission lines' electrical properties, and the generators' supply and capacity is a promising direction for the future work extension. Such model is expected to provide risk mitigation strategy and corrective action to suppress the cascade failure propagation. Subsequently, future studies should cover others resilience metrics (i.e., Rebuild and Reconfigure) to address the "draw-up" resilience phase.

3.7. ACKNOWLEDGMENT

This research was supported by the Canadian Nuclear Energy Infrastructure Resilience under Systemic Risk (CaNRisk) – Collaborative Research and Training Experience (CREATE) program of the Natural Science and Engineering Research

Council (NSERC) of Canada. Additional support through the INTERFACE Institute and the INViSiONLab of McMaster University is acknowledged.

3.8. REFERENCE

Albert, R., I. Albert, and G. L. Nakarado. 2004. "Structural vulnerability of the North American power grid." Physical review E, 69(2): 25103. https://doi.org/10.1103/PhysRevE.69.025103.

Barabási, A.-L., and M. Pósfai. 2016. Network science, Cambridge United Kingdom: Cambridge University Press.

Berkeley III, A. R., W. Mike, and C. Constellation. 2010. "A framework for establishing critical infrastructure resilience goals.", Final Report and Recommendations by the Council, National Infrastructure Advisory Council.

Bernstein, A., D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman. 2014. "Power Grid Vulnerability to Geographically Correlated Failures - Analysis and Control Implications." In Proc., IEEE INFOCOM 2014 - IEEE Conference on Computer Communications: 2634–2642. https://doi.org/10.1109/INFOCOM.2014.6848211.

Bonacich, P. 1987. "Power and centrality: A family of measures." American journal of sociology, 92(5): 1170–1182. https://doi.org/10.1086/228631.

Brandes, U., and F. Daniel. 2005. "Centrality measures based on current flow." In Annual symposium on theoretical aspects of computer science: 533–544: Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-31856-9_44.

Brin, S., and L. Page. 1998. "The anatomy of a large-scale hypertextual web search engine.". https://doi.org/10.1016/S0169-7552(98)00110-X.

Cetinay, H., K. Devriendt, and P. van Mieghem. 2018. "Nodal vulnerability to targeted attacks in power grids." Applied network science, 3(1): 34. https://doi.org/10.1007/s41109-018-0089-9.

Cetinay, H., F. A. Kuipers, and P. van Mieghem. 2016. "A topological investigation of power flow." IEEE Systems Journal, 12(3): 2524–2532. https://doi.org/10.1109/JSYST.2016.2573851.

Conover, W. J. 1998. Practical nonparametric statistics: Chapter 6: Statistics of the Kolmogorov-Smirnov Type: John Wiley & Sons.

Ezzeldin, M., and W. E. El-Dakhakhni. 2019. "Robustness of Ontario power network under systemic risks." Sustainable and Resilient Infrastructure: 1–20. https://doi.org/10.1080/23789689.2019.1666340.

Fang, J., C. Su, Z. Chen, H. Sun, and P. Lund. 2016. "Power system structural vulnerability assessment based on an improved maximum flow approach." IEEE

Transactions on Smart Grid, 9(2): 777–785. https://doi.org/10.1109/TSG.2016.2565619.

Freeman, L. C. 1977. "A Set of Measures of Centrality Based on Betweenness." Sociometry, 40(1): 35. https://doi.org/10.2307/3033543.

Freeman, L. C. 1978. "Centrality in social networks conceptual clarification." Social Networks, 1(3): 215–239. https://doi.org/10.1016/0378-8733(78)90021-7.

Gasser, P., P. Lustenberger, M. Cinelli, W. Kim, M. Spada, P. Burgherr, S. Hirschberg, B. Stojadinovic, and T. Y. Sun. 2019. "A review on resilience assessment of energy systems." Sustainable and Resilient Infrastructure: 1–27. https://doi.org/10.1080/23789689.2019.1610600.

Golbeck, J. 2013. "Network Structure and Measures." In Analyzing the Social Web: 25–44: Elsevier. https://doi.org/10.1016/B978-0-12-405531-5.00003-1.

Hansen, D. L., B. Shneiderman, M. A. Smith, and I. Himelboim. 2020. "Calculating and visualizing network metrics." In Analyzing Social Media Networks with NodeXL: 79–94: Elsevier. https://doi.org/10.1016/B978-0-12-817756-3.00006-6.

Heinimann, H. R., and K. Hatfield. 2017. "Infrastructure resilience assessment, management and governance–state and perspectives." In Resilience and risk: 147–187: Springer.

Hines, P., E. Cotilla-Sanchez, and S. Blumsack. 2010. "Do topological models provide good information about electricity infrastructure vulnerability?" Chaos: An Interdisciplinary Journal of Nonlinear Science, 20(3): 33122. https://doi.org/10.1063/1.3489887.

Lee, R.M., M.J. Assante, and T. Conway. 2016. "Analysis of the cyber attack on the Ukrainian power grid." SANS Industrial Control Systems, Washington, DC, USA, Tech. Rep.,

Li, C., W. Liu, Y. Cao, H. Chen, B. Fang, W. Zhang, and H. Shi. 2014. "Method for evaluating the importance of power grid nodes based on PageRank algorithm." IET Generation, Transmission & Distribution, 8(11): 1843–1847. https://doi.org/10.1049/iet-gtd.2014.0051.

Motter, A. E., and Y.-C. Lai. 2002. "Cascade-based attacks on complex networks." Physical review. E, Statistical, nonlinear, and soft matter physics, 66(6 Pt 2): 65102. https://doi.org/10.1103/PhysRevE.66.065102.

NERC. 2019. "Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities.", North American Electric Reliability Corporation <https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf>.

Newman, M., ed. 2010. Networks: an introduction: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199206650.001.0001.

O'Flaherty, K. 2019. "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks.", Forbes <https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#5fddd4d53191>.

Opsahl, T., F. Agneessens, and J. Skvoretz. 2010. "Node centrality in weighted networks: Generalizing degree and shortest paths." Social Networks, 32(3): 245–251. https://doi.org/10.1016/j.socnet.2010.03.006.

Pagani, G. A., and M. Aiello. 2011. "Towards decentralization: A topological investigation of the medium and low voltage grids." IEEE Transactions on Smart Grid, 2(3): 538–547. https://doi.org/10.1109/TSG.2011.2147810.

Pagani, G. A., and M. Aiello. 2013. "The power grid as a complex network: a survey." Physica A: Statistical Mechanics and its Applications, 392(11): 2688–2700. https://doi.org/10.1016/j.physa.2013.01.023.

Pahwa, S., M. Youssef, and C. Scoglio. 2014. "Electrical networks: an introduction." In Networks of networks: the last frontier of complexity: 163–186: Springer. https://doi.org/10.1007/978-3-319-03518-5_8.

Panteli, M., and P. Mancarella. 2017. "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events." IEEE Systems Journal, 11(3): 1733–1742. https://doi.org/10.1109/JSYST.2015.2389272.

Pu, C., and P. Wu. 2019. "Vulnerability Assessment of Power Grids Based on Both Topological and Electrical Properties." arXiv preprint arXiv:1909.05789.

Rosato, V., S. Bologna, and F. Tiriticco. 2007. "Topological properties of high-voltage electrical transmission networks." Electric Power Systems Research, 77(2): 99–105. https://doi.org/10.1016/j.epsr.2005.05.013.

Ruhnau, B. 2000. "Eigenvector-centrality—a node-centrality?" Social Networks, 22(4): 357–365. https://doi.org/10.1016/S0378-8733(00)00031-9.

Salama, M., M. Ezzeldin, W. El-Dakhakhni, and M. Tait. 2020. "Temporal networks: a review and opportunities for infrastructure simulation." Sustainable and Resilient Infrastructure: 1–16. https://doi.org/10.1080/23789689.2019.1708175.

Shahpari, A., M. Khansari, and A. Moeini. 2019. "Vulnerability analysis of power grid with the network science approach based on actual grid characteristics: A case study in Iran." Physica A: Statistical Mechanics and its Applications, 513: 14–21. https://doi.org/10.1016/j.physa.2018.08.059.

Siemens PTI. 2015. Power System Simulator for Engineering (PSSE): PSSE 34.0.1, Siemens Industry, Inc., Siemens Power Technologies International.

Sussman, B. 2019. "Critical Infrastructure: Revealed: Details of 'First of Its Kind' Disruptive Power Grid Attack.", SecureWorld

<https://www.secureworldexpo.com/industry-news/first-U.S.-power-grid-attack-details>.

Wang, J.-W., and L.-L. Rong. 2009. "Cascade-based attack vulnerability on the US power grid." Safety Science, 47(10): 1332–1336. https://doi.org/10.1016/j.ssci.2009.02.002.

Wang, J.-W., and L.-L. Rong. 2011. "Robustness of the western United States power grid under edge attack strategies due to cascading failures." Safety Science, 49(6): 807–812. https://doi.org/10.1016/j.ssci.2010.10.003.

Wang, Z., A. Scaglione, and R. J. Thomas, eds. 2010. Electrical centrality measures for electric power grid vulnerability analysis: IEEE. https://doi.org/10.1109/CDC.2010.5717964.

Xu, Y., A. J. Gurfinkel, and P. A. Rikvold. 2014. "Architecture of the Florida power grid as a complex network." Physica A: Statistical Mechanics and its Applications, 401: 130–140. https://doi.org/10.1016/j.physa.2014.01.035.

Yan, J., Y. Tang, H. He, and Y. Sun. 2015. "Cascading failure analysis with DC power flow model and transient stability analysis." IEEE Trans. Power Syst., 30(1): 285–297. https://doi.org/10.1109/TPWRS.2014.2322082.

3.9. TABLES

Table 3.1: Summary of literature on power grid vulnerability and robustness based on CNT centrality measures.

Reference	Geography	Nodes	Links	Network Representation	CNT Centrality Measures				
					Degree	Eigenvector	PageRank	Betweenness	Closeness
(Motter and Lai 2002)	western U.S.	4941	-	Undirected, Unweighted	✓				
(Albert et al. 2004)	North American	14099	19657	Undirected, Unweighted	✓				
(Rosato et al. 2007)	Italian, French, Spanish	127, 146, 98	171, 223, 175	Undirected, Unweighted	✓				
(Wang et al. 2010a)	New York	2935	6567	Undirected, Weighted	✓	✓			✓
(Hines et al. 2010c)	40 control areas in Eastern U.S.	336 – 1473	-	Directed, Unweighted	✓			✓	
(Pagani and Aiello 2011)	Netherlands	663, 4185	683, 4574	Undirected-Unweighted, Undirected-Weighted	✓			✓	
(Li et al. 2014)	IEEE 118-bus	118		Directed, Weighted			✓	✓	
(Xu et al. 2014)	Florida	84	200	Undirected, Unweighted	✓				
(Fang et al. 2016)	Western Danish	-	-	Directed, Weighted				✓	
(Liu et al. 2017)	IEEE 30-bus, IEEE 57-bus	30, 57		Directed, Weighted		✓		✓	
(Cetinay et al. 2018)	5 power girds of European countries	35 – 449	43 - 613	Undirected-Unweighted, Directed-Weighted	✓	✓		✓	✓
(Shahpari et al. 2019)	Iran	68	98	Directed, Weighted			✓		

Reference	Geography	Nodes	Links	Network Representation	CNT Centrality Measures				
					Degree	Eigenvector	PageRank	Betweenness	Closeness
(Pu and Wu 2019)	IEEE 118-bus, IEEE 145-bus, IEEE162-bus	118,145,162	-	Directed, Weighted	✓				
(Ezzeldin and El-Dakhakhni 2019)	Ontario	1000	1210	Undirected, Unweighted	✓			✓	✓
Current Study	Ontario	3653	4503	Undirected-Unweighted, Directed-Weighted	✓	✓	✓	✓	✓

Table 3.2: Summary of different centrality measures used in the current study.

Centrality Measure	Simple Network	Weighted Network	
Degree	$D(i) = \sum_j^N a_{ij}$	$D(i)^w = \sum_j^N f_{ij} * a_{ij}$	
Eigenvector	$E(i) = \frac{1}{\lambda max} \sum_j^N a_{ij}\ E(j)$	$E(i)^W = \frac{1}{\lambda max_w} \sum_j^N a_{ij_w}\ E(j)^w$	
PageRank	$PR(i) = (1-d) + d\ \sum_{j \in N_i} \frac{PR(j)}{L(j)}$	$PR(i)^W = (1-d) + d\ \sum_{j \in N_i} \frac{PR(j)^W}{f_{jout}}$	
		Weighted Shortest path Based	*Current-Flow Based*
Betweenness	$B(i) = \frac{\sum_{i \neq j \neq k} \sigma_{jk}(i)}{\sum_{i \neq j \neq k} \sigma_{jk}}$	$B(i)^W = \frac{\sum_{i \neq j \neq k} \sigma_{jk}(i)^W}{\sum_{i \neq j \neq k} \sigma_{jk}{}^W}$	$B(i)^{CF} = \frac{\sum_{s \neq d} f_i{}^{(s \to d)}}{0.5\,(N-1)\,(N-2)}$
Closeness	$C(i) = \frac{1}{N-1} \sum_j^N \frac{1}{S_{ij}}$	$C(i)^W = \frac{1}{N-1} \sum_j^N \frac{1}{S_{ij}{}^W}$	$C(i)^{CF} = \frac{N-1}{\sum_j V_i{}^{(i \to j)} - V_j{}^{(i \to j)}}$

Table 3.3: KS Test results for different random sample sizes.

		Topology Index		***Functionality Index***	
	D(n,m,∝)	*D*	*P-Value*	*D*	*P-Value*
Random Sample 10	*0.45*	*0.07*	*0.045*	*0.05*	*0.24*
Random Sample 20	*0.33*	*0.04*	*0.5*	*0.03*	*0.66*
Random Sample 50	*0.23*	*0.03*	*0.75*	*0.02*	*0.99*

3.10. FIGURES

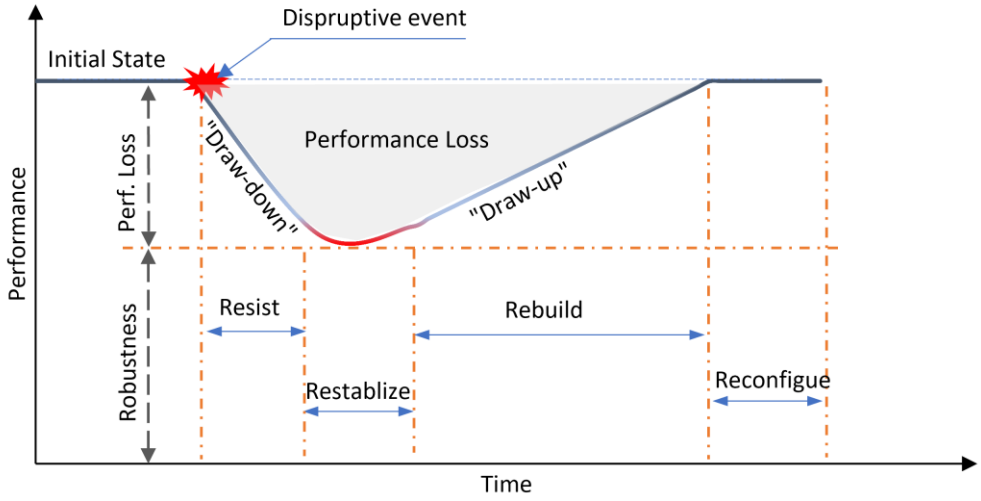

Figure 3.1: Resilience attributes.

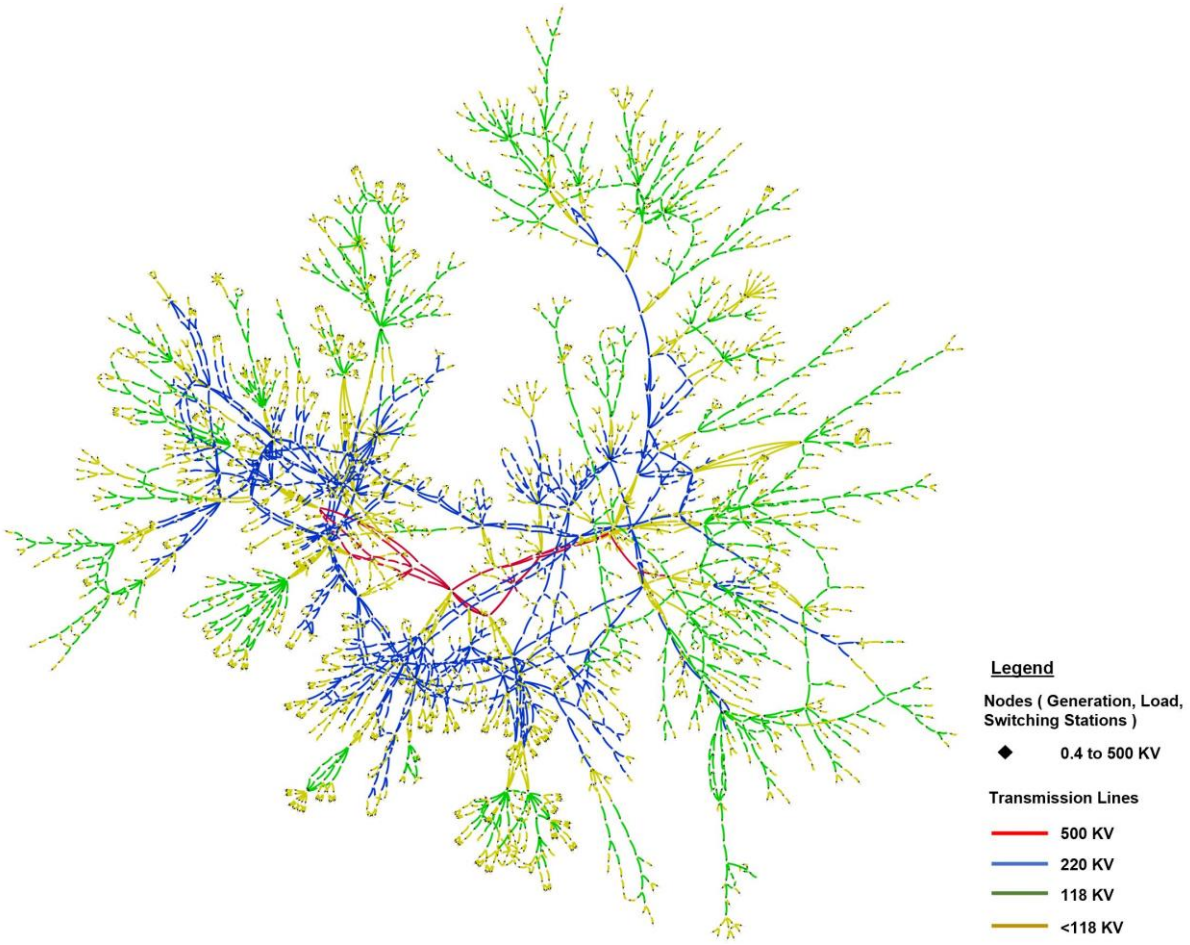

Figure 3.2: Topology of low to high voltage of the Ontario power grid.

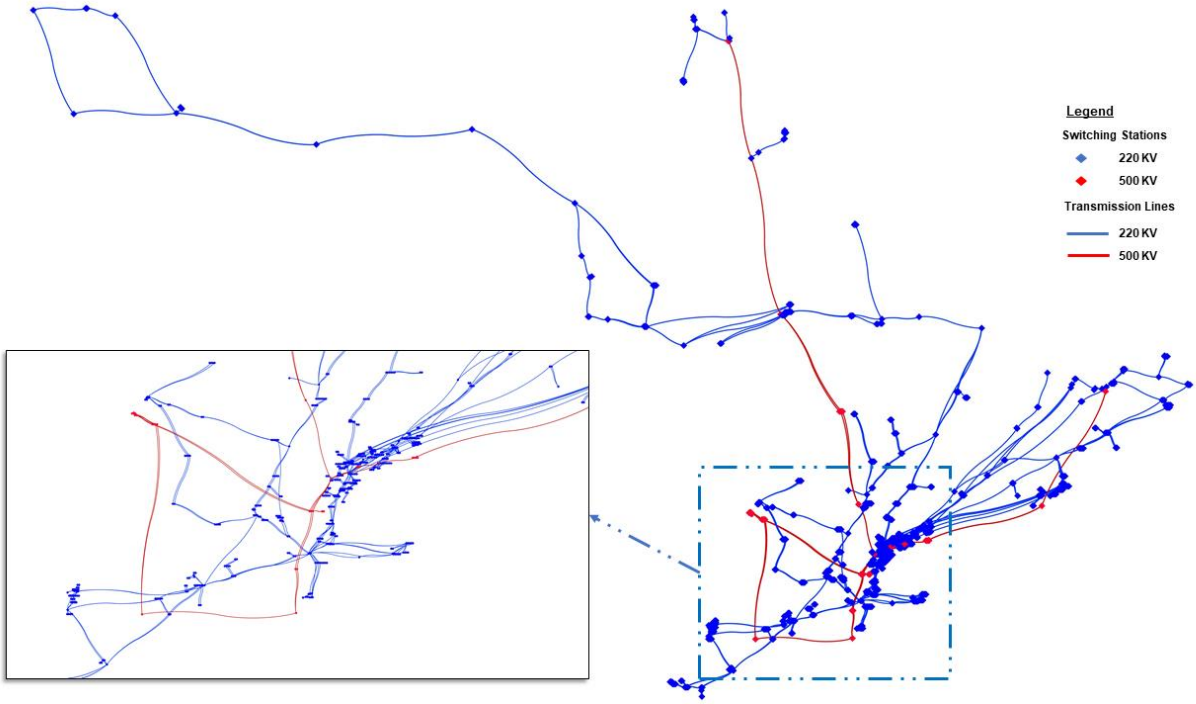

Figure 3.3: Topology of high-voltage transmission Ontario power grid network. The blue color is for transmission lines and switching stations of 220 kV, while the red color for 500 kV.

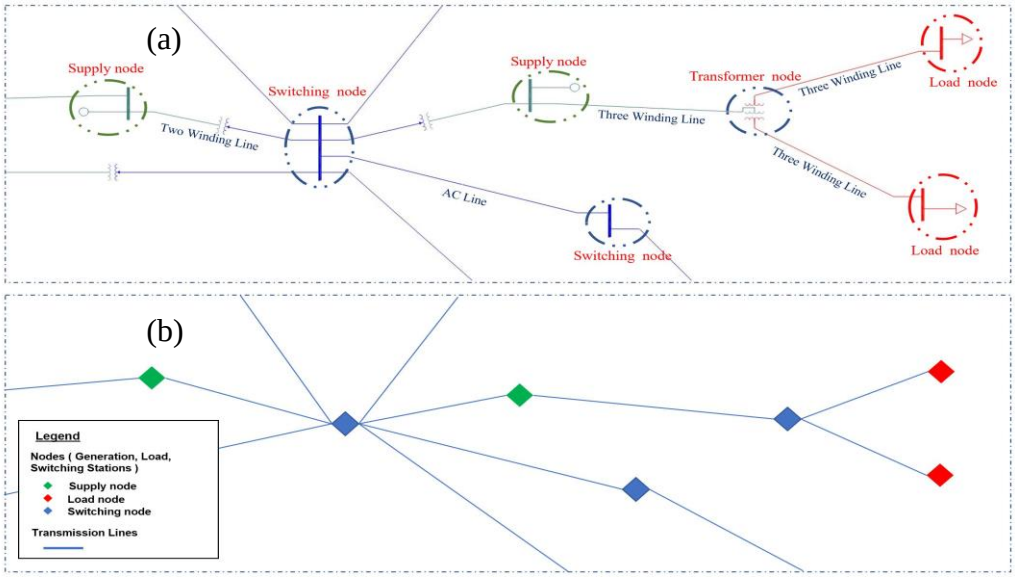

Figure 3.4: Schematic diagram presents a portion of a power grid. a) Single line diagram from PSSE software; and b) Portion of the topology illustration of the network. The stations presented as nodes that have been classified into three groups: supply nodes (in green), load nodes (in red), and switching nodes (in blue). Whiles the AC lines, two winding transformers, and three winding transformers presented as links.

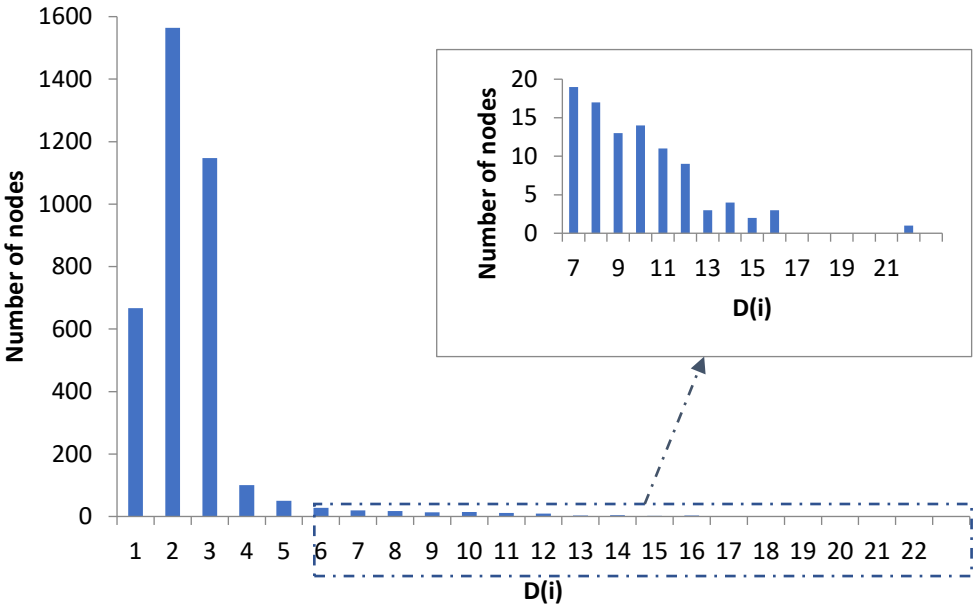

Figure 3.5: The degree centrality distribution of the Ontario power grid.

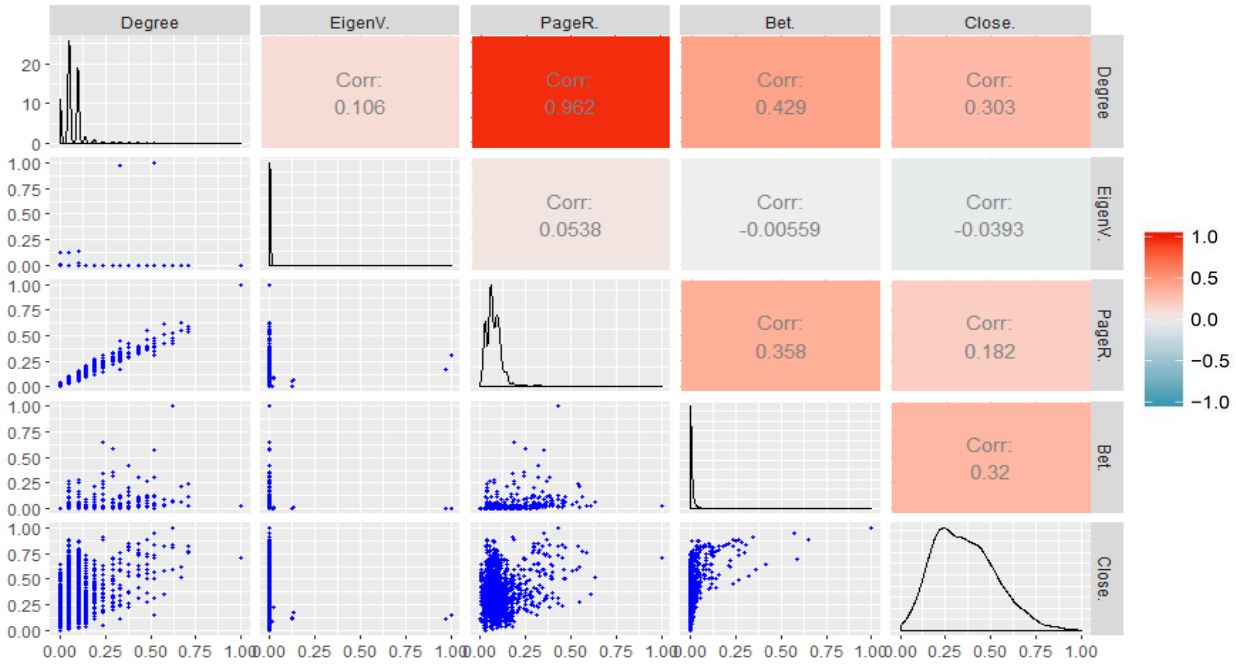

Figure 3.6: The distribution of different centrality measures and the correlation between them for the unweighted network.

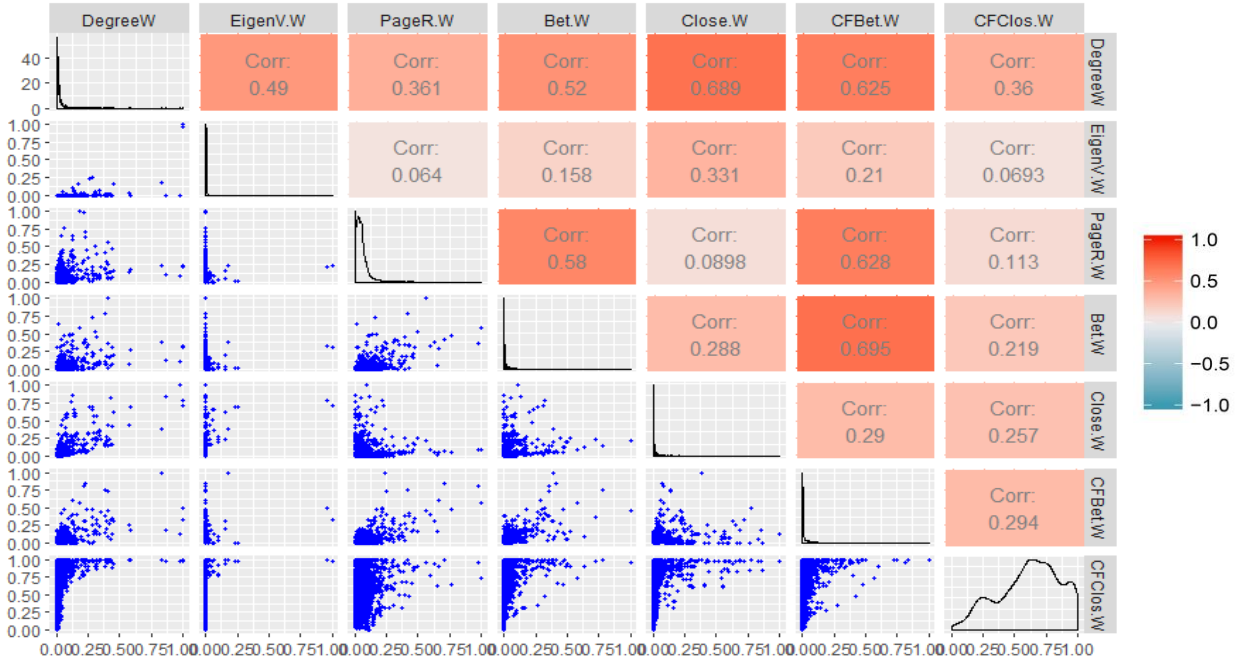

Figure 3.7: The distribution of different centrality measures and the correlation between them for the weighted network.

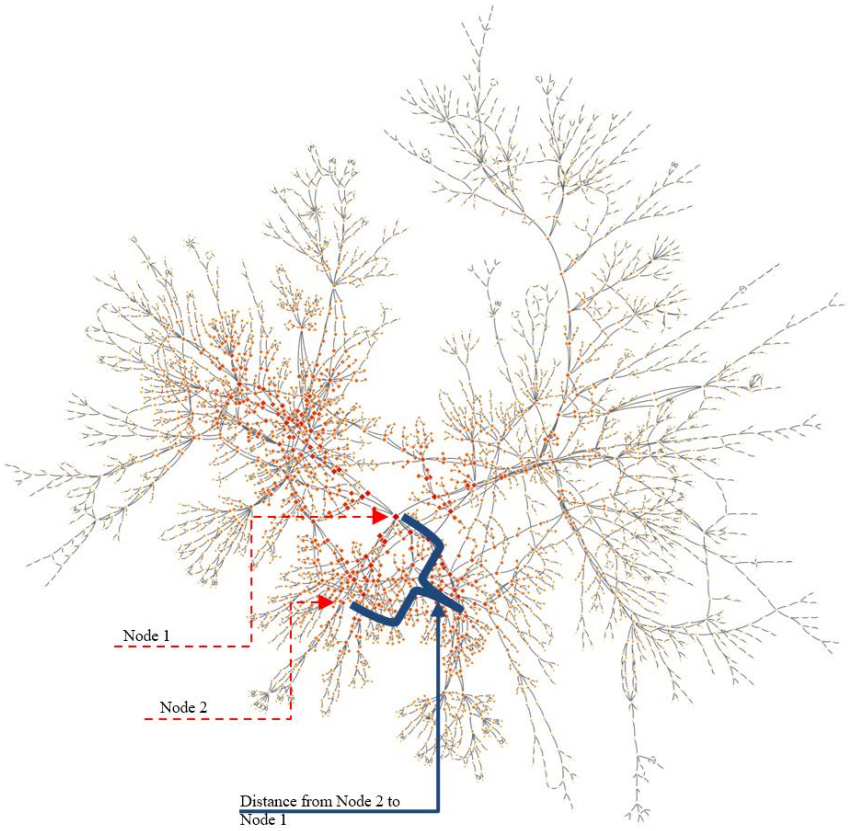

Figure 3.8: The topology of Ontario power grid where the nodes color and size changes gradually to indicate the normalized closeness centrality value $C(i)$.

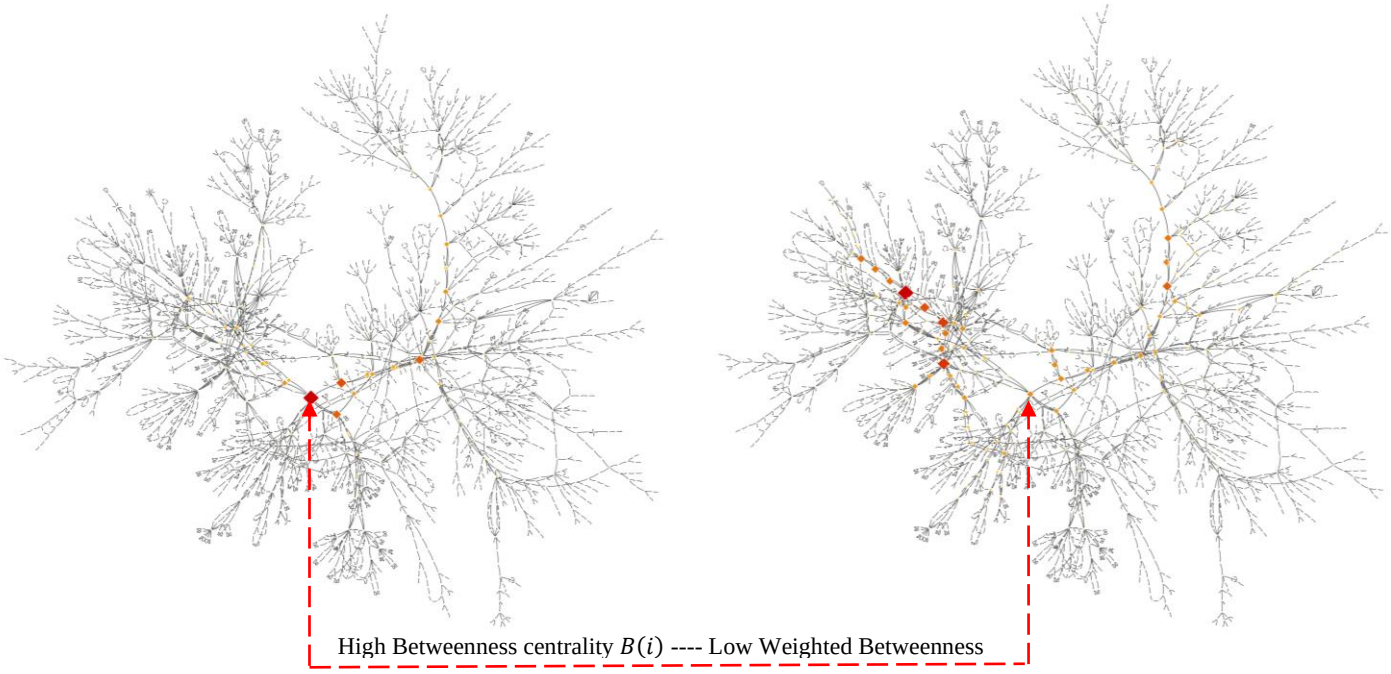

Figure 3.9: The topology of Ontario power grid where the nodes color and size changes gradually to indicate the normalized betweenness centrality value; unweighted betweenness centrality $B(i)$ (left), unweighted betweenness centrality $B(i)^w$ (right).

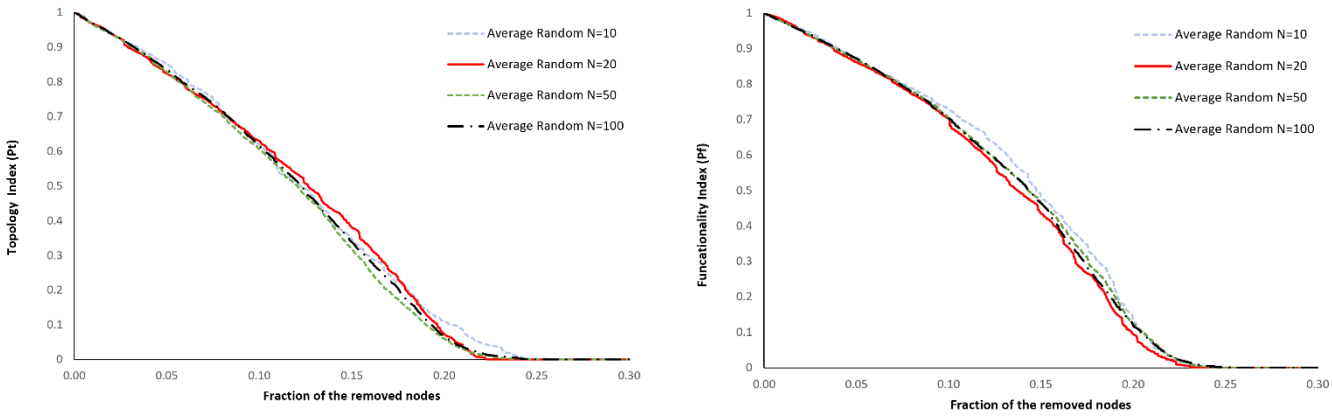

Figure 3.10: The robustness of the grid against random cyberattacks with different number of random scenarios evaluated by the topology index (left) and the functionality index (right).

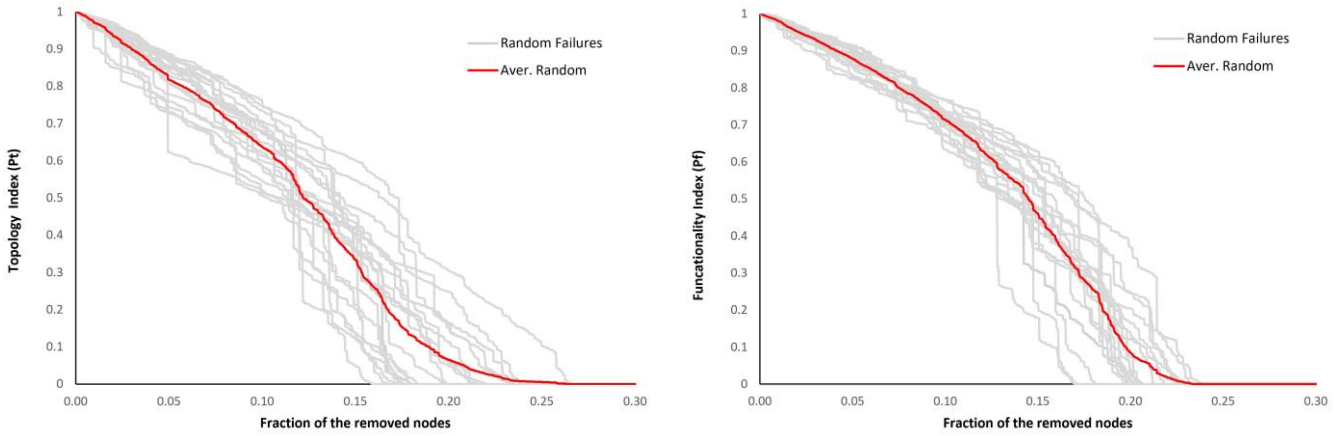

Figure 3.11: The robustness of the grid against random cyberattacks evaluated by the topology index (left) and the functionality index (right).

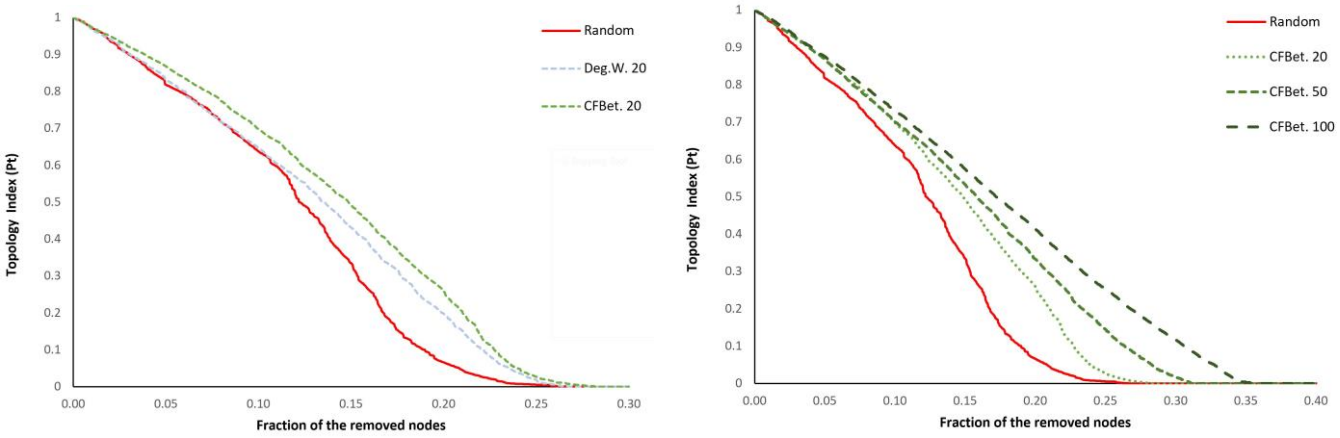

Figure 3.12: The robustness of the grid against random cyberattacks with mixed strategy evaluated by the topology index. Selected the top 20 weighted degree and current flow betweenness hubs as protected nodes (left) and selected the top 20, 50, and 100 current flow betweenness hubs as protected nodes (right)

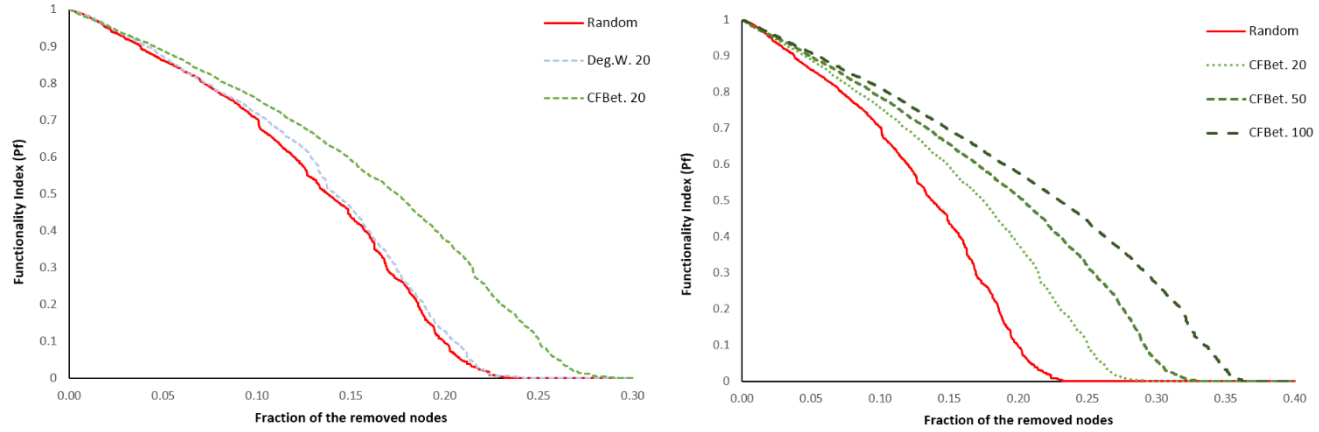

Figure 3.13: The robustness of the grid against random cyberattacks considering the mixed strategy evaluated by the functionality index. Selected the top 20

weighted degree and current flow betweenness hubs as protected nodes (left) and selected the top 20, 50, and 100 current flow betweenness hubs as protected nodes (right).

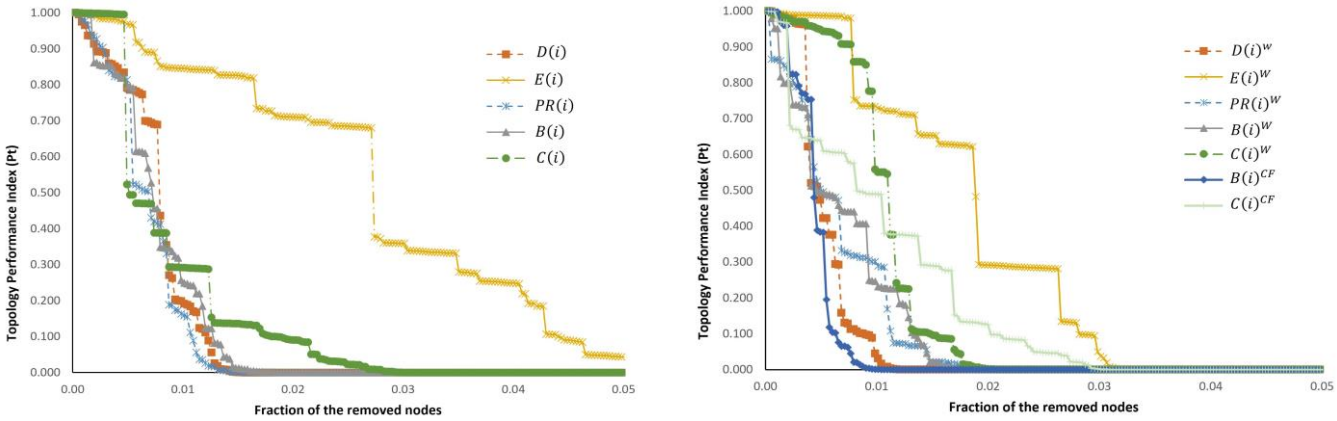

Figure 3.14: The topology performance index with removal of the nodes based on different targeted cyberattack scenarios for the unweighted network (left) and the weighted network (right).

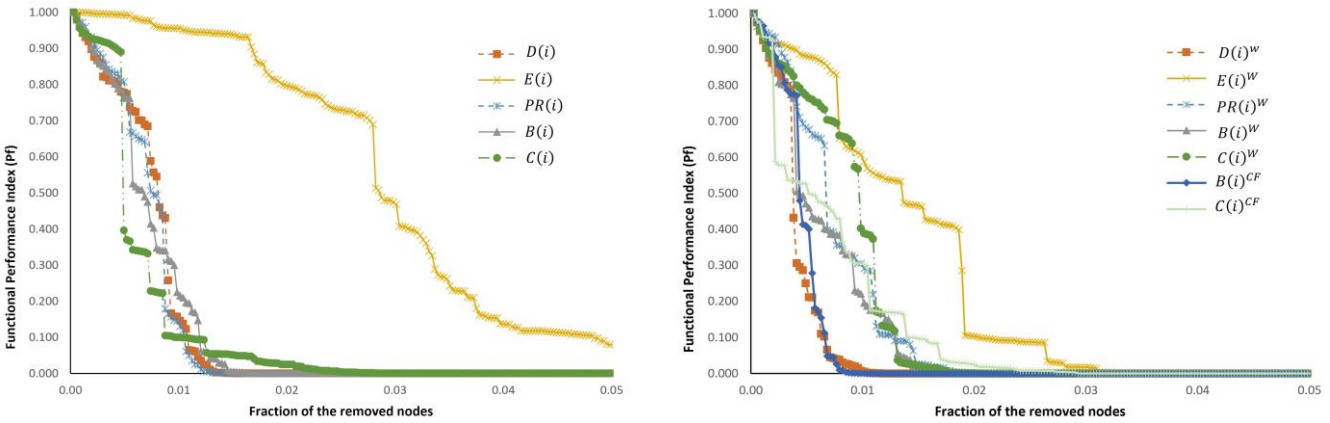

Figure 3.15: The functional performance index with removal of the nodes based on different targeted cyberattack scenarios for the unweighted network (left) and the weighted network (right).

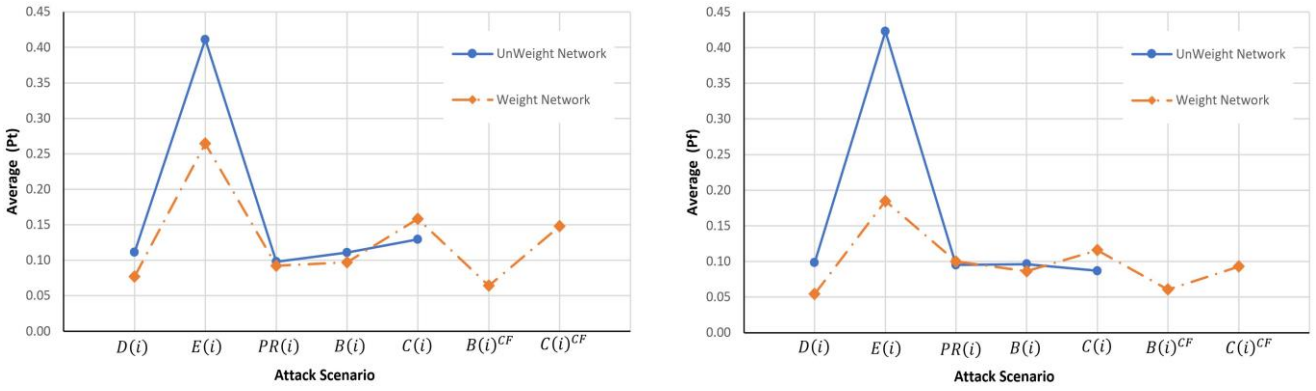

Figure 3.16: The average topology performance index (left) and the average functional performance index (right) for weighted and unweighted network against different targeted attack scenarios.

Chapter 4 : Dynamic Network Flow Model for Power Grid Systemic Risk Assessment and Resilience Enhancement

ABSTRACT

Power infrastructure networks are susceptible to performance disruptions induced by natural or anthropogenic hazard events. For example, extreme weather events or cyberattacks can disrupt the functionality of multiple network components concurrently or sequentially, resulting in a chain of cascade failures throughout the network. Mitigating the impacts of such system-level cascade failures (systemic risks) requires analyzing the entire network considering the physics of its dynamic power flow. The current study focuses on the "draw-down" phase of power infrastructure network resilience—assessing the power grid vulnerability and robustness, through simulating cascade failure propagations using a dynamic cascade failure physics-based model. The study develops and demonstrates the utility of a link vulnerability index, for constructing power transmission line vulnerability maps; as well as a node importance index, for power (sub)stations ranking according to the resulting cascade failure size. Overall, understanding the criticality of different network components provides stakeholders with the insights for building resilience and subsequently managing it within the context of power grids, and supports policymakers and regulators in making informed decisions

pertaining to the tolerable degree of systemic risk constrained by available resources.

Keywords: Complex network theory, Dynamic cascade failure, Power infrastructure networks, Vulnerability analysis, Physical flow model.

4.1. INTRODUCTION

National economy and public safety relies on the continuous operation of critical infrastructure networks that are *"essential for the maintenance of vital societal functions, health, safety, security, economy or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions*" (Rome et al. 2014). Power grids are at the forefront of critical infrastructure networks for modern societies (Panteli and Mancarella 2017) as the operations of most other critical infrastructure network (e.g., communication and transportation) depend on an adequate and reliable power supply. As such, the risk of a large-scale blackout poses a serious threat to other power-dependent critical infrastructure networks—affecting the overall national economy and citizens wellbeing. A blackout can be initiated by different causes, including those attributed to weather conditions, component failures, human errors, deliberate physical, or cyberattacks, whereas most reported blackouts occurred because of extreme weather events (Haggag et al. 2021). Although designed to be robust, past events have shown that even a small disruption in some key network components may lead to overload on other components and thus a chain of cascade failures, which can rapidly spread throughout the network causing catastrophic system-level cascade failure (*systemic risks*) (Bernstein et al. 2014b; Costa et al. 2011). For example, The Northeast blackout of 2003 started with local failure whereby the failure of one transmission line due to contact with a tree, combined

with an alarm system malfunctioning, propagated to a large part of the connected network and affected more than 50 million people in Canada and the US' North East (Andersson et al. 2005).

Natural hazard events (e.g., the 2011 Japan earthquake and tsunami, and 2012 hurricane Sandy) have highlighted the vulnerability of critical power infrastructure networks (Ouyang 2014). Anthropogenic hazard (e.g., cyber-attacks) poses yet another challenge in the era of smart grids. For example, in March 2019 hackers exploited firewall vulnerabilities to cause periodic 'blind spots' for grid operators in the western US for about 10 hours (NERC 2019). In addition to natural and anthropogenic hazard events, the risk of failure due to the aging of power infrastructure components and/or asset mismanagement coupled with the increased demand on power due to population growth necessitate the need to investigate, analyze, and evaluate the vulnerability of these networks in an effort to enhance their resilience.

In general, studies focused on evaluating power grid infrastructure resilience have broadly adopted either topology- or physical flow-based network models (Ouyang 2014; Salama et al. 2020). Topology-based models simulate infrastructure networks based solely on their topological and connectivity properties. Such over simplified models inherently disregard flows and physical properties of/within the network, and instead represent the underlying network in an abstract manner, as a set of nodes and links (Rosato et al. 2007) including those

by (Albert et al. 2004; Crucitti et al. 2005; Rosato et al. 2007; Wang et al. 2010b). In addition, some studies model cascade failures by assuming power flow and load redistribution based on network component topology properties (Fang et al. 2014; Kinney et al. 2005; Motter and Lai 2002; Sun et al. 2008; Wang and Rong 2009, 2011), whereas other studies proposed risk mitigation strategies without considering actual power flow characteristics (Motter 2004; Wang 2013a). Although abstract in nature, topology-based models can nonetheless provide indications of network behavior and vulnerability, albeit such models lack the ability to draw a complete picture of infrastructure real behavior since all infrastructure networks are governed by the laws of physics and are subjected to constraints pertaining to demand and supply (Hines et al. 2010a; Salama et al. 2021).

Unlike network models based solely on topology, high-fidelity models of power grid should take into consideration the real power flow, the transmission lines electrical properties, and the generation actual supply and capacity limits (Ouyang 2014; Pagani and Aiello 2013b). Despite the recent advance in conceptual modeling of cascade failure propagation (Ju 2018; Li et al. 2018; Yan et al. 2015; Zhao et al. 2018), a major obstacle still remains due to the lack of high resolution data, which is typically restricted for security reasons. In the absence of such data, it is very unlikely to provide a realistic network vulnerability analysis to ensure the reliability and resilience of power grids. In this respect, Yang et al. (2017) provided

a large-scale model for the US power grids to investigate their vulnerability. Furthermore, compared to their topology-based counterparts, such physical flow-based models usually require significant computational time and more data to simulate the functionality of network components. Several studies have assumed transmission line properties and the demand/supply at each node to calculate the power flow (Schäfer and Yalcin 2019), whereas other studies assumed transmission line capacities to check the overloaded network components (Bernstein et al. 2014b).

4.2. OBJECTIVES

The current research focuses on the "draw-down" phase of power infrastructure network resilience to assess power grid vulnerability and robustness by simulating the cascade failure propagation based on a physical power flow model. The developed cascade failure model was subsequently used to construct transmission line vulnerability map of a demonstration power grid application. In addition, the study estimated the node importance index (NII) based on both cascade failure effect and the nodal centrality measures. There are four main contributions of the current study. First, the study proposes a high-fidelity dynamic cascade failure physics-based model of power grid that consider the actual power flow, the transmission lines' electrical properties, and the generators' typical supply and capacity limits. Second, the dynamic cascade failure model adopted the DC flow-

based model to consider power redistribution through network after disruptions. Third, the cascade failure model considers the operational corrective actions in case of failure to rebalance the supply and demand (i.e., implement dispatch and load shedding). Subsequently, the cascade failure model is used to construct transmission line vulnerability map of the power grid and estimate the node importance index based on both cascade failure effect and the nodal centrality measures. Finally, the study demonstrates the model application on a real large-scale network with data ranging from low to high voltage.

Following this section, the vulnerability assessment framework, cascade failure model procedures, explanation, and assumptions are presented in Section 4.3. Section 4.4 then provides a brief description of the power grid used to demonstrate the developed model application. Subsequently, the results from the cascade failure model to assess the network links vulnerability and node importance index are presented. Finally, concluding remarks are provided in Section 4.5.

4.3. VULNERABILITY ASSESSMENT FRAMEWORK

The proposed framework focuses on evaluating the vulnerability of power grids by simulating cascade failure propagation throughout the network components. The proposed vulnerability assessment framework consists of power grid dynamic cascade failure physics-based model. The model is then applied to construct grid vulnerability map and compute component (node) importance index for a

demonstration power grid.

Within the context of CNT (Newman 2010a), the main components of the network are simulated by nodes (e.g., substations in power networks), whereas links represent the interdependencies between these nodes within such a network (e.g., transmission lines in power networks). The model considers node heterogeneity where the nodes have been classified into three groups, namely: supply station nodes 'generator', demand station nodes 'load', switching station node 'junction'. The transmission lines are classified into three groups: AC lines, and two- and three winding transformers. AC lines connect two stations at the same voltage, whereas two- and three winding transformers connect two or three stations with different voltages. The three winding transformers are visualized as three links intersecting at one junction node.

4.3.1. DYNAMIC CASCADE FAILURE MODEL

Figure 4.1 illustrates a flowchart for the dynamic cascade failure propagation model for power networks. Within the context of the current study, the dynamic modelling approach refers to power flow redistribution and supply-demand balancing following each loop in the cascade failure model. The parameters for the cascade failure model are described in detail next.

4.3.1.1 INITIAL FAILURE

Recently, the increased frequency and magnitude of various disasters, such as hurricanes, ice storms, earthquakes, and cyberattacks have significantly increased the potential failures of power networks, through failure of multiple links (Wu et al. 2016). In addition, the initial failure of a node (e.g., a substation) can result in a system-level (systemic) impact on the network performance due to the subsequent impact on the different links connected to the failed node (Yan et al. 2015). Therefore, the study implements both potential failure types: initial failures of a single or multiple links, or initial failure of a node (Figure 4.1). Once a failure is initiated, the cascade failure model procedure starts with dispatch and load shedding, flow redistribution, followed by checking overloaded components until network stability.

4.3.1.2 DC POWER FLOW MODEL

The developed cascade failure model is a physics-based network flow model which calculates the actual power flow using a direct current (DC) power flow model. DC power models are widely used to simplify alternating current (AC) power flow analysis in power grids (Bernstein et al. 2014b; Pahwa et al. 2014; Yan et al. 2015). The DC power model is used wherever repetitive and fast load flow estimations are required, whereas this method is non-iterative and absolutely convergent. The Power System Simulator for Engineering (PSSE) software (Siemens PTI 2015) has been used to compute the transmission lines power flow. However, there are some

limitations to the proposed DC power flow model due to using the linear equations instead of the nonlinear equations of the AC power model. For example, the outage of the transmission lines may not result in direct thermal overload, but may otherwise cause system failures due to voltage and/or transient instability during the transient period. In the DC power model, nonlinear equations of the AC power model are simplified to a linear form based on the following assumptions:

- Line resistance R_{ij} is negligible compared to line reactance x_{ij} (i.e., $R_{ij} \ll x_{ij}$).
- The voltage profile is flat (i.e., magnitudes of node voltages are set to 1.0 per unit).
- Voltage angle differences between nodes are small (i.e., $\sin(\delta_{ij}) = \delta_{ij}$ and $\cos(\delta_{ij}) = 1$).

As such, based on the above assumptions, the power at each node f_i pertains to all the "in" and the "out" power flows, as:

$$f_i = \sum f_{ij} = \begin{cases} S_i , & \text{Generation nodes} \\ -D_i , & \text{Load nodes} \\ 0 , & \text{Junction nodes} \end{cases} \quad (1)$$

where, f_{ij} is the power flow for the link from node i to node j, S_i and D_i is the given power at generator and load nodes, respectively.

To calculate power flow, the following equations are applied from ref. (Pahwa et al. 2014).

$$f_{ij} = \frac{\delta_{ij}}{x_{ij}} \quad (2)$$

where, $\delta_{ij} = (\theta_i - \theta_j)$ is the difference in the phase angle between node i and node j, and x_{ij} is the transmission line reactance.

4.3.1.3 DISPATCH AND LOAD SHEDDING

Dispatch and load shedding describe the process to rebalance demand and supply after disruptive events (Yan et al. 2015). Each iteration in the simulation starts by tripping the overloaded transmission lines. Following their removal, the network is checked if it remains as one connected grid or is separated into isolated sub-grids (i.e., islands). For each sub-grids, the dispatch and load shedding procedures are implemented in the following order of importance:

- For each isolated island, the generator with the largest capacity is selected to be the "slack bus" (i.e., the generator with power output that can be adjusted from zero to the generator's capacity which is necessary to apply the DC power flow model).
- For each isolated island, in case that ($\sum P_s > \sum P_d$) , scale down the generators' output until the balance point between demand and supply is realized.
- For each isolated island, in case that ($\sum P_s < \sum P_d$), scale up the generators' output accordingly. If the generators reached its maximum capacity prior to achieving load balance, scale down the demand to the balance point (i.e., load shedding)."

The dispatch and load shedding process is summarized in a flowchart, shown in Figure 4.2.

4.3.1.4 NETWORK PERFORMANCE MEASURES

The network performance following cascade failure development is evaluated through both its topological and functional characteristic, assessed at the conclusion of failures. Two measures for cascade failure sizes are assumed which describing the loss of service, as follows:

- Cascade size based on the topology S_l can be calculated as the percentage of the failed links N_f (i.e., out of service transmission lines due to initial failure and the overloaded lines) to the total number of links *N*.

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

- Cascade size based on the power flow S_p can be calculated as the percentage of the loss of demand load to the original load of the network.

$$S_p = \frac{\sum P_d - \sum P_d{}'}{\sum P_d} \quad (4)$$

where, $\sum P_d$ is the total original load, and $\sum P_d{}'$ is the total demand load at the end of cascade failures.

4.3.2. NETWORK VULNERABILITY ANALYSES

The dynamic cascade failure model is used to estimate the vulnerability of links (i.e., link vulnerability index) and the importance of nodes (i.e., node importance index) in the network. The link vulnerability index indicates the probability of failure for each link in the network due to an initial failure of a random set of links. On the other hand, the node importance index ranks the nodes' influence according to the cascade failure size triggered by initial node failure.

4.3.2.1 LINK VULNERABILITY INDEX

The cascade failure model is used to evaluate the link vulnerability index and thus construct the grid vulnerability maps through Monte Carlo simulation (Zio 2013) by tripping n_i randomly selected transmission lines and compute the probability of failure for each link in the grid after repeating the cascade failure simulation for N times. The n_i random lines initial failures represent transmission lines outages due to disruptive events such as extreme weather (natural hazard) or due to inadequate maintenance (anthropogenic hazard). The n_i initial lines failures were selected completely randomly (i.e., transmission lines were selected randomly based on a uniform distribution). After repeating this random initial failure and the cascade failure model for N times, the Kolmogorov-Smirnov Test (KS Test) (Conover 1998) is employed to ensure the validity of the number of repeated simulations, N, needed to provide a representative failure probability for each transmission line. The proposed link vulnerability index can thus be used to evaluate the failure probability of any line in the grid under the different scenarios. Selecting the initial failure process to be fully random is justified as this removes any bias in the failure probability evaluation that would be introduced through selecting only pre-specified lines. Following this approach, the model highlights the primary and secondary failed lines where the primary failed lines are the lines that tripping due to overloaded condition (i.e., the automatically switching off the overloaded lines to prevent permanent damage). The secondary failed lines on the other hand are the lines that do not carry flow at the end of the cascade failure model (i.e., out of

service lines due to the outage of other lines). Therefore, three failure probabilities for each link in the network are stored: primary P_{lf_P}; secondary P_{lf_S}; and total P_{lf_T} (i.e., the summation of the primary and secondary failure probability for each link, $P_{lf\_T} = P_{lf\_P} + P_{lf\_S}$). The purpose of evaluating line failure probabilities is to identify the lines that are more prone to failure because they either operate near their capacity limits or they are at the center of flow distribution and are thus more susceptible to disruption instigated by the different cascade failure scenarios. Accordingly, the developed grid vulnerability map can be used to rank the line maintenance priority, whereas the lines with high failure probability should also receive a correspondingly higher upgrade priority.

4.3.2.2 NODE IMPORTANCE INDEX

The Node Importance Index NII is useful for ranking the relative importance of stations in the power grid, which will latter support regulators and decision-makers to optimize the upgrade schedule constrained by available resources. In this section, NII is estimated according to two methods. The first method relies on the cascade failure model whereas the second one relies on centrality measures of network topology with considering both weighted and unweighted links (i.e., links weight according to the power flow). Subsequently, the NIIs from the two methods are compared to indicate to what extent the topology-based model can use to assess power grid vulnerability.

4.3.2.2.1 NII: Based on Cascade Failure Effect

The influences of different nodes on the overall network behavior (i.e., Node Importance Index NII) is evaluated using the proposed cascade failure model. NII can be estimated according to the cascade failure size that results in the network due to the initial failure of this node. For example, the node with the highest cascade failure size considers as the node with the most influence on the overall network behavior (i.e., having the highest NII).

4.3.2.2.2 NII: Based on Centrality Measures

In topology-based network studies, the centrality measures were typically used to indicate the node importance index. There are different measures for centrality that can be used according to the underlying application. In some cases, the importance of a node is related to the number of connections between this node and other nodes in the same network (i.e., the degree centrality). In other cases, the importance is related to the total number of shortest paths that traverse through this node (i.e., the betweenness centrality).

Degree Centrality: One of the key measures to identify node importance is its degree centrality. The degree centrality of a node is the total number of links connected directly to this node (Opsahl et al. 2010), as presented in Eq. 5. In topology-based models, power grids are modeled as directed-weight networks, with the weight and the direction of network links assumed according to the power flow value and direction at the initialization power grid state. This approach implicitly

assumes that transmission lines that carry more flow have more influence than the lines that carry lower level of power flow. However, node connectivity in the power grid with other nodes is not only related to how many links connected to it but also related to the connection strength of each link (Wang et al. 2010a); and the power flow of each link reflects such strength.

In weight networks, the degree centrality has been extended to sum the weights of links connected directly to the node (Opsahl et al. 2010), as presented in Eq. 6. For a better comparison, the degree centrality is normalized to 1.0 as presented in Eq. 7. According to the degree centrality, the node with the highest degree is the most central node (i.e., hub) (Barabási and Pósfai 2016).

$$C_D(i)^{UnW} = \sum_j L_{ij} \quad (18)$$

$$C_D(i)^{W} = \sum_j f_{ij} \; L_{ij} \quad (19)$$

$$\text{Normalized } (C_D(i)) = \frac{C_D(i) - \text{Min } C_D}{\text{Max } C_D - \text{Min } C_D} \quad (20)$$

where, L_{ij} = 1 if and only if there is a link between nodes *i* and *j*, 0 otherwise.

Betweenness Centrality: This centrality measure is one of the most widely used measures to indicate the node importance in topology-based network studies. This measure identifies nodes that play a central role between other nodes in the network (Opsahl et al. 2010). The betweenness centrality measure of node *i* is

calculated as the number of shortest paths between pairs of other nodes that passes through node *i* (Freeman 1977; Opsahl et al. 2010), as presented in Eq. 8.

In weighted networks, each line weight is multiplied by $1/f_{ij}$ which results in shorter paths for higher power lines, as presented in Eq. 9. Subsequently, nodes central to high power lines will be also central to shortest paths, and will thus have high betweenness centrality values. This hypothesis assumed that shortest path is not only related to the number of links but also the level of power flow passing through that path. Eq. 10 represented the normalization betweenness centrality to insure the values between 0 and 1.

$$C_B(i)^{UnW} = \frac{\sum_{i \neq j \neq k} \sigma_{jk}(i)}{\sum_{i \neq j \neq k} \sigma_{jk}} \quad (21)$$

$$C_B(i)^{W} = \frac{\sum_{i \neq j \neq k} \sigma_{jk}(i)^{W}}{\sum_{i \neq j \neq k} \sigma_{jk}{}^{W}} \quad (22)$$

$$\text{Normalized } (C_B(i)) = \frac{C_B(i) - \text{Min } C_B}{\text{Max } C_B - \text{Min } C_B} \quad (23)$$

where $\sigma_{jk}(i)$ is the total number of shortest paths between nodes *j* and *k* that passes through node *i*, while σ_{jk} is the total number of shortest paths between nodes *j* and *k*, with $\sigma_{jk}(i)^{W}$ and $\sigma_{jk}{}^{W}$ calculated based on the weighted shortest paths.

4.4. APPLICATION DEMONSTRATION

To demonstrate the application of the proposed approach, the Ontario power grid was modelled as 3,653 nodes and 4,503 links. The initial demand in the case study

was based on the Ontario power grid data through the Independent Electricity System Operator (IESO) Summer Case scenario. Following a disruptive event (i.e., initial failure), the dispatch and load shedding process is initiated to rebalance demand and supply. Subsequently, the model checks the transmission line capacity against the recalculated power flow due to such event. For a typical Ontario summer operating scenario, the predicting thermal overloads 15-minute limited time ratings are used. In general, thermal ratings are based on pre-load, ambient temperature, and wind speed. For clarity, only the high voltage transmission network (i.e., the stations and transmission lines with base voltage equal to 220 and 500 KV) are presented.

4.4.1. LINK VULNERABILITY INDEX

Following the procedures in previous section, it was possible to construct the links vulnerability map for the Ontario power grid. In the current study, the initial failure was assumed as a failure of any three random AC transmission lines (i.e. $n_i = 3$) (Yang et al. 2017).

The cascade failure model has been repeated for different numbers N (i.e., sample sizes) to compute the line failure probability (i.e., run the cascade failure model for 1500, 3000, 4000, and 5000 random scenarios). Figure 4.3 presents the total line failure probability based on the four sample sizes. It can be inferred that the line failure probability values are close to each other regardless of the sample

size and converge between 4000 and 5000. The Kolmogorov-Smirnov Test (KS Test) (Conover 1998) was used to compare between the lines failure probability result of the four sample sizes to select the appropriate one. KS Test computes the maximum difference between the cumulative distribution function of two sample sizes, as presented in Eq. 11.

$$D_{n,m} = \max|F(x) - G(x)| \qquad (11)$$

Whereas the first sample has size m with a cumulative distribution function of $F(x)$ and that the second sample has size n with a cumulative distribution function of $G(x)$.

The null hypothesis is rejected at level 0.05 if $D_{n,m} > D_{n,m,\propto}$. The null hypothesis is that the curves of the two samples are similar.

$$D_{n,m,\propto} = 1.36 \times \sqrt{\frac{m+n}{mn}} \qquad (12)$$

Table 4.1 summaries the KS test results. The lines failure probability of sample size 1500, 3000, and 4000 have been compared to lines failure probability of sample size 5000 (i.e., n = 1500, 3000, or 4000 while m = 5000). The null hypothesis is accepted for sample size 4000 where $P - value > 0.05$ and $D_{n,m} < D_{n,m,\propto}$. It was concluded that that there is no significant difference between the line failure probability of sample size 4000 and 5000 (i.e., the difference is less than

5%). Therefore, the 5000 runs scenarios for the cascade failure model were found to be statistically adequate to provide a good representation to compute the line failure probability.

Based on the above analyses, the simulation explained in link vulnerability index subsection repeated 5,000 times (i.e., $N = 5{,}000$). For clarity, Figure 4.4 only presents the high-voltage transmission lines vulnerability map of the Ontario power grid.

Any failure probability under 0.5% was neglected and assumed as no failure indicated at the relevant link. According to the links vulnerability map for the whole power grid, it was found that about 12%, 5%, and 8% of the AC transmission lines and two- and three winding transformers underwent a primary failure, respectively. The number of lines underwent secondary failures were on average three times the primary ones for the whole network. Figure 4.5 presents the primary and secondary failure probability for the whole network lines after excluding lines with failure probability less than 0.5%. It can be inferred that number of lines underwent the secondary failures is much higher than number of lines underwent primary failures. In total, 36% of all links have $P_{lf\_T} > 0.5\%$, and the maximum P_{lf_T} noted was 12%. The links vulnerability map can be used to rank the link maintenance priority, whereas the links with high probability failure have a higher priority to get updated or changed in the network upgraded schedule.

4.4.2. NODE IMPORTANCE INDEX

Figure 4.6 presents the NII according to two cascade failure size measures: the percentage of the failed links S_l and the percentage of the load loss S_p at the end of the cascade failure model.

As can be inferred, the highest cascade failure sizes caused due to initial failure of one switching station were $S_l = 30\%$, and $S_p = 70\%$. This switching station is connected to ten high voltage transmission lines (i.e., 500 KV) and disconnected of this node leads to a significant redistribution of power flow followed by extensive overloaded lines in the network which results in dividing the networks to many isolated islands. Failure propagation through the network can be observed in Figure 4.7, with the number of failed lines and the load loss are presented step by step in Figure 4.8.

In addition, Figure 4.9 presents the NII based on two centrality measures: degree centrality $C_D(i)$ and betweenness centrality $C_B(i)$.

4.4.3. NII MEASURE CORRELATIONS

To test the extent to which the topology-based model can accurately reflect power grid vulnerability, the NIIs based on the cascade failure model have been compared with that based on the centrality measures. All measures were normalized between 0 and 1 to facilitate the comparison, as shown in Figure 4.10. The NII is divided

into four class from high to low based on the normalized load loss % S_P at the end of the cascade failure model. It can be inferred that the correlation between NII based on the centrality measures and based on the cascade failure model is poor. The low correlation between topology-based indices and others based on the cascade failure model, demonstrate how both approaches consider different information and thus yield different insights. For example, the nodes with high centrality measures based solely on topology model may be of less influence on cascade failure propagation in comparison to other nodes with low centrality measures. Topology-based indices rank nodes (and sometimes links) based on centralities measures which typically employ static network structure characteristics (i.e., number of links, or shortest paths) as explained earlier in the manuscript. On the other hand, indices generated using cascade failure models rank nodes (e.g., substations) and links (e.g., transmission lines) based on power flow, redistribution and failure propagation in order to assess the grid vulnerability.

Although topology-based indices provide a rapid indication of the important components (e.g., substations) in the grid (Hines et al. 2010a; Salama et al. 2021), such indices lack the ability to represent a complete picture of real power grid vulnerabilities as they do not consider the underlying physics governing the grid behavior. As such, physics-based vulnerability indices based on cascade failure models, although more complex to evaluate, provide more comprehensive measures as they consider the dynamic failure propagation, power redistribution,

dispatch and load shedding processes throughout the grid. Furthermore, cascade failure model-based indices evaluate both substation importance levels (i.e., through the node importance index) and transmission line vulnerabilities (i.e., through the link vulnerability index).

4.5. CONCLUSION

This chapter developed a dynamic cascade failure simulator to assess the power grid vulnerability and evaluate its performance under disruptions triggered by component failures. The model adopted the DC flow-based model to consider power redistribution through network after disruptions. To demonstrate its application, a real low to high voltage power network was analysed. The network data included the actual electric characteristics of the network components including the transmission lines impedance and rating capacity, real power at supply nodes, the capacity of supply nodes, and the power demand at load nodes. The model simulates the cascade failure propagation in the network due to initial failure regardless of what caused such failure, including natural and anthropogenic hazard sources. In this respect, two initial case failure scenarios have been implemented in the model: failures of multiple transmission lines, or failure of a network component (e.g., substation). The model subsequently computes the link vulnerability index and node importance index. The link vulnerability index was used to generate a vulnerability map of the power grid which indicates both primary

and secondary probability of failure for each link in the network. The node importance index is estimated according to the cascade failure size that results in the network due to the failure of an initiating node. Furthermore, the results of node importance index from the two different modelling approaches were compared. Overall, the developed approach facilitates identifying critical power grid components crucial to evaluate the grid robustness and enhancing their resilience against random failure and targeted attacks.

Future studies can possibly extend the current work to include maintenance scenarios based on the developed indices and other more conventional ones, and subsequently compare the level of grid resilience improvements. In addition, future studies may consider covering other resilience metrics (i.e., Rebuild and Reconfigure) to address the "draw-up" resilience phase.

4.6. ACKNOWLEDGMENT

This research was supported by the Canadian Nuclear Energy Infrastructure Resilience under Systemic Risk (CaNRisk) – Collaborative Research and Training Experience (CREATE) program of the Natural Science and Engineering Research Council (NSERC) of Canada. Additional support through the INTERFACE Institute and the INViSiONLab of McMaster University is acknowledged.

4.7. REFERENCE

Albert, R., I. Albert, and G. L. Nakarado. 2004. "Structural vulnerability of the North American power grid." Physical review E, 69(2): 25103. https://doi.org/10.1103/PhysRevE.69.025103.

Andersson, G., P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal. 2005. "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance." IEEE Trans. Power Syst., 20(4): 1922–1928. https://doi.org/10.1109/TPWRS.2005.857942.

Barabási, A.-L., and M. Pósfai. 2016. Network science, Cambridge United Kingdom: Cambridge University Press.

Bernstein, A., D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman. 2014. "Power Grid Vulnerability to Geographically Correlated Failures - Analysis and Control Implications." In Proc., IEEE INFOCOM 2014 - IEEE Conference on Computer Communications: 2634–2642. https://doi.org/10.1109/INFOCOM.2014.6848211.

Conover, W. J. 1998. Practical nonparametric statistics: Chapter 6: Statistics of the Kolmogorov-Smirnov Type: John Wiley & Sons.

Costa, L. d. F., O. N. Oliveira, G. Travieso, F. A. Rodrigues, P. R. Villas Boas, L. Antiqueira, M. P. Viana, and L. E. Correa Rocha. 2011. "Analyzing and modeling real-world phenomena with complex networks: A survey of applications."

Advances in Physics, 60(3): 329–412. https://doi.org/10.1080/00018732.2011.572452.

Crucitti, P., V. Latora, and M. Marchiori. 2005. "Locating critical lines in high-voltage electrical power grids." Fluct. Noise Lett., 05(02): L201-L208. https://doi.org/10.1142/S0219477505002562.

Ezzeldin, M., and W. E. El-Dakhakhni. 2019. "Robustness of Ontario power network under systemic risks." Sustainable and Resilient Infrastructure: 1–20. https://doi.org/10.1080/23789689.2019.1666340.

Fang, X., Q. Yang, and W. Yan. 2014. "Modeling and analysis of cascading failure in directed complex networks." Safety Science, 65: 1–9. https://doi.org/10.1016/j.ssci.2013.12.015.

Freeman, L. C. 1977. "A Set of Measures of Centrality Based on Betweenness." Sociometry, 40(1): 35. https://doi.org/10.2307/3033543.

Gasser, P., P. Lustenberger, M. Cinelli, W. Kim, M. Spada, P. Burgherr, S. Hirschberg, B. Stojadinovic, and T. Y. Sun. 2019. "A review on resilience assessment of energy systems." Sustainable and Resilient Infrastructure: 1–27. https://doi.org/10.1080/23789689.2019.1610600.

Haggag, M., A. Yorsi, W. El-Dakhakhni, and E. Hassini. 2021. "Infrastructure performance prediction under Climate-Induced Disasters using data analytics."

International Journal of Disaster Risk Reduction, 56: 102121. https://doi.org/10.1016/j.ijdrr.2021.102121.

Heinimann, H. R., and K. Hatfield. 2017. "Infrastructure resilience assessment, management and governance–state and perspectives." In Resilience and risk: 147–187: Springer.

Hines, P., E. Cotilla-Sanchez, and S. Blumsack. 2010. "Do topological models provide good information about electricity infrastructure vulnerability?" Chaos: An Interdisciplinary Journal of Nonlinear Science, 20(3): 33122.

Ju, W. 2018. "Modeling, Simulation, and Analysis of Cascading Outages in Power Systems.".

Kinney, R., P. Crucitti, R. Albert, and V. Latora. 2005. "Modeling cascading failures in the North American power grid." Eur. Phys. J. B, 46(1): 101–107. https://doi.org/10.1140/epjb/e2005-00237-9.

Li, J., C. Shi, C. Chen, and L. Dueñas-Osorio. 2018. "A cascading failure model based on AC optimal power flow: Case study." Physica A: Statistical Mechanics and its Applications, 508: 313–323. https://doi.org/10.1016/j.physa.2018.05.081.

Motter, A. E. 2004. "Cascade control and defense in complex networks." Physical review letters, 93(9): 98701. https://doi.org/10.1103/PhysRevLett.93.098701.

Motter, A. E., and Y.-C. Lai. 2002. "Cascade-based attacks on complex networks." Physical review. E, Statistical, nonlinear, and soft matter physics, 66(6 Pt 2): 65102. https://doi.org/10.1103/PhysRevE.66.065102.

NERC. 2019. "Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities.", North American Electric Reliability Corporation <https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf>.

Newman, M., ed. 2010. Networks: an introduction: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199206650.001.0001.

Opsahl, T., F. Agneessens, and J. Skvoretz. 2010. "Node centrality in weighted networks: Generalizing degree and shortest paths." Social Networks, 32(3): 245–251. https://doi.org/10.1016/j.socnet.2010.03.006.

Ouyang, M. 2014. "Review on modeling and simulation of interdependent critical infrastructure systems." Reliability Engineering & System Safety, 121: 43–60. https://doi.org/10.1016/j.ress.2013.06.040.

Pagani, G. A., and M. Aiello. 2013. "The power grid as a complex network: a survey." Physica A: Statistical Mechanics and its Applications, 392(11): 2688–2700. https://doi.org/10.1016/j.physa.2013.01.023.

Pahwa, S., M. Youssef, and C. Scoglio. 2014. "Electrical networks: an introduction." In Networks of networks: the last frontier of complexity: 163–186: Springer. https://doi.org/10.1007/978-3-319-03518-5_8.

Panteli, M., and P. Mancarella. 2017. "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events." IEEE Systems Journal, 11(3): 1733–1742. https://doi.org/10.1109/JSYST.2015.2389272.

Rome, E., P. Langeslag, and A. Usov. 2014. "Federated modelling and simulation for critical infrastructure protection." In Networks of networks: the last frontier of complexity: 225–253: Springer.

Rosato, V., S. Bologna, and F. Tiriticco. 2007. "Topological properties of high-voltage electrical transmission networks." Electric Power Systems Research, 77(2): 99–105. https://doi.org/10.1016/j.epsr.2005.05.013.

Salama, M., W. El-Dakhakhni, and M. Tait. 2021. "Mixed Strategy for Resilience Enhancement of Power Grid under Cyberattack." Sustainable and Resilient Infrastructure. https://doi.org/10.1080/23789689.2021.1974675.

Salama, M., M. Ezzeldin, W. El-Dakhakhni, and M. Tait. 2020. "Temporal networks: a review and opportunities for infrastructure simulation." Sustainable and Resilient Infrastructure: 1–16. https://doi.org/10.1080/23789689.2019.1708175.

Schäfer, B., and G. C. Yalcin. 2019. "Dynamical modeling of cascading failures in the Turkish power grid." Chaos: An Interdisciplinary Journal of Nonlinear Science, 29(9): 93134. https://doi.org/10.1063/1.5110974.

Siemens PTI. 2015. Power System Simulator for Engineering (PSSE): PSSE 34.0.1, Siemens Industry, Inc., Siemens Power Technologies International, United States, New York.

Sun, H. J., H. Zhao, and J. J. Wu. 2008. "A robust matching model of capacity to defense cascading failure on complex networks." Physica A: Statistical Mechanics and its Applications, 387(25): 6431–6435. https://doi.org/10.1016/j.physa.2008.07.028.

Wang, J. 2013. "Mitigation strategies on scale-free networks against cascading failures." Physica A: Statistical Mechanics and its Applications, 392(9): 2257–2264. https://doi.org/10.1016/j.physa.2013.01.013.

Wang, J.-W., and L.-L. Rong. 2009. "Cascade-based attack vulnerability on the US power grid." Safety Science, 47(10): 1332–1336. https://doi.org/10.1016/j.ssci.2009.02.002.

Wang, J.-W., and L.-L. Rong. 2011. "Robustness of the western United States power grid under edge attack strategies due to cascading failures." Safety Science, 49(6): 807–812. https://doi.org/10.1016/j.ssci.2010.10.003.

Wang, Z., A. Scaglione, and R. J. Thomas, eds. 2010a. Electrical centrality measures for electric power grid vulnerability analysis: IEEE. https://doi.org/10.1109/CDC.2010.5717964.

Wang, Z., A. Scaglione, and R. J. Thomas. 2010b. "The Node Degree Distribution in Power Grid and Its Topology Robustness under Random and Selective Node Removals." In Proc., 2010 International Conference On Communications Workshops: 1–5. https://doi.org/10.1109/ICCW.2010.5503926.

Wu, B., A. Tang, and J. Wu. 2016. "Modeling cascading failures in interdependent infrastructures under terrorist attacks." Reliability Engineering & System Safety, 147: 1–8. https://doi.org/10.1016/j.ress.2015.10.019.

Yan, J., Y. Tang, H. He, and Y. Sun. 2015. "Cascading failure analysis with DC power flow model and transient stability analysis." IEEE Trans. Power Syst., 30(1): 285–297. https://doi.org/10.1109/TPWRS.2014.2322082.

Yang, Y., T. Nishikawa, and A. E. Motter. 2017. "Small vulnerable sets determine large network cascades in power grids." Science (New York, N.Y.), 358(6365). https://doi.org/10.1126/science.aan3184.

Zhao, K., C. Ma, J. Sun, B. Zhang, L. Ma, and L. Wang, eds. 2018. A New Simulation Method for Complicated Successive Power System Faults in Extreme Weather: IEEE. https://doi.org/10.1109/CIEEC.2018.8745920.

Zio, E. 2013. The Monte Carlo Simulation Method for System Reliability and Risk Analysis, London: Springer London. https://doi.org/10.1007/978-1-4471-4588-2.

4.8. TABLES

Table 4.1: KS Test results for different sample sizes.

		P_{lf_T}	P_{lf_P}	P_{lf_S}
	D (n, m, ∝)	*D*	*D*	*D*
Sample size 1500	0.040	0.084	0.033	0.010
Sample size 3000	0.031	0.051	0.022	0.061
Sample size 4000	0.029	0.027	0.07	0.028

4.9. FIGURES

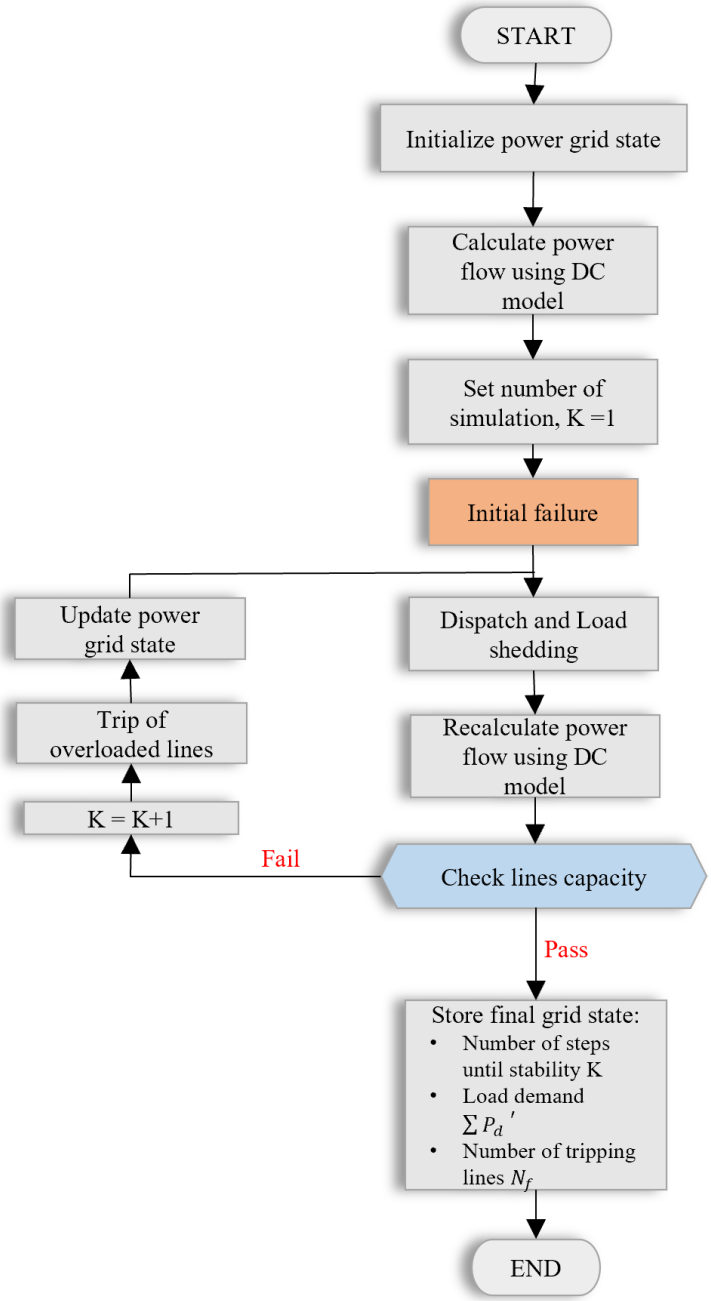

Figure 4.1: Flowchart of the Dynamic Cascade Failure Model procedures.

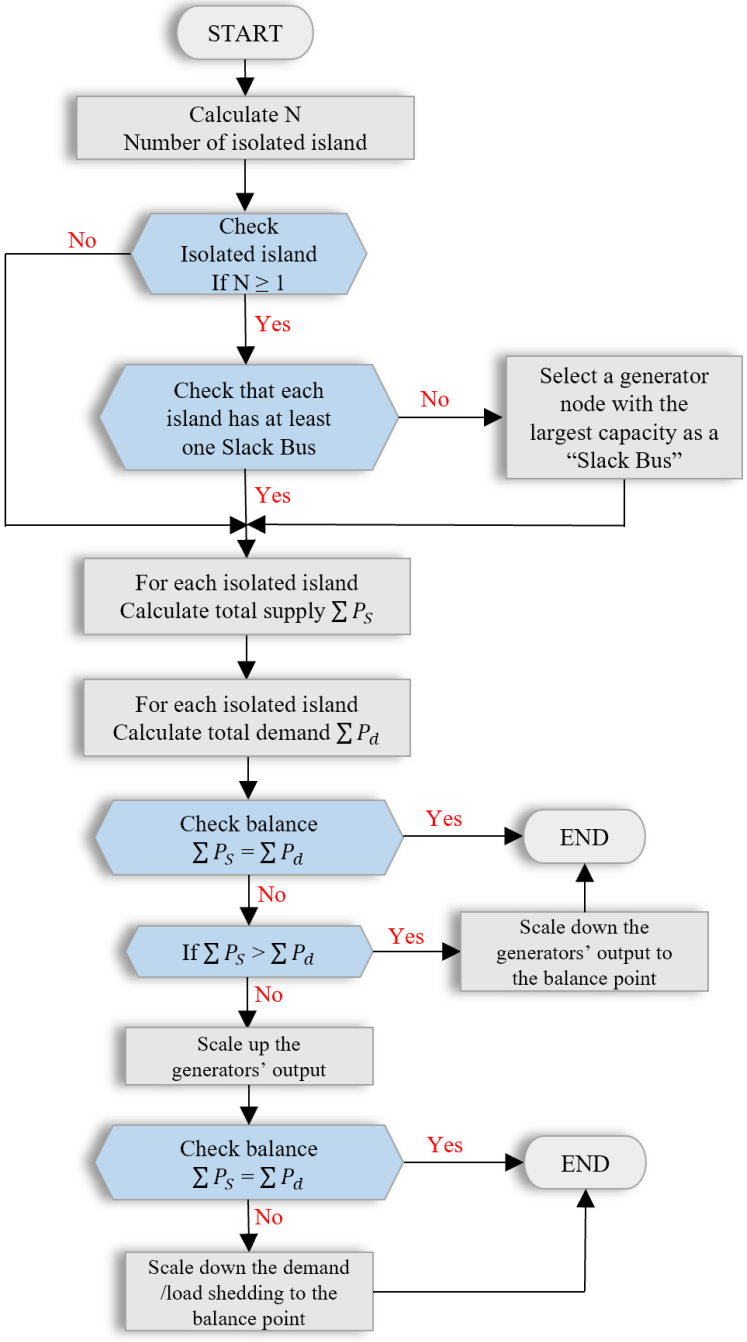

Figure 4.2: Flowchart of the Dispatch and Load shedding procedures.

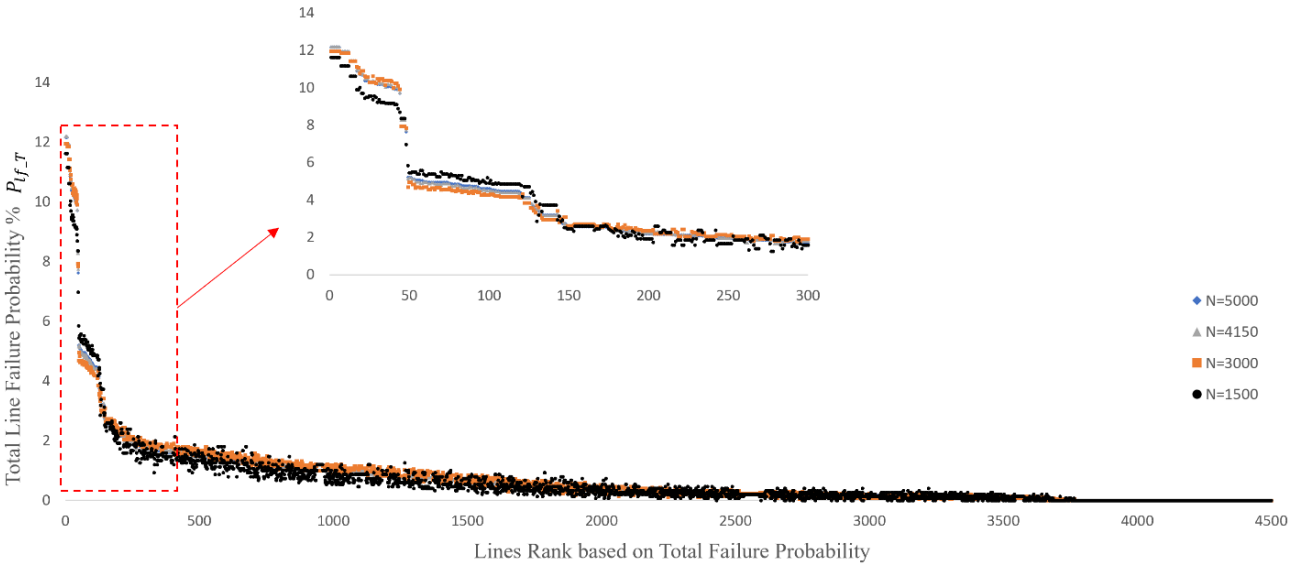

Figure 4.3: The total line failure probability based on different sample sizes (i.e., 1500, 3000, 4000, and 5000).

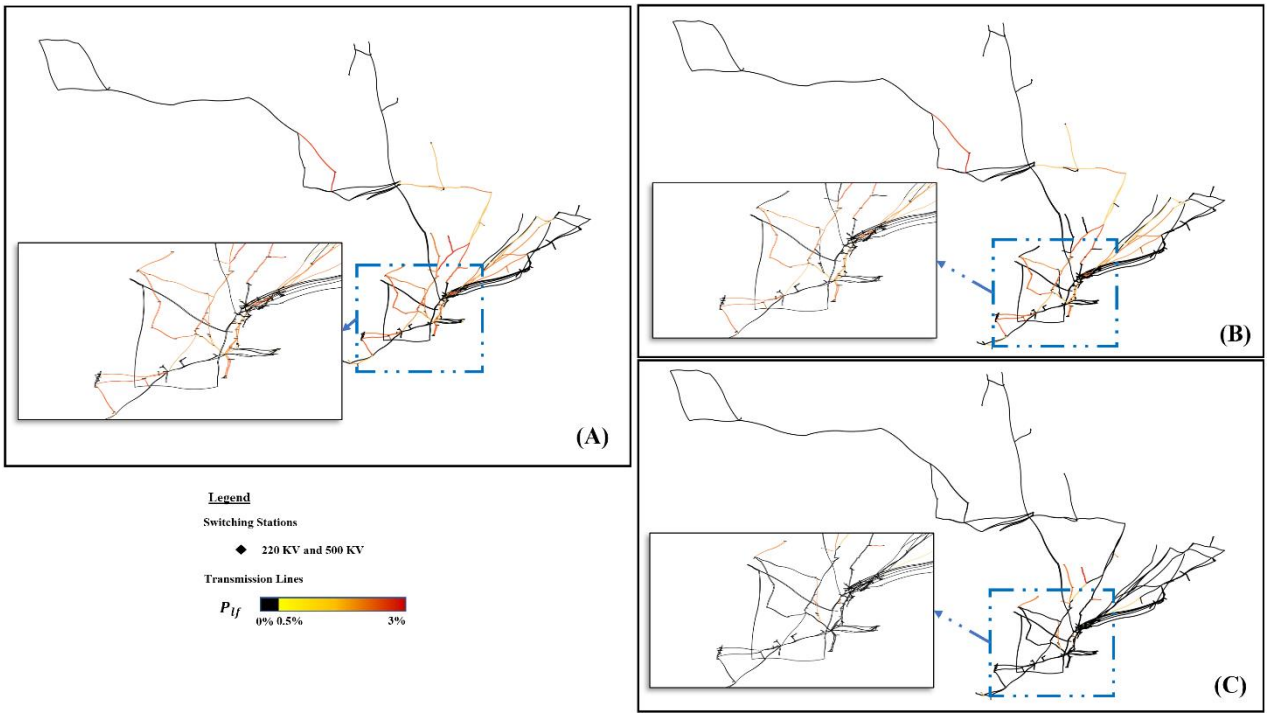

Figure 4.4: Links Vulnerability Index map for the high-voltage transmission lines of Ontario power grid. **(A)** the total failure probability P_{lf_T}. **(B)** the primary failure probability P_{lf_P}. **(C)** the secondary failure probability P_{lf_S}. The transmission line color changes gradually to indicate the failure probability P_{lf} which represents the link vulnerability index (Black links represent the lines with less than 0.5% failure probability).

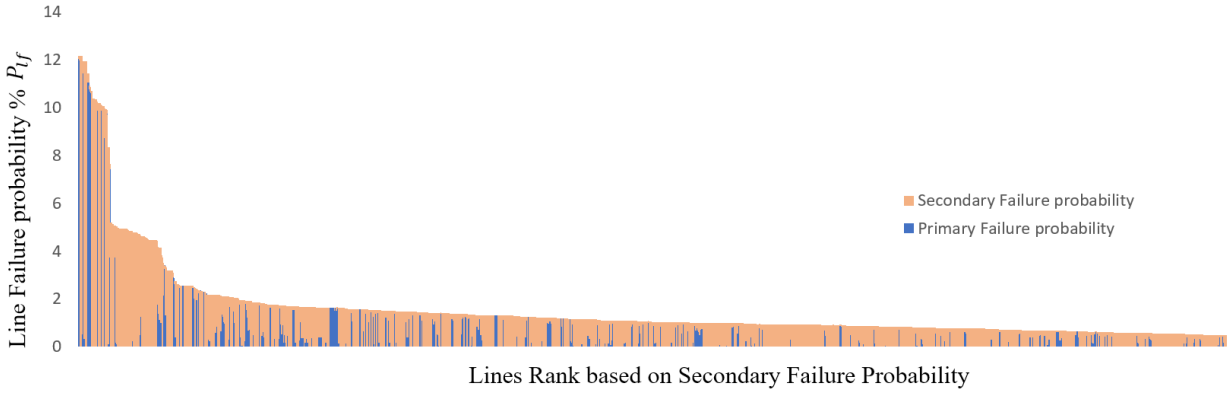

Figure 4.5: The primary and secondary line failure probability.

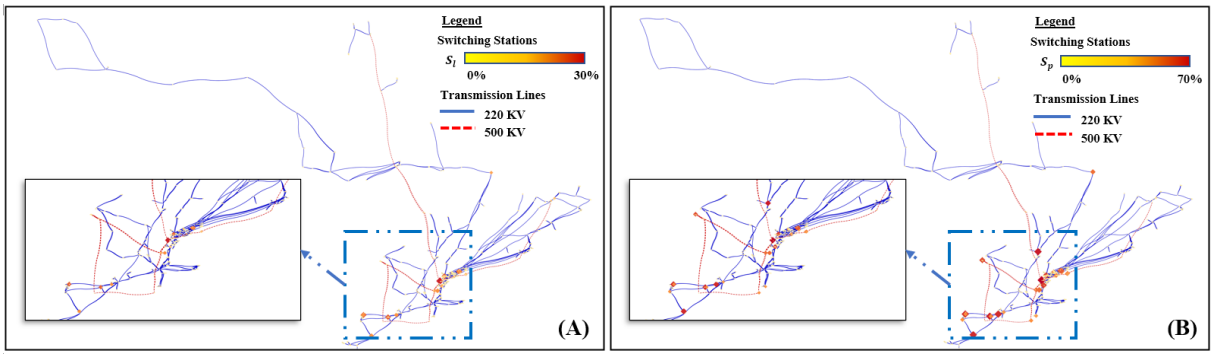

Figure 4.6: Node Importance Index map based on cascade failure effect for the high-voltage transmission lines of Ontario power grid. **(A)** NII measures by the failed lines% S_l at the end of the cascade failure model. **(B)** NII measures by the load loss% S_p at the end of the cascade failure model (Nodes color and size change gradually to indicate the cascade failure size which represents the node importance index).

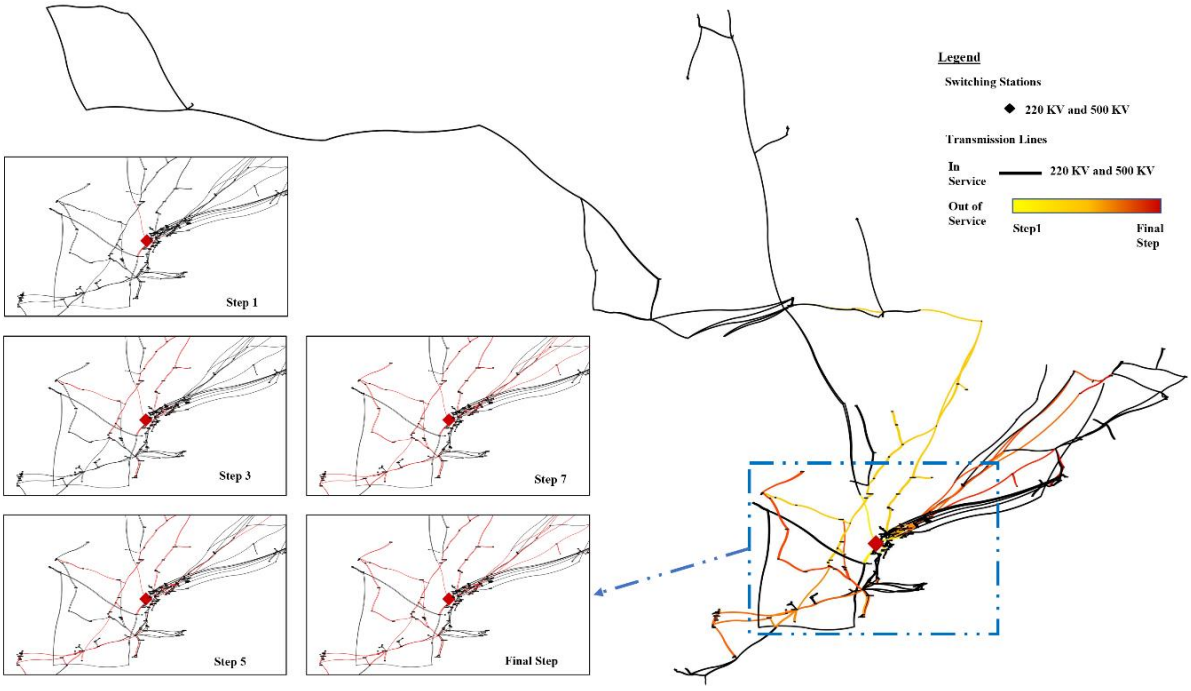

Figure 4.7: Illustration of cascade failure propagation step by step until network stability due to initial failure of the highest NII switching station. The transmission line color changes gradually to represent the step in which the lines faulted (Black links represent the lines that remain in service until the model analysis stops).

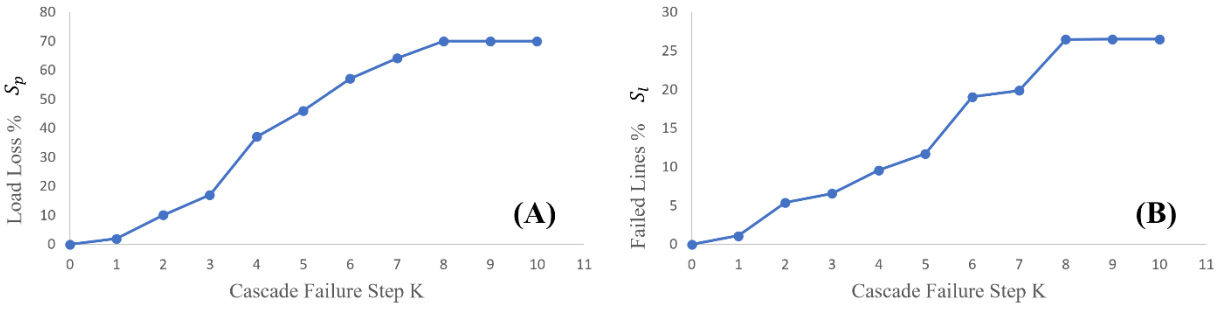

Figure 4.8: Cascade failure size step-by-step evolution until network stability due to initial failure of the highest NII switching station. **(A)** Load loss% S_P , while **(B)** Failed lines% S_l.

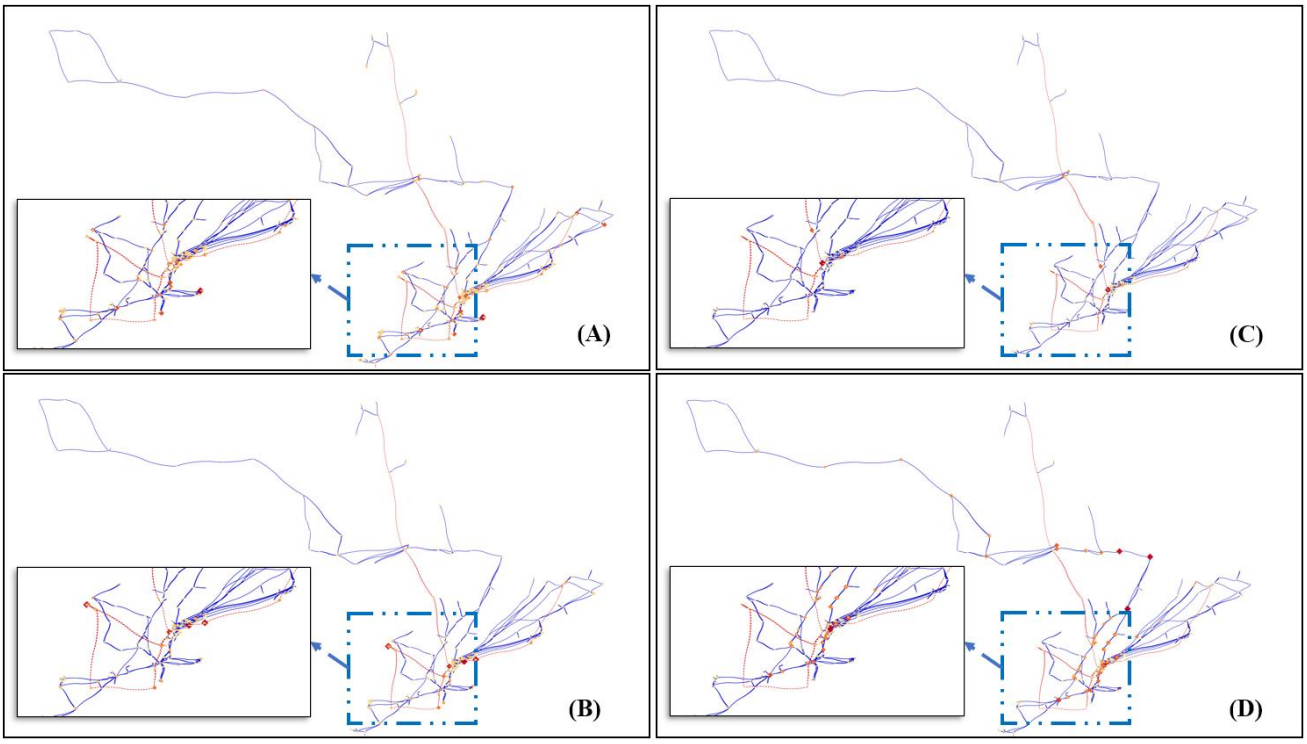

Figure 4.9: Node Importance Index map based on centrality measures for the high-voltage transmission lines of Ontario power grid. **(A)** NII measures by unweight degree centrality $C_D(i)^{UnW}$. **(B)** NII measures by weight degree centrality $C_D(i)^{W}$. **(C)** NII measures by unweight betweenness centrality $C_B(i)^{UnW}$. **(D)** NII measures by weight betweenness centrality $C_B(i)^{W}$(Nodes color and size changes gradually to indicate the normalized centrality measure which represents the node importance index).

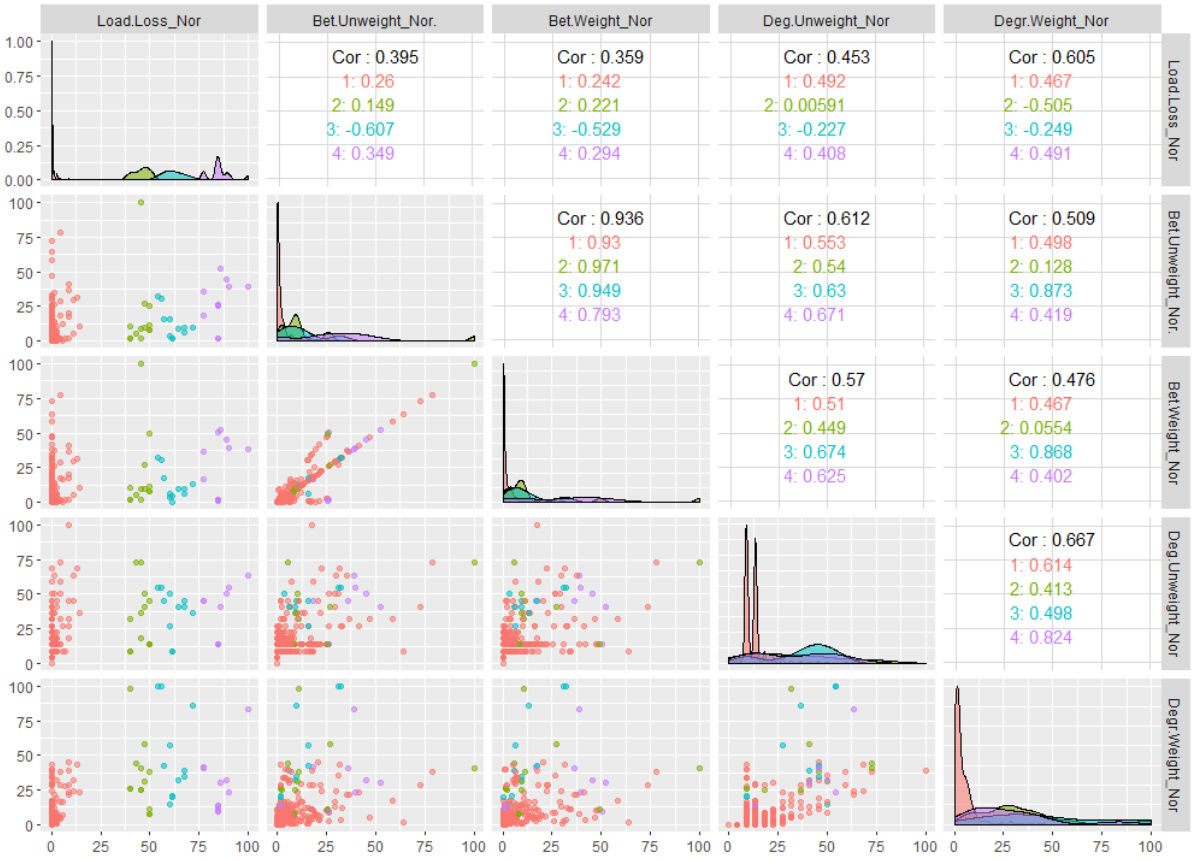

Figure 4.10: Correlation between NII based on load loss and different centrality measures (Node color indicated which class the node belongs to according to the normalized load loss% S_P).

Chapter 5 : Intentional Controlled Islanding and Flow Rebalance for Power Grid Systemic Risk Mitigation

ABSTRACT

Power grids are prone to damage induced by natural or anthropogenic hazard events that might disrupt the functionality of multiple grid components concurrently, resulting in a chain of cascade failures throughout. Through integrating operation-with structure-guided strategies, the current study focuses on mitigating the risk of such cascade failure (known as systemic-risk) to minimize the possibility of large-scale catastrophic blackouts. The operation-guided strategy is implemented through dispatch and load shedding to rebalance demand and supply after disruptive events. On the other hand, the structure-guided strategy adopted intentional controlled islanding approach through employing a constrained spectral clustering algorithm. Introducing the algorithm within the cascade failure model facilitated identifying the optimal cut-set lines to separate the grid into functioning sub-grids following initial failure and prior to failure propagation. To assess the effectiveness of the mitigation strategy, a real power scale grid was modelled under different systemic risk scenarios to compare the cascade failure size with and without the proposed strategy for different number of sub-grids. The simulations demonstrate that a well-developed controlled islanding strategy can effectively boost grid robustness and mitigate blackout systemic risks.

Keywords: Intentional Controlled Islanding, Constrained Spectral Clustering, Risk Mitigation Strategy, Cascade Failure.

5.1. INTRODUCTION

The ever-evolving interconnectedness and complexity of power grids have increased their vulnerability to disruptions. Furthermore, the growing energy demand has been forcing operators to push power grids near their operational limits (LIN et al. 2016). In the last 20 years, the number of major blackouts has increased significantly, sometimes leading to catastrophic socio-economic consequences (Kyriacou et al. 2018).

Cascade failure is a chain of failures initiated by a disruption in key network components (e.g., tripping of overloaded transmission lines), thus overloading other components and, as a result, propagate throughout the network (Bernstein et al. 2014b; Yang et al. 2017). Furthermore, the growth in the networks' complexity, interconnectedness, and interdependency leads to extending the risk from component- to systems-level failure (i.e., *systemic risk*). As such, there has been pressing demands to provide mitigation strategies to suppress failure propagation and reduce the possibility of system-level failures, thus increasing the grid ability to withstand and keep operating in the face of disruptive events (i.e., *grid robustness*). Power grid risk mitigation strategies can be categorized into three main categories: device-guided (i.e., smart devices like FACTS devices to control network transmission line power flow, voltage and/or PSS devices), operation-guided (e.g. dispatch and load shedding, and load rejection), and structure-guided

(e.g., redesigning critical components, adding redundancy, and intentional controlled islanding) (Ahangar et al. 2020).

Previous studies (Ahangar et al. 2020; Li et al. 2010) have shown that grid separation into a number of controlled functioning islands (*intentional controlled islanding*) can be an effective defence strategy to save them from a large-scale uncontrolled blackout. However, such separation must be performed diligently, or it can introduce even further destabilization in the grid, potentially boosting the cascade failure, which it is expected to suppress. Intentional Controlled Islanding (ICI) aims to split the grid into stable and functioning sub-grids in an optimized way to minimize the power flow disruption or minimize the power flow imbalance (Ding et al. 2014; Quirós-Tortós et al. 2015). ICI can identify the optimal set of transmission lines to be disconnected to protect the resulting islands from the disturbance.

In an attempt to solve the network cluster problem, some researchers used approaches, including graph search (Aghamohammadi and Shahmohammadi 2012; Maharana and Swarup 2010), heuristic search methods (Theodoro et al. 2012; Trodden et al. 2013), neural network (Wang 2005; Wang and Chang 1994), and spectral clustering (Ding et al. 2014; Quirós-Tortós et al. 2015). To minimize the power flow disruption, the ICI can be modelled as the graph-cut problem, which can be solved efficiently using complex network theoretic techniques such as spectral clustering approach (Kyriacou et al. 2018). Spectral clustering has the

advantage of providing a deterministic solution in a polynomial time (Luxburg 2007). Generally, spectral clustering uses the eigenvalues and eigenvectors associated with a weighted network, that represents the power grid, to solve the graph-cut problem.

Most previous studies (Ahangar et al. 2020) focused on determining the optimal splitting algorithm considering solution time variation, number of clusters and/or controlled constraints, without testing these algorithm capabilities in suppressing the failure propagation considering a dynamic cascade failure model. As such, there is a lack of integration between large-scale failure propagation simulations and intentional controlled islanding solutions to evaluate the effectiveness of ICI as a risk mitigation strategy.

This chapter focuses on providing and testing a strategy for suppressing power grid cascade failure propagations by integrating operation- and structure-guided mitigation strategies. First, operation-guided strategy is implemented by dispatch and load shedding to rebalance demand and supply after disruptive events. Second, structure-guided strategy is introduced by embedding the Constrained Spectral Clustering (CSC) algorithm in the cascade failure model to intentionally split the power grid. Following this section, CSC algorithm description, explanation, and assumptions are presented in Section 5.2. Next, a brief description of the cascade failure model that has been used to evaluate the improvement in network performance due to the use of CSC is provided in Section. Subsequently,

the results of applying the mitigation strategy utilizing actual power grid cascade failure simulations are presented in Section 5.4. Finally, concluding remarks are provided in Section 5.5.

5.2. INTENTIONAL CONTROLLED ISLANDING (ICI)

ICI is a corrective control action for grid under a severe contingency (i.e., loss / failure of power grid components such as transmission lines, generators, or transformers) to prevent the cascade failure propagation. ICI essentially splits the grid into several isolated sub-grids as a defences strategy following instabilities and prior to the grid becomes uncontrollable (Ding et al. 2018). ICI techniques focus on determining, in real-time, the set of transmission lines to be disconnected to create stable functioning sub-grids. Specifically, the optimal ICI solution, that will result in a minimal power flow disruption, can be determined similar to the graph-cut problem using spectral clustering (Goubko and Ginz 2019). Therefore, CSC can be viewed as an extension of the spectral clustering method by introducing a constrain matrix to exclude some transmission lines from the clustering solution.

CSC is an efficient complex network theoretic technique that enables splitting the network using the network eigenvalues and eigenvectors that represent the power grid. The CSC algorithm used in the current study has been proposed by Wang et al. (2014). This section presents relevant complex network theoretic

metrics, Laplacian matrix, eigenvalues, constrain matrix, the objective function, and CSC algorithm description

5.2.1. POWER GRID AS A COMPLEX NETWORK

Within a complex network theory context, A power grid can be represented by weighted and undirected network $G(N, L)$ with N nodes (e.g., substations in power networks) and L links represent the interdependencies between these nodes within such a network (e.g., transmission lines in power grids) (Salama et al. 2020). The N nodes have been classified into three groups, namely: $N_S \in N$ supply-station nodes "generator", $N_D \in N$ demand-station nodes "load", and $N_J \in N$ switching-station nodes "junction". In a weighted network, each link is assigned a weight based on the power flow value. This approach assumes that transmission lines that carry more flow have more influence than the lines that carry the smaller flow. Therefore, a link weight w_{ij} represents the weight factor associated with the link L_{ij} is calculated as follows:

$$w_{ij} = w_{ji} = \begin{cases} \dfrac{|f_{ij}| + |f_{ji}|}{2} & if \quad L_{ij} \in L \\ 0 & Otherwise \end{cases} \qquad (1)$$

Where, f_{ij} is the power flow in the transmission lines from substation i to substation j. The power flow can be calculated based on the Direct Current power flow model (DC power model). The DC power model is widely used as an approximation method for the alternating current power model to simplify the power flow analysis in the power network (Pahwa et al. 2014; Salama et al. 2021).

Therefore, A is weight adjacency $n\ x\ n$ matrix of the network G. A matrix is symmetric and non-negative computed as follows:

$$A = \begin{cases} A_{ij} = w_{ij} \\ A_{ji} = w_{ji} \\ A_{ii} = 0 \end{cases} \quad (2)$$

The diagonal matrix D is called the degree matrix of network G computed as follows:

$$D_{ii} = \sum_{j=1}^{N} A_{ij} \quad (3)$$

5.2.2. LAPLACIAN MATRICES/EIGENVALUES

Laplacian matrices are the basis for network spectral clustering (Luxburg 2007). Typically, there are two types of Laplacian matrices: the '*unnormalized*' Laplacian matrix L_{un} and the '*normalized*' Laplacian matrix L_n. The *unnormalized* Laplacian matrix L_{un} of network G:

$$L_{un} = D - A \quad (4)$$

While the *normalized* Laplacian matrix L_n of network G:

$$L_n = D^{-\frac{1}{2}} L_{un} D^{-\frac{1}{2}} \quad (5)$$

Previous studies (Quirós-Tortós et al. 2015; Wang et al. 2014) showed that the normalized Laplacian matrix L_n results in better solution compared with the unnormalized for weighted networks. Hence, the below algorithm uses the eigenvectors associated with the eigenvalues of the normalized Laplacian matrix.

5.2.3. CONSTRAINT MATRIX

Constraint matrix Q contained two main types of constraints: '*Must-Link*' ML and '*Cannot-Link*' CL (Luxburg 2007). ML $(\mathrm{I,j})$ constraint indicates that node i and node j must be in the same cluster, while CL $(\mathrm{I,j})$ constraint indicates that node i and node j cannot be clustered together. Therefore, ML constraint represents the transmission lines that must exclude from the islanding solution (i.e., transmission lines that are important for network stability).

$$Q_{ij} = Q_{ji} = \begin{cases} +1 & \text{if (i, j)} \quad ML \\ -1 & \text{if (i, j)} \quad CL \\ 0 & \text{Otherwise} \end{cases} \quad (6)$$

Therefore, the *normalized* constraint matrix is:

$$Q_n = D^{-\frac{1}{2}} Q D^{-\frac{1}{2}} \quad (7)$$

5.2.4. OBJECTIVE FUNCTION

Shi and Malik (2000) demonstrated that the eigenvectors of the normalized Laplacian matrix are related to the normalized *min-cut* of the network G. Therefore, the objective function can be written as:

$$argmin \;\; V^T L_n V \qquad (8)$$

Subjected to:

$$V^T Q_n V \geq 0 \qquad (9)$$

$$V^T V = vol \qquad (10)$$

$$V \neq D^{\frac{1}{2}} 1 \qquad (11)$$

Where, V is the eigenvector of the normalized Laplacian matrix, vol is the volume of the network G ($vol = \sum_{i=1}^{N} D_{ii}$).

$V^T L_n V$ represents the cost of the cut, which is the power flow disruption due to network splitting. The objective function in Eq.8 is to get the optimal $(K-1)$ eigenvectors V^* to cluster the nodes in a way minimizing the power flow disruption (i.e., select the top $K-1$ in term of minimizing $V^T L_n V$). K is the number of the clusters. The first constrain represents the constraint matrix Q, the second constraint normalizes the eigenvectors, and the third constraint removes the trivial eigenvector solution. Therefore, the optimal cluster indicator vector u^* can be calculated as:

$$u^* = kmeans\,(D^{\frac{1}{2}} V^*, K) \qquad (24)$$

The optimal cluster indicator vector identifies which cluster each node in the network will belong to. Based on the optimal cluster indicator, the optimal cut-set lines (i.e., the set of lines to be removed/switch off to separate the grid into functioning sub-grids) will be selected.

The above optimization problem can be solved by using CSC algorithm presented in (Wang et al. 2014) through applying the following steps:

1. **Generate candidates:** Solve the generalized eigenvalue problem $L_n V = \lambda\, Q_n\, V$ to establish all eigenvectors for the normalized Laplacian matrix and normalized constraint matrix**.**

2. **Find feasible set:** Exclude eigenvector associated with negative eigenvalue to remove the trivial eigenvector solution and subsequently normalize the rest eigenvector such that $V^T\, V = vol$

3. **Choose optimal solution:** Select the optimal $(K-1)$ eigenvectors V^* which minimizes the cut cost $V^T L_n\, V$.

The CSC algorithm is implemented in the model as follows:

	Constrained Spectral Clustering Algorithm:
	Input: Weighted network adjacency matrix A, Constrained matrix Q, Number of Clusters K
	Output: Optimal cluster vector u^*
1	**Start**
2	Establish the degree matrix $D_{ii} = \sum_{j=1}^{N} A_{ij}$, Network volume $vol = \sum_{i=1}^{N} D_{ii}$
3	Establish the unnormalized Laplacian matrix $L_{un} = D - A$
4	Establish the normalized Laplacian matrix $L_n = D^{-1/2} L_{un} D^{-1/2}$
5	Establish the normalized constrained matrix $Q_n = D^{-1/2} Q D^{-1/2}$
6	Solve the generalized eigenvalue problem $L_n V = \lambda Q_n V$
7	Remove eigenvector associated with negative eigenvalues
8	Normalize the rest of eigenvectors such that $V^T V = vol$
9	Calculate the cost $V^T L_n V$ for all rest eigenvectors
10	Choose the optimal $(K-1)$ eigenvectors V^* which has the minimum cost calculated in the previous step
11	**Return** the optimal cluster vector $u^* = kmeans\ (D^{1/2} V^*, K)$
12	**End**

5.3. SYSTEMIC RISK MITIGATION STRATEGY

5.3.1. CASCADE FAILURE MODEL

Cascade failure starts with a disruption in some key network components leading to overloading of other components and subsequently initiating a chain of failures, which can rapidly spread throughout the network, causing catastrophic failures (Bernstein et al. 2014b; Costa et al. 2011). A dynamic cascade failure model has been used to simulate failure propagation through the grid (Salama et al. 2022). The

model integrates the network topology with physics-based network flow that calculates the actual power flow using the DC power model. In the DC power model, nonlinear equations of alternating current power model are simplified to a linear form. The DC power model is used wherever repetitive and fast load flow estimations are required, whereas this method is non-iterative and absolutely convergent.

Following a disruptive event (i.e., initial failure), the dispatch and load shedding process is initiated to rebalance demand and supply. Subsequently, the model checks the transmission line capacity against the recalculated power flow due to disruptive event. Each iteration in the propagation simulation begins with tripping the overloaded transmission lines. Following each overloaded component removal, the network is examined to assess if it remains as one connected grid or is separated into isolated sub-grids (i.e., islands). The dispatch and load shedding process thus attempts to maintain the balance by scale up/down the generator's output or scale down the demand according to the supply-to-demand unbalance. This process is the initial operational corrective to decrease grid instability (Yan et al. 2015). More explanation of the cascade failure model and dispatch and load shedding algorithm can be found in (Salama et al. 2022). At the conclusion of failure, the loss of service is quantified based on two measures:

1. Cascade size based on the topology S_l, calculated as the percentage of failed links N_f (i.e., out of service transmission lines due to initial failure and the overloaded lines) to the total number of links *N*.

$$S_l = \frac{N_f}{N} \qquad (13)$$

2. Cascade size based on the power flow S_p, calculated as the percentage of the loss of demand load to the original load of the network.

$$S_p = \frac{\sum P_d - \sum P_d{}'}{\sum P_d} \qquad (14)$$

where, $\sum P_d$ is the total original load, and $\sum P_d{}'$ is the total demand load at the end of cascade failures.

5.3.2. CASCADE FAILURE MODEL WITH CSC

The CSC algorithm has been integrated within the cascade failure model described above in Section 5.3.1 to suppress the cascade failure based on ICI, as shown in Figure 5.1. The ICI shifts the cascade failure scenario to follow another path through the network. Noteworthy, the proposed strategy is different from *network interdiction*, which relies on reinforcement the weak components identified (i.e., redesign critical components and/or adding redundancy) (Salmeron et al. 2009). The proposed strategy is also distinguished by its direct implementation ability within a power grid network with less additional cost compared to network interdiction strategies.

The cascade failure model with CSC algorithm is implemented as follows:

	Cascade Failure with CSC Algorithm:
	Input: Initial Grid State $G(N,L)$, Lines Capacity C_{ij}, Lines Reactance x_{ij}, Number of Simulation $t = 1$
	Output: Final Grid State, Load demand $\sum P_d{}'$, t
1	**Start**
2	Compute Power Flow; f_{ij} (DC model)
3	Introduce the initial failure (Contingency)
4	Adjust demand and supply (Dispatch and Load Shedding Algorithm)
5	Recompute Power Flow; ${f_{ij}}^t$ (DC model)
6	***If:*** lines power flow ${f_{ij}}^t$ < lines capacity C_{ij} Store final grid state and **End** ***Else***; *CSC algorithm*
7	Adjust demand and supply (Dispatch and Load Shedding Algorithm)
8	Recompute Power Flow; ${f_{ij}}^t$ (DC model)
9	***While:*** Lines power flow ${f_{ij}}^t$ > Lines capacity C_{ij} Find the set of overloaded lines Trip the overloaded lines Adjust demand and supply (Dispatch and Load Shedding Algorithm) Recompute Power Flow; ${f_{ij}}^t$ (DC model) $t = t + 1$
10	Store final grid state; Load demand $\sum P_d{}'$, Number of steps until stability t
11	**End**

5.4. MODEL APPLICATION DEMONSTRATION

The Ontario power grid has been considered herein to demonstrate and assess the effectiveness of ICI technique based on CSC as a mitigation strategy to suppress the propagation of the failure in large-scale grid. Ontario power grid based on Independent Electricity System Operator (IESO) base case scenario was modelled as 3,653 nodes and 4,503 links. For clarity, only the high voltage transmission

network (i.e., the stations and transmission lines with base voltage equal to 220 and 500 kV) are presented.

The cascade failure model explained above in Section 5.3.1 has been used to identify the worst-case scenarios that cause the maximum damage in the network structure (i.e., maximum cascade failure size based on power flow loss S_p), as a result of single component failure (i.e., removal). Subsequently, the cascade failure model with CSC has been used to split the grid into sub-grids following initial failure triggering and prior to failure propagation for the same worst-case scenarios specified from the model without CSC. Finally, the results of the two models were compared to assess the proposed approach effectiveness. Figure 5.2 illustrates the cascade failure propagation due to the worst-case initial single bus failure scenario without and with CSC implementation to split the grid into two or three sub-grids. In addition, the cascade failure size based on power flow S_P (i.e., load loss) and based on topology S_l (i.e., failed lines) are demonstrated in a step-by-step manner in Figure 5.3. It can be observed that the cascade failure size based on power flow S_P is reduced from 70% to 34% and 41% considering two and three sub-grids, respectively. This is double the network robustness relative to the failure scenario without the proposed mitigation strategy. Whereas the cascade failure size based on topology S_l is reduced from 27% to 4% and 8% for case of two and three sub-grids, respectively. In addition, it can be noticed that the number of cascade failure steps (i.e., the number of steps until the network reaches stability) are reduced for

both cluster cases. For example, the number of steps until stability without CSC is nine, whereas this value decreases to five and seven steps in the two and three sub-grid cases, respectively. Therefore, the network in case of CSC algorithm reached stability earlier than the network without CSC, which results in yet another improvement in network robustness and systemic risk mitigation.

To measure the robustness improvement under different failure scenarios, the top 15 worst-case initial single bus failure scenarios have been used to compare the cascade failure size without and with CSC. Figure 5.4 and Figure 5.5 present the cascade failure size S_p and S_l, respectively for the top 15 worst-case failure scenarios. It can be noticed that there is a significant improvement in grid robustness (i.e., less cascade failure size in terms of load loss and failed lines) considering the CSC use with two sub-grids. It can also be observed that using CSC with three sub-grids was less effective in comparison to the CSC with two sub-grids, further, it increased the failure in some scenarios. Accordingly, selecting a higher number of clusters (i.e., sub-grids), in the demonstrated power grid, leads to more lines being out of service, which may cause more damage to the network structure and introduce additional failures.

Figure 5.6 presents the reduction in the cascade failure size due to the proposed mitigation strategy in case of using the CSC to split the grid into two or three sub-grids. It can be noticed that in case of using CSC with two sub-grids, most failure scenarios (i.e., twelve out of the top 15 worst-case) have a smaller cascade

failure size with an average reduction equals to 37% and 62% for S_p and S_l, respectively. While, in case of using CSC with three sub-grids, the average reduction is 4% and 26% for S_p and S_l, respectively. For example, using CSC with two sub-grids results in a reduction in the cascade failure size based on the topology (i.e., number of failed lines S_l) for all the cascade failures scenarios addressed here. While, in case of using CSC with three sub-grids, there are three failure scenarios that ended with a higher number of failed lines S_l in comparison to the cascade model without the CSC. Moreover, regarding the reduction in the cascade failure size based on the power flow (i.e., load loss S_p), there is a significant reduction in the case of using CSC with two sub-grids except for three failures scenarios. While, in case of using CSC with three sub-grids, only five out of the 15 failures scenarios have less S_p in comparison to the cascade model without the CSC. It can be concluded that there is a general improvement in network robustness with implementing CSC mitigation strategy; however, the CSC results are sensitive to the numbers of sub-grids and the constrained matrix. Therefore, it is important to diligently choose the constrain matrix and number of the clusters in CSC algorithm to exclude critical transmission lines from the cut-set to prevent introduce additional failure to the grid. The critical transmission lines can be identified by network topology (Salama et al. 2021), electric characteristics (Bai and Miao 2015), failure mechanism (Yang et al. 2017), and integrated methods (Wang et al. 2017a).

5.5. CONCLUSION

This chapter presented an effective mitigation strategy to suppress the cascade failure propagation in power grids through integrating operation-guided mitigation strategy (i.e., dispatch and load shedding) and the structure-guided mitigation strategy (i.e., intentional controlled island). The effectiveness of the mitigation strategy has been illustrated through the cascade failure model on a realistic large-scale network with data ranging from low to high voltage. A high-fidelity physics-based model of power grid that considers the actual power flow, the transmission lines' electrical properties, and the generators' supply and capacity has been used. The cascade failure model adopted the DC flow-based model to consider power redistribution through the network after contingencies.

The cascade failure model employed the spectral constrained clustering algorithm to select the optimal cut-set lines to minimize the power flow disruption. The ICI is a low-cost corrective action that can directly apply to a power grid with the least additional cost. The numerical results emphasize that the ICI mitigation strategy is an efficient technique to boost the network robustness. However, the ICI of a power grid should be performed diligently, or it might add more destabilization in the grid. Moreover, the proposed strategy can be implemented automatically to any component failure in the network, not only in the worst-case scenario.

Accordingly, this strategy presents an adaptive control-oriented risk mitigation strategy.

Nevertheless, further studies are required before an implementation of ICI scheme in real-life power grids. Future studies would extend the current CSC algorithm with multi-objective to minimize power flow disruption, minimize load shedding in each sub-grid, and fairly distributed the generators between the sub-grids. Subsequently, future studies shall determine in a real-time manner, the suitable number of sub-grids, the most suitable time to implement the ICI into the grid, and the planning for grid reconfigure phase.

5.6. ACKNOWLEDGMENT

This research was supported by the Canadian Nuclear Energy Infrastructure Resilience under Systemic Risk (CaNRisk) – Collaborative Research and Training Experience (CREATE) program of the Natural Science and Engineering Research Council (NSERC) of Canada. Additional support through the INTERFACE Institute and the INViSiONLab of McMaster University is acknowledged.

5.7. REFERENCE

Aghamohammadi, M. R., and A. Shahmohammadi. 2012. "Intentional islanding using a new algorithm based on ant search mechanism." International

Journal of Electrical Power & Energy Systems, 35(1): 138–147. https://doi.org/10.1016/j.ijepes.2011.10.006.

Ahangar, A. R. H., G. B. Gharehpetian, and H. R. Baghaee. 2020. "A review on intentional controlled islanding in smart power systems and generalized framework for ICI in microgrids." International Journal of Electrical Power & Energy Systems, 118(3): 105709. https://doi.org/10.1016/j.ijepes.2019.105709.

Bai, H., and S. Miao. 2015. "Hybrid flow betweenness approach for identification of vulnerable line in power system." IET Generation, Transmission & Distribution, 9(12): 1324–1331.

Bernstein, A., D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman. 2014. "Power Grid Vulnerability to Geographically Correlated Failures - Analysis and Control Implications." In Proc., IEEE INFOCOM 2014 - IEEE Conference on Computer Communications: 2634–2642.

Costa, L. d. F., O. N. Oliveira, G. Travieso, F. A. Rodrigues, P. R. Villas Boas, L. Antiqueira, M. P. Viana, and L. E. Correa Rocha. 2011. "Analyzing and modeling real-world phenomena with complex networks: A survey of applications." Advances in Physics, 60(3): 329–412. https://doi.org/10.1080/00018732.2011.572452.

Ding, L., Y. Guo, P. Wall, K. Sun, and V. Terzija. 2018. "Identifying the Timing of Controlled Islanding Using a Controlling UEP Based Method." IEEE

Trans. Power Syst., 33(6): 5913–5922. https://doi.org/10.1109/TPWRS.2018.2842709.

Ding, L., P. Wall, and V. Terzija. 2014. "Constrained spectral clustering based controlled islanding." International Journal of Electrical Power & Energy Systems, 63(4): 687–694. https://doi.org/10.1016/j.ijepes.2014.06.016.

Goubko, M., and V. Ginz. 2019. "Improved spectral clustering for multi-objective controlled islanding of power grid." Energy Systems, 10(1): 59–94.

Kyriacou, A., P. Demetriou, C. Panayiotou, and E. Kyriakides. 2018. "Controlled Islanding Solution for Large-Scale Power Systems." IEEE Trans. Power Syst., 33(2): 1591–1602. https://doi.org/10.1109/TPWRS.2017.2738326.

Li, J., C.-C. Liu, and K. P. Schneider. 2010. "Controlled Partitioning of a Power Network Considering Real and Reactive Power Balance." IEEE Trans. Smart Grid, 1(3): 261–269. https://doi.org/10.1109/TSG.2010.2082577.

LIN, Z., F. WEN, J. ZHAO, and Y. XUE. 2016. "Controlled islanding schemes for interconnected power systems based on coherent generator group identification and wide-area measurements." J. Mod. Power Syst. Clean Energy, 4(3): 440–453. https://doi.org/10.1007/s40565-016-0215-6.

Luxburg, U. von. 2007. "A tutorial on spectral clustering." Stat Comput, 17(4): 395–416. https://doi.org/10.1007/s11222-007-9033-z.

Maharana, M. K., and K. S. Swarup. 2010. "Graph theoretic approach for preventive control of power systems." International Journal of Electrical Power & Energy Systems, 32(4): 254–261. https://doi.org/10.1016/j.ijepes.2009.09.010.

Pahwa, S., M. Youssef, and C. Scoglio. 2014. "Electrical networks: an introduction." In Networks of networks: the last frontier of complexity: 163–186: Springer.

Quirós-Tortós, J., R. Sánchez-García, J. Brodzki, J. Bialek, and V. Terzija. 2015. "Constrained spectral clustering-based methodology for intentional controlled islanding of large-scale power systems." IET Generation, Transmission & Distribution, 9(1): 31–42. https://doi.org/10.1049/iet-gtd.2014.0228.

Salama, M., W. El-Dakhakhni, and M. Tait. 2021. "Mixed Strategy for Resilience Enhancement of Power Grid under Cyberattack." Sustainable and Resilient Infrastructure. https://doi.org/10.1080/23789689.2021.1974675.

Salama, M., W. El-Dakhakhni, and M. Tait. 2022. Forthcoming, "Dynamic Network Flow

Model for Power Grid Systemic Risk Assessment and Resilience Enhancement", Journal of Infrastructure Systems, https://doi.org/10.1061/(ASCE)IS.1943-555X.0000677.

Salama, M., M. Ezzeldin, W. El-Dakhakhni, and M. Tait. 2020. "Temporal networks: a review and opportunities for infrastructure simulation." Sustainable and Resilient Infrastructure: 1–16. https://doi.org/10.1080/23789689.2019.1708175.

Salmeron, J., K. Wood, and R. Baldick. 2009. "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids." IEEE Trans. Power Syst., 24(1): 96–104. https://doi.org/10.1109/TPWRS.2008.2004825.

Shi, J., and J. Malik. 2000. "Normalized cuts and image segmentation." IEEE Trans. Pattern Anal. Machine Intell., 22(8): 888–905. https://doi.org/10.1109/34.868688.

Theodoro, E.A.R., R.A.S. Benedito, J.B.A. London, and L.F.C. Alberto. 2012. "Algebraic-graph method for identification of islanding in power system grids." International Journal of Electrical Power & Energy Systems, 35(1): 171–179. https://doi.org/10.1016/j.ijepes.2011.10.010.

Trodden, P. A., W. A. Bukhsh, A. Grothey, and K.I.M. McKinnon. 2013. "MILP formulation for controlled islanding of power networks." International Journal of Electrical Power & Energy Systems, 45(1): 501–508. https://doi.org/10.1016/j.ijepes.2012.09.018.

Wang, M.-H. 2005. "Extension neural network-type 2 and its applications." IEEE transactions on neural networks, 16(6): 1352–1361. https://doi.org/10.1109/TNN.2005.853334.

Wang, M.-H., and H.-C. Chang. 1994. "Novel clustering method for coherency identification using an artificial neural network." IEEE Trans. Power Syst., 9(4): 2056–2062. https://doi.org/10.1109/59.331469.

Wang, X., B. Qian, and I. Davidson. 2014. "On constrained spectral clustering and its applications." Data Min Knowl Disc, 28(1): 1–30. https://doi.org/10.1007/s10618-012-0291-9.

Wang, Z., J. He, A. Nechifor, D. Zhang, and P. Crossley. 2017. "Identification of Critical Transmission Lines in Complex Power Networks." Energies, 10(9): 1294. https://doi.org/10.3390/en10091294.

Yan, J., Y. Tang, H. He, and Y. Sun. 2015. "Cascading failure analysis with DC power flow model and transient stability analysis." IEEE Trans. Power Syst., 30(1): 285–297. https://doi.org/10.1109/TPWRS.2014.2322082.

Yang, Y., T. Nishikawa, and A. E. Motter. 2017. "Small vulnerable sets determine large network cascades in power grids." Science (New York, N.Y.), 358(6365). https://doi.org/10.1126/science.aan3184.

5.8. FIGURES

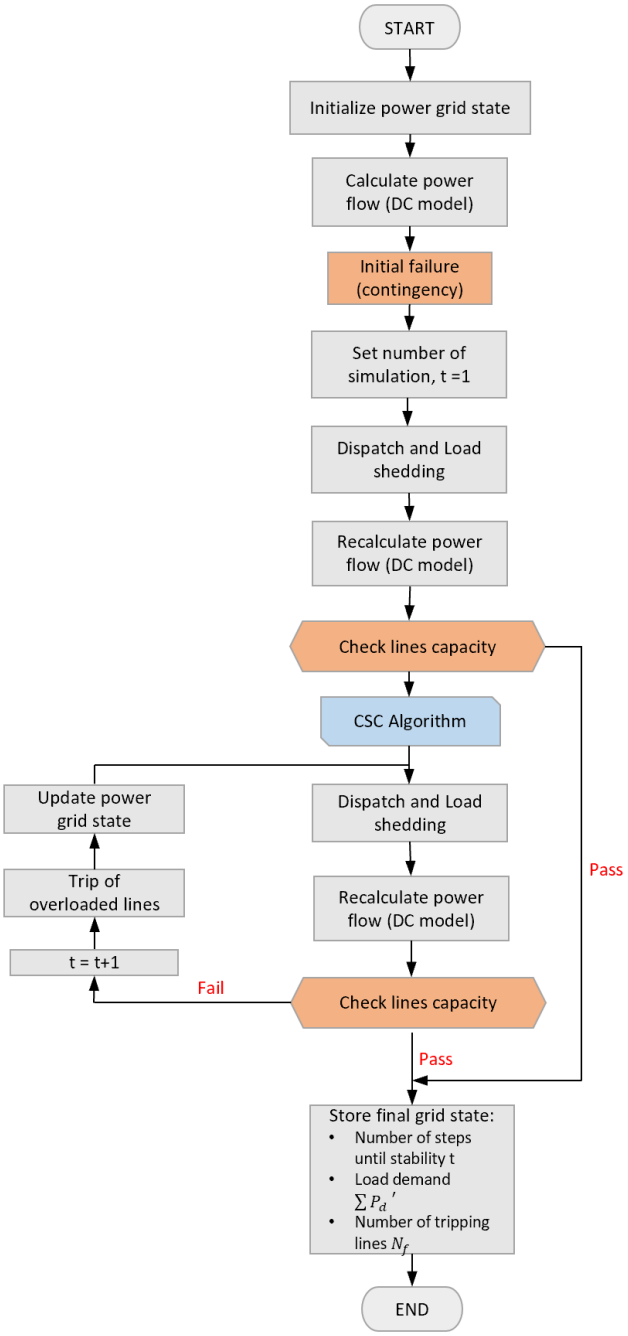

Figure 5.1: Flowchart of the Cascade Failure Model with CSC Mitigation Strategy

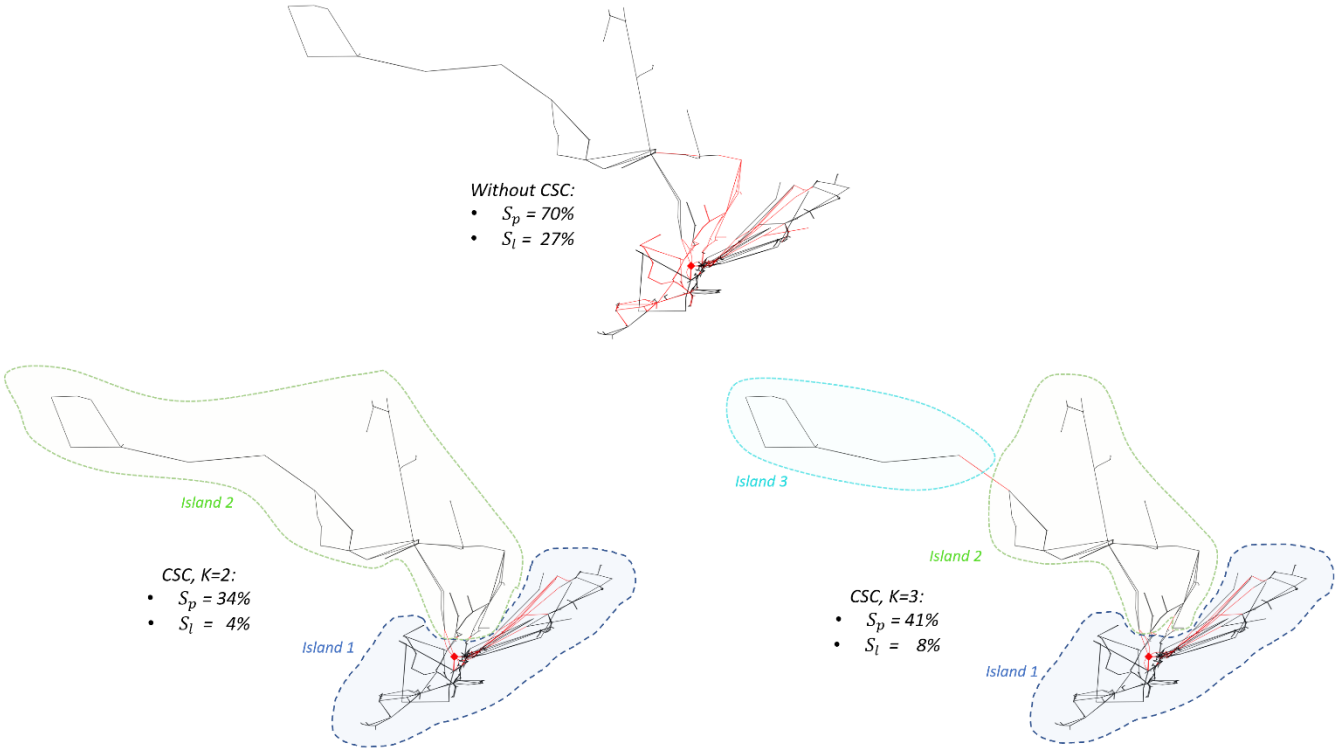

Figure 5.2: Illustration of cascade failure propagation until network stability due to the worst-case initial single bus failure scenario without and with CSC. The red links represent the out-of-service overloaded transmission lines, while the black links represent the in-service lines.

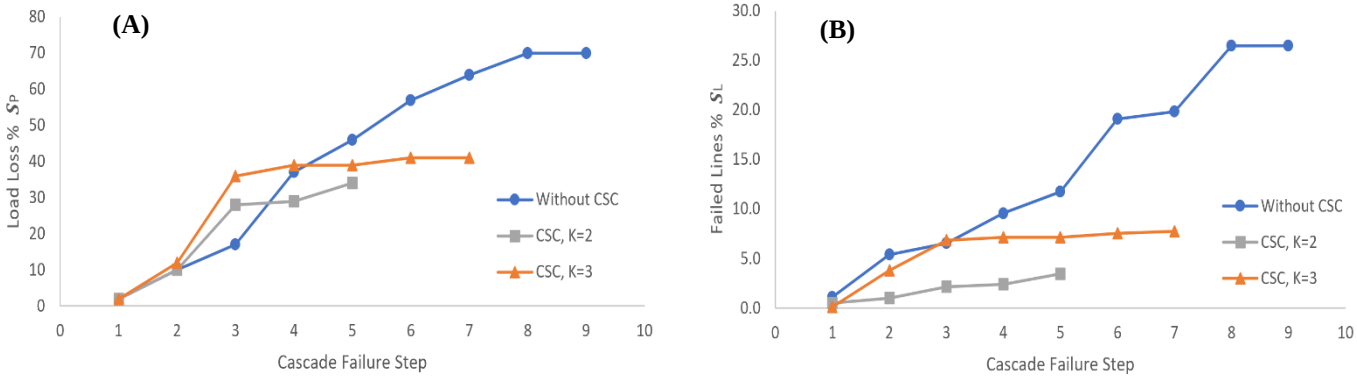

Figure 5.3: Cascade failure size step-by-step evolution until network stability due to the worst-case initial single bus failure scenario without and with CSC. (A) Load loss% S_P , while (B) Failed lines% S_l.

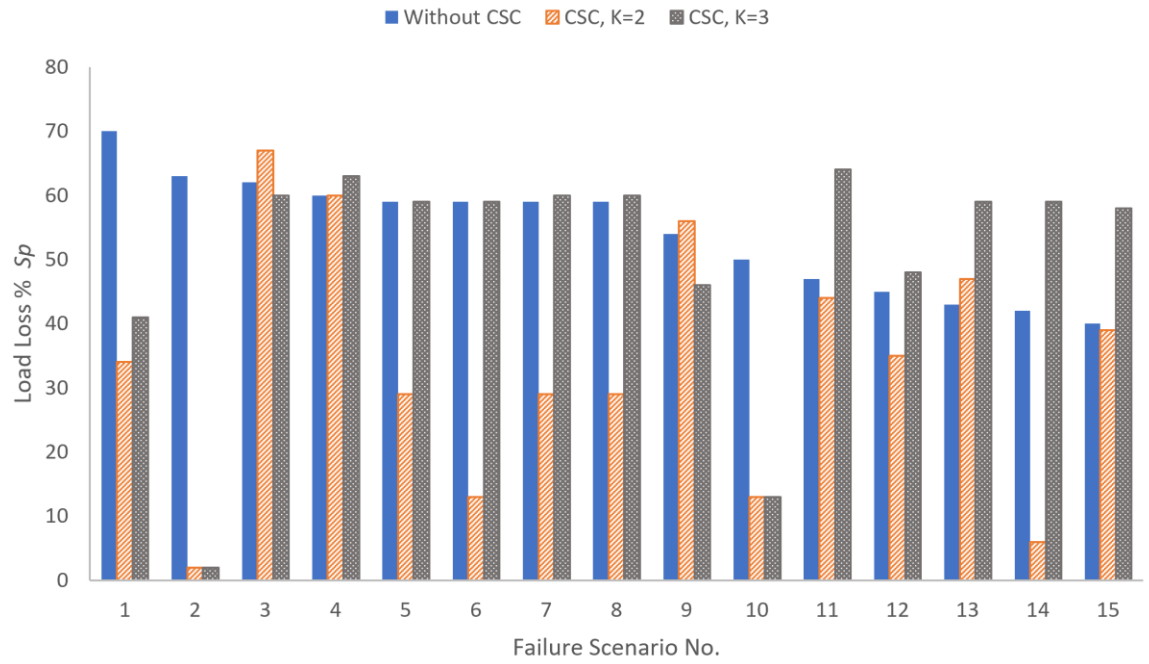

Figure 5.4: The load loss % S_P due to different cascade failure scenarios without and with CSC.

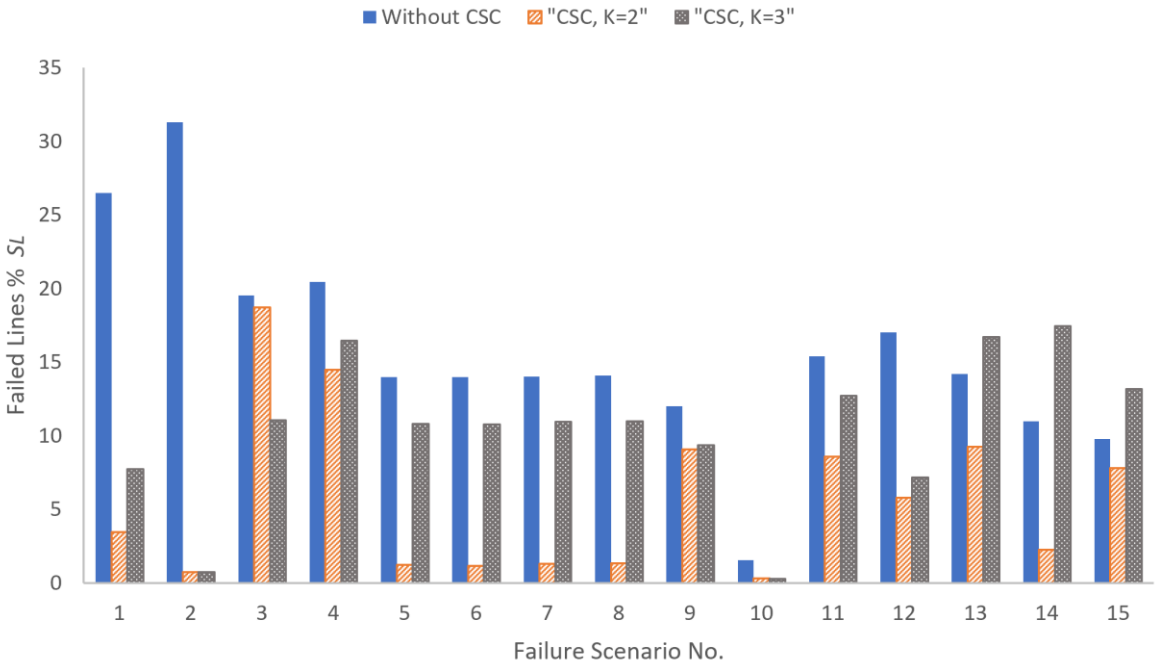

Figure 5.5: The failed lines % S_l due to different cascade failure scenarios without and with CSC.

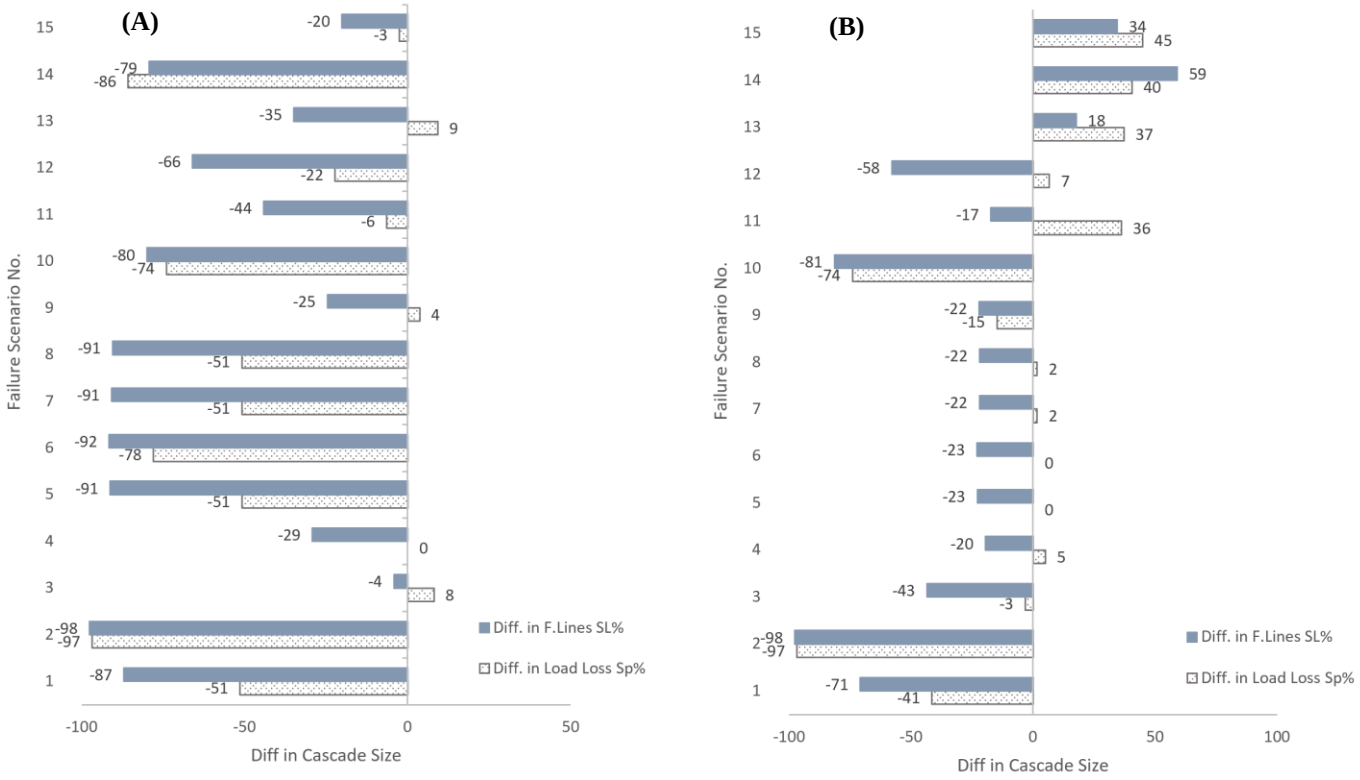

Figure 5.6: Change in Cascade failure size for different failure scenarios due to using CSC mitigation strategy. (A) CSC, K=2, while (B) CSC, K=3.

Chapter 6 : SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

6.1. SUMMARY

The overarching goals of this dissertation were to enhance the energy infrastructure networks robustness and overcome the challenges facing the existing simplified topology-based models. This has been achieved through the development of a dynamic cascade failure physical flow-based model to simulate the failure propagation throughout a high-fidelity model, as well as provide a risk mitigation strategy to suppress the cascade failure propagation and mitigate the risk of catastrophic system-level cascade failures (systemic risks). As a first step in this endeavour, a comprehensive review has been presented to introduce the Complex Network Theory (CNT) metrics, topological network characteristics, and several centrality measures. Furthermore, this review described the different network-based model classes and highlighted the need to consider the dynamics and physics behaviours in simulating the infrastructure networks.

A CNT was utilized to evaluate the network vulnerability by identifying the critical network components considering unweight and weight network approaches. Network vulnerability is quantified considering five different scenarios (i.e., guided by either the degree, Eigenvector, PageRank, betweenness, or the closeness centralities) through evaluating two key performance metrics—Topology and Functionality indices. Therefore, the network robustness was evaluated by

subjecting the network to stress tests through removing nodes either randomly or specifically targeting them based on their centrality measures. Furthermore, the model implemented a mixed strategy to improve the network robustness by isolating the key components from the cyberattacks.

The dynamic Cascade Failure Model (CFM) was subsequently established by adopting the Direct Current (DC) power flow model to provide a physical flow-based model for the network representing the network physics behavior. The dynamic CFM has been utilized to provide two key vulnerabilities indices; Link Vulnerability Index (LVI), for transmission lines the failure probability according to different failure scenarios; as well as a Node Importance Index (NII), for power (sub)stations ranking according to the resulting cascade failure size. Furthermore, the LVI has been used to construct a power transmission line vulnerability map that can be utilized to rank the maintenance priority, whereas the transmission lines with high probability failure have a higher priority to get updated or changed in the network upgraded schedule.

Finally, a systemic risk mitigation strategy was developed through integrating operation- with structure-guided strategies to minimize the consequences of catastrophic large-scale blackouts. The operation-guided strategy was implemented through dispatch and load shedding to rebalance demand and supply after disruptive events. The structure-guided strategy adopted an ICI approach by employing a CSC algorithm. To evaluate the effectiveness of the

mitigation strategy a real power scale grid was modelled under different cascade failure scenarios to compare the cascade failure size with and without the proposed algorithm for different sub-grid numbers.

6.2. CONCLUSIONS AND CONTRIBUTIONS

The dissertation intensively investigated the previously outlined objectives of the research and studied the vulnerabilities and network robustness through utilizing CNT models, simulating cascade failure propagation based on a physical flow-based model, and providing a systemic risk mitigation strategy. In light of the research findings reported in this dissertation, the following sections present the conclusions and contributions for Chapters 2 to 5.

6.2.1. CONCLUSIONS AND CONTRIBUTIONS FROM CHAPTER 2

Review of CNT characteristics and metrics are presented and discussed in both static and dynamic approaches. Afterward, simulation approaches and applications to infrastructure were presented to investigate the main challenges facing CIN studies and the opportunities of dynamic modelling in providing more accurate and realistic simulation for the infrastructure networks. The main conclusions and contributions from Chapter 2 are:

- Static CNT models have numerous limitations that can result in an inadequate assessment of the vulnerability and robustness of the infrastructure networks.

- Dynamic network measures provide more realistic and accurate results compared to static ones. Therefore, the dynamic network simulation approach can be considered a more appropriate framework to simulate and analyze infrastructure networks.
- Most previous studies simulate infrastructure networks based only on the connectivity and topology properties (i.e., topology-based model) with disregarding flow and physical properties within the network. Such simplified models lack the ability to capture the physics nature of these networks.
- Physical flow-based models yield more realistic analysis results, especially when simulating the dynamics of cascade failure, developing systemic risk mitigation strategies, and enhancing the resilience of infrastructure networks.

6.2.2. CONCLUSIONS AND CONTRIBUTIONS FROM CHAPTER 3

The CNT models were developed considering unweighted and weighted network approach to study the network vulnerabilities and evaluate robustness against random and targeted cyberattacks. A family of centrality measures, including degree, Eigenvector, PageRank, betweenness, and the closeness centralities were calculated to identify the critical network components. Furthermore, a mixed strategy was introduced to assess the effectiveness of isolating key network components to the robustness. The main conclusions and contributions from Chapter 3 are:

- The CNT centrality measures provide a quick and initial indication to rank the importance of the network nodes (i.e., substations in case of power grids).
- The power grid is highly vulnerable to targeted cyberattacks. Subsequently, recognizing the critical network components in advance can support the operators in enhancing network robustness by upgrading, protecting, monitoring the vulnerabilities, and limiting the hacker's access to key network nodes.
- For random cyberattacks, the proposed mixed strategy can boost the grid robustness by one and half times compared to random cyberattacks without the mixed strategy.
- Between the various centrality measures that have been used to rank the substations importance, current flow betweenness centrality is the most representative for substation importance. Whereas targeted cyberattacks based on the current flow betweenness centrality are the most destructive attack scenarios. On the other side, the Eigenvector centrality in both unweighted and weighted networks is not successful in identifying the key nodes and cyberattacks based on it are the least destructive cyberattack scenarios.
- However, the degree centrality depends on the local connectivity, removing degree hubs nodes has a sizeable global effect on overall network performance.

6.2.3. CONCLUSIONS AND CONTRIBUTIONS FROM CHAPTER 4

The dynamic cascade failure model based on a physical flow-based model was developed to simulate the failure propagation through the network. Two performance measures were used to evaluate the network robustness through topological and functional characteristics. Afterward, the CFM has been utilized to compute two vulnerability indices related to the main network components (i.e., transmission lines and substations). The main conclusions and contributions from Chapter 4 are:

- The dynamic cascade failure model is utilized to compute network components vulnerability indices: the vulnerability of links (i.e., link vulnerability index) and the importance of nodes (i.e., node importance index).
- The link vulnerability index is used to construct the overall grid vulnerability map, which highlights the vulnerable grid transmission lines based on their probability of failure over different random scenarios.
- For the demonstrated grid application, it was found that about 12% of the transmission lines underwent a primary failure. The number of lines that underwent secondary failures was on average three times the primary ones. In total, 36% of all links have total failure probability larger than 0.5%, and the maximum total failure probability noted was 12%.

- NII provides an effective way to rank the relative importance of the substations in the power grid based on the cascade failure size that results in the network due to the initial failure of this substation. Therefore, NII will support regulators and decision-makers to optimize the upgrade schedule constrained by available resources.
- The correlation between NII based on the dynamic cascade failure model and based on centrality measures is poor. This low correlation indicates that neglecting the physics pertaining to power flow redistribution and failure propagation may provide misleading conclusions.

6.2.4. CONCLUSIONS AND CONTRIBUTIONS FROM CHAPTER 5

Utilizing the CFM developed in Chapter 4, a systemic risk mitigation strategy was introduced to enhance the network robustness and suppress the failure propagation. The proposed mitigation strategy is based on the ICI approach implemented using CSC to select the optimal network splitting that minimizes the power flow disruption. Furthermore, operation- and structure-guided strategies were integrated. The main conclusions and contributions from Chapter 5 are:

- The proposed systemic risk mitigation strategy based on the CSC algorithm reduces the cascade failure size based on the power flow to the half for the worst-case failure scenario (i.e., boost the network robustness to the double). Also, the grid reaches the stability earlier by applying CSC for both cluster cases

in comparison with the grid failure scenario without CSC (i.e., the cascade failures steps are reduced), which in return reduces the restoration time and enhances the network response to the disruptive events.

- A significant improvement in grid robustness can be noticed by applying the proposed systemic risk mitigation strategy to the top 15 worst-case failure scenarios in case of using the CSC with two sub-grids. While less effective improvement can be noticed by increasing the number of clusters to three.
- The results emphasize that intentionally splitting for the power grid controlled by the proposed mitigation strategy is an effective strategy to suppress the cascade failure propagation. However, this ICI should be implemented diligently, or it might destabilize the grid.
- The proposed mitigation strategy is a low-cost corrective action applicable for any failure scenarios not only the worst-case scenario and can be implemented directly without redesign, reinforcement, or additional redundancy required for the network interdiction strategies.

6.3. RECOMMENDATIONS FOR FUTURE RESEARCH

The research in the present dissertation focuses on the "draw-down" phase of the infrastructure network resilience to analyze the power grid vulnerability and evaluate its performance under disruptions triggered by component failures.

Furthermore, the CNT centrality measures and vulnerability indices based on the CFM developed in this study represent an early effective indication tool that can support the grid operators and policymakers with quick and accurate predictions of network vulnerabilities and failure propagation, which enhance the network robustness under abnormal conditions. Moreover, the proposed mitigation strategy represents a line of defence to minimize the possibility of catastrophic large-scale blackouts. In light of the findings/results presented in this dissertation, this section presents possible research extensions that can be carried out to expand the current developed CFM model and the proposed mitigation strategy.

- The CFM can be coupled with AC power flow model to analyze the transient stability and model sympathetic tripping. Furthermore, the model can be used to study other infrastructure networks that are subjected to repeated failures and cascade propagations, such as transportation networks.
- The CFM can be extended to the "draw-up" resilience phase by including various maintenance scenarios based on the developed indices and other conventional ones to cover other resilience metrics (i.e., rebuild and reconfigure).
- The dynamic in the CFM can be extended to account for the changing of service demand, topological adjustments, the growth of the interdependencies, in addition to the post-event improvements such as enhancements of component capacities, and the integration with the new technologies.

- Regarding the mitigation strategy, the CSC algorithm can be extended to consider multi-objective to minimize power flow disruption, minimize load shedding in each sub-grid, and distribute the generators between the sub-grids. Therefore, the enhancement algorithm can determine the suitable number of sub-grids and the most suitable time for implementing the ICI to the grid.
- Finally, the developed CFM model can be integrated with other CIN models to simulate the interdependencies between the different infrastructure networks to enhance the network-of-network efficiencies.