Control Methods for Network Dynamics and Criticality Phenomena

Claudia Catalina Caro Ruiz

Universidad Nacional de Colombia
Facultad de Ingeniería, Departamento de Ingeniería Eléctrica y Electrónica
Bogotá, Colombia
2019

Control Methods for Network Dynamics and Criticality Phenomena

Claudia Catalina Caro Ruiz

A thesis submitted in partial fulfillment of the requirements for the degree of:
Doctor of Engineering

Thesis Director:
Eduardo Mojica Nava, Ph.D.
Thesis Co-director:
Andrés Pavas, Ph.D.

Research line: Complex Networks
Research group:PAAS-UN

Universidad Nacional de Colombia
Facultad de Ingeniería, Departamento de Ingeniería Eléctrica y Electrónica
Bogotá, Colombia
2019

To my family.

Métodos de Control para Análisis de Dinámica de Redes y Fenómenos Críticos

Claudia Catalina Caro Ruiz

Universidad Nacional de Colombia
Facultad de Ingeniería, Departamento de Ingeniería Eléctrica y Electrónica
Bogotá, Colombia
2019

Métodos de Control para Análisis de Dinámica de Redes y Fenómenos Críticos

Claudia Catalina Caro Ruiz

Tesis presentada como requisito parcial para el titulo de:
Doctor en Ingeniera

Director:
Eduardo Mojica Nava, Ph.D.
Co-director:
Andrés Pavas, Ph.D.

Linea de Investigacin: Redes Complejas
Grupo de Investigacin:PAAS-UN

Universidad Nacional de Colombia
Facultad de Ingeniería, Departamento de Ingeniería Eléctrica y Electrónica
Bogotá, Colombia
2019

To my family.

Acknowledgements

I want to express my gratitude and appreciation to several people, all who have helped and supported me during this process. First, my more sincere thanks to Colciencias for having granted me the scholarship/condonable loan (Ref. 647) to pursue the doctoral degree at the Department of Electrical Engineering at the Universidad Nacional de Colombia. I would also like to thank the Vicedecanatura de Investigación y Extensión, Facultad de Ingeniería, and the Dirección de Área Curricular Posgrados Facultad de Ingeniería for having supported me with funds to participate in various conferences and internships during these years. I would also like to thank the Fundación de Ciencia y Tecnología Colombo-Alemana -FUNCYTCA for helping me to do my research internship at the Fraunhofer IFF Institute in Germany.

Second, I want to thank my supervisors Prof. Eduardo Mojica-Nava and Prof. Andrés Pavas from Universidad Nacional de Colombia, for their support during this process. They have contributed to my professional development with their advice and experience. They have also given me the possibility to begin this study through the challenging and beautiful topic of complex networks and explore several issues to develop my research interest. Their friendship and company were vital to make me fill supported and confident during this journey.

Third, I want to thank Dr. Lombardi from the Fraunhofer Institute for Factory and Automation IFF, at Magdeburg, Germany, for accepting me as a visiting researcher in the Convergent Infrastructures Division. I also want to thank Prof. David Hill from the University of Sydney for having received me as a visiting researcher at the Centre for Future Energy Grids. Being honored in receiving his advice and experience give me a completely new vision about my life, my thesis, and my future research career. I also want to thank Prof. Jin Ma from the University of Sydney, for his unwavering support and guidance through the project. His advice and comments improved undoubtedly the results.

Fourth, I am very thankful for my colleagues and friends at the PAAS research group. Their company, intellectual discussions, and funny stories at the lunchtime make these years memorable. I learned small, beautiful things about life from each one of them. Thanks also, to my friends all around the world who share with me valuable experience and comfort words during these times.

Finally, I owe my gratitude to my parents Otto Caro and Silvia Ruiz, my sister Melissa Caro and my brothers Otto M. Caro and Andres Caro for loving me every day the way they do and encourage me to explore and enjoy life and the researcher path. I also want to thank my uncle, Captain Miguel Antonio Caro for believe in me and help me to start this process.

Abstract

This dissertation studies the role of the network structure on the emergence and mitigation of critical phenomena in complex power networks. In particular, the event to consider is the emergence of cascading failures due to congestion mechanism. The main contributions of this thesis are the proposal of a vulnerability analysis framework to study network influence on critical phenomena and the design of a control framework combining Network theory with Markov Decision Processes and Stochastic Games in order to choose best strategies to reduce the impact of cascading failures. The vulnerability analysis framework includes the identification of main properties influencing cascading failures triggering and propagation, the study of the central role of cut-sets in cascading propagation and the proposal of new metrics to evaluate global and local vulnerability. The control framework includes control strategies to generate worst-case failure scenarios and optimal solutions for damage control on those scenarios employing the dynamic setting of transmission lines capacity. This dissertation is developed around these two contributions, as is described in the following.

The first part of this thesis studies the influence of the network connectivity in failure triggering and propagation. Network science theory had been used to study relevant network connectivity properties. A methodology based on the connectivity properties is evaluated to measure the network robustness. A cascading failures model based on hybrid systems theory is proposed to define the congestion mechanism and describe the structure-function power network interdependence. The network Cut-sets (CS) identified as central elements for failures propagation are used to propose a critical link identification algorithm evaluated over the Quasy Stable State (QSS) approach of the proposed cascading failures model.

The second part of this dissertation proposes a network-based vulnerability analysis framework and propose a control framework to integrate network properties, electric properties, event-triggered failures, and control. Several algorithms are developed to evaluate different triggers and propagation events. The framework is developed analytically by the integration of Networks theory with Markov Decision Processes and Stochastic Games. Finally, using the previously obtained results about connectivity and vulnerability, a control strategy is designed to mitigate the damage of failures propagation by dynamically control the transmission lines capacity. An attacker-defender stochastic game framework is used to formulate the control problem. In the problem, the defender selects lines which are the best candidates to apply transmission capacity control as a response to the imminent risk of cascading failures related to the attacker actions. To solve the control problem,

we propose a system of multi-population state-dependent replicator dynamics where their fitness change with the long term discounted expected reward in the game. The solution of the replicator equations converges to the Nash equilibrium of the game and coincides with the best strategy for control the cascading failures damage related to worst scenarios produced by optimal attacks.

Keywords: Cascading Failures, Complex Networks, Decision Making, Network Congestion, Power Systems.

Resumen

Esta disertación estudia el rol que la estructura de la red y su dinámica tiene en la ocurrencia de fenómenos críticos y su posible mitigación con aplicación particular en sistemas de potencia siendo estos modelados como redes complejas. En particular se considera como fenómeno critico la propagación de fallas en cascada debidas a mecanismos de congestión. La contribuciones principales de esta tesis son la integración del concepto de conjuntos de corte y métricas de congestión en el análisis de vulnerabilidad de redes durante eventos de falla, y la propuesta de una estrategia de control para disminuir el impacto de la propagación de fallas en red mediante el control dinámico de la capacidad de las líneas. La disertación se desarrolla alrededor de estas dos contribuciones como se describe a continuación.

La primera parte de esta tesis estudia la influencia de la conectividad de la red en la generación y propagación de fallas en cascada en las redes de potencia. Teoría de redes complejas es utilizada para evaluar diferente propiedades de conectividad de la red y la evaluación de su cambio bajo la influencia de escenarios de falla diseados es asimilado como medida de robustez de la estructura. Los conjuntos de corte (Cut-sets) de la red son identificados como elementos propagadores de fallas en la red y un algoritmo de identificación de elementos críticos basado en esta teoría es propuesto. Un modelo de fallas en cascado dinámico basado en teoría de sistemas híbridos es propuesto para describir el mecanismo de propagación de fallas por congestion.

La segunda parte de esta tesis desarrolla un framework de evaluación de vulnerabilidad de redes de potencia sujetas a fallas en cascada y propone estrategias de control para mitigar el dao causado por estos fenómenos. El modelo de fallas en cascada propuesto en la parte previa es simplificado hasta una versión de estado cuasi estable (Quasy Stable State) e integrado en algoritmos de ataques de red para evaluar diferentes eventos detonantes y su propagación. El framework se desarrolla analìticamente tras integrar teoría de redes complejas, procesos de Markov y juegos estocá sticos. Finalmente usando información en cuanto a la interacción entre propiedades eléctricas y estructurales y la evaluación de vulnerabilidad de la red, se propone una estrategia de mitigación de impacto de la propagación de fallas en red mediante estrategias de control dinámico de la capacidad de transmisión de las líneas.

El framework de vulnerabilidad es integrado en un juego estocástico de atacante-defensor, donde el defensor selecciona las mejores candidatas para control de capacidad de transmisión como respuesta a amenazas de disparo de efectos en cascada debidas a acciones del atacante. Para solucionar el problema de control de vulnerabilidad de la red formulado como juego estocástico

de descuento de recompensa en el largo plazo se propone un conjunto de ecuaciones de replicador multi-poblaciones acopladas en estado. La solución de las ecuaciones converge a la solución del juego de suma cero, convergiendo a la vez a su equilibrio de Nash.

Palabras Clave: Congestion en Redes, Fallas en Cascada, Redes Complejas, Sistemas de Potencia, Toma de Decisiones.

Contents

List of Figures

List of Tables

Part I

Preliminaries

Chapter 1

Introduction

1.1 Motivation

Climate change, natural hazards, intentional/malicious attacks, accidents equipment failures, and thigh coupling with communication technologies have pushed governments and industry to develop new politics and strategies aiming to decrease the vulnerability of power systems infrastructure and improve their resilience. The development of flexible frameworks to identify the broad spectrum of grid attributes, as well as threats and hazards to grid components and to characterize the behavior and vulnerability of essential infrastructure components adequately is the common denominator expected for most of the new strategies proposed by the scientific community.

Studies on power grid vulnerability and recovery have been developed by governments (Carlson et al., 2012) and the scientific community (National Academies of Sciences & Medicine, 2017). The main recommendation observed on current studies is the necessity to shifts the focus strictly from physical components to grid structure and operations and their role in enhancing the reliability and resilience of the energy supply. To do this, efforts should be directed to obtain an accurate and detailed descrition of grid attributes (e.g., connectivity, topology, and configuration, physical asset properties and operational characteristics, critical assets and load, interdependenties with other infrastructure), to provide an essential starting point for the analysis and assessment of enhanced approaches to resilient grid operations.

Consequently, complex network science has become a useful tool to transform traditional vulnerability assessment approaches. Previous studies had evidenced a lack of integration between functionality and structural properties of networks in grid assessment and operation. The disconnection between structure and functionality in the traditional framework presents challenges for the scientific community looking to propose frameworks able to identify possible cascade propagation and trigger by considering both structure and electrical properties. Besides, new approaches should consider other challenges for grid analysis like size, complexity, parameters identification, and network evolution during operation and contingencies. Most approaches have suggested an increase in dependency on communication and data technology. However, this approach rises also the risk to potential cyber attacks in the grid by recognizing the system topology and vulnerabil-

ities. It is clear, therefore, that new vulnerability frameworks considering the grid attributes need to be developed and tested, including information regarding threats and hazards. The new frameworks will provide the basis from which to select and conduct vulnerability assessments and to determine grid assets that affect overall network vulnerability.

Cascading failure models play a leading role in the development of these vulnerability analysis frameworks. The cascade mechanism generally used is the overloaded branches propagation. Overload failures generally propagate through undetectable paths as a result of self-organized interactions in the system. The models that include network and electrical properties perform well to describe the cascading effect. However, they are not aimed to differentiate between failure triggers effects and failure propagation path. The interplay between the network flow reorganization and transmission capacity allows some unpredictable small disturbances to produce massive failures. Identifying and including in the models trigger and propagation mechanisms provide useful information about the overall system resilience. It is also found that single, small, vulnerable set implied in the failure propagation of a large-scale outage can be determined. Despite the many vulnerability frameworks and cascading failure models found in the literature, the problem of identifying how failures propagate in terms of time and space, what are the main cascade trigger events, and how to model the cascading failure patterns effectively in the power network remain open. A good insight into the interplay of electrical and structural properties as well as its use to recognize network vulnerability is relevant to continue the study of this problem and contribute to improving future networks resiliency.

Vulnerability assessment frameworks primary purpose is to bring useful information for the design and application of control strategies that mitigate failures damage by the choosing of proper actions over local components that change global behavior. Network reinforcement, topology changing, load shedding, dispatch, controlled system separation are some of the strategies used for the mitigation of cascading failure effects. Analysis of network dynamics under a given control policy had been studied recently; however, control design is still less understood. Prediction of possible failures, cascade propagation, vulnerable elements, and relevant properties should be part of an informed and predictive selection of control actions.

This dissertation aims to integrate network-based properties of power networks into a vulnerability and analysis framework for power networks, where network dynamics can be identified and controlled in order to predict and modify the system risk. The control framework and the strategy proposed to mitigate the failures damage are directly related to information obtained and understood from the network-based vulnerability analysis of the power network. Due to the dynamical and stochastic nature of the phenomena, the control framework integrates stochastic theory with evolving network models in order to get optimal control strategies that applied locally at each instant respond to diminish future failure risk. The primary motivation of this integrated framework is the possibility of considering the network as a whole system evolving dynamically in time and be able to modify its dynamic behavior by predicting its future behavior. This approach will give light about the process of evolution of cascading and possible strategies to mitigate the cascading propagation and damage.

1.2 Research Questions and Objectives

This dissertation aims to study the vulnerability of power networks during cascading failure events and to control its effects by using network-based approaches. The following key research questions motivate the main research goal of this thesis:

Q1 How the dynamical properties of networks change across a critical transition?

Q2 How to design control actions that can handle critical changes in network dynamics?

Q3 How to reduce the impact of dynamical changes in networks under critical transitions?

Besides, the research results fulfill the following specific objectives:

O1 Design a model that includes transitions in network dynamics and its structure.

O2 Analyze the structural and dynamical properties of network dynamics under critical transitions.

O3 Propose a control methodology by considering the nature of the critical phenomena in networks.

O4 Apply the proposed control methodology in power networks.

1.3 Thesis Outline

The dissertation is developed in four parts

I Preliminaries.

II Network connectivity and the cascading collapse of power network.

III Cascading collapse attacks and defense.

IV Concluding remarks.

Part II develops objectives *O1* and *O2*. Part III develops objectives *O2* and *O3*

Given that the approach of this research is mainly applied to power networks, the Objective *O4* is fulfilled at long all the chapters of this dissertation.

The contents of Chapters 2 - 9 are summarized as follows:

Chapter 2: Literature Review and Background

This chapter presents a literature review covering all the topics of this dissertation. First, it presents recent results in the use of Network science methods to approach power systems problems. Then, the literature on recent results in the study of cascading failures in power networks is described. Finally, a literature review for vulnerability assessment strategies and control in power networks is presented.

Chapter 3: Strength of Connectivity and Robustness of Power Networks

This chapter treats the study of structural and functional connectivity properties of power networks. Usually, structural properties as node degree and centrality are evaluated for random and target failures. However, when the power network is considered, the appropriated properties to evaluate vulnerability and robustness should consider structural and functional properties at the same time. In this chapter, it is proposed to use connectivity measures as, natural connectivity, edge connectivity, and minimum cut-sets to evaluate the vulnerability of networks when a failure process is present. This chapter partially answers the research question *Q1* and fulfills objective *O2*.

Chapter 4: Modeling Network Evolution during Cascading Failures

A cascading failures process based on congestion that can be used to complement analysis in Chapter 3 is presented here. This chapter proposes the hybrid dynamical model of cascading failures in complex networks. The model shows the interplay between network evolution and node dynamics due to constraints in transmission capacity. Therefore the model presents how can network dynamics evolve due to changes in control actions in controlled nodes, state variables, and

network structure. A case study is presented to validate the novel model. This chapter partially answers the research question *Q1* and fulfills objective *O1*.

Chapter 5: Identification of Cascading Propagation Paths

This chapter evaluates the influence of edges in cascading propagation due to its connectivity. The analysis predicts possible propagators by the use of cut-sets metrics established in Chapter 3. Cascading failures are modeled by applying a Quasy Stable State (QSS) approach of the model in Chapter 4. It is shown that the failures propagators are the critical edges identified by its connectivity properties and nodes connecting these edges results in the most affected during failures. This fact makes the cut-set measure a suitable candidate to predict and control the influence of elements affecting failures propagation. This chapter partially answers the research question *Q3* and fulfills objective *O2*.

Chapter 6: A Minimum Cut-Set Vulnerability Analysis of Power Networks

This chapter deals with the issue of considering the influence of some elements on the triggering of cascading failures in power networks. To this end, this chapter presents a vulnerability assessment framework combining network-based methods with sequential attacks and cascading failure process. Moreover, it is shown how to solve the minimum cardinality attacks problems bring lights to identify the vulnerable elements that generate the cascading. Furthermore, attack efficiency metrics are developed to evaluate the edges vulnerability and compare them over networks with different properties. This chapter partially answers the key research question *Q3* and fulfills objectives *O1* and *O2*.

Chapter 7:Markov Decision Process Model of Cascading Attacks in Power Network

This chapter presents an analytical approach to the problem of attacks in power networks. One of the main drawbacks of vulnerability analysis methods is the misleading of attacks and threats models that emulate hazards that could move the network to a critical point. The approach integrates network-based methods with Markov decision processes in order to predict the network evolution during cascading failures and identify the most suitable targets to attack achieving the maximum damage to the network. After the best attack is analytically identified, ideas about the reinforcement of some target edges are developed to reduce the attack impact. This chapter partially answers the research questions *Q2* and *Q3* and fulfills objective *O3*.

Chapter 8: Dynamic Line Rating Defense Against Cascading Attacks: A Stochastic Network Game

This chapter proposes a control method to defend power networks against cascading failure attacks. Network-based methods are integrated within a stochastic game to identify the best defender to respond against the best possible attack. Dynamic control of line transmission capacity is proposed

as an alternative to alleviate congestion produced by trigger attacks reducing the impact of the attack. Suitable candidates for dynamic line rating are generated by the optimal solution of the stochastic game. Moreover, it is shown how the stochastic game solution can be approached dynamically opening opportunities to develop at future distributed control reinforcement strategies. This chapter answers the key research questions *Q2* and *Q3*, and fulfills objectives *O3*

Chapter 9: Contribution and Concluding Remarks

This chapter draws the concluding remarks of this dissertation and proposes some open research questions as future work. The key research questions presented in Chapter 1.2 are also addressed in this chapter.

1.4 Publications

The following publications had resulted from the thesis contributions. This document does not cover some of them.

Networks Interdependency

- C. Caro-Ruiz, P. Lombardi, M. Richter, A. Pelzer, P. Komarnicki, A. Pavas, E. Mojica- Nava, Coordination of optimal sizing of energy storage systems and production buffer stocks in a net zero energy factory, Applied Energy, Volume 238, 2019, Pages 851- 862, ISSN 0306-2619, doi: https://doi.org/10.1016/j.apenergy.2019.01.125.

Cascading Failures in Power Networks

- C. Caro-Ruiz, A. Pavas, E. Mojica-Nava, A Hybrid Systems model of Cascading Failures in Power Networks, to appear in the 2019 IEEE 4th Colombian Conference on Automatic Control (CCAC), Medellín, October 2019
- C. Caro-Ruiz, J. Ma, A. Pavas, E. Mojica-Nava, PowerNet - A Toolbox for Network based Analysis of Power Systems, to appear in the Latin American Conference on Complex Networks LANET-2019, Cartagena, Colombia, August 2019.
- C. Caro-Ruiz, J. Ma, D.J. Hill, A. Pavas, E. Mojica-Nava,"Qualifying Transmission Line Significance on Cascading Failures using Cut-sets, to appear in The 13th IEEE PowerTech 2019, Milano, Italy, June 2019.
- C. Caro-Ruiz, J. Ma, D.J. Hill, A. Pavas, E. Mojica-Nava, A Minimum Cut-Set Vulnerability Analysis of Power Networks, Submitted to Sustainable Energy, Grids and Networks, 2019

Voltage Instability and Collapse in Power Networks

- C. Caro-Ruiz, A. Pavas and E. Mojica-Nava, "Voltage distributed control for power networks with DERs," in Proc. of the 2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Minneapolis, MN, 2016, pp. 1-5, doi: 10.1109/ISGT.2016.7781154.
- C. Caro-Ruiz, A. Pavas and E. Mojica-Nava, "Controllability criterion for random tree networks with application to power systems," in Proc. of the 2016 IEEE Conference on Control Applications (CCA), Buenos Aires, 2016, pp. 137-142, doi: 10.1109/CCA.2016.7587834.
- C. Caro-Ruiz and E. Mojica-Nava, "Centrality measures for voltage instability analysis in power networks," 2015 IEEE 2nd Colombian Conference on Automatic Control (CCAC), Manizales, 2015, pp. 1-6, doi: 10.1109/CCAC.2015.7345182.

- C. Caro-Ruiz and E. Mojica-Nava, "Voltage collapse analysis in a graph theoretical framework," 2015 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM), Montevideo, 2015, pp. 667-672, doi: 10.1109/ISGT-LA.2015.7381236.

Network Transitions and Desynchronization

- C. Caro-Ruiz, A. Pavas and E. Mojica-Nava, "Desynchronization of pulse-coupled oscillators in cycle networks: A hybrid systems approach," in Proc. of the 2017 IEEE 3rd Colombian Conference on Automatic Control (CCAC), Cartagena, 2017, pp. 1-5, doi: 10.1109/CCAC.2017.8276398.

- C. Caro-Ruiz, D. Téllez-Castro, A. Pavas and E. Mojica-Nava, "Self-organi- zation in networks: A data-driven koopman approach," 2017 IEEE 3rd Colombian Conference on Automatic Control (CCAC), Cartagena, 2017, pp. 1-6, doi: 10.1109/CCAC.2017.8276384.

- Claudia Caro-Ruiz, Andrés Pavas, Eduardo Mojica-Nava , Hybrid Model of Pulse- Coupled Oscillators in Dynamic Networks, in Proc. of the 1st Latin American Conference on Complex Networks LANET, Puebla, México, 2017.

- Claudia Caro-Ruiz, Andrés Pavas, Eduardo Mojica-Nava, Criticality in Complex Networks: A Hybrid Systems Approach, in Proc. of the Conference on Complex Systems CCS, Cancun, Mexico, 2017.

Chapter 2

Literature Review and Background

"The problem with experts is that they do not know what they do not know (Taleb, 2007)."

Nassim Nicholas Taleb
The Black Swan: The Impact of the Highly Improbable

2.1 Complex Power Networks

Complex networks represent the behavior of nature and human systems displaying signs of order and self-organization. They exist ubiquitously and at every scale (Newman, 2003). Examples include biological and ecological systems, societies, and technological networks like the Internet, the Power grid, and Transportation. Mostly, they have a large number of interacting parts, whose collective behavior cannot be inferred from the behavior of its components. Also, the interaction between components can be as significant as the parts themselves (Porter & Gleeson, 2016).

Self-organization is an implicit mechanism governing the behavior of complex networks. Even if the dynamics are tending to a stable and cooperative regime, or if it is tending to criticality (see (Noël, Brummitt, & D'Souza, 2014), (Y. Wang, Fan, Lin, Lai, & Wang, 2016)), the dynamics in networks are subjected to the emergence of local patterns of behavior that changes in a discontinuous way. In particular, critical transitions in networks are a significant indicator of complexity in system dynamics, as is described by (Dorogovtsev, Goltsev, & Mendes, 2008). Any system dynamics approaching its critical region shows a keen sensitivity to external perturbations and parameter variations of its micro-scale dynamics. By this, stability, and predictability of system dynamics can change significantly. Control and operation actions designed for systems out of the critical regime cannot manage these changes correctly.

Spatial patterns can arise before a critical transition. For instance, scale-invariance distributions of avalanche clusters occurrence, the general trend towards increasing spatial coherence, and the increasing of nodes cross-correlation as is presented in (Scheffer et al., 2009). Also, work in (Moon & Lu, 2015) shows a way to rebuild network properties by using spatial patterns and coherency

of the network near a critical transition. Moreover, the identification of changes in local patterns can be used to predict the occurrence of transitions, as described by (Zhang, Kuehn, & Hallerberg, 2015). Most of the described results concern to general models, but most of the patterns and shifts in real large scale complex systems cannot be identified analytically because dimension and complexity evade the modeling and identification process. However, analytical tools based on probability theory and graph theory have been developed to identify main properties governing these systems.

A set of graph theoretical tools, such as degree distribution, centrality measures, assortative, homogeneity between others, have been used to qualify these interactions (Newman, 2003). These structural properties describe the network in a steady-state. Beyond the structure, if the network has non-equilibrium dynamics (Nicolis, Prigogine, et al., 1977), the state of each node is governed by its dynamics and the coupling between node dynamics. The change in intrinsic dynamics of a component depends not only on its current state but also on those of its neighbors, and the network encodes which elements interact with each other and how strongly they interact (Porter & Gleeson, 2016). Also, it not only can affect the component dynamics, but also these dynamics influence the network structure and global dynamic processes over it. During the last decades, researchers have studied the structural and algebraic properties from networks. However, a lack still exists in the understanding of control principles to govern it and analytical tools to approach them.

Besides, some strategies to study dynamic and control properties have been studied. Properties such as degree distribution, homogeneity, size, and its dynamics make the control of networks a challenging topic. First approaches to network control are related to controllability (Y.-Y. Liu & Barabási, 2016), (Gao, Liu, D'Souza, & Barabási, 2014), (Caro-Ruiz, Pavas, & Mojica-Nava, 2016). Complex networks present intrinsic dynamical properties as nonlinearity, dissipative dynamics, multiple equilibriums, high phase-space dimensionality, constraints on the possible control interventions, decentralized behavior, noise in the dynamics, and parameters uncertainty (Motter, 2015). A combination of these properties makes that possible actions by the understanding and manipulation of such systems have a different character when compared to traditional control problems. Studying the problem includes three topics: controllability, steering the network dynamics to desired states, and controlling collective behavior (Y.-Y. Liu & Barabási, 2016).

Controllability measures the impact of network topology on control and the energy required to applied it (Y.-Y. Liu, Slotine, & Barabási, 2011), (Zhao & Cortes, 2016). Steering problem has been approached by applying perturbations to parameters and state variables (Cornelius, Kath, & Motter, 2013), by mapping the control problem to a combinatorial optimization problem of the network, and by using geometrical properties of the structure to modify its state (L.-Z. Wang et al., 2016). Also, collective behavior has been approached, mainly focused on pinning control and synchronization (Yu, Chen, & L, 2009).

Steering network dynamics and controlling collective behavior in networks is of significant interest. This issue concerns the design of tools for control network dynamics through the desired state. A large number of interacting parts, the impossibility to model its entire behavior, the relevance of interactions and self-dynamics, and the appearance of not inferrable collective dynamics

from the actions of the elements themselves restricts the control of complex networks. Results in (Cornelius et al., 2013) explain that each desirable state has a basin of attraction representing a region of initial conditions whose trajectories converge to it. Based on this idea, they use an approach of compensatory perturbations, but it requires prior knowledge of dynamics. Open questions in this method are the study of the favorable rate of this approach in systems with parameter uncertainty and noise. Also, it is required to devise how to choose the optimal control set of elements accessible to compensatory perturbations so that control objectives like the number of pinning nodes or the amount of energy can be minimized. Other approaches use perturbation of the system parameters and geometrical control.

Controlling collective behavior is one of the most studied problems in networks. The collective behavior problem is similar to controllability, but it requires that control actions applied to these pinning nodes contribute to collective synchronized behavior. Usually, the solution focuses on the adaptation of control gains and coupling gains from pinned nodes. Some other research directions in control of complex networks are: control of multilayer networks (Brummitt, D'Souza, & Leicht, 2012), (Y.-Z. Chen et al., 2015), control of adaptive networks (Y. Wang et al., 2016), stability of complex networks, and control of complex networks under critical phenomena (Noël et al., 2014), (Y.-Z. Chen, Huang, & Lai, 2014), (Brummitt, Barnett, & D'Souza, 2015). *In this research, we focus on the analysis of network dynamics under critical phenomena and its control.*

Up until now, progress in those issues had been made by the use of graph theory. The approach manly centers on the study of the relationship between the network's graph topology and linear dynamic properties networks. It presents some results for controllability by solving matching problems (Gao et al., 2014), and some results on stability and stabilizations through relations between spectral properties and zero dynamics in networks (Torres & Roy, 2014). Also, centrality measures have been used to specify the role of nodes on stability and controllability properties (Pasqualetti, Zampieri, & Bullo, 2014). Statistical physics approach uses mainly probability models as the configuration model and branching process to study changes in network behavior in terms of some defined control variables (Noël, Brummitt, & D'Souza, 2013). A few control theory analytical tools as Master stability functions (H. Sun & Hill, 2008), Lyapunov exponents, energy cost, and structural controllability (Yuan, Zhao, Di, Wang, & Lai, 2013) have been used to describe rigorously the observations raised statistically for controllability and stability of linear networks. Moreover, the multi-agent approach uses consensus and population dynamics theory to solve problems in synchronization and pinning control (Ramírez-Llanos & Martnez, 2014), (Awad, Chapman, Schoof, Narang-Siddarth, & Mesbahi, 2015).

An essential attribute from complex networks that is not commonly considered in most of the approaches found in the literature is criticality (Kuehn, 2015). It depicts the main properties that have not been considered in the design of control for complex networks before. It stresses that it is not just a matter of dimensionality; it is a matter of multiscale dynamics complexity (Kuehn, 2011). For dynamical processes over networks, the system out of equilibrium will have some identifiable instabilities. Representative changes will occur when dynamics approach a critical transition. Also, global changes in dynamic network behavior arise only upon strong coupling

when each component leaves its natural stable state. Those scenarios can be used to define significant qualitative and quantitative changes affecting the control design and restricting the steering actions. By considering instabilities in network dynamics, it is possible to understand the mechanisms that govern dynamics on networks and how it preserves or not these characteristics near critical transitions (Bak, Tang, & Wiesenfeld, 1988), (Dorogovtsev et al., 2008). Also, this approach gives clues about the design of control strategies capable of dealing with rough properties as dissipative dynamics and multiple equilibria (Brummitt et al., 2015), (Gao, Barzel, & Barabási, 2016).

Nowadays, there exists an increasing interest in the research of power systems from the complex network perspective. New techniques of modeling and analysis have been developed to capture the whole power network structure complexity (Pagani & Aiello, 2013). These techniques comprise both the requirements in structure and dynamics (P. Hines, Blumsack, Sanchez, & Barrows, 2010; P. Hines, Cotilla-Sanchez, & Blumsack, 2010; Caro-Ruiz & Mojica-Nava, 2015a, 2015b; Sanchez, Caire, & Hadjsaid, 2013). The deep understanding and application of complex network framework in power systems are essential to the advancement in the design and control of these techniques (Hill & Chen, 2006).

By considering instabilities in control principles, it will be possible to advance the understanding of the mechanisms that govern dynamics on networks and how they preserve or not this characteristic near critical transitions (Bak et al., 1988), (Dorogovtsev et al., 2008). Also, this approach will give clues about the design of distributed control strategies capable of dealing with rough properties as dissipative dynamics and multiple equilibria, which are poorly looking at in standard approaches (Brummitt et al., 2015), (Gao et al., 2016).

2.2 Cascading Failures

For power networks, the problem of instabilities and network dynamics can be mainly studied by the cascading failure effect. This phenomenon in power networks have the properties of scale-invariance, self-organization, and propagation patterns from the critical transition in the power network. General cascading failures models are related to the property of Self-Organized Criticality (SOC). The SOC in systems is related to the dynamic of a system tending to a critical point. Thus, the macroscale behavior of the network displays a spatial and temporal scale-invariance characteristic. It means that a power law indicates that the stationary state or attractor is critical. SOC behavior is present in many examples in nature as landscapes, forest fires, geodesic formations, and earthquakes. SOC concept studies usually apply sandpile models. The classical Bak-Tang-Wiesenfeld sandpile model SOC model has been presented in (Goh, Lee, Kahng, & Kim, 2003). In (Corral & Díaz-Guilera, 1997), a dynamical approach to the sandpile model is presented. In (Blanchard, Cessac, & Krüger, 1997) and (Blanchard, Cessac, & Krüger, 2000), the dynamical properties of this model are studied. Another model presented in the literature is the Bak-Sneepen Model (Bak & Sneppen, 1993). The Bak-Sneppen model is a simple mathematical model of bi-

ological macroevolution. It describes the adaptation process of interacting species. The entire model evolves to a self-organized criticality state where periods of not evolution alternate with avalanches of extinctions producing evolutionary changes. Extinctions of all sizes, including mass extinctions, maybe a simple consequence of ecosystem dynamics (Bak & Sneppen, 1993). Because of the modularity and higher interactions in scale-free networks, localized behavior is very uniform. Results from (Dobson, Carreras, Lynch, & Newman, 2001) presents an application of this model for the analysis of cascading failures in power systems. Also, a theory for optimization has been developed based on this model (Lu, Chen, Chen, Chen, & Zeng, 2016). Applications of sandpile models had been extended through literature, however more detailed models are required for the application in complex power networks.

Several models had been proposed using a complex networks approach. Sandpile modes and disease spread were two frameworks commonly used to model the failures spread (Hoffmann & Payton, 2014). Those models based on agents interaction across a network structure bring lights to the problem of cascading collapse in networks. They result useful for different infrastructures but, for power systems analysis, they are laking on considering the functional connectivity produced by agents dynamic and functional connectivity (Cupac, Lizier, & Prokopenko, 2013).

For the power system, cascading failure models play a central role in the vulnerability analysis framework (Bialek et al., 2016). The cascade mechanism of overloaded branches is generally used for all vulnerability methodologies. Different deterministic and probabilistic models with the same cascade mechanism are benchmarked in (Henneaux et al., 2018). This study shows that the cascading risk estimation over several different models is similar, but, a lack of adequate identification of the critical elements was observed (Zhai, Zhang, Xiao, & Pan, 2017). Also, most of the models are long-term stationary approaches and does not include node dynamics (Dobson et al., 2001). Failures events produce immediate transient dynamics on system state, that if considered could bring light about the possible control actions to be developed on each node in order to reduce the failure spread. Also, discrete time dynamics for cascading failures in power networks are shown in (Ba & Savla, 2016) and (Soltan, Mazauric, & Zussman, 2014) The models combine discrete dynamics with DC power flow and are used to analyze network vulnerability, and propose power flow routing strategies. Node dynamics are neither considered

Due to the nature of cascading failures events where network functioning affects the structural connectivity, a hybrid systems approach could be beneficial for the analysis of the system behavior. Classical approaches on power systems stability analysis are based on algebraic differential equations. Voltage collapse analysis is usually based on this theory. In (Song, Cotilla-Sanchez, Ghanavati, & Hines, 2016), a hybrid differential algebraic formulation is proposed to include discrete changes in system due to protective relays. Results are promising and include a toolbox in MATLAB useful for the analysis of the N-K contingencies. Due to the detailed models of machines included in cosmic, the model could result too slow to be used on large-scale statistical analyzers.

Different from previous work, in Chapter 4, we propose a hybrid systems model of cascading

failures in power networks. The proposed model includes angle dynamics and discrete network evolution due to transmission line congestion. The power network is modeled by an admittance matrix that changes over time as a response of a jump map where power flow excess in edges produces a discrete state transition of the adjacency matrix. Chapter 4 is based on the framework defined by (Goebel, Sanfelice, & Teel, 2012) and notation in (Phillips & Sanfelice, 2016). Hybrid systems models had been proposed to study different self-organization phenomena in networks. This theory combined with the analysis of critical transitions has essential applications in communications, electronic converters, mental diseases, and control over wireless networks (Díaz-Guilera & Arenas, 2008). Different self-organization patterns on systems including synchronization (Prignano, Sagarra, & Díaz-Guilera, 2013), desynchronization (Caro-Ruiz, Pavas, & Mojica-Nava, 2017),(Phillips & Sanfelice, 2016), and chimera (Wildie & Shanahan, 2012) have been studied, but models for cascading failures have not been proposed from this approach.

Primary failure mechanism studied in literature is transmission line overload. The mechanism of overload failures usually propagates through invisible paths as a result of the system self-organized behavior (Shunkun, Jiaquan, & Dan, 2016). The interplay between network flows reorganization, and edge capacities allow that some unpredictable small disturbances lead to a massive failure. Recent results in (Yang, Nishikawa, & Motter, 2017) found that a single, small, vulnerable set is usually implied in the failure propagation of a large-scale outage. However, the exact solution for the problem of how failures propagate in time and space in the network remains unknown. A measure combining topological and electrical properties could partially approach this problem, helping to identify edges where possible optimal control actions and its similar self-healing technologies will enhance network resilience.

Network-based methods have been introduced to the power systems analysis to identify the vulnerable set (Cuffe & Keane, 2017; Kim, Eisenberg, Chun, & Park, 2017; Pagani & Aiello, 2013). Generally, vulnerability assessment in power networks is associated with the network structure and its influence during a sequence of cascading events that may include malfunctions or undesirable elements operation (Beyza, M, J, & F, 2018), (Saleh, Esa, & Mohamed, 2018). Structural (Motter & Lai, 2002) and connectivity measures (Ellens & Kooij, 2013; Werho, Vittal, Kolluri, & Wong, 2016) have been proposed to assess network robustness. However, the use of those measures is limited due to the lack of electrical properties consideration. Combined network-electric centrality measures including admittance matrix (P. Hines & Blumsack, 2008), power flow operation point (Caro-Ruiz & Mojica-Nava, 2015a; Rincón, Pavas, & Mojica-Nava, 2016), electrical distance (Poudel, Ni, & Sun, 2018), and extended betweenness (Bompard, Pons, & Wu, 2012) have been proposed to evaluate vulnerability. These measures perform better than pure network based measures, but they have not been studied during cascading failures events. In Chapter 3, the aim is to understand how the interplay between the network structure and dynamics affects the failure propagation. Different graph properties had been studied but mainly related to topology and flow connectivity at the same time.

Maximum flow measures have shown better approaches, pointing to the relevance of topology and power flow interaction during cascading events (J. Fang, Su, Chen, Sun, & Lund, 2018). The

main shortcoming of these existing network-based attempts to measure the network vulnerability of electrical grids lies in the failure to explicitly incorporate the physical laws governing the power flow in the network (Z. Wang, Hill, Chen, & Dong, 2017). Most vulnerability measures quantify the element importance as if an element failure or its targeted attack significantly degrade the network performance. However, they rarely approach the prediction of elements involved in failure propagation. Besides, the results found in the literature are performed over generic networks (Shunkun et al., 2016) or include high-cost computational methods (Pi, Cai, Li, & Cao, 2018).

A Cut-set (CS) vulnerability metric is proposed in Chapter 5 to quantify the significance of transmission lines in the propagation of the cascading overload failures. The power network is modeled as a weighted undirected graph with transmission lines represented by edges. Line transmission capacity is equivalent to edge weight. CS measures are related to the network robustness properties on different networks (Marzo, Calle, Cosgaya, Rueda, & Maosa, 2018) and infrastructures (Le & Sankar, 2016; Psaltoglou & Calle, 2018; Dinh & Thai, 2015). The proposed metric uses edge power flow capacity of the minimum edge-cut-sets to identify vulnerabilities. If minimum cut-set capacity is reduced (or the equivalent cut), power flow will be infeasible and will generate flow redistributions, edge overloads, and subsequent load disconnection. The measure identifies all the cut-sets with minimum capacity in the network. Elements from these sets are fragile because their edge removal reduces transmission capacity and makes power flow infeasible. As a result, it generates flow redistributions, edge overloads, and subsequent load disconnection.

Compared with previous methods, the CS measure evaluates the role of the line from the combined effect of network topology and flow transmission capacity, identifies edges whose removal deteriorates the connectivity properties of the network, improves the prediction of failures path propagation, and reduces the vulnerability forecast the computational cost. At the same time, the algorithmic setup is proposed for measure calculation and evaluation of the cascading failures model based on DC-power flow.

2.3 Vulnerability Assessment

As power grids expand and integrate new technologies, their ability to respond and recover from hazard events play a major role in system planning and operation. Models to anticipate adverse events, as well as their immediate and long-term resulting consequences, are required to assess the extent to which the network is prepared for the threats it faces (Carlson et al., 2012). In this context, three main issues have attracted considerable interest: network-based vulnerability analysis (Cetinay, Kuipers, & Mieghem, 2018; Wei, Zhao, Huang, & Bompard, 2018; Chu & Iu, 2017; Zhang & Tse, 2015), cascading failures (Cetinay, Soltan, Kuipers, Zussman, & Mieghem, 2018; Soltan, Mazauric, & Zussman, 2017; Dey, Mehra, Kazi, Wagh, & Singh, 2016), and attack robustness of the power network (Liao, Salinas, Li, Li, & Loparo, 2017; S. Liu, Chen, Zourntos, Kundur, & Butler-Purry, 2014).

Vulnerability analysis frameworks combining cascading failures and attacks have been pro-

posed in the literature. Game theory (Cheng, Crow, & Ye, 2016a) and stochastic games combined with machine learning methods are used to propose vulnerability assessment frameworks (Liao et al., 2017). In (Moussa, Akaber, Debbabi, & Assi, 2018), a similar approach is presented to assess vulnerability in cyber-physical systems. Optimization approaches based on N-K contingency, are used in (Bienstock, 2015) to identify operational conditions affecting vulnerability to cascading failures. An attack strategy under limited network information is shown in (X. Liu & Li, 2017). All these approaches integrated attacks with cascading failures into a vulnerability analysis framework, but network properties and their influence on the vulnerability were not considered.

Network structural vulnerability is roughly related to the fraction of affected elements (from failures or external attacks) required to produce cascading failures. For the external adversary, the finding of such a set of fragile components whose removal would cause high damage to the network would be rather valuable (S. Liu et al., 2014). For a network operator, the information about this set of elements at risk and the set relation to network topological properties would serve to plan effective strategies that enhance network resilience (G. Chen, Dong, Hill, Zhang, & Hua, 2010; J. Fang et al., 2018). Hence, when this small number of elements is attacked, network vulnerability in terms of cascading failures is revealed. An alternative to identify these elements and get an effective attack can be approached by combining electric and network properties into the metrics for the identification of critical elements.

Centrality measures (Nie, Guo, Zhao, & Lu, 2015; Bilis, Kröger, & Nan, 2013), network degree distribution (Motter & Lai, 2002), and spectral properties have been extensively used to measure the structural relevance of network components. These methods aim to recognize the vulnerability of power network topologies to target attacks and the vulnerability rank of the element depending on its location, interconnections, and intermediation. However, practical applications of these approaches have not been developed yet because the cascading failure models used to perform the vulnerability analysis do not include electrical properties (Y. Fang, Pedroni, & Zio, 2017; Zhai et al., 2017; Z. Wang, Chen, Hill, & Dong, 2016; Cupac et al., 2013). For power systems, a collapse is not only a matter of breaking network topology. It is also the product of overloads resulting from cascading failures, the unavailability of transmission paths, disturbances, and network flow redistribution. Power systems structural vulnerability should aim to identify the fraction of elements whose disconnection damages the network ability to carry power and breaks irretrievably the supply/demand balance (Savla, Como, & Dahleh, 2014). For these reasons, interdependence between electrical and structural attributes in the network should be considered (Z. Wang et al., 2016; Azzolin, Dueñas-Osorio, Cadini, & Zio, 2018; Z. Wang et al., 2017).

New vulnerability methods propose to combine electrical properties with network-based metrics in order to include relevant structural interdependences (Poudel et al., 2018; Caro-Ruiz & Mojica-Nava, 2015a; Bilis et al., 2013). Vulnerability measures combining edge betweenness, outage transfer distribution factors and power transfer distribution factors are presented in (Bai & Miao, 2015) and (Bompard et al., 2012). Although the metrics combine the influence of network topology on path flows with the electrical coupling between elements, these metrics depend on DC power flow. The study in (Z. Wang et al., 2017) presents a measure of flow betweenness not

constrained to linealized power flow. However, these metrics assess separately each element and do not measure the overall network vulnerability. Effective network resistance is proposed as an index to measure vulnerability in (Coelho, Paiva, Segatto, & Caporossi, 2018). Likewise, other methods seek to include flows using maximum flow graph properties, but ignore flow routing constraints due to line impedances (J. Fang et al., 2018; Fan, Huang, & Mei, 2016; Ghanbari, Jalili, & Yu, 2016; Dwivedi & Yu, 2013).

Cascading failure models play a main role in the vulnerability analysis framework (Bialek et al., 2016). The cascade mechanism of overloaded branches is generally used for all vulnerability methodologies. Different deterministic and probabilistic models with the same cascade mechanism are benchmarked in (Henneaux et al., 2018). This study shows that the cascading risk estimation over several different models is similar, but, a lack of adequate identification of the critical elements was observed.

Another relevant issue is cascade propagation. Overload failures generally propagate through undetectable paths as a result of self-organized interactions in the system. In (Guo, Liang, Zocca, Low, & Wierman, 2018), techniques to identify cascading failure paths are studied based on tree partitioning. In (P. D. H. Hines, Dobson, & Rezaei, 2017), an influence graph, different from the physical network, is proposed to model the cascade propagation. In (Carreras, Reynolds-Barredo, Dobson, & Newman, 2019), a cascading failure model validation is presented for a network of thousands of nodes, pointing at the relevance of considering properties of network structure in order to establish suitable strategies for determining cascade propagation and reducing redundant information. The models that include network and electrical properties perform well to describe the cascading effect. However, they are not aimed to differentiate between failure triggers effects and failure propagation path.

The interplay between the network flow reorganization and transmission capacity allows some unpredictable small disturbances to produce massive failures. Recent results reported in (Dobson & Newman, 2017) point to the relevance of identifying the difference between initial failure events and propagation events. Identifying and including in the models the mechanism that contributes to the cascade propagation provide useful information about the overall system resilience. The results of (Yang et al., 2017) show that a single, small, vulnerable set is usually implied in the failure propagation of a large-scale outage. Despite the many vulnerability frameworks and cascading failure models which can be found in the literature, the problem of identifying how failures propagate in terms of time and space, what are the main cascade trigger events, and how to model effectively the cascading failure patterns in the power network remain open. A good insight into the interplay of electrical and structural properties as well as its use to recognize network vulnerability is relevant to continue the study of this problem and contribute to improve future networks resiliency.

This thesis propose a different view of the cascading failures modeling and assessment proposing a deterministic cut-set vulnerability basis for their study. We propose a model where the difference between the initial event and the propagation mechanism is modeled to show the overall system resilience. This framework offers a view to identify the possible precursor to cascade prop-

agation, and measures the risk of propagation associated to each edge, in terms of flow network connectivity properties. These insights about the cascading likelihood of elements will contribute to the identification of plausible targets for the deployment of mitigation and reinforcement strategies.

In contrast with previous frameworks where the system is modeled by the incidence graph, we use a graph-based approach, as in (Savla et al., 2014); there a flow network can represent more precisely the system and cascade propagation. Flow networks have been used extensively to model network properties of different supply/demand systems like transportation, communications, and supply chains. In addition, the duality between flows and cuts in this model can be used to identify relationships between power flow and network properties. In particular, the Minimum Cut-Set (MCS) arises as a network measure with potential to be used in power systems analysis. The MCS has several applications in network connectivity, network reliability, bipartite matching, and network intrusion detection. Despite its extended use in engineering applications, to the best of our knowledge, this measure has not been used in vulnerability or attacks analysis framework.

In the context of flow networks, the MCS depends not only on the network structural properties, but it also considers the lines capacity and distinguishes supply/demand nodes. Different from the critical links identification metrics available in the literature, the MCS offers information of global and local network vulnerability at the same time, with good efficiency and low computational costs. Besides, due to its intrinsic network properties, the attack strategy could be extended to be used for interdependent networks vulnerability assessment. For cyber-physical systems, the MCS of the information layer can be attacked with false data injection producing misleading operator actions and triggering cascading failures. MCS attacks in the control layer can also affect connectivity between controllers impacting on its coordination capacity or affecting state estimation with the consequent occurrence of cascading failures in the power network layer (Di Muro et al., 2017).

The main necessities identified from the literature and covered in this thesis are at first, the definition of a deterministic cascading failure model is proposed based on dynamic flow networks. The model facilitates to study the influence of structural properties on the power grid. The inclusion of a cascade mechanism due to overload and network flows is defined by means of the routing policy generator based on the DC power flow. From this model, a flow bottleneck measuring cascading potential depending on network congestion is proposed. The measure is used to identify critical elements by means of the increase in the network cascade potential, reducing the set of targets to elements into the MCS.

Second, the necessity for a strategy based on the MCS to identify the smallest set of vulnerabilities causing a cascading collapse. The strategy should be based on sequential targeted attacks where targets are selected according to its potential to increase flow bottleneck. Computational algorithms to obtain this including modification for the maximum flow algorithm should be designed to classify the target edge set. Using this strategy, proposed in the Part II, will be posible to assess the power grid vulnerability by measuring the damage and size of the attack and identify possible contrameasures. Also, the proposed strategy derives an upper bound for the exact solution of the target attack problem.

A third necessity is validate the effects of the designed attack against several network-based and electrical based-indices over various IEEE test systems. The main network properties involved in the system vulnerability reveal insights about an important relationship among: 1) transmission line capacities, connectivity, and flow bottlenecks; 2) the influence of supply/demand node placement on the resilience, and 3) the tradeoff between network efficiency and robustness. Results in Chapter 6, 7, and 8 will be cover these necesities.

2.4 Mitigation Strategies

Recently, questions about the control of complex networks became an important research topic. From the analysis of network dynamics as present in disease spread and synchronization has been learned that topology affects the dynamical process taking place in networks. In the same way, it also affects the ability to control them(Gates & Rocha, 2016). Main topics approached by the literature concerns the many requisites for networks control. In general, three issues are approached in literature: Controllability, trajectories steering, and control of collective behavior. However, the research efforts to understand the control principles of complex networks is just beginning.

First approaches to network control are related to controllability. It is related to the minimum number of external control signals required to steer the system behavior from an initial state to a desired final state (Y.-Y. Liu & Barabási, 2016), (Gao et al., 2014). Results in literature present results about the analysis of node characteristics associated with controllability in directed networks (Campbell, Ruths, Shea, & Albert, 2015) and the optimization of controllability and observability metrics (Summers, Cortesi, & Lygeros, 2016). Also, some analytical tools designed for the study of controllability in directed and undirected networks are developed (Y.-Y. Liu et al., 2011), (Yuan et al., 2013). Also, there exist some results on controllability properties of networks with a specific structure as circular networks (Nabi-Abdolyousefi & Mesbahi, 2013), random tree networks (Caro-Ruiz et al., 2016), or networks modeled by bilinear systems (Ghosh & Ruths, 2016).

Previous attempts, developed during this research, to understand the control of complex power network were on the integration of optimization methods and graph theory for the control of voltage and dispatch. In (Caro-Ruiz, Pavas, & Mojica-Nava, 2016), a distributed control strategy based on state-based potential games was designed to correct voltages out of limits by applying optimal changes of control variables (active and reactive power flow of DG). The proposed control considers under design restrictions related to network controllability and its dependency on the network structure. In (Caro-Ruiz et al., 2016), we studied the controllability properties of complex networks with a random tree structure. Our motivation was the usefulness of these results for the analysis and control of power systems with radial structure. Random Tree Networks (RTNs) were used to model the network topology from active power distribution networks. These networks consist of traditional Medium Voltage (MV) and Low Voltage (LV) feeders, commonly with radial topology, including some Distributed Energy Resources (DERs). Also, by the inclusion of multiple points of power injection (multiple DERs), we assume the network undirected. In (Caro-Ruiz

et al., 2019) interdependency between manufacturing processes and power generation integration were controlled and planned by the use of optimization algorithms. Algorithms to maximize the matching between RES power generation and flexible demand. These previous results were used as insights to understand the possible relationship between network-based methods and control systems for the mitigation of cascading failures.

Control problem for cascading failures in power networks is much less studied and understood than modeling and vulnerability assessment. The problem mainly focuses on the design of strategies to minimize the load loss or minimize failure propagation. Optimization problems are usually defined for objective functions oriented to those purposes, and control variables are defined depending on the selected control approach. The strategies found in literature mainly focuses on load shedding (Ba & Savla, 2017), dispatch (Reynolds-Barredo, Newman, Carreras, & Dobson, 2016), network reconfiguration (Qi, Sun, & Mei, 2015), and controlled sectioning (K. Sun, Hou, Sun, & Qi, 2019). Frameworks to approach the problem are build mainly from network-based methods, optimization, control systems, and computational approaches. Control problems are defined in (Bienstock, 2015) as optimization problems that combine electric and network properties on their constraints. Mainly solutions proposed are based on network-based methods and control approaches (Bienstock, 2011).

Network-based approaches are mainly focused on the identification of network properties influencing cascading failures and the network reconfiguration strategies to improve those properties. Results in (Zhou & Elmokashfi, 2018) propose the addition of new nodes and to study its effects over networks with a different structure. The central observation in this work is the influence of heterogeneity of networks in its recovery. In (Tang, Liu, & Hao, 2016), a meta-heuristic algorithm is used to reconfigure the network in order to improve its robustness. The algorithm generates new connections between nodes to increase redundancy. In (Brummitt et al., 2012), branching processes are used to estimate the level of connectivity between networks that reduce failure propagation. Opposite results in (Fan et al., 2016) propose the controlled tripping of selected links in order to stop the propagation of failures. Also, results in (Hoffmann & Payton, 2014) propose controlled upgrades in the tripping threshold of lines in order to reduce propagation. Most of the approaches result in useful information about the influence of network structure; however, models used to simulate cascading failures does not include power flows and system dynamics.

On the other side, control systems approaches are mainly related to the analysis of stability and feasibility conditions in networks modeled as dynamical discrete-time systems. Work in (Savla et al., 2014) proposes a cascading failures model in flow networks for a single commodity. Coupling between network dynamic and flow dynamic is evident in this work. A measure for resiliency is defined according to the minimum of the possible disturbances in the network. Disturbances are modeled as cumulative capacity changes for all the links. Flow routing is defined based on local conditions to improve resilience margin. Results in Chapter 6 will be an extension of work in (Savla et al., 2014) by the use of flow networks and the proposed flow bottleneck metric. Following a similar model, results in (Ba & Savla, 2017) define an optimization problem focused on the reduction of load shedding required to control the network during cascading failures. The method-

ology used in this work is mainly connecting computational methods with mathematical properties of the discrete-time dynamics of the cascading failure model. Work in (Como, 2017) generalize flow network models first to order dynamical systems and summarize analytical results on the resilience of those systems and analyze its stability properties; control objective of controllers is mainly focused on maximizing demand service. However, the analysis is not directly applied to power systems. Other approaches from control systems suitable to integrate network methods and control properties are game theory. Results in (Cheng, Crow, & Ye, 2016b) resent a game theory framework for the analysis of vulnerability in networks. In Chapter 7, we define a framework to study optimal attacks strategies that generates worst-case scenarios of cascading failures. The framework in (Cheng et al., 2016b) is extended from analyzing one-stage phenomena to integrate several stages and evaluate conditions for maximum damage in the long term. The framework integrate hidden failures models based on network topology evolution and failure probabilities due to overflows.

Stochastic approaches are also proposed to identify relevant elements influencing vulnerability, and possible control actions that mitigate failure risk in the long term. Zero-sum stochastic games are used in (Ma, Yau, Lou, & Rao, 2013) for the integration of failure models and mitigation strategies on power networks. The advantage of this kind of approaches is the possibility to evaluate several stages f the event and the interaction that the operator can have with the network in order to mitigate the effect of the failure propagation process. Hidden failures models can be integrated to predict risk (Liao et al., 2017). Besides, transition probability estimation can be modeled based on data historical or by the used of transition probability estimation by expert system. Based on results in (Savla et al., 2014), (Liao et al., 2017), and Chapter 8, we solve the control problem of minimizing lost of load by defining a stochastic game where optimal defender strategies respond to works case scenarios and modify network transmission capacity according to the possible future effects of cascading failures triggered by the action of the opponent. The integration of flow networks and stochastic control make suitable the control of cascading failure risk by the solution of the zero-sum stochastic games.

2.5 Conclusions

In the present chapter, a literature review concerning a network approach for power systems analysis during cascading failures was presented. Main network properties were established, and the critical behavior of cascading failures was developed. Models for cascading failures were also reviewed, and vulnerability assessment frameworks were described in order to define primary necessities covered in this work. Finally, mitigation strategies were reviewed, and the main results from the literature used as a base for this work were summarized. Part II will start with the development of the obtained results of this research that are based on the literature covered in this chapter.

Part II

Network Connectivity and the Cascading Collapse of Power network

Chapter 3

Strength of Connectivity and Robustness of Power Networks

"Although cascading failures may appear random and unpredictable, they follow reproducible laws that can be quantified and even predicted using the tools of network science. First, to avoid damaging cascades, we must understand the structure of the network on which the cascade propagates. Second, we must be able to model the dynamical processes taking place on these networks, like the flow of electricity. Finally, we need to uncover how the interplay between the network structure and dynamics affects the robustness of the whole system (Barabási et al., 2016)."

Albert-László Barabási
Network Science

Power network upon criticality phenomena and without control will experience uncontrollable changes in operation and connectivity. To quantify these effects, we should identify main connectivity properties changing under the influence of the event. This chapter aims to investigate the strength of connectivity and robustness of power systems by evaluating three main properties of the power systems: natural connectivity, edge connectivity, and flow bottleneck. Natural connectivity property quantifies how robust the network is by measuring its paths redundancy having a measure of closed walks between components at all lengths. Edge-connectivity property quantifies how robust the connectivity of the network is against edge failures by measuring how many elements should fail before the number of network-connected components increases Flow bottleneck property quantifies how robust the network is by measuring how its transmission capacity varies during failure events. The properties are studied under failures scenario generated by node-degree distribution. Several case studies are used to evaluate connectivity.

3.1 Structural Connectivity

The power system is modeled as a finite undirected weighted graph $\mathcal{G}$ such that

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}), \tag{3.1}$$

where the node set $\mathcal{V}$ and the edge set $\mathcal{E}$, with cardinality $|\mathcal{V}| = n$ and $|\mathcal{E}| = m$, represent buses and transmission lines, respectively. Also edges connecting nodes v_i and v_j are denoted by $e = (v_i, v_j)$. Let k_i be the degree of node v_i and $k_{\min}$, $k_{\max}$ the minimum and maximum degree of the network respectively. Let the adjacency matrix of $\mathcal{G}$ be $A = (a_{ij})_{N\times N}$ where $a_{ij} = a_{ji} = 1$ if nodes v_i and v_j are adjacent and $a_{ij} = a_{ji} = 0$ otherwise. Following A is a real symmetric matrix with real eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$. The set $\{\ \lambda_1, \lambda_2, \cdots, \lambda_N\}$ is the spectrum of G. A set toolbox of functions in MATLAB based on MATPOWER case files is developed to model the power system as a network. For more detail about toolbox see Appendix A.

In order to evaluate structural controlability and robustness we describe at next three properties used to analyse the connectivity of the network: natural connectivity, edge-connectivity, and the minimum cut set in flow networks. Following the three properties are described.

Natural Connectivity

Redundancy of paths between nodes can be useful to present an intuitive notion of graph robustness Consider a network with a source node and a sink connected by different paths between them. When one path fails, communication can still exist through alternative paths. The more the alternative paths in the network, the more robust connection between the nodes. Natural connectivity measures the redundancy of alternative routes as the scaled number of closed walks of all lengths. A walk of lenght l in a graph $\mathcal{G}$ is a sequence of edges and vertices alternated $(v_0, e_1, v_1, e_2, v_2, \ldots, e_l, v_l)$. A walk is closed if $v_0 = v_l$. Considers the weighted sum of numbers of the shorter closed walks

$$S = \sum_{k=0}^{\infty} \frac{n_l}{l!}, \tag{3.2}$$

where n_l is the number of closed walks of length l. By matrix theory

$$n_l = \sum_{i_1, i_2, \ldots, i_l} a_{i_1 i_2} a_{i_2 i_3} \ldots a_{i_l i_1} = trace(A^l) = \sum_{i=1}^{N} \lambda_i^l \tag{3.3}$$

where λ_i is the i*th* largest eigenvalue of A. Then

$$S = \sum_{l=0}^{\infty} \frac{n_l}{l!} = \sum_{l=0}^{\infty} \sum_{i=1}^{N} \lambda_i^l = \sum_{i=1}^{N} \sum_{l=0}^{\infty} \lambda_i^l = \sum_{i=1}^{N} e^{\lambda_i} \tag{3.4}$$

The equation above shows that the graph spectrum can be used to obtain the weighted sum of closed walks of all lengths. Scaling S by the number of nodes as follows,

$$\bar{\lambda} = \ln\left(\frac{S}{N}\right) = \ln\left(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}\right). \tag{3.5}$$

Then, it is easy to see that natural connectivity increase strictly monotonically as edges are added and is bounded by

$$0 \leq \bar{\lambda} \leq \ln((N-1)e^{-1} + e^{N-1}) \tag{3.6}$$

presenting an asymptotic behavior for $N \to \infty$, given by $0 \leq \bar{\lambda} \leq N - \ln N$. Then, $\bar{\lambda}$ provides a sensitive metric for robustness during network evolution (Jun, Barahona, Yue-Jin, & Hong-Zhong, 2010).

Edge-Connectivity

For the network in (3.1) connectivity is defined as follows (Newman, 2003),

Definition 3.1.1 *Connectivity in the network: The network $\mathcal{G}$ is connected if it contains a path between v_i and v_j for all $v_i, v_j \in \mathcal{V}$.*

Suppose connectivity is a non-decreasing property of $\mathcal{G}$ for adding new edges. Then, the global resilience of $\mathcal{G}$ with respect to connectivity can be defined as follows.

Definition 3.1.2 *Global resilience: Let connectivity be a non-decreasing property with respect to adding new edges to network $\mathcal{G}$. The global resilience of $\mathcal{G}$ concerning connectivity is the minimum number $\mu(\mathcal{G})$ such that by deleting $\mu(\mathcal{G})$ edges from $\mathcal{G}$ one can obtain a not connected graph.*

Consider the definition of edge connectivity for a graph,

Definition 3.1.3 *Edge connectivity: The minimum number of edges $\mu(\mathcal{G})$ whose deletion from a graph $\mathcal{G}$ disconnects $\mathcal{G}$.*

Definition 4. By comparing 3.1.2 and 3.1.3 we can suggest the proposition that follows.

Proposition 3.1.1 *Global resilience with respect to connectivity in a graph $\mathcal{G}$ is equivalent to its edge connectivity.*

By using edge connectivity of graph $\mathcal{G}$, we can evaluate the global resiliency of $\mathcal{G}$ as follows. Considers an edge cut of $\mathcal{G}$ as a set $\mathcal{S} \subset \mathcal{E}$ such that every directed path from v_i to v_j uses at least one edge from$\mathcal{S}$. Define $|\mathcal{S}|$ as the cardinality of set $\mathcal{S}$. Then, the global resilience (edge connectivity) $\mu(\mathcal{G})$ is

$$\mu(\mathcal{G}) = \min_{\mathcal{S} \subset \mathcal{E}} |\mathcal{S}|. \tag{3.7}$$

In addition, let be $k_{\min}$ the minimum node degree of $\mathcal{G}$. The upper bound for global resiliency (edge connectivity) of $\mathcal{G}$ is $\mu(\mathcal{G}) \leq k_{\min}$.

Functional Connectivity

Finally, we consider functional connectivity. Given a network $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c})$ with a single source node v_s and a single link node v_t, a chain is a set of distinct arcs of $\mathcal{G}$ that can be arranged as $e_{ij}, e_{jl}, e_{ll}, \ldots, e_{pq}$ where the nodes $v_i, v_j, v_l, \ldots, v_q$ are distinct. A chain joins its edge vertices v_i and v_q. In addition, considers a chain flow from v_s to v_t denoted by ζ, x_{st} composed of a chain ζ and a non-negative number representing the fow along ζ from source to sink. A flow in a network is a collection of chain flows. A flow has the property that the sum of the x_{ij} of all chain flows that contain any edge e_{ij} is not greater than the capacity of that arc $c_{e_{ij}}$, i.e. $c_{ij} \geq x_{ij} \geq 0 \quad$ for all$e_{ij} \in \mathcal{E}$. A cut set S is a collection of edges which has the property that every chain joining s and j meets the collection. The value of a cut set S denoted by $W(S)$ is the sum of the capacities of its individual members. The value of the minimum cut set can be defined as follows.

Theorem 3.1.1 *MInimal Cut Converse Theorem(Ford & Fulkerson, 1987)*
The minimal value of a cut set $W(S)$ taken from the all cut sets is the maximal flow value obtained in a network.

Proof 3.1.1 *Following the previous Theorem, finding the minimum cut set between v_s and v_t is the dual oprimization problem of a Maximum flow problem between the nodes. Then*

$$\min_{S_{st}} W(S) = \max_{e_{sj}} x_{sj}. \tag{3.8}$$

In the following section, we will evaluate the changes in network connectivity, using the properties described before, for multiple failure scenarios.

3.2 Study of Random and Target Failures Impact on Connectivity

This section describes the results obtained for the analysis of connectivity changes in power networks due to a different kind of failures. First, we define the set of case studies and the methodology to generate the failures scenario. In the second part, we evaluate the failures scenario for the case study and compare changes in the properties described before to identify patterns in connectivity change.

3.2.1 Experimental Setup and Case studies

Algorithms to calculate natural connectivity, edge connectivity and minimum cut ser during failures escenary are developed. Algorithm 1 summarize the experiment.

Algorithm 1 Function `robustness`

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, A, type
Output: res

switch (the value of type)
case random**:**
    $\mathbf{e}_{orden} \leftarrow$ edgeList($\mathcal{G}$,random)
case high-high**:**
    $\mathbf{e}_{orden} \leftarrow$ edgeList($\mathcal{G}$,high-high)
case high-low**:**
    $\mathbf{e}_{orden} \leftarrow$ edgeList($\mathcal{G}$,high-low)
case low-low**:**
    $\mathbf{e}_{orden} \leftarrow$ edgeList($\mathcal{G}$,low-low)
end switch
res$\leftarrow$ Connectivity(A)
$(\mathcal{G}_{new}, A_{new})$=delNextEdge$(\mathbf{e}_{orden}, \mathcal{G})$
if $\mathcal{E}_{new} \neq \emptyset$ **then**
    res$\leftarrow$ [res, robustness$(\mathcal{G}_{new}, \mathcal{A}_{new}, type)$]
else
    res$\leftarrow$ res
end if
return $\mathbf{e}_{orden}$.

Four failure scenary are shown. First random failures, where failure edge is selected randomly. High-high scenario removes elements connected between nodes with high degree. High-low scenario removes edges connected between nodes with high degree and nodes with low degree. Finally, low-low scenary disconnects edges between nodes with low degree. The algorithm is evaluated iteratively, until all elements are removed. Each measure is calculated for all the scenarios. Network edges are ranked acording their connection nodes in order to obtain target list. Metric

is calculated and graph should be updated to iterate the algorithm over the remaining network. Depending on the criteria to calculate, other algorithms are used in order to calculate the measures. More detail about algorithms used to calculate natural connectivity, edge connectivity and minimum cut set can be seen in the Appendix.

Case studies to evaluate connectivity are IEEE 14-bus, IEEE 30-bus, IEEE 33-bus, IEEE 39-bus, IEEE 57-bus, IEEE 89-bus, IEEE 118-bus, IEEE 145-bus, and IEEE-300. Networks properties are summarized in Table 3.1

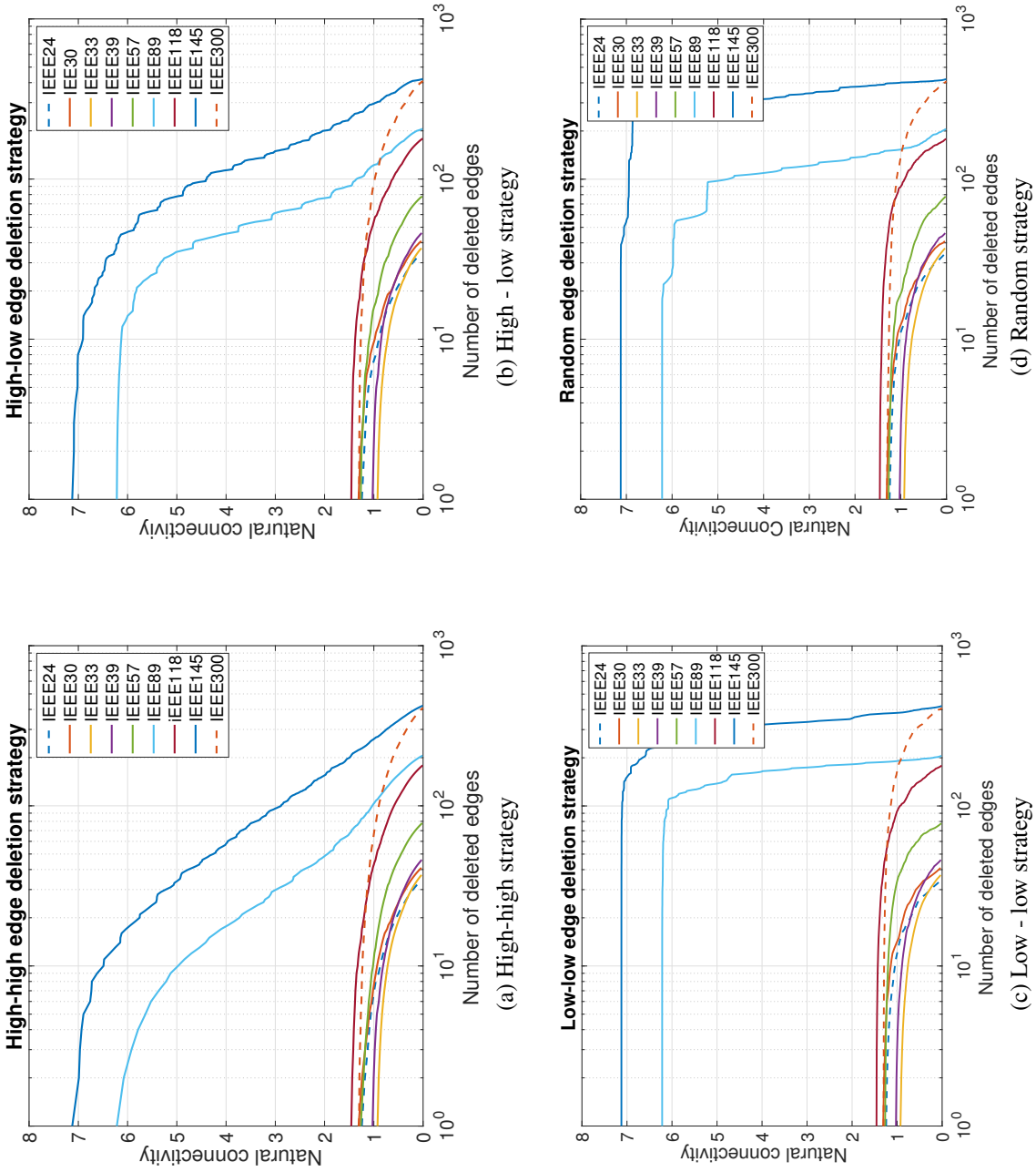
Table 3.1: Network properties for the studied IEEE testbeds.

	$\|\mathcal{V}\|$	$\|\mathcal{E}\|$	$\langle k \rangle$	k_{max}	k_{min}	γ	$load$
IEEE 24	24	34	2.83	5	1	1.4167	2850 MW
IEEE 30	30	41	2.73	7	1	1.3667	179.2 MW
IEEE 33	33	37	2.24	3	1	1.1212	3.7 MW
IEEE 39	39	46	2.36	5	1	1.1795	6254.2 MW
IEEE 57	57	78	2.73	6	1	1.3684	1250.8 MW
IEEE 89	89	206	4.62	15	1	2.3146	5727.9 MW
IEEE 118	118	179	3.03	9	1	1.5169	4242 MW
IEEE 145	145	422	2.73	20	1	2.9103	283051.2 MW
IEEE 300	300	409	2.72	11	1	1.3633	23525.8 MW

3.2.2 Results and Discussion

Figure 3.1 presents natural connectivity $\bar{\lambda}$ for each one of the power networks described in table 3.1. Networks with the highest natural connectivity are the IEEE 145-bus system with $\bar{\lambda} = 7.1$ and the IEEE 89-bus with $\bar{\lambda} = 6.2$. All other networks have an initial natural connectivity between $\bar{\lambda} = 1$ and $\bar{\lambda} = 1.5$. Networks with high $\bar{\lambda}$ have maximum degree $k_{max} > 10$. Other networks have a lower maximum degree. The system IEEE 300 has poor connectivity, although it is the system with more edges elements. Natural connectivity seems to be directly connected to network density. Networks with higher density have higher redundancy than a network with low density.

Figure 3.1a shows changes in $\bar{\lambda}$ due to the failure of edges connected between high degree nodes Edges are ranked according to the degree of their ending nodes and are removed on that order. Networks with higher $\bar{\lambda}$ present significant changes in its connectivity after the removal of the first ten edges. IEEE 89-bus system reduces its connectivity in more than 25% when less than 10% of its edges are disconnected. Also, IEEE 145-bus lost almost $1/3$ of its redundancy when less than 10% of its edges are disconnected. On the other side, IEEE 118-bus is not sensitive to failures on its highly connected edges. Figure 3.1b shows changes in $\bar{\lambda}$ for the failure of edges connecting nodes with a high degree to nodes with low degree. Networks are less sensitive to these failures, requiring almost three times distressed edges to reduce the same proportion of natural connectivity. Changes in connectivity appear later than in high-high edges failure; however, the transition is faster for this process.



(a) High-high strategy (b) High - low strategy (c) Low - low strategy (d) Random strategy

Figure 3.1: The network natural connectivity as a measure of robustness versus the number of deleted edges for four edge elimination strategies: 3.1a high-high strategy, 3.1b high-low strategy, 3.1c low-low strategy, and 3.1d random strategy. The initial networks are described in Table 3.1

Figure 3.1c shows changes in $\bar{\lambda}$ for the failure of edges connected between nodes with low degree. Edges connecting low-low nodes seems to do not influence connectivity or redundancy of networks. Transition threshold for natural connectivity loss occurs after more than 50% of the network is affected.

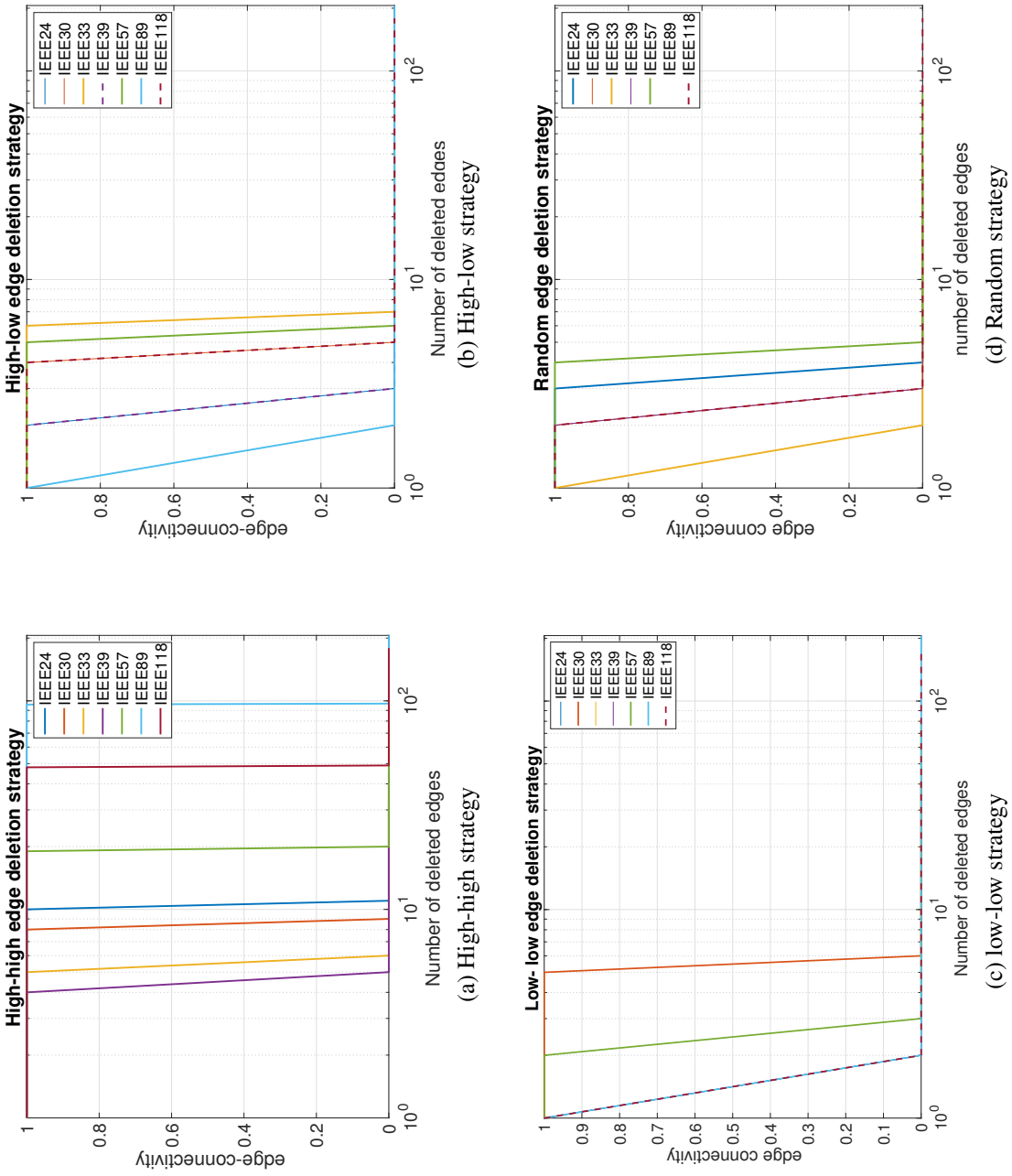
The same behavior can be observed in Figure 3.1d, where natural connectivity changes due to random edges disconnection are shown. Network connectivity is more sensitive to the random process than low-low failure process. However, significant changes occur also, for edge failures of more than 50%.

In general, it is possible to observe that network robustness due to redundancy is related to the network density and a high node degree. Also, network redundancy is more sensitive to target failures against edges connecting nodes with a high degree than random failures or failures in edges connecting nodes with low degree. The existence of a single connected component is assessed by using edge connectivity. Been power systems with sparse networks with a low average degree and low density, edge connectivity is a measure of how easily nodes or components can be isolated from the main component. All the networks present low edge connectivity equal to $k_{min} = 1$.

Figure 3.2 presents changes in edge connectivity for the different target and random disconnection processes. Figure 3.2a shows that target attacks to edges connected between highly connected components do not change edge connectivity. This result shows that bridges connecting dense subcomponents in the network do not exist. Thus, redundancy on inter-component connectivity exists. For the other three cases High-low in Figure 3.2b, low-low in Figure 3.2c and random process in Figure 3.2d, edge connectivity change very fast because low connected nodes have minimum degree producing node isolation once its corresponding edge is disconnected. Even if edge connectivity does not give information about how redundant network is, it also gives information about more vulnerable nodes to be easily disconnected from the grid due to a failure process.

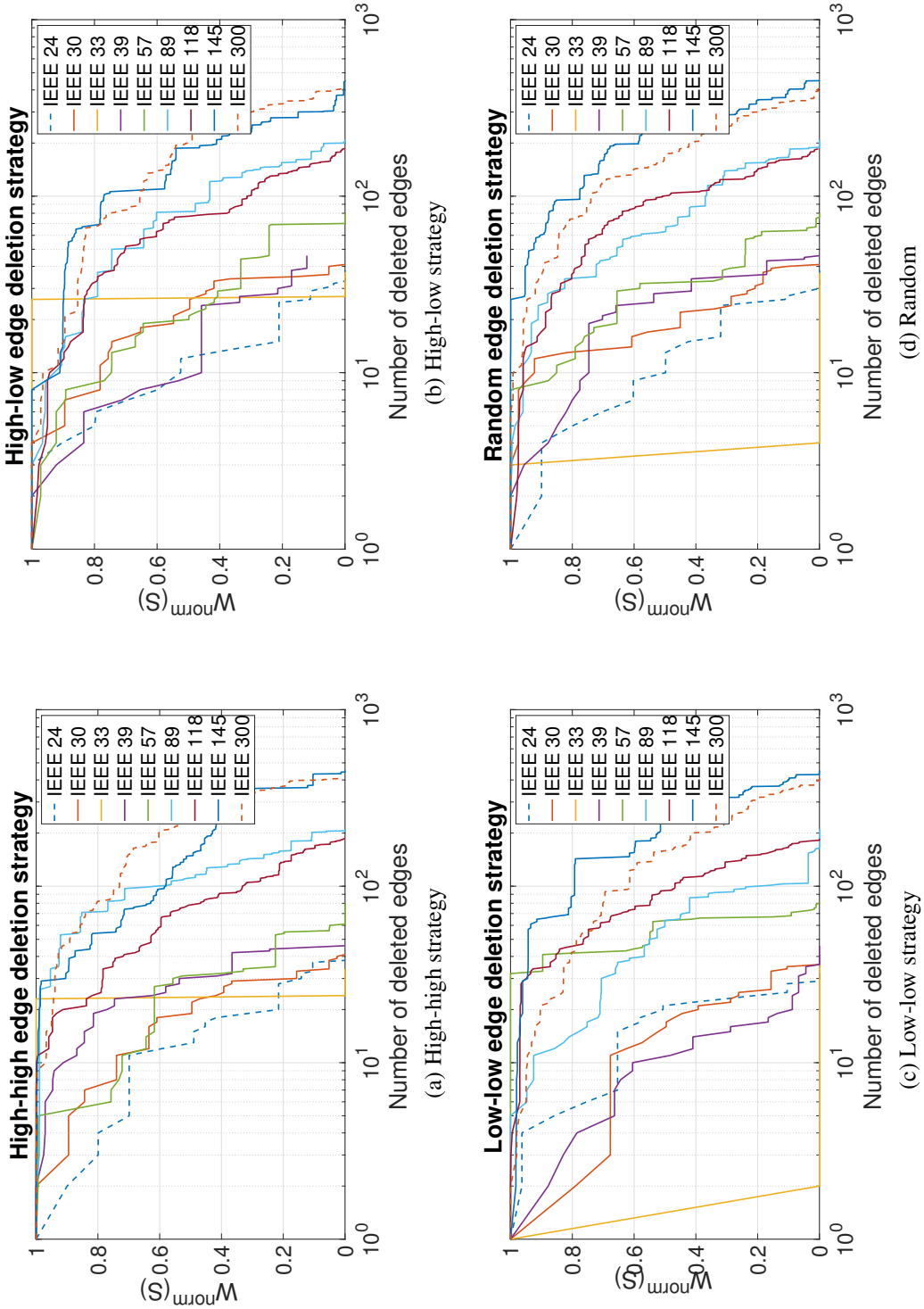
Figure 3.3 presents a developed measure of edge connectivity, where connectivity between supply and demand is measured. MCS gives information about the transfer capacity between supply and demand nodes. MCS weight is normalized according to its initial weight. Evaluating the change in the weight of the MCS, we evaluate how functional connectivity, related to power transfer capability is affected due to different failure or processes.

Figure 3.3a presents changes in the weight of the MCS during the removal process of edges connected between the nodes with the highest degrees. Different from the results in Figure 3.1 and 3.2, the IEEE 300-bus system behaves more robust to this removal process than the other networks. It means that edges connecting highly connected nodes do not compose the MCS of the IEEE-300bus systems but, edges connecting low degree nodes as can be observed in Figure 3.3c where MCS weight change due to the removal of edges connected to low degree nodes. The network loses the 20% of its transmission capacity five times faster than in 3.3a. The IEEE-89-bus systems are also sensible to transmission capacity loss due to the removal of edges connecting low degree nodes. While it lost 30% of the transmission capacity in the high-high process when 10^2 edges are removed It lost 95% of its transmission capacity with the same number of deleted nodes in the low-low process. The IEEE 145-bus systems if more fragile to failures in edges connected



(a) High-high strategy (b) High-low strategy (c) low-low strategy (d) Random strategy

Figure 3.2: The network robustness measured by edge connectivity versus the number of deleted edges with four different edge elimination strategies: a)3.2a high-high strategy, b) 3.2b high-low strategy, c) 3.2c low-low strategy, and d) 3.2d random strategy,. The initial networks are described in Table 3.1



(a) High-high strategy (b) High-low strategy (c) Low-low strategy (d) Random

Figure 3.3: The robustness of the network measured by the capacity of the minimum cut-set measured vesus the number of deleted edges with four different edge elimination strategies: 3.3a high-high strategy, 3.3b high-low strategy, 3.3c low-low strategy, and 3.3d random strategy. The initial networks are described in Table 3.1

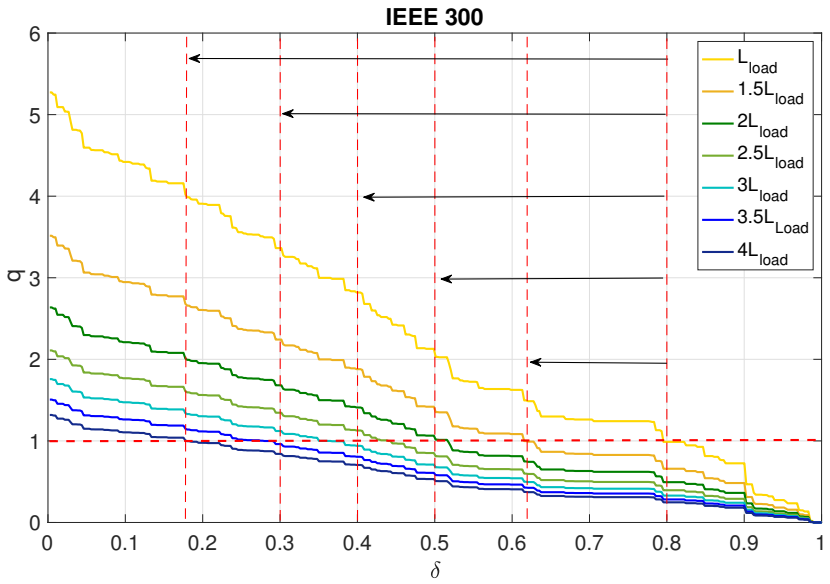
to high degree nodes. It means that the minimum cut set contains more connected nodes than other networks. The IEEE- 39 system has a single edge connecting generation to load. Then it lost all its transmission capacity when this single edge connected to low degree nodes failures. Systems IEEE-30 and IEEE-39 have edges connected between low degree nodes in their minimum cut set, and then these systems are vulnerable to low-low disconnection process and high-low disconnection process in Figure 3.3b. Figure 3.3d presents random process. All network present less fragility to random disconnection process than target processes.

Figure 3.4 present flow bottleneck described by Equation () a ratio between MCS capacity and network loading present a rate of congestion or flow bottleneck in the network. Closes values to $q = 1$ present a condition of flow infeasibility. Figure 3.4a presents the changes in q due to a random deletion process for the IEEE 300-bus system. In this figure, we can observe how network congestion increase by the removal of edges selected by random until they achieve a point where flow infeasibility exist $(q = 1)$. The figure also shows how an increase in load increases this congestion. Network heavy loaded $(4L_{load})$. The network is very close to the limit, and the removal of 20% of the edges results in flow unfeasibility. Also For network not loaded the Flow infeasibility point is achieved when 80% of the network is disconnected. Figure 3.4b presents the flow bottleneck constant changing due to the random deletion process for the IEEE-89 bus system. When the network is heavily loaded, it is less vulnerable than IEEE-300 system. The network presents initial lower congestion than IEEE 300-bus system. However, the system IEEE 89-bus lost faster transmission capacity than the system in Figure 3.4a.

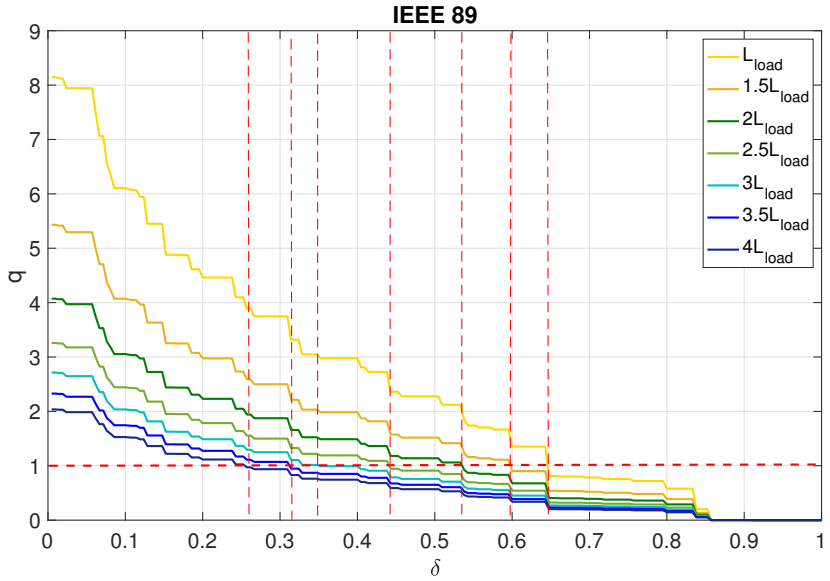
In general, we can observe how network robustness depends on degree connectivity of elements a network density. Edge-connectivity for power networks is very low due to the low average degree of networks The minimum cut set combines structural connectivity with transmission capacity. Networks with a low degree are more fragile to low connected component failures than high degree connected elements. The minimum cut set gives more information about how functional capabilities could be affected by the nature of the structure. In order to evaluate this, consider the measure of flow bottleneck where demand is compared to minimum cut-set weight. Flow bottleneck presents a better measure of changes in functionality depending on changes in structure. Depending on power demand, changes in the structure can affect more or less the functionality of the system. Networks heavy loaded will achieve faster the point of failure, but this rate of change will depend on network structure.

3.3 Conclusions

Three different properties, natural connectivity for redundancy, edge connectivity for connected components, and the minimum cut set for transfer capacity were used to evaluate the strength of connectivity and robustness of the power networks. Flow bottleneck dependency on-demand increase is also assessed. Failures scenario in random and target process are presented. Results show the necessity to consider the cascading failures scenario and metrics that include changes in



(a) Transmission capacity for IEEE 300



(b) Transmission capacity for IEEE 89

Figure 3.4: The impact of random failures in transmission capacity for different demand scenario.

structure due to functionality and change in functionality due to the network topology. In general response to failure changes under this methodology does not consider how the structure can change the limits of functionality. Also, the network is affected by flows, so it is necessary to model a failures mechanism that connects changes in structure with functionality and transmission capacity of the networks. Also, failures strategy in these simulations is only considering trigger failures. However, failures propagation is not modeled. So it is necessary to model failures consequences for structures and functionality and also changes the spread of failures. Next chapter will model and

describe a cascading failures mechanism where changes in structure and functionality are related to limits in transfer capacity of edges. Besides, results showed the necessity to define metrics able to be used in the comparison of different graphs and operation conditions. A need to evaluate failures scenario that relates the reflect functionality and structure is also found. Finally, they reflect the necessity to model the network considering its flow capacity and including power flow routing. Next chapters will develop these approaches.

Chapter 4

Modeling Network Evolution during Cascading Failures

"Self-organized criticality is a new way of viewing nature... perpetually out-of-balance, but organized in a poised state (Bak, 1996)."

Per Bak
How Nature Works: The Science of Self-Organized Criticality

Chapter 3 evaluates connectivity evolution due to random and target failures based on nodes properties. However, to analyze connectivity during failure events for power systems due to the nature of the failure, connectivity changes should be related to functional properties as transmission line congestion. A hybrid systems approach could be beneficial for the analysis of system behavior under these events. In this chapter, we present a model of cascading failures based on congestion in power networks. The model includes node angle dynamics and discrete network evolution due to transmission line limits. The power network is modeled by an admittance matrix that experiences a discrete state transition due to the power flow excess in edges. When edges achieve its capacity limit, the jump map generates the transition in the matrix configuration, by switching of elements related to the saturated edge. Finally, we present a case study based on a small cycle network.

4.1 System Model

Assume that the transmission lines are lossless and the voltage magnitudes are constant at 1.0 unit. The physical topology of the power network is described by an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where n network nodes indexed in the set $i \in \mathcal{V} = \{1, \dots n\}$ and edges set $\mathcal{E}$. Let $\mathcal{V}_s \subset \mathcal{V}$ and $\mathcal{V}_d \subset \mathcal{V}$ be the set of supply and demand nodes respectively. Transmision nodes without supply or demand are $\mathcal{V}_b \subset \mathcal{V}$. Each node holds a time-dependent phase angle state $\theta_i : \mathbb{R}_{\geq \nvDash} \to \mathbb{R}$. Also, consider a node associated supply-demand vector $\mathbf{p} := (p_1, p_2, \dots, p_n)$, where $p : \mathbb{R}^{\mathcal{V}}$; $p_i > 0$ for $i \in \mathcal{V}_s$, $p_i < 0$ for $i \in \mathcal{V}_d$, and $p_i = 0$ for $i \in \mathcal{V}_b$. We assume pure reactive lines, implying that each edge $(i, j) \in \mathcal{E}$ is characterized by its reactance $r_{ij} = r_{ji} > 0$. Given the power supply/demand vector p and reactance values, a power flow is a solution (f, θ) of

$$\sum_{i \in \mathcal{N}(i)} f_{ij} = p_i, \qquad \forall i \in \mathcal{V}, \tag{4.1}$$

$$\theta_i - \theta_j - r_{ij} f_{ij} = 0, \quad \forall (i, j) \in \mathcal{E}, \tag{4.2}$$

where N_i is the set of node neightbors for node i, f_{ij} is the power flow from node i to node j. Eq. (4.1) guarantees flow conservation and (4.2) captures the dependency of the flow on the reactance values and phase angles. Additionaly, it implies that $f_{ij} = -f_{ji}$. When the total supply equals the total demand on each connected component of $\mathcal{G}$, Eqs. (4.1) and (4.2) have a unique solution and can be written as the following matrix equation:

$$\mathbf{L}\Theta = \mathbf{p} \tag{4.3}$$

where $\Theta := \mathbb{R}^{\mathcal{V}}$ and $L \in \mathbb{R}^{\mathcal{V} \times \mathcal{V}}$ is the admittance matrix of the system, defined as follows:

$$l_{ij} = \begin{cases} 0 & \text{if} \quad i \neq j \quad \text{and} \quad (i, j) \notin \mathcal{E} \\ -1/r_{ij} & \text{if} \quad i \neq j \quad \text{and} \quad (i, j) \in \mathcal{E} \\ -\sum\limits_{z \in \mathcal{N}(i)} l_{i,z} & \text{if} \quad i = j \end{cases}. \tag{4.4}$$

Notice that the admittance matrix L is the Laplacian matrix of the graph $\mathcal{G}$ and the solution of the power flow is obtained by

$$\bar{\mathbf{\Theta}} = L^{\dagger}\mathbf{p}, \tag{4.5}$$

where $L^{\dagger}$ is the pseudoinverse of L.

Consider also a time-varying interaction pattern where for $(h, k) \in \mathcal{V} \times \mathcal{V}$, such that $h \neq k$, nodes h and k share a flow if $a_{hk} = a_{kh} \in \{0, 1\}$ is set to 1. The binary values a_{hk} represent the

state of edges in $\mathcal{G}$, and they are determined for all indices (h, k) taking values in the index edges set:

$$\mathcal{E} := \{(i, j) : i \in \mathcal{V}, j \in \mathcal{V} \setminus \{i\}\}. \tag{4.6}$$

Besides, a vector-based on the previous index set is defined as follows

$$\mathbf{a} := (a_{12}, \ldots, a_{1n}, \ldots, a_{n-1,n-1}, a_{n-1,n}), \tag{4.7}$$

where $\mathbf{a} \in \{0, 1\}^{n(n-1)}$. The elements of $\mathbf{a}$ describe all the possible pairwise interactions among nodes in $mathcalV$ Thus, the edges in a are state-dependent, and each node may have a changing value number of active connections with other nodes. The degree of node i, for each $i \in \mathcal{V}$ is defined as follows

$$k_i = \sum_{j \neq i} a_{ij}. \tag{4.8}$$

The model proposed in this chapter aims at integrating both a continuous approach of the power flows (described by suitable variations in state θ) and the discrete variations in the network topology pattern concerning to violations on lines power capacity were the state a instantaneous jumps specify violations). The modeling of the continuous changes and instantaneous jumps of the state of the power network during cascading failures is based on a hybrid systems framework. Hence, the state of the system $\mathbf{x} := (\mathbf{\Theta}, \mathbf{a}, \mathbf{p})$ evolves in the set:

$$(\mathbf{\Theta}, \mathbf{a}, \mathbf{p}) \in \mathbb{X} := \mathbb{R}^n \times \{0, 1\}^{n(n-1)} \times \mathbb{R}^n. \tag{4.9}$$

Respecting the dynamics of the system model, we consider flow equations for the overall state variable (θ, a, p):

$$\begin{cases} \dot{\theta}_i = \sum_{j \in \mathcal{I} \setminus \{i\}} a_{ij} (\theta_j - \theta_i) + p_i + u_i & \text{for all} \quad i \in \mathcal{I} \\ \dot{a}_{ij} = 0 & \text{for all} \quad (i, j) \in \mathcal{E} \\ \dot{p}_i = 0 & \text{for all} \quad i \in \mathcal{V}, \end{cases} \tag{4.10}$$

,

or in their matricial form

$$\begin{cases} \dot{\mathbf{\Theta}} & = -\mathbf{L}\Theta + \mathbf{p} + \mathbf{u} \\ \dot{\mathbf{a}} & = 0 \\ \dot{\mathbf{p}} & = 0 \end{cases} \tag{4.11}$$

The following observation motives dynamics in (4.10): the equilibrium point of the flow map in (4.10) is an approached solution of the DC power flow in (4.5). Also, the control action is event-triggered and are defined as equally distributed loads.

The interactions are constrained to pairs of nodes (i, j) sharingan active edge $(a_{ij} = 1)$. On the flow dynamics in (4.11), the network graph remains constant $(\dot{a}_{ij} = 0)$ during the flowing of the hybrid solution.Thus, structure changes of the power network graph are captured by the jumps of the hybrid solution while leaves the angles $\mathbf{\Theta}$ unchanged. Jumps only affect the elements a_{ij} of $\mathbf{a}$ by following the set of jump rules applied for each $(h, k) \in \mathcal{E}$ as follows:

$$\begin{cases} \theta_i^+ = \theta_i & \text{for all} \quad i \in \mathcal{V} \\ a_{hk}^+ = 1 - a_{hk} & (\mathbf{\Theta}, \mathbf{a}, \mathbf{p}) \in D_{hk} \\ a_{ij}^+ = a_{ij} & \text{for all} \quad (i,j) \in \mathcal{E} \setminus \{(h,k)\} \\ p_i^+ = 0 & (\mathbf{\Theta}, \mathbf{a}, \mathbf{p}) \in D_{hk} \cap \{k_i - a_{hk} = 0\} \\ p_i^+ = p_i & \text{for all} \quad i \in \mathcal{V} \setminus \{h,k\} \end{cases} \tag{4.12}$$

According to the above equation, a jump (toggle between 0 and 1) of edge a_{hk} is enabled when the state $(\mathbf{\Theta}, \mathbf{a}, \mathbf{p})$ belongs to the set

$$D_{hk} := \{a_{hk} = 1\} \cap \{|\theta_h - \theta_k| \geq c_e\} \qquad \text{for all } (h,k) \in \mathcal{E}. \tag{4.13}$$

Jump equation in (4.12) shows that across one jump hybrid solutions only experience the change of one edge $(i, j) \in \mathcal{E}$. This performance does not prevent the simultaneous deactivation of multiple edges. However, the hybrid solution with its multiple jumps conveniently represents such simultaneous activation/ deactivation. This description of the DC power flow networks enables the qualitative analysis of its solutions by estimating the impact of edge dynamics by the independent change of one edge a_{ij} at a time under the condition that $(\theta, a, p) \in D_{ij}$.

In the jump set D_{hk} of (4.12), $c_e > 0$ is the line capacity. The connection between nodes deactivated when the two nodes share a flow superior to the transmission capacity of its connection. For this reason, jump rule permits the evaluation of sectorized cascades in isolated network areas. The solution of the dynamics in (4.10) and (4.12) will converge to a unique global stable solution of the power flow after failures.

The jump dynamics is finally written by compactly representing (4.12) by the update laws:

$$\begin{bmatrix} \theta^+ \\ a^+ \\ p^+ \end{bmatrix} = g_{h,k}(\theta, a, p, u), \qquad (\theta, a, p, u) \in D_{hk},\ \forall (h,k) \in \mathcal{E}, \tag{4.14}$$

which can be grouped together into a set-valued map enabling any of the allowable jumps:

$$\begin{bmatrix} \theta^+ \\ a^+ \\ p^+ \end{bmatrix} \in G(\theta, a, p, u) := \bigcup_{(h,k):(\theta,a,p,u)\in D_{hk}} g_{hk}(\theta, a, p, u), \tag{4.15}$$

where $D := \bigcup_{(h,k)\in\mathcal{E}} D_{hk}$ is the jump set of the hybrid dynamics and $(\theta, a, p, u) \in D$. Finally, the hybrid dynamical model includes the flow map (4.10) described in terms of the following state-dependent Laplacian matrix $L(a) \in \mathbb{R}^{n\times n}$:

$$L(a) := \{l_{ij}(a)\}_{(i,j)\in\mathcal{V}\times\mathcal{V}}, \tag{4.16}$$

where

$$l_{ij}(a) := \begin{cases} -a_{ij}, & \text{if} \quad i \neq j, \\ \sum\limits_{j\in\mathcal{V}\setminus\{i\}} l_{ij}(a), & \text{if} \quad i = j. \end{cases} \tag{4.17}$$

Using the above definition, the dynamics in (4.10) can be written compactly as the flow equation:

$$\begin{bmatrix} \dot{\theta} \\ \dot{a} \\ \dot{p} \end{bmatrix} \dot{x} = f(x, u) = f(\theta, a, p, u), \tag{4.18}$$

and

$$f(\theta, a, p, u) := \begin{bmatrix} -L(a)\theta + p + u \\ 0 \\ 0 \end{bmatrix}, \quad (\theta, a, p, u) \in C, \tag{4.19}$$

where flow set

$$C := \bigcap_{(h,k)\in\mathcal{E}} \overline{\mathbb{X} \setminus D_{hk}} \tag{4.20}$$

is defined according to the state space $\mathbb{X}$ defined in (4.9) as the closed complement of the jump set D. If the state belongs to the interior of the jump set, the definition of C ensures that solutions to the system dynamics cannot flow. Finally, the power network cascading failure based on hybrid

systems could be described in the form:

$$\mathcal{H} : \begin{cases} \dot{x} \in f(x,u), & x \in C \\ x^{+} \in g(x,u), & x \in D. \end{cases} \tag{4.21}$$

In order for the flux to be well defined, the control action u must be balanced concerning the active link set $\mathcal{E}$. This is ensured by the following definition of the state-dependent control space $\mathcal{U}(\boldsymbol{\Theta}, \mathbf{a}, \mathbf{p})$:

$$\mathcal{U}(\boldsymbol{\Theta}, \mathbf{a}, \mathbf{p}) = cube(p) \bigcap \mathcal{B}_L, \tag{4.22}$$

where

$$(p+u) \in \mathcal{B}_L := \left\{ u \in \mathbb{R}^{\mathcal{V}} | \sum_{i \in \mathcal{V}} (p_i + u_i) = 0,\ i \in \mathcal{V} \right\}, \tag{4.23}$$

and $cube(p)$ characterizes the load shedding property and is defined by:

$$\begin{aligned} cube(p) := \big\{ u \in \mathbb{R}^{\mathcal{V}} | 0 \leq u_v \leq p_v \text{ for } p_v \geq 0 \\ p_v \geq u_v \geq 0 \text{ for } \quad p_v < 0 \big\}. \end{aligned}$$

$U(\boldsymbol{\Theta}, \mathbf{a}, \mathbf{p})$ includes all admissible load shedding controls at state $(\boldsymbol{\Theta}, \mathbf{a}, \mathbf{p})$. In particular, if all the supply and demand nodes are disconnected from each other at state $(\boldsymbol{\Theta}, \mathbf{a}, \mathbf{p})$, then $\mathcal{B}_L = \{\mathbf{0}\}$, and in this case $U(\boldsymbol{\Theta}, \mathbf{a}, \mathbf{p}) = \{\mathbf{0}\}$.

4.2 Case Study

This section presents the behavior of the model for different failure scenarios. The network dynamic is shown, and the changes in jump set and the jump map due to failure spread are also shown.

4.2.1 Case 1: no failure

Considers a cycle graph $\mathcal{G}$ with $N = 10$ with adjacency matrix A_0. Each node has an associated phase state θ_i and initial condition $\theta_0 \in [-0.5, 0.5]$. Also, each node has a power value p_i; this value is positive for generator nodes and negative for demand nodes. In this example $p = [1, -1, 1, -1, 1, -1, 1, -1, 1, -1]$. The system achieves an equilibrium point where the power flows are filling c_e constraints. Figure 4.1 shows the network flows for no failure case. The nine flows can be seen in different colors. Every flow achieves the same absolute value; The positive or negative value assigns a direction to each flow. For example, for generator node v_1 flows f_{12} and f_{1-10} are positive because power, from node 1, flows through load nodes 2 and 10. During

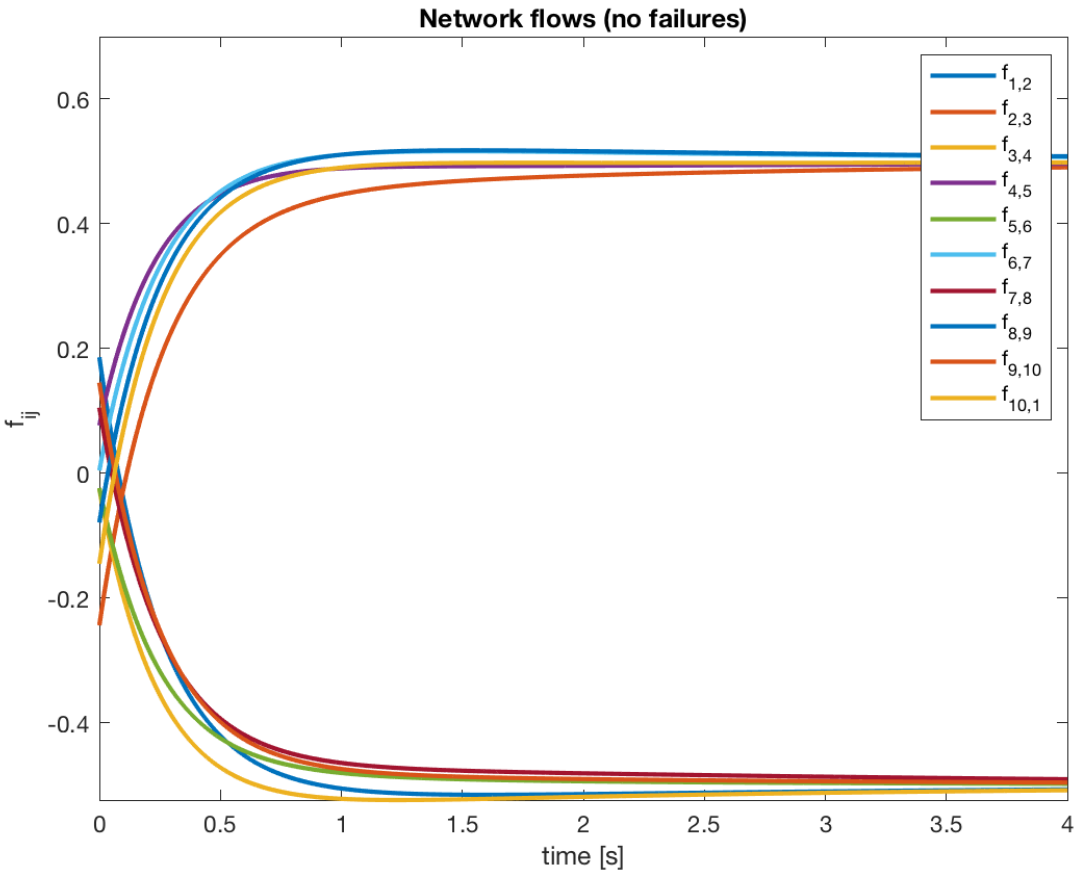


Figure 4.1: Solutions to $\mathcal{H}_n$ for network flows $f_{ij} = \theta_i - \theta_j$ on each edge of a cycle graph $\mathcal{G}$ that asymptotically converge to the solution for the continuos dynamis with random initial conditions in $\theta_0 \in [-0.5, 0.5]$. The equilibrium state for θ is the unique solution for p_0 where $\sum p_0 = 0$.

the process, the balance between power and demand is achieved. The phase variables θ_i for each node achieves bounded values too. Convergence times and equilibrium points depend on the graph structure, adjacency matrix weights, and node power values.

4.2.2 Case 2: few failures

In case 2, the initial system condition is the final equilibrium state in Figure 4.1.

A process of failure initiate by outages of the edges connecting demand node 2 to the network. As a consequence, the system power balance is broken, $p_{gen} > p_{load}$. The system's balance occurs, reducing the generated power by a quantity of δp. The systems move to a different flow balanced point. However, at this point, trying to achieve equilibria the system does not fill maximum power conditions. As a result, some edges are disconnected. Figure 4.3 presents the changes in network topologies as a result of the failures.

In the first stage, node two is disconnected by the edges connecting node 2 with 1 and 3. This

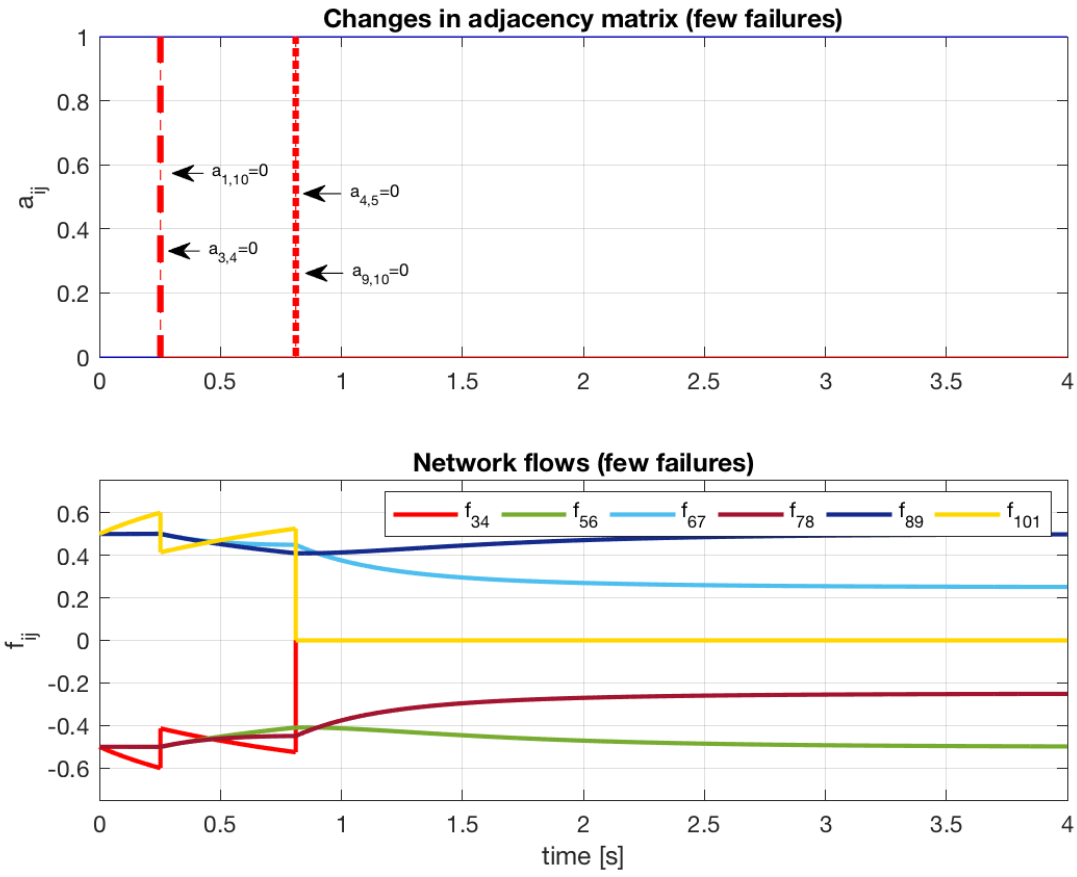


Figure 4.2: Upper figure depicts jump events for A where edges a_{ij} goes to zero when a failure occurs. Bottom figure shows solutions to $\mathcal{H}_n$ for network flows $f_{ij} = \theta_i - \theta_j$ on each edge. After failure process ends, the final connected component stabilizes itself.

jumps occurs by changing a_{21} and a_{23} from 1 to 0. The system flows again, but a loss of balance takes power flows in occurring to disconnect edges, and power flows during the time. The following jumps occur by an excess of power in $f_{1,10}$ and $f_{3,4}$. Nodes 3 and 1 are now disconnected from the network. Changes in p_i balance power. However conditions in θ takes the flows again up to the constraints on flows f_{10-9} and f_{45}. As a result, a new failure event occurs; nodes 4 and 10 are disconnected now. Finally, the system stabilizes, and a final connected component remains between nodes 5, 6, 7, 8, and 9. Figure 4.2 shows jumps in the a state representing changes in network topology, in time. Also on the bottom side, it shows power flows f_{ij} and its jumps, and final stable state. The final power associated to nodes are $p = [0,\ 0,\ 0,\ 0,\ 0.5,\ -0.75,\ 0.5,\ -0.75,\ 0.5]$.

4.2.3 Case 3: cascade failure

In the last case, a cascading failure process occurs disconnecting the entire system. In this case, the process begins with initial conditions far from the solution point obtained from case 1. As in case

2, failure process initiated by outages of the edges connecting the demand node 2 to the network. The sequence of failures originated by this event is shown in Figure 4.7. The order and time of failure occurrence can be observed in Figure 4.4. The associated changes for each time in f_{ij} and θ can be seen respectively in Figures 4.5 and 4.6 respectively. Node dynamics is not smooth because of sudden changes occurring in edges.

4.3 Conclusions

The chapter proposes a hybrid dynamical model of cascading failures in power systems. First-order flow equations are used to model the dynamic behavior of the power flow, and transitions due to power congestion in lines define the discrete dynamics in network evolution. At the future, studies of the model can include stability analysis of an output designed function that represents the state of load during the time. Besides, the framework will include proposed control strategies to reduce power losses.

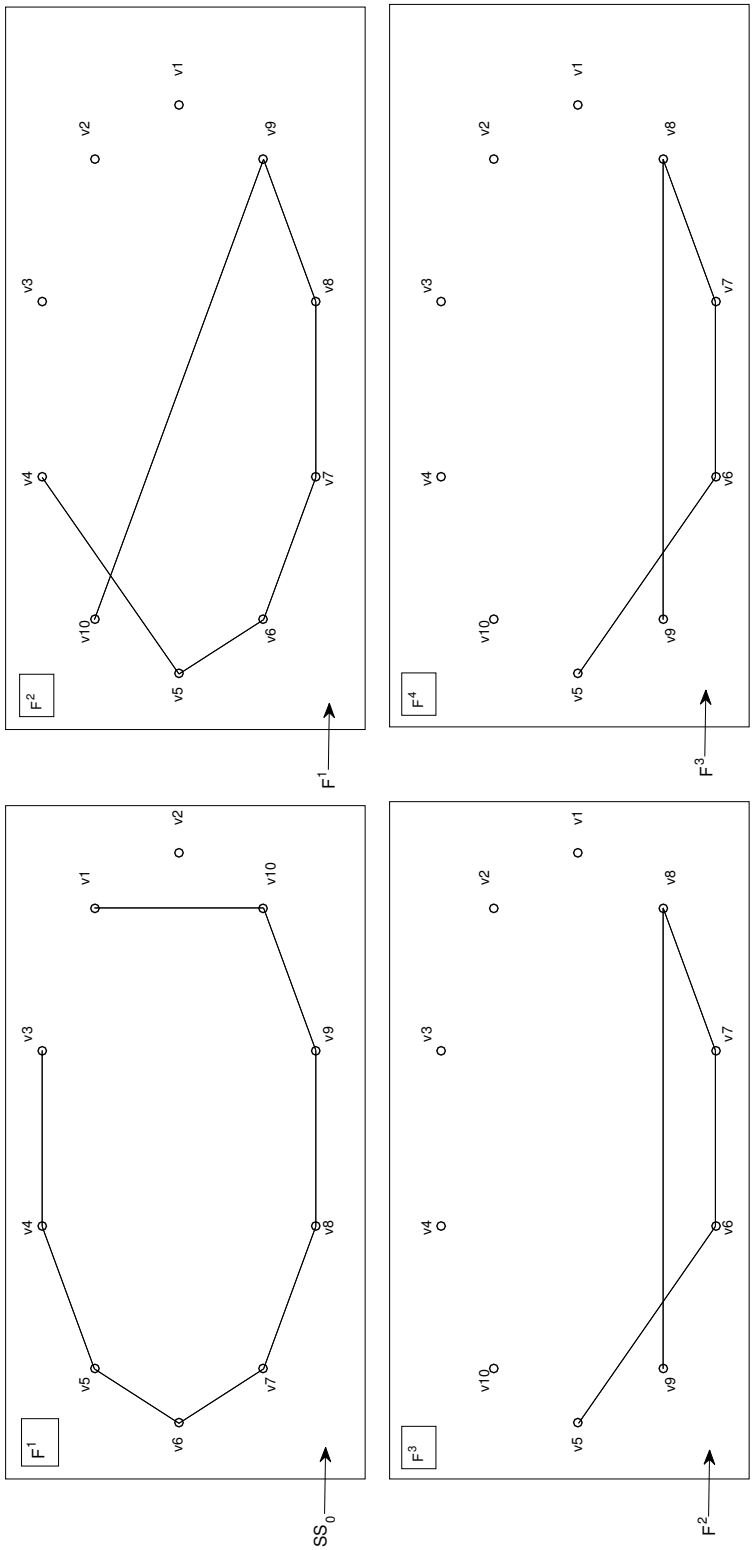


Figure 4.3: Picture of a small failure process initiated by outages of the edges connecting a demand node to the network. An small connected component continues active when failure stops. Initial conditions are the final state of no failure process described in ”no failure” case.

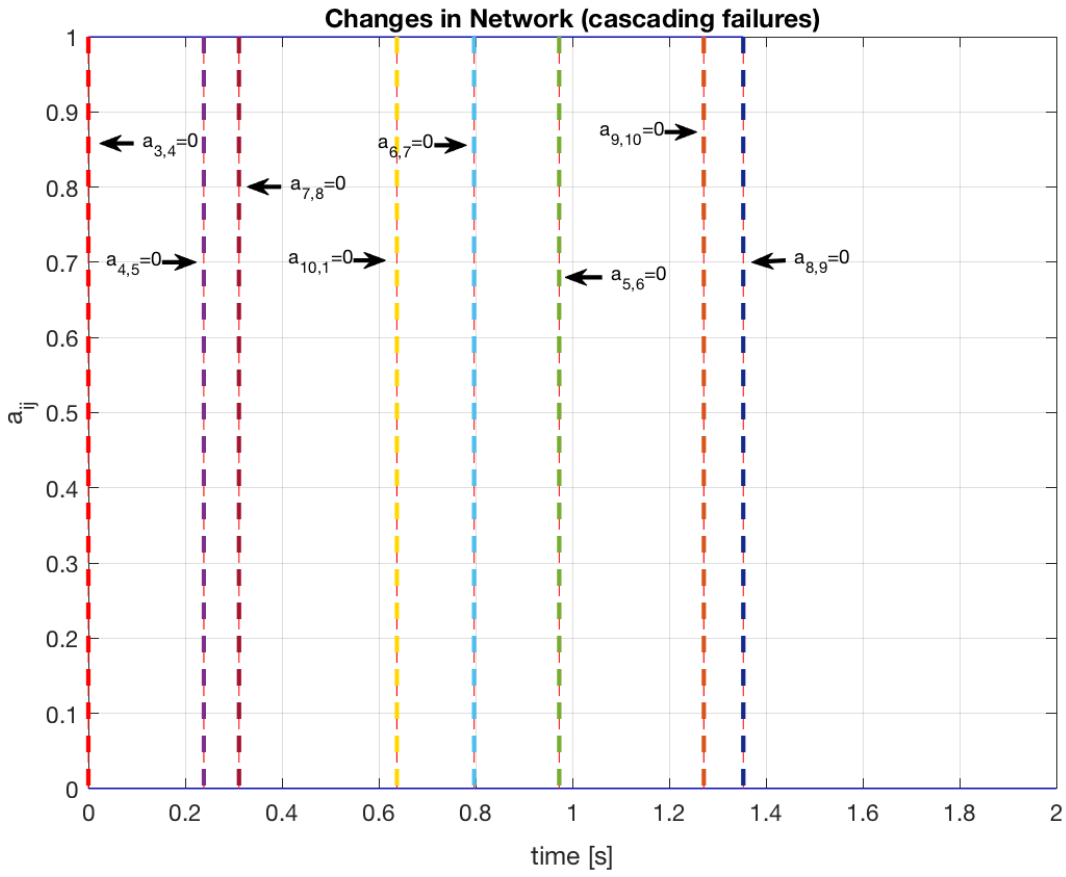


Figure 4.4: Jump events for A where edges a_{ij} goes to zero if a failure occurs. All edges of graph $\mathcal{G}$ are disconnected when the cascade failures end

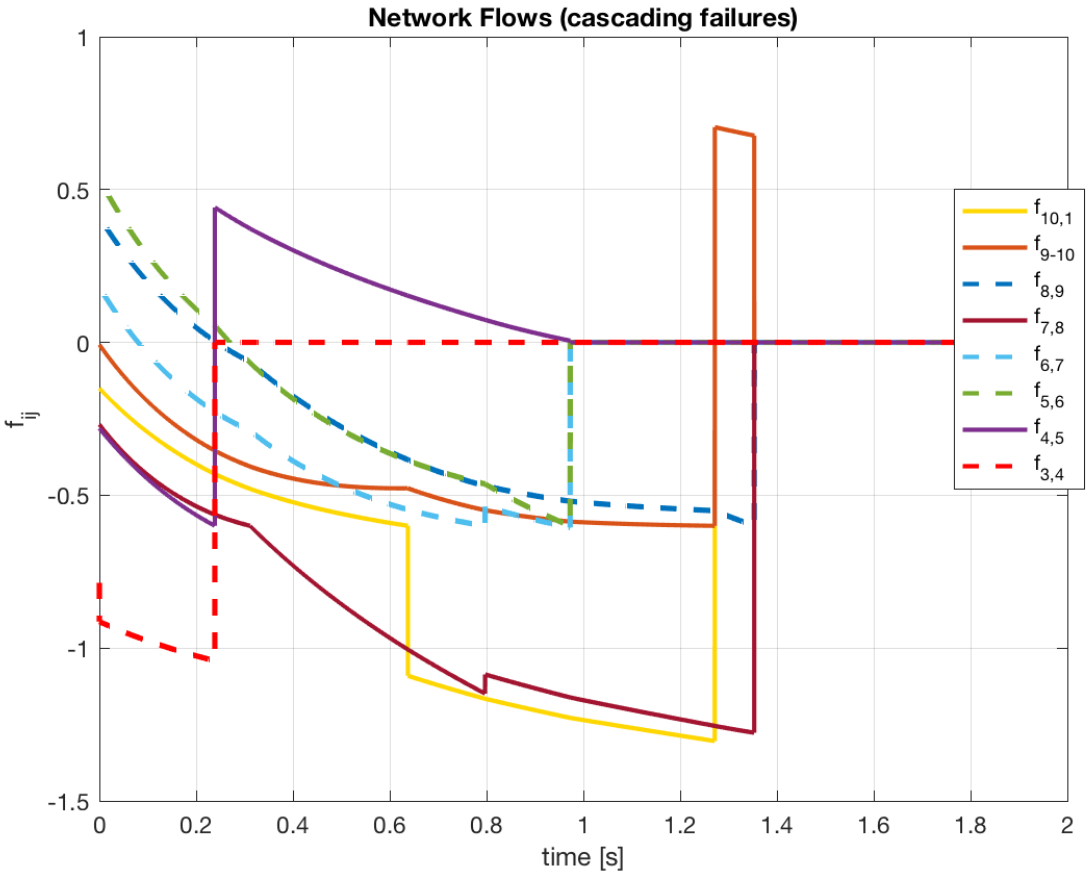


Figure 4.5: Solutions to $\mathcal{H}_n$ for network flows $f_{ij} = \theta_i - \theta_j$ on each edge of a cycle graph $\mathcal{G}$. A cascade failure process occur affecting the stability of the solutions. The failure event occurs in all the network making every flow goes to zero.Initial conditions are randomized in $\theta_0 \in [-0.5, 0.5]$

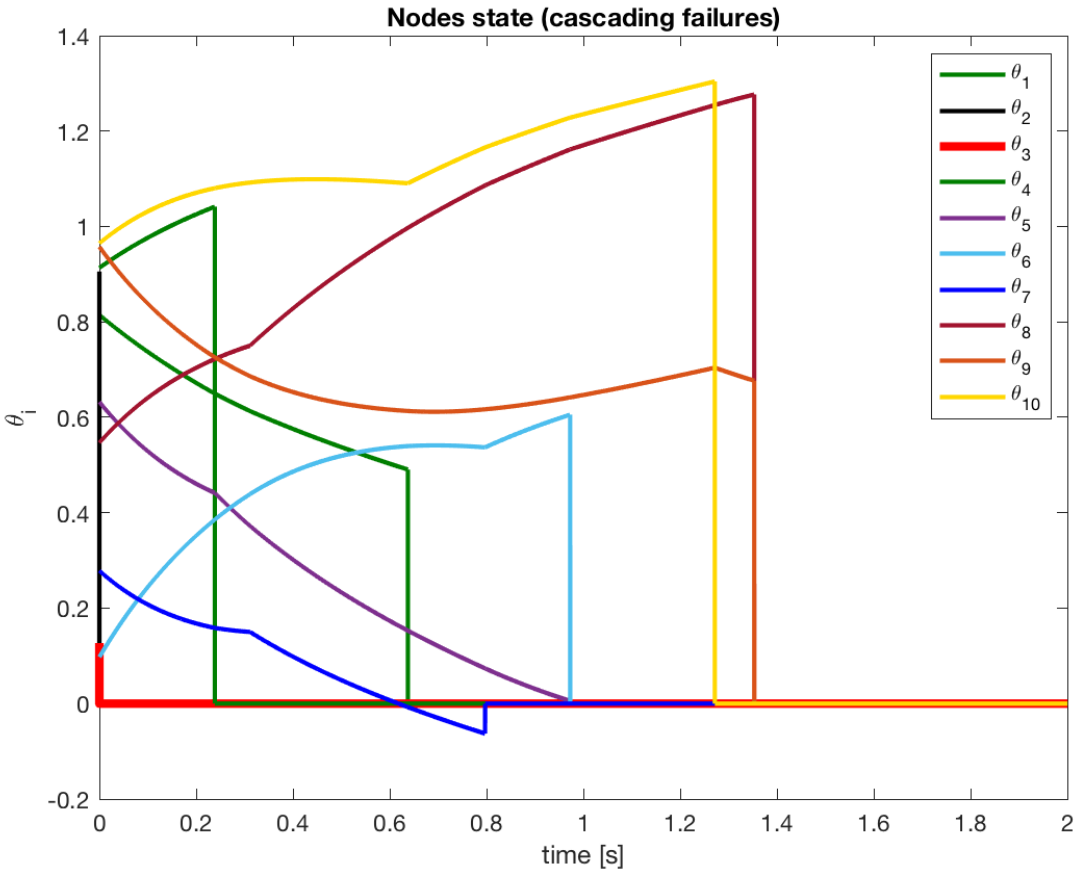


Figure 4.6: Flows of phase angle θ_i for every node in $\mathcal{G}$ during a cascade failure process. State of node variables jumps depending on network connectivity

Figure 4.7: Picture of a cascade failure process initiated by outages of the edges connecting a demand node to the network. No connected component continues when failure stops.

Chapter 5

Identification of Cascading Propagation Paths

"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that (Carroll & DAL, 2015)."

Lewis Carroll
Alice in Wonderland

Prediction of vulnerable lines during cascading failures is an essential issue for power networks. The identification of critical lines may enable the application of targeted countermeasures and reduce cascading failure effects. Based on topological information and line power transmission capacity, we propose the use of cut-sets (CS) to quantify the line significance during cascading failures phenomenon. We calculate a CS-based measure by the use of the Nagamochi-Ibaraki algorithm. Then, we compare the CS measure with other network-based and flow-based indices: the edge-betweenness centrality and the power flow centrality over cascading failures in a Quasy Stable-State (QSS) approach of the model in Chapter 3. Simulation results show that the CS measure outperforms in predicting the edges significance for the cascading failure propagation path.

First, the network model is described. It involves inherent electrical properties regarding the transmission line capacity of every element. Second, the Nagamochi-Ibaraki algorithm is presented. This algorithm identifies the critical edges. Third, the cascading failures algorithm is introduced. Cascading failures will be simulated for different failures. Failures propagation paths are identified. The results are compared with the results of the CS-measure and benchmark measures.

5.1 Network Model

We model power networks as finite undirected weighted graphs

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c}), \tag{5.1}$$

where $\mathcal{V}$ and $\mathcal{E}$ are the sets of nodes and links, representing buses and transmission lines, respectively, $\mathbf{c} := [\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_e, \ldots \mathrm{c}_M]$ is the vector of link capacities and $M = |\mathcal{E}|$. The physical topology of the grid is described by an $n \times n$ weighted adjacency matrix W with elements w_{ij}, where n is the cardinality of $\mathcal{V}$. For every transmission line connecting bus i and j, $w_{ij} = \mathrm{c}_e$, where e represents the edge between nodes v_i and v_j. Parallel circuits are simplified to a single edge with increased capacity.

5.2 Nagamochi-Ibaraqui Algorithm

The Nagamochi-Ibaraki algorithm is a computational method to calculate the edge-connectivity of a graph $\mathcal{G}$ identifying the CS with minimum capacity between all the nodes. The algorithm presents advantages over other methods that require flows, paths, or network flow direction (Frank, 1994). Consider the undirected weighted graph in (5.1). Let $c(v_x, v_y)$ denote the minimum weight of a cut separating nodes v_x and v_y. The edge connectivity $\lambda(\mathcal{G})$ of $\mathcal{G}$ is the minimum of $c(v_x, v_y)$ values over all the pairs of nodes.

For two disjoint subsets of nodes $\mathcal{V}_X, \mathcal{V}_Y$, let $d(\mathcal{V}_X, \mathcal{V}_Y)$ denote the edges weight sum for edges connecting $\mathcal{V}_X$ and $\mathcal{V}_Y$. Consider a node order $v_1, v_2, \ldots, v_n$ of the nodes in $\mathcal{G}$. $\mathcal{V}_i$ denotes the set of the first i elements. A node order is defined as legal if

$$d(\mathcal{V}_{i-1}, v_i) \geq d(\mathcal{V}_{i-1}, v_j), \tag{5.2}$$

for every pair i, j $(2 \leq i < j \leq n)$. If we delete the edges connecting v_n and v_{n-1}, the legal ordering remains legal, i.e., $v_1, v_2, \ldots, v_{n-1}$ for $\bar{\mathcal{G}}_1 := \mathcal{G} \setminus \{v_n\}$ and $v_1, \ldots, v_{n-2}, v_n$ is legal for $\bar{\mathcal{G}}_2 := \mathcal{G} - v_{n-1}$. Consider also that

$$c(v_n, v_{n-1}) = d(v_n, \mathcal{V}_{n-1}). \tag{5.3}$$

The algorithm is based on the existence of a legal node order, following (5.2), in the weights of the cut-set (5.3) and the following observation from (Frank, 1994): *Let v_x and v_y be two nodes for which $d(v_x) = c(v_x, v_y)$. If there is a minimum cut of $\mathcal{G}$, $\mu(\mathcal{G})$ between v_x and v_y, then $\mu(\mathcal{G}) = d(v_x)$, and the star of x is such a cut. If no minimum cut of G separates v_x and v_y, then, shrinking v_x and v_y into one node does not destroy any minimum cut. In this case the edge connectivity of $\mathcal{G}$ is equivalent to the edge-connectivity of the shrunken graph.*
Algorithm 2 presents the steps of the Nagamochi-Ibaraki Algorithm. In addition, Algorithm 3 identifies the vulnerable edges.

Algorithm 2 Nagamochi-Ibaraki Algorithm

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c})$
Output: $\mu(G)$
1: $\mathcal{G}_1 := \mathcal{G}$
2: **for** $i = 1$ to $i = n - 1$ **do**
3: Determine a legal ordering of the nodes of $\mathcal{G}_i$ according to (5.2) and (5.3).
4: Put in a list the last node v_i of this order along with the value $d(v_i)$.
5: Construct $\mathcal{G}_{i+1}$ from $\mathcal{G}_i$ by shrinking the last two nodes of the ordering.
6: **end for**
7: Choose an element v_j of the list for which $d(v_j)$ is minimum.
8: **return** $\mu(\mathcal{G}) = d(v_j)$.

Algorithm 3 counts and identifies the critical edges. If several minimum cut-sets exist in the graph, the function includes the edges from all the minimum edge cuts. The algorithm deletes one edge at a time and evaluates Algorithm 2. If the network minimum cut is reduced by removing e_{ij}, then, the edge e_{ij} is added to the critical list.

Algorithm 3 Critical Edges Algorithm

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c})$
Output: $\mathcal{E}_{critic}$
Find $\mu(\mathcal{G})$ by Algorithm 2.
2: **for** all $e \in \mathcal{E}$ **do**
Remove edge e, $\hat{\mathcal{E}} \leftarrow \mathcal{E} \setminus \{e\}$.
4: $\hat{\mathcal{G}} \leftarrow (\mathcal{V}, \hat{\mathcal{E}})$.
Find $\mu(\hat{\mathcal{G}})$ by Algorithm 2.
6: Check $\mu(\hat{\mathcal{G}}) < \mu(\mathcal{G})$.
if YES **then**
8: increase the number of critical edges $s = s + 1$.
Add edge e to the critical edge set $\mathcal{E}_{critic}$.
10: **end if**
end for
12: **return** $\mathcal{E}_{critic}$.

5.3 Cascading Failures Algorithm

The cascading failures process is shown in Algorithm 4. Each simulation starts with the initial state of the power system before a trigger failure or attack. First, it generates the network-based model for the power system and calculates the DC power flow by using the input information of the network described by the tuple $\mathcal{C} = (B, T, \mathbf{p})$. The object $\mathcal{C}$ includes all the information of the network structure in the branches matrix T. It also includes the operation supply/demand for each node in $\mathbf{p}$ and buses classification in matrix B.

After the power flow calculation, the algorithm evaluates the branches overload as the rate of use $RoU_e = \frac{f_e}{c_e}$ of every edge, where f_e is the power flow on edge e. It also evaluates the maximum overload, RoU^*= $\max_{e \in \mathcal{E}} RoU_e$. If its value is higher than a defined maximum threshold of overload in the network, then it disconnects the overloaded edges. Once it finishes, it evaluates if a feasible flow exists for the system and repeats the process. If the threshold value is not exceeded, the simulation stops and returns the new state of the network with all its parameters updated.

The algorithm also identifies isolated nodes and dismisses them for a new iteration of the cascade failures algorithm. If the network is separated in several groups of connecting elements, the algorithm stops and returns the final network state. The algorithm also updates parameters and the tuple $\mathcal{C}_{new} = (B_{new}, T_{new}, \mathbf{p}_{new})$ to be evaluated by the routing policy generator.

5.4 Experimental Setup

This section presents the benchmark measures to be used. All measures are compared against the CS-based measure calculated in Section 5.2. Better prediction corresponds to measures closer to the edges identified with high failure probability. Three metrics are used: edge failure probability, edge-betweenness centrality, and flow rate of use. The metrics are described in the following. The edge failure probability $\rho(e)$ is calculated by several iterations of the cascading failures algorithm resulting in different failure conditions. The edges with a probability of failure $\rho(e) \geq 0.02$ are considered vulnerable, as well as members of the most common cascading failures paths. Edge-betweenness centrality $B(e)$ counts the shortest paths between a pair of nodes passing through the edge as:

$$B(e) = \sum_{i \neq j} \frac{\sigma_{ij}(e)}{\sigma_{ij}}, \tag{5.4}$$

where σ_{ij} is the number of shortest paths from node i to j, and $\sigma_{ij}(e)$ is the number of shortest paths from i to j that pass through edge e. A parameter Rate of Use (RoU) is defined for each edge, measuring the edge loading with respect to its capacity

$$RoU_e = \frac{f_e}{c_e} \quad \text{for all} \quad e \in \mathcal{E}. \tag{5.5}$$

5.5 Results and discussion

The IEEE 30-bus power system is considered a case study. The graph model of the power network with edge weights assigned depending on edge transmission capacities are shown in Figure 5.1. The schematic of the system is shown in Figure 5.2. The system has 30 nodes, 41 edges, six generators, and 20 loads. Its primary power injections come from generators in nodes 2 and 13. Also,

Algorithm 4 Cascading Failures Simulation

Input: $\mathcal{C} = (B, T, \mathbf{p})$
Output: $\hat{\mathcal{E}}$ for all the trials.

while trials ≥ 0 **do**
  Initialize the network $\mathcal{G}$ based on $\mathcal{C} = (B, T, \mathbf{p})$.
  Select and apply a random trigger failure e^*.
  Get power flow f. Check for power flow convergence.
  if YES **then**
    for all the edges $e \in \mathcal{E}$ **do**
      Evaluate the rate of use $RoU_e = f_e/\mathrm{c}_e$.
    end for
    Evaluate maximum rate of use, RoU^*= $\max_{e \in \mathcal{E}} RoU_e$.
    Check condition $RoU^* \geq 1$.
    if YES **then**
      Disconnect overloaded edges,
      $\hat{\mathcal{E}} := \{e \in \mathcal{E} \mid RoU_e \geq 1\}$.
      Recursively repeat the algorithm.
    else
      return Disconnected edges set $\hat{\mathcal{E}}$.
    end if
  else
    Find unintentional disconnected nodes set $\mathcal{I}$ where $\mathcal{I} := \{v_i \mid \mathcal{N}(v_i) = \emptyset\}$.
    Find all the connected components $\mathcal{P}$ where,
    $\mathcal{P} = \{\mathcal{V}_i \subseteq \mathcal{V} \mid \text{for all } (i,j), \quad \mathcal{V}_i \cap \mathcal{V}_j = \emptyset \wedge \mathcal{N}(\mathcal{V}_i) = \emptyset\}$.
    Check if there is more than one connected component, $|\mathcal{P}| > 1$.
    if YES **then**
      return $\mathcal{G}, \hat{\mathcal{E}}$
    else
      Update the network without the isolated nodes.
      Recursively repeat algorithm.
    end if
  end if
  Merge the data $\hat{\mathcal{E}}$ for trial i.
end while
return $\hat{\mathcal{E}}$ for all the trials.

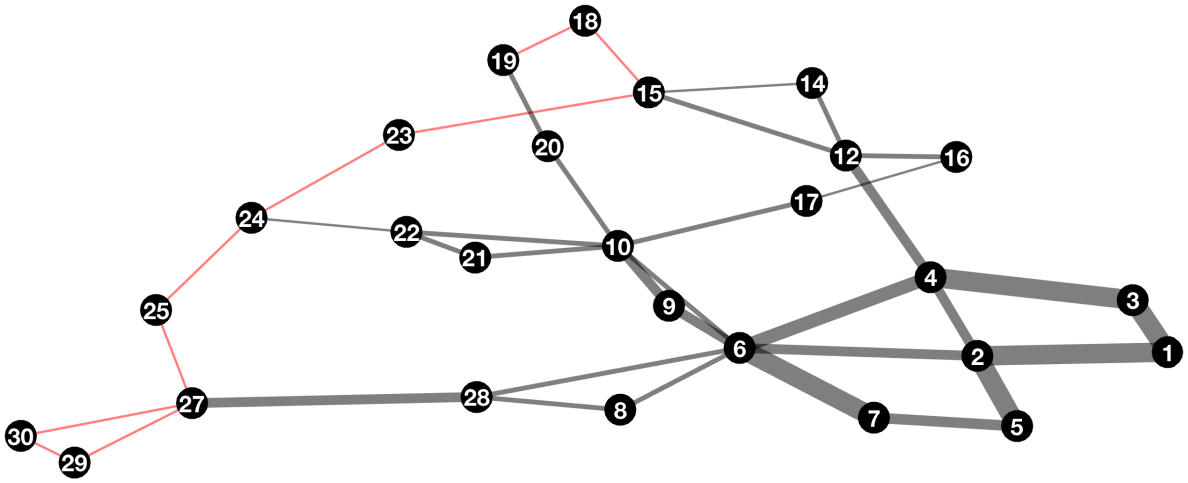


Figure 5.1: Network representation of the k-core of IEEE 30- buses power system with $k = 2$. The edges thickness represent their weights, i.e., transmission line capacities. Highlighted edges correspond to the critical elements identified by the CS method.

the higher loads are located on node 2, node 7, and node 8. Highlighted red edges in Figure 5.1 and Figure 5.2 are the critical edges identified by the CS measure. More vulnerable lines are connected between them and located in a reduced system area. None of the nodes has a high connectivity degree, and all edges have low capacities. Next, benchmark measures for identification of vulnerable edges are performed according to (5.4), (5.5) and Algorithm 3. Betweenness centrality, RoU_e and CS results are shown in Figure 5.3a.

Each measure evaluates edges significance depending on its steady-state operation. The edges significance based on topological and electrical properties is quite different. On the other hand, some edges, such as e_{6-28}, e_{10-6} and e_{12-4}, are at a critical significance according to the betweenness measure, but null significance according to the RoU_e centrality. On the other hand, edges such as e_{6-8} and e_{15-23} are at a critical significance according to power flow centrality but have no significance according to betweenness centrality. Finally, the CS measure identifies significant edges that none of the previous measures had pointed out: edge e_{15-18}, edge e_{18-19}, e_{23-24}, and e_{24-25}. The CS measure shows that most of the edges have no significance, and all the significant edges in the system are placed between nodes v_{15} to v_{30}.

Cascading failures simulations are performed according to Section 5.3. Experiments for $trials = 4000$ with different combinations of q-trigger events, q values, and cascading effects are performed. For each q-trigger, where q is the number of initially disconnected edges, elements are randomly selected and disconnected. After that, the cascading effects are evaluated following the described cascade simulation algorithm. After q-trigger edges are removed, the system could continue in the same state, or cascading failures of different sizes could occur. Cascading failures occur for $q = 4$. Below this q value, the network is robust and maintains its function without cascade.

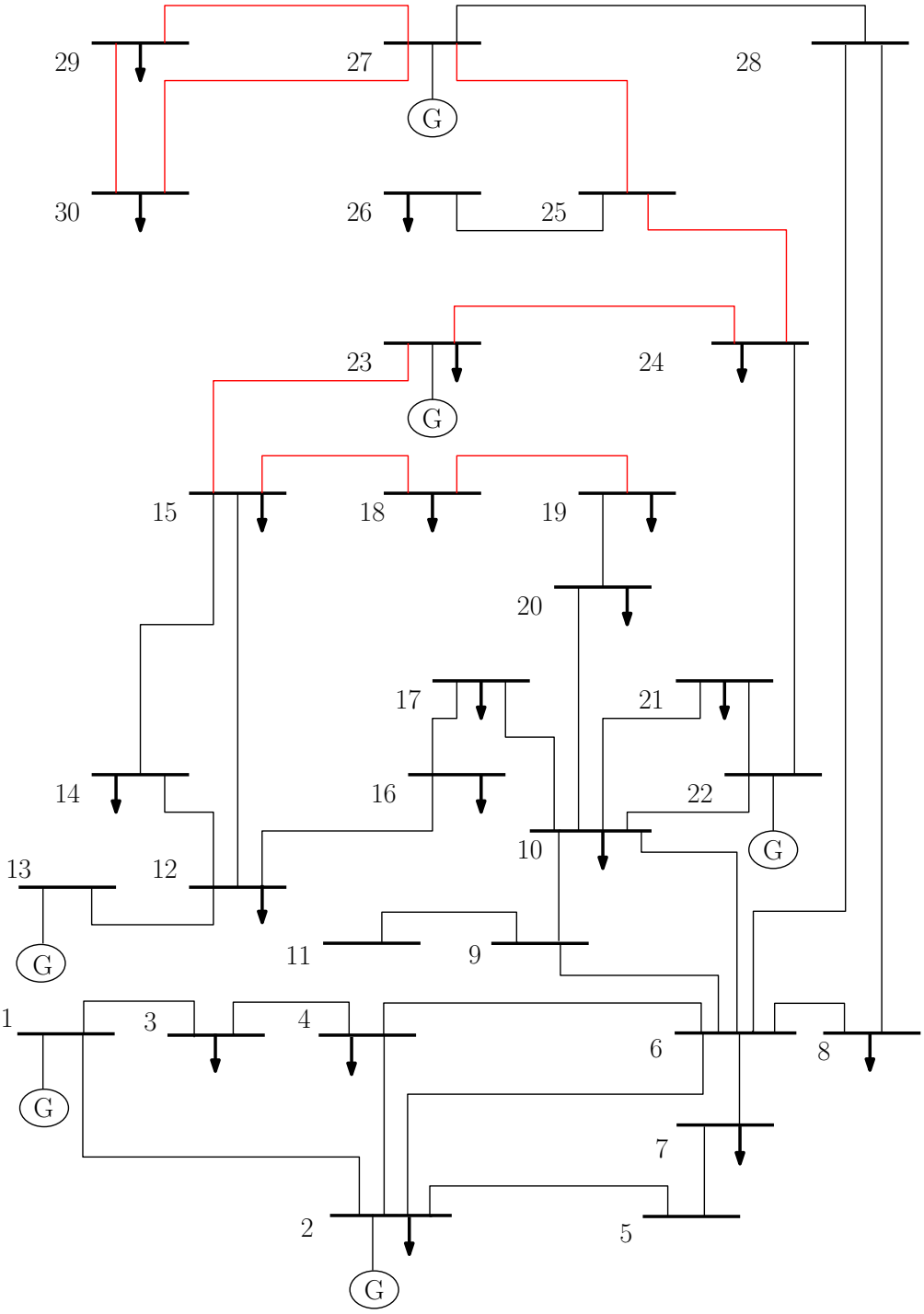
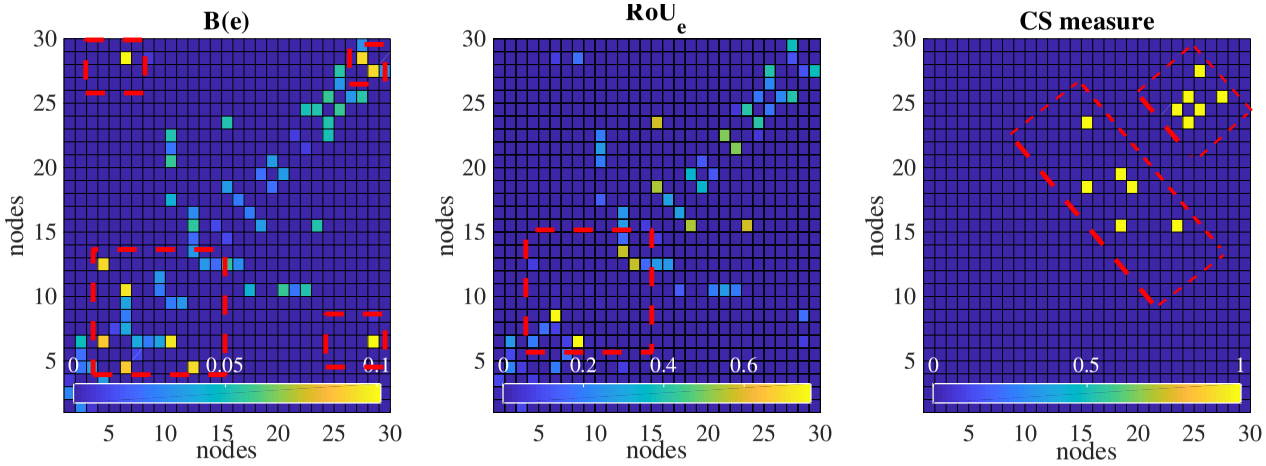
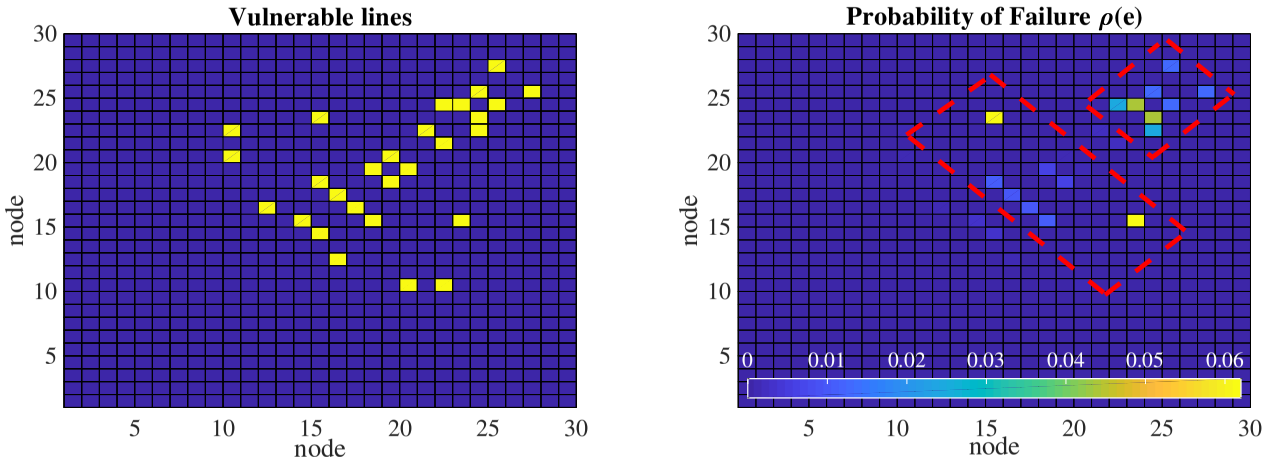


Figure 5.2: IEEE 30-bus system.

After experiments are performed, a probability of failure is calculated for each one of the edges according to its participation in cascading propagation. All the edges that exist in the cascading failures propagation path for more than one trial of cascading failure simulation are identified and shown in Figure 5.3b. The edge failure probability is also shown on the right side of the figure. Results show that 34% of the edges participate in cascading failures scenarios, but, only 7.3% of



(a) Centrality measures for the IEEE 30-bus: Betweenness centrality, rate of use and CS measure.



(b) Edges with significant failure probability during cascade effects. 4000 q-trigger experiments are performed. Cascading failures occur for $q = 4$.

Figure 5.3: Centrality measures and identification of the failure propagation path.

the edges have a high probability of failure. Edges found by the experiments and its probability of participation in a failure event are used to compare the effectivity of the proposed measures and thus predict the edges in the cascading failures paths. Failure predictions are compared between the different measures in Figure 5.4.

Betweenness centrality identifies edges with a normalized value of $B(e) > 0.5$ as vulnerable. For power flow centrality, lines with $RoU_e > 0.5$ are considered weak. Probability of failure is also normalized according to its maximum value. Results show that the most significant edge is identified by RoU_e centrality and CS measure. Also, the second most significant is identified by $B(e)$ centrality and CS measure. RoU_e centrality predicts failures in edge 22, edge 29, and edge 30. Betweenness centrality $B(e)$ predicts failures in edge 20, edge 21, edge 29, and edge 32. The CS measure identifies most of the significant edges: edge 30 and edge 32. Also, CS identify three significant edges not identified by the other measures: edge 23, edge 33, and edge 35. The CS measure joins topological and flow-capacity network properties that reflect the consequences occurring during cascade effects. A hidden failure with high probability is identified in edge 31; however, it is not predicted by any measure. Possibly, it could be related to a similar effect in the node neighborhood of the CS edge set.

Figure 5.5 shows the nodes that experiment cascading failures effects. More affected nodes with the highest probability of failure $\rho(v)$ could be identified by considering the incidence nodes for edge members of the CS. Node 15, node 23, and node 24 are the most affected. Nodes out of the CS node set have significantly lower probabilities of failure. All the cascade events considered are occurring before the network partition. Isolated nodes are considered, but disconnected components and re-dispatch are not considered at the first stage of the cascade. In this way, the CS measure proposed in this work gives information about contingencies that the network could experience before significant unintentional network separation. Even if not all possible events of failure are predicted, the CS measure helps in cascading failures path prediction and shows essential information about the most vulnerable areas of the network. By combining topological and electrical properties in the measure and comparing it with experimental setup and cascading failures simulation, we can state the applicability of the proposed vulnerability measure.

In this work we have presented a CS-based vulnerability measure that consists in identifying the set of edge-cuts with the minimum capacity in a given power network. A computational method based on the Nagamochi-Ibaraki algorithm is used to calculate the CS. Computational simulations of cascading failures for the IEEE 30-bus case study show that the CS method is more effective in qualifying the significance of an edge than betweenness and power flow centrality. Lines in the minimum cut-sets are influential in the cascading failures propagation path. If q-triggered failures of any kind are performed in the network, then, the probability of occurrence of cascading failures effects on the edges in the cut-sets is higher than in all other edges. The aim of applying the proposed CS method to power networks is the prediction of edges in the cascading failures path. This information will be useful to increase the capacity of the network or reinforce its connectivity and reduce the probability of cascade. For future work, CS methods will be used to improve the robustness of the power network against cascading failures by considering lines of reinforcement

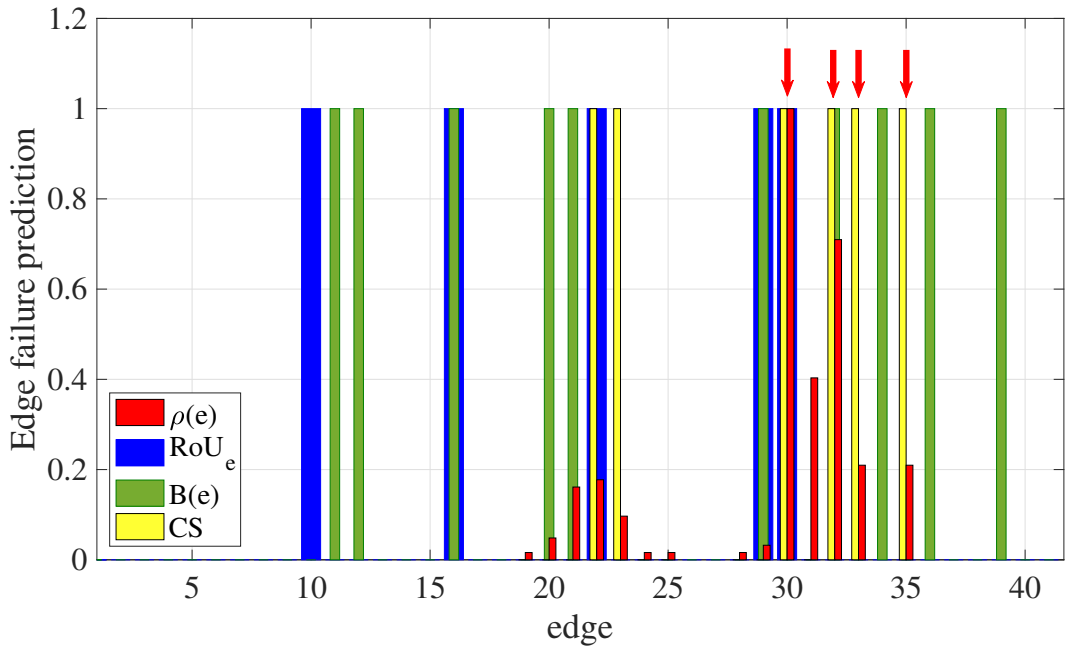


Figure 5.4: Comparison of failure prediction between the different measures. Probability of failure is normalized.

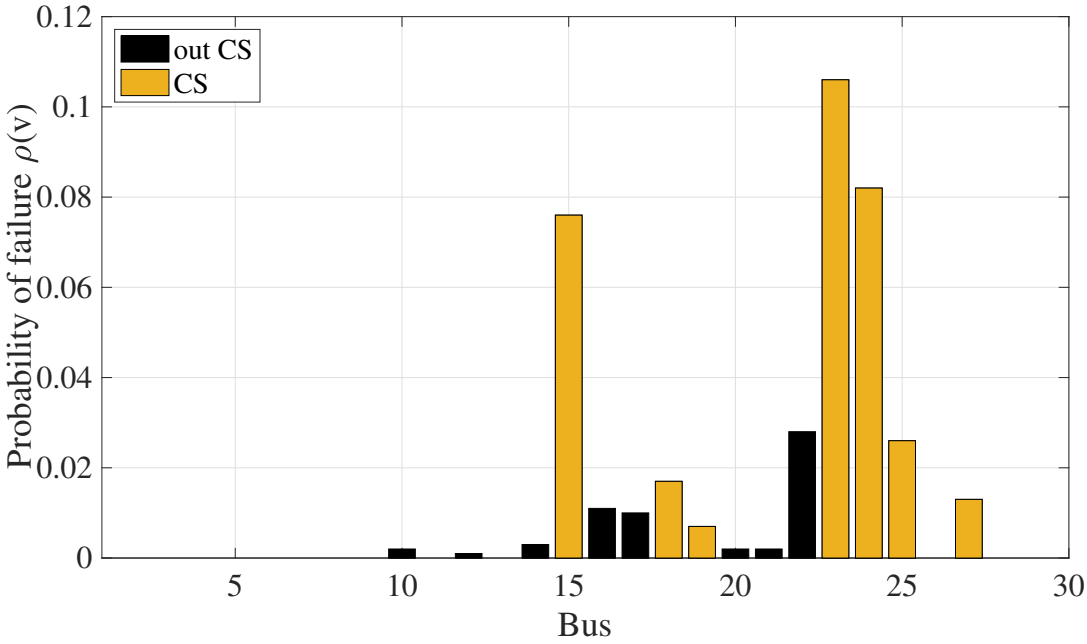


Figure 5.5: Incident nodes significance compared between elements identified by the CS measure and all the implied nodes.

in planning.

5.6 Conclusions

In this chapter we have presented a CS-based vulnerability measure which consists of identifying the set of edge-cuts with the minimum capacity in a given power network. A computational method based on the Nagamochi-Ibaraki algorithm is used to calculate the CS. Computational simulations of cascading failures for the IEEE 30-bus case study shows that the CS method is more effective in qualifying the significance of an edge than betweenness and power flow centrality. Lines in the minimum cut-sets are influential in the cascading failures propagation path. If q-triggered failures of any kind are performed in the network, then, the probability of occurrence of cascading failure effects on the edges in the cut-sets is higher than all other edges. The aim of applying the proposed CS method in power networks is towards the prediction of edges in the cascading failure path. This information will be useful to increase their capacity or reinforce its connectivity and reduce the probability of cascade. In the following chapters, CS methods will be used to improve the robustness of the power network against cascading failures by considering lines reinforcement in planning.

Part III

Controlling Cascading Collapse in Power Networks

Chapter 6

A Minimum Cut-Set Vulnerability Analysis of Power Networks

"You may never know what type of person someone is unless they are given opportunities to violate moral or ethical codes (Taleb, 2012)."

Nassim Nicholas Taleb
Antifragile: Things That Gain From Disorder

Reducing vulnerability to cascading failures and attacks is a critical challenge for the energy grid of the future. For this, new frameworks and metrics should be proposed to identify network characteristics affecting system vulnerability. This chapter studies the minimum cut set (MCS) vulnerability. The study aims to attack the MCS and evaluate subsequent cascading failures as the vulnerability analysis framework, allowing the assessment of global and local vulnerability generated by congestion within the transmission network. Network model and analysis consider supply/demand placement. The chapter shows an extension of the QSS model to include the re-dispatch of power flow after cascading failures events. The network evolves either by cascading failures or sequential attacks. We propose an MCS attack strategy. The strategy is designed to maximize the attack long-term expected reward while reducing attack sequence duration. We develop algorithms for identifying targets and updating power flow solutions and system balance during network evolution. Case studies are used to verify the framework results. A vulnerability index, based on attacks efficiency, has been proposed to assess the network response to different targets selection. Finally, we assess the minimum cut-set vulnerability analysis on networks with different properties and sizes.

6.1 Cascading Failures Model based on Flow networks

The network-based power system model proposed in this work generates valuable information about connectivity, nodes interaction, network evolution and failures. The model includes the rela-

tion between network-based characteristics (e.g. graph topology, adjacency matrix, edge weights) and system-based characteristics, such as generation/load profile, power flows and cascading failures.

6.1.1 Network-based Characteristics

The power system is modeled as a finite undirected weighted flow graph $\mathcal{G}$ such that

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c}), \tag{6.1}$$

where the node set $\mathcal{V}$ and the edge set $\mathcal{E}$, with cardinality $|\mathcal{V}| = n$ and $|\mathcal{E}| = m$, represent buses and transmission lines, respectively. In addition, $\mathbf{c}^t \in \mathbb{R}^m$ is a vector with link flow transmission capacities. In this model, we equate capacities with edge weights. Parallel circuits between buses are represented by a single edge with the sum of their respective capacities.

6.1.2 System-based Characteristics

For the power network in (7.1), let $\mathcal{V}_s \subset \mathcal{V}$ be the set of supply nodes and let $\mathcal{V}_d \subset \mathcal{V} \setminus \mathcal{V}_s$ be the set of demand nodes in the network. Transmission nodes without supply or demand are $\mathcal{V}_b \subset \mathcal{V}$. Consider a node associated with supply/demand vector $\mathbf{p}$ where $\mathbf{p} \in \mathbb{R}^n$; $p_v > 0$ for $v \in \mathcal{V}_s$, $p_v < 0$ for $v \in \mathcal{V}_d$, and $p_v = 0$ for $v \in \mathcal{V}_b$ and $\sum_{v \in \mathcal{V}} p_v = 0$. Consider a flow vector at time t, $\mathbf{f}^t \in \mathbb{R}^m$ where f_e^t is the flow at edge e and satisfies capacity constrain $|f_e^t| < c_e^t$ on every link $e \in \mathcal{E}$ and flow conservation $\sum_{e \in \mathcal{E}_v^t} f_e^t = p_v$ for every node v where $\mathcal{E}_v^t \subseteq \mathcal{E}$ is the set of all incident edges to the node v. The vector flow $\mathbf{f}^t$ is defined by a routing policy $\mathbf{\Xi}^t$. The routing policy defines the magnitude and direction of every edge flow in the network. In this study, we consider a linear routing policy such that

$$\mathbf{f}^t = \mathbf{\Xi}^t \mathbf{p}, \tag{6.2}$$

where $\mathbf{\Xi}^t$ is an $m \times n$. The matrix $\mathbf{\Xi}^t$ maps the supply/demand profile $\mathbf{p}$ onto the power flows going through each edge. The flow routing will depend on the electric and topological properties of the power system. In this study, we use a routing policy based on the DC power flow.

To derive $\mathbf{\Xi}^t$, following (Cetinay, Kuipers, & Mieghem, 2018), consider the DC power flow equations of the power network in terms of the network adjacency matrix $\mathbf{A}$,

$$p_v = \sum_{i=1}^{n} = a_{vi} b_{vi} (\theta_v - \theta_i) = \theta_v \sum_{i=1}^{n} a_{vi} b_{vi} - \sum_{i=1}^{n} a_{vi} b_{vi} \theta_i. \tag{6.3}$$

The terms θ_v and θ_i are the voltage phase angles at bus v and i. b_{ik} is the reciprocal of the transmission line reactance between buses. Then, consider an auxiliary adjacency weighted

matrix $\mathbf{H}$, where $h_{vi} = a_{vi}b_{vi}$ is an edge weight associated with the impedance. Then, the corresponding matrix representation of the DC power flow equation in the power network is $\mathbf{p} = \left\{\mathbf{diag}\left(\sum_{i=1}^{n} h_{vi}\right) - \mathbf{H}\right\}\mathbf{\Theta} = (\mathbf{D} - \mathbf{H})\,\mathbf{\Theta}$, where $\mathbf{D}$ is a weighted degree diagonal matrix. Introducing the weighted laplacian matrix $\tilde{\mathbf{Q}} = \mathbf{D} - \mathbf{H}$, the equation can be described as $\mathbf{p} = \tilde{\mathbf{Q}}\mathbf{\Theta}$. Calculating a pseudoinverse $\tilde{\mathbf{Q}}^{+}$ of the weighted laplacian it is possible to describe voltage angles of $\mathbf{\Theta}$ as a function of $\mathbf{p}^t$ as $\mathbf{\Theta} = \tilde{\mathbf{Q}}^{+}\mathbf{p}$. The flow f_e at the edge e between node v and node i can be determined as $f_e = b_{vi}\,(\theta_v - \theta_i)$, with its related matrix representation $f^t = \tilde{\mathbf{B}}^{\top}\mathbf{\Theta}$. The term $\tilde{\mathbf{B}}$ is the weighted incidence matrix with $\tilde{b}_{ve} = h_{vi}$ if edge flow f_e goes from v to i, or $\tilde{b}_{ve} = -h_{vi}$ if edge flow f_e goes from i to v and zero otherwise. Then, replacing $\mathbf{\Theta}$ by the matrix equation as a function of the pseudoinverse, we get $\mathbf{f}^t = \tilde{\mathbf{B}}^{\top}\tilde{\mathbf{Q}}^{+}$. As a result the routing policy matrix is $\mathbf{\Xi}^t = \tilde{\mathbf{B}}^{\top}\tilde{\mathbf{Q}}^{+}$ with the element $\xi_{ij}^t = \tilde{b}_{ei}\tilde{q}_{vi}^{+}$.

6.1.3 Network Evolution and Cascading Failures

The network dynamics presented here follows the nomenclature and the model presented in (Savla et al., 2014). Consider the power system modeled as a flow network in (7.1) with supply/demand vector $\mathbf{p}$ and flows in (7.2) evolving in time. Let $\mathcal{G}^t = (\mathcal{V}^t, \mathcal{E}^t, \mathbf{c}^t)$ and $\mathbf{f}^t$ describe the state of the system at every time $t = 0, 1, \ldots$, where $\mathcal{V}^t \subseteq \mathcal{V}$ and $\mathcal{E}^t \subseteq \mathcal{E}$ are the active nodes and links at time t.

For the initial condition of the system $(\mathcal{G}^0, \mathbf{f}^0)$, all the elements of the node and edge set start active, i.e. $\mathcal{V}^0 = \mathcal{V}$, $\mathcal{E}^0 = \mathcal{E}$, and $\mathbf{f}^0$ is the initial flow. At every time t, network $\mathcal{G}^t$ should be connected. Define $\hat{\mathcal{G}}^t$ as the largest connected component in $\mathcal{G}^t$ and $\hat{\mathcal{G}}^0 \equiv \mathcal{G}^0$. The largest connected component of the network refers to the biggest connected part of the entire nodes set where a feasible flow exist. Considering the largest connected component, we are modeling the network in its natural dynamical behavior. Edge disconnection produced by cascade propagation may generate uncontrolled component islanding. Uncontrolled islanding or redispatch is considered during the cascade propagation. In this way, the small connected components could have only load nodes or unbalanced supply-demand nodes that collapse during the cascade evolution. Attack-defender threat models could include controlled actions, but defender actions are out of the scope of this model. The network changes its state as follows. Edges become overloaded when its current flow exceeds the transmission capacity. All the overloaded edges are disconnected along with all the edges in small subcomponents isolated from the largest connected component $\hat{\mathcal{G}}^t$. Accordingly,

$$\mathcal{E}^{t+1} = \mathcal{E}^t \setminus \left\{e \in \mathcal{E} : f_e^t \geq c_e\right\} \cup \left\{e \in \mathcal{E}_v^t : v \notin \hat{\mathcal{V}}^t\right\}. \tag{6.4}$$

Next, all active nodes v that have no incident edges, along with all those not included in the large connected component become inactive, i.e.

$$\mathcal{V}^{t+1} = \mathcal{V}^t \setminus \left\{v \in \mathcal{V}^t : \mathcal{E}_v^t = \emptyset\right\} \cup \left\{v \notin \hat{\mathcal{V}}^t\right\}. \tag{6.5}$$

Nodes and edges disconnection is irreversible. For each $e \in \mathcal{E}$, the routing policy in (7.2) determines its current flow. In addition, the capacity vector $\mathbf{c}^t$ is changed by a disturbance $\delta^t \in \mathbb{R}^m$,

$$c_e^{t+1} = c_e^t - \delta_e^t, \qquad e \in \mathcal{E}^t. \tag{6.6}$$

Disturbance δ is defined according to the attack strategy (e.g. single line attack or multiple line attacks) as will be described in Section 6.2.2. The initial equilibrium flows $\mathbf{f}^0$ are generated by the given routing policy. The network state does not change as long as $\delta^t = 0$. The initial line transmission capacity $\mathbf{c}^0$ is defined by $\mathbf{c}^0 = \alpha \mathbf{f}^0$, where α is a tolerance parameter and $\alpha \geq 1$.

Modelling the power network and its evolution during failures as a dynamic flow network gives us the advantage to study the influence of the network structure and its interdependency on the physical properties of the power flow. Connectivity analysis can be considered in terms not only of structure but also of flow dynamics at the same time.

6.2 Minimum Cut-Set Sequential Attacks

In this section, we present a mathematical model of the attacker, the attacker control problem modeled as a minimum cardinality optimization problem.

6.2.1 The Minimum Cut Set

Consider an edge cut-set $\hat{\mathcal{S}} \subseteq \mathcal{E}$ of the flow network $\mathcal{G}$ as a set of edges such that every flow path from the supply nodes set $\mathcal{V}_s$ to the demand nodes set $\mathcal{V}_d$ uses at least one edge from $\hat{\mathcal{S}}$. Then, $\mathcal{E} - \hat{\mathcal{S}}$ disconnects all the elements from $\mathcal{V}_s$ to $\mathcal{V}_d$. The edge cut-set has an associated weight defined by $W\left(\hat{\mathcal{S}}\right) = \sum_{e \in \hat{\mathcal{S}}} c_e$. Accordingly, the minimum cut-set (MCS) $\mathcal{S}$ for the network $\mathcal{G}$ can be defined as the edge cut-set between $\mathcal{V}_s$ and $\mathcal{V}_d$ with minimum weight as follows:

$$S := \left\{ e \in \mathcal{E} : W(\mathcal{S}) = \min_{\hat{\mathcal{S}} \subseteq \mathcal{E}} W\left(\hat{\mathcal{S}}\right) \right\}. \tag{6.7}$$

Flow feasibility in the network can be described in terms of the MCS, as it's defined in the Ford-Fulkerson minimum cut theorem (Ford & Fulkerson, 1987). The maximum feasible flow value obtained in a network $\mathcal{G}$ is equivalent to the weight $W(\mathcal{S})$. A flow f^t is feasible if it satisfies the edge capacity limit and flow conservation for each node. For a power system modeled as a flow network, the minimum cut theorem implies that a feasible power flow between supply nodes and demand nodes exists only if demand profile is equal or lower than the MCS weight. Then the MCS defines the real transmission capacity of the network.

Definition 6.2.1 *The flow bottleneck constant q^t measuring the ratio between the transmission*

capacity of the MCS and the power demand is defined as follows

$$q^t = \frac{W\left(\mathcal{S}^t\right)}{\sum\limits_{v \in \mathcal{V}_d \cap v \notin \mathcal{I}^t} p_v}, \tag{6.8}$$

where $\mathcal{I}^t$ is the set of isolated nodes at time t.

The flow bottleneck constant q is defined based on (Taylor & Hover, 2011), where a flow-based Cheeger constant is proposed to identify Laplacians for flow networks. For the existence of a feasible flow between $\mathcal{V}_s$ and $\mathcal{V}_d$, a sufficient condition can be defined in terms of q^t as $q^t \geq 1$. For values of q^t close to 1 the network presents flow congestion. This means that power demand value is close to the transmission capacity limit of the network, which in general is subject to the structure of the network and the placement of supply and demand nodes in it. Higher values of q^t (i.e. $q^t \gg 1$) represent nonexistence of congestion. The MCS weight represent an upper limit for transmission in the established network configuration

6.2.2 MCS Attack Strategy

Attacker Model

The attack model assumes a single intruder threatening the network. The attack is repeated in time. For every stage t the attacker has to choose an action δ^t. Consider the sequence $\Delta =: (\delta^1, \delta^2, \ldots)$ of progressive disturbances representing the external adversary intervention against the power network. At every stage, the disturbance δ^t is modeled by $\delta^t = \Gamma^t \mathbf{c}^t$ where Γ^t is an $m \times m$ matrix and $\Gamma^t = diag\left(\gamma_1, \gamma_2, \ldots, \gamma_m\right)$. Disturbance δ^t is applied in (7.6) generating false system information about edge transmission capacities. In this work, to emulate edge removal, the elements γ_e^t are equal to 1 if edge e is attacked at the stage t, and zero elsewhere. For future work, values of γ_i in $[0, 1]$ could be considered. At every attack stage, a resulting cascade effect and lost load λ^t occurs in the network. The lost load is defined by $\lambda^t = \sum\limits_{v \in \mathcal{I}^t \cap \mathcal{V}_d} p_v$, where $\mathcal{I}^t$ is isolated nodes set resulting from the cascading failures at stage t. As a result, the attacker obtains a reward $g(\delta^t)$ at every stage t.

The most attractive target for the attack at each stage is the edge, whose failure would cause an increase in the system flow congestion. After the edge attack generates congestion, the system is more prone to evolve into a cascading failure. To measure the benefit of the attack in the stage t, we compare the flow bottleneck q after and before the element's attack. The component that reduces the value of q is identified as a critical component. Let q_e represent the bottleneck when edge e is attacked. Then, the change in the network congestion is given by $\Delta q_e^t = q^t - q_e$ and the best attack in the stage t is $\underset{e}{\operatorname{argmax}}\, \Delta q_e^t$. Change in network congestion can be described in terms

of (6.8) as

$$\Delta q_e^t = \frac{1}{\sum\limits_{v \in \mathcal{V}_d \cap v \notin \mathcal{I}^t} p_v} \left(W\left(\mathcal{S}^t\right) - W\left(\mathcal{S}^t \setminus e\right)\right). \tag{6.9}$$

Assume that the demand remains constant at the stage t except when edge isolates a demand node. If $e^* \in \mathcal{S}$, then $W\left(\mathcal{S}^t\right) - W\left(\mathcal{S}^t \setminus e^*\right) > 0$, and also if $e \notin \mathcal{S}$, then $W\left(\mathcal{S}^t\right) - W\left(\mathcal{S}^t \setminus e\right) = 0$, following $\Delta q_{e^*}^t > \Delta q_e^t$ for all elements in $\mathcal{S}$. Finally, If edge e^* isolates a node, $\Delta q_e^t \geq 0$. Considering this, the attack reward for the stage t can be described as $g(\delta^t) = \Delta q_e^t$ and fills the following condition

$$g(\delta_{e^*}^t) \geq g(\delta_e^t) \quad \text{for all} \quad e^* \in \mathcal{S}, e \notin \mathcal{S}. \tag{6.10}$$

Thus, the reward is zero if q^t is not affected or increased by the attack, and higher than zero if the attack produces an effect on the flow bottleneck.The best targets are the elements in the MCS. We consider the network as an indifferent agent subject to unpredictable (in most of the cases) intrinsic technological factors governing whether a cascading failure occurs, i.e. routing policy, network structure, physical properties or hidden failures, etc. In this way, the network does not receive any reward for its actions, thus network actions could be better considered as states. In addition, attacker reward depends only on the rational selection of the strategy with the best outcome. Time preference is modeled by assuming that future rewards are discounted at some rate $\beta \in (0, 1]$. Then, the attacker interaction with the network is a repeated attack in which a one-stage target is selected at each time for a duration of t^* stages. The long-term attack reward is described by $\mathcal{U}(\Delta) = \sum\limits_{t=0}^{t^*} \beta^t g(\delta^t)$. In this way, the attacker should observe and form an estimate of the possible lost load λ^t and cascade effects and maximize its benefit at every attack stage $\delta^t \in \operatorname{argmax} \mathcal{U}(\Delta) = \operatorname{argmin} \|\Delta\|^0$. At every stage, the attacker has $\mathcal{E}$ as the set of targets and $m = |\mathcal{E}|$ as the number of targets. The reward of an attack against target j depends on its influence on the flow bottleneck. Consider the flow bottleneck q^t defined in (6.8), measuring the flow bottleneck in the network, where $\mathcal{S}^t \subseteq \mathcal{S}$. Inequality (6.10) relates the flow bottleneck dependency on the capacity of the MCS. As a result, target selection strategy is dominated by the selection of MCS elements. Therefore, the target attacked at every stage corresponds to an MCS capacity reduction by one edge elimination at every step.

The Sequential Attacks Problem

Let $\mathcal{G}$ be a power network, $\mathbf{p}$ a vector of power supply/demand, and Ξ a routing policy. The network attack $\mathcal{A}\left(\mathcal{G}, \mathbf{p}, \Xi\right)$ is defined as a disturbance sequence Δ with minimum cardinality producing

network cascading collapse, i.e.,

$$\begin{aligned} \mathcal{A}\left(\mathcal{G}, \mathbf{p}, \Xi\right) := & \min_{\Delta} \|\Delta\|^0 \\ & \text{s. t.} \quad \Delta \in \mathcal{D}, \\ & \quad Eq.(7.1) - (7.6) \end{aligned} \tag{6.11}$$

where $\mathcal{D}$ is the feasible attack set and $\|\cdot\|^0$ the L_0 norm. Without considering cascading failure effects at every stage, the feasible set cardinality is $|\mathcal{D}| = s!$, where s is the cardinality of the minimum cut-set, i.e. $s = |\mathcal{S}|$. The minimum cardinality problem is NP-Hard despite the reduction of the feasible set of solutions by means of the cascade propagation. The exact solution of the problem is out of the scope of this work, but we provide a suboptimal solution using simulation-based optimization. We design a computational algorithm to produce a pool of feasible MCS attacks $\mathcal{D}^* \subset \mathcal{D}$ and choose the attack with minimum cardinality $\mathcal{A}^*\left(\mathcal{G}, \mathbf{p}, \Xi\right) \in \mathcal{D}^*$. Following this, we can say that

$$\mathcal{A}\left(\mathcal{G}, \mathbf{p}, \Xi\right) \leq \mathcal{A}^*\left(\mathcal{G}, \mathbf{p}, \Xi\right) \tag{6.12}$$

Then, the proposed attack is an upper bound for the optimal solution of (6.11).

6.3 Experimental Setup

In this section, we define attack efficiency metrics and connectivity metrics used to evaluate the vulnerability of the networks. Besides, computational algorithms are developed to apply the vulnerability assessment methodology.

6.3.1 Performance Indices and Measures

First, we measure the attack impact using the residual load $\lambda_{res}^t = 1 - \frac{\lambda^t}{\lambda_{init}}$ where λ_{init} is the initial demand profile and the lost load λ^t. Residual load measures the demand in the giant component relative to the initial load. Also consider the cumulative fraction of edges attacked $\rho^t = t/m$ where one single edge is attacked at a time. Second, a set of measures based on (Requião da Cunha, González-Avella, & Gonçalves, 2015) is used to compare the performance and attack efficiency on different networks. The attack efficiency $\pi^t = \lambda_{res}^{t,null}/\lambda_{res}^t$ is measured in terms of the residual load by comparing it with the residual load $\lambda_{res}^{t,null}$ resulting from a reference attack strategy. For the purpose of this paper we choose the random attack strategy as the reference strategy. The quantity increases as the attack strategy turns into a more efficient rather than reference strategy. The values $(\rho^{t^*}, \lambda_{res}^{t^*})$ represent the final state of the attack. Based on the efficiency gain, the overall final performance $\eta = \pi^{t^*} \times \left(\rho^{t^*,null}/\rho^{t^*}\right)$, compares how quick the MCS attack strategy collapses the network with respect to the reference method by comparing the cumulative fraction of attacked edges ρ^t of the proposed strategy with the same quantity for the reference strategy $\rho^{t^*,null}$. The

overall efficiency gain η will be used to benchmark the attack efficiency on several testbeds and comparing them according to their connectivity properties. To evaluate changes in connectivity and its relation with the network structure we propose the use of the following propoerties. First, we propose a connectivity density index $\nu = s/m$ measuring the relative size of the minimum edge cut-set where s is the MCS cardinality and m the cardinality of $\mathcal{E}$. This measure gives us information about the strength of connection between generator and load nodes according to a specific network topology. Besides, we propose a measure based on community detection for demand nodes grouping $\mu_d = \sum_{v \in \mathcal{V}_d} k_v^{ext} / \sum_{v \in \mathcal{V}_d} k_v$ where k_v^{ext} is the number of edges that connect node v to supply nodes and k_v is the node degree of v. Values of $\mu_d < 1/2$ imply that strong coupling exists between demand nodes connecting them lightly with supply nodes. Other traditional measures used in this study are network density $d = |\mathcal{E}| / (2|\mathcal{V}||\mathcal{V} - 1|)$, the average degree $\langle k \rangle$, and algebraic connectivity λ_2 .

6.3.2 Simulation Algorithms

We design a set of algorithms to analyse the power grid under the attacks scenario. A sequence of attacks is applied to the network until the network collapse. For each attack the damage is calculated in terms of power loss, and new post-contingency network is founded. By the end of the sequential attack the vulnerability of the network and its component is measured. A pre-contingency power flow is solved to define edge transimission capacities. Targets to attack are identified by Algorithm 6 and effects of attacks are calculated by Algorithm 5 . Network vulnerability is finally calculated by the proposed metric evaluated for the results of the attacks. The MCS-based vulnerability method works as follows:

1. Identify the elements of the MCS.
2. Removed a line target from the MCS from the undamaged network structure.
3. Compute the post failure flows and evaluate the cascading failures effect
4. Find the giant components in the damage grid
5. If network is connected and not additional cascading failures occurs evaluates continues to the next attack in step 1.
6. If network is not fully connected small islanded components with single nodes, without generator, or disbalanced are isolated.
7. Evaluate again cascading failures until the network achieves balance.
8. Compute attacks damage by quantifying the power loss.
9. Repeated 1 - 8 until network is fully collapsed.

10. Evaluate the network vulnerability using the results of the sequential attack.

The aim of the recursive simulation in Algorithm 5 is to provide the pool of attacks, generate the attacks and process the state of the system due to cascading failures. Node islanding due to cascade propagation is considered in the algorithm. The power network data received include network connections and impedances.

Algorithm 5 Attacks Algorithm

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c})$, $\mathbf{p}$, λ_{init}.
Output: $\mathcal{A}^* (\mathcal{G}, \mathbf{p}, \Xi)$, λ^t.

```
Initialize the flow network G^0 and the power flow f^0; λ^0 = 0.
Identify the target set S in (6.7).
Set the size of the attack pool |D*|.
while l ≤ |D*| do
    while (λ_init − λ^t) > 0 do
        Trigger attack δ^t
        Check for flow feasibility f in (7.2).
        if YES then
            recursively evaluate the cascading failure propagation and the network state by (7.1) - (7.6) until
            no risk exists or no feasible flow exists.
        else
            Check for node islanding or connected component separation in the network.
            if YES then
                Identify giant component Ĝ. Check for supply nodes in the giant component.
                if YES then
                    Recursively evaluate cascading failures and network state by (7.1) - (7.6) until no overload
                    exists or no feasible flow exists.
                end if
            end if
            Find and save λ^t
        end if
        t ← t + 1. Go back to trigger attack.
    end while
    Save data for the attack Δ on iteration l. l ← l + 1
end while
Get A* (G, p, Ξ) from (6.11) and (6.12).
```

The algorithm for targets identification determines the edge members of the MCS in $\mathcal{G}$ based on the minimum-cut maximum-flow equivalence. To find the minimum cut-set in a multi-source multi-sink network, the Ford-Fulkerson algorithm cannot be applied directly. Then, the algorithm is modified by introducing virtual source and virtual sink nodes, v_s^{vi} and v_d^{vi}, respectively. All the nodes in $\mathcal{V}_s$ are connected by edges with infinite capacity to v_s^{vi}. Additionally, all the nodes in $\mathcal{V}_d$ are connected by edges with infinite capacity to v_d^{vi}. By adding the new virtual nodes, the multi-source multi-sink problem flow transfers the problem between supply and demand changes

to a single-source single-sink problem between v_s^{vi} and v_d^{vi}. Subsequently, the MCS is found. A general description of the process to find the targets is described in Algorithm 6.

Algorithm 6 Algorithm for Targets Identification

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c})$.
Output: $\mathcal{S}, W(\mathcal{S})$.

```
Get the list of supply/demand node sets V_s and V_d.
Include virtual nodes for supply v_s^vi and demand v_d^vi, V ← V ∪ {v_s^vi, v_d^vi}.
for each supply node v ∈ V_s do
    Add an edge from the supply node v to v_s^vi,
end for
for each demand node v ∈ V_d do
    Add an edge from the demand node v to v_d^vi,
end for
Get S and W(S) by the use of Ford- Fulkerson algorithm between v_s^vi, v_d^vi.
```

We identify the cascading potential of each edge according to its participation in the flow bottleneck increase, which is equivalent to its participation in $\mathcal{S}$. Computation of the cascading potential of the edges takes at most $\mathcal{O}\left(|\mathcal{E}|W(\mathcal{S})\right)$. The subroutine to determine the cascade propagation has complexity $\mathcal{O}\left(\tau|\mathcal{V}|^3\right)$, where τ is the number of cascade rounds, i.e. $\tau = t^*$. Given that targets are identified previously and cascade evolution is evaluated only when a target is attacked, the total complexity is $\mathcal{O}\left(|\mathcal{E}|W(\mathcal{S}) + \log(\mathcal{E}) \cdot (\tau|\mathcal{V}|^3)\right)$. Most of the approaches from the literature point out to the problem of the minimum set of attacks (or failures), that cause a cascade with maximum damage, to be NP-Hard for modeling approaches as random failures, the minimum cardinality problem, and the set cover problem (Soltan et al., 2017; Seo, Mishra, Li, & Thai, 2015; Moussa et al., 2018). In this case, our approach reduces the running time to find a suitable set of attacks, even if complexity increases with the number of elements in the network.

6.4 Results and Discussion

This section demonstrates the results derived for the proposed attack strategy in Section 6.2.2. We validate the results using the IEEE 30-bus system and the IEEE 300-bus system as case studies. Additional test systems are also included for attack efficiency analysis, i.e., the IEEE 39-bus, IEEE 57-bus, and IEEE 89-bus (Bialek et al., 2016). A scenario of edge elimination, based on different attack strategies, is proposed as a benchmark to evaluate the results of the proposed strategy. For each strategy one edge is attacked at each step. Four benchmark attack strategies are used. First, *random* strategy where the algorithm selects the target edges randomly. After getting a pool of random attacks, it applies the best strategy. Second, the *rich* strategy selects as target edges those connecting higher degree nodes. Third, *rich-poor* strategy select as target edges those connecting higher degree nodes with lower degree nodes. Finally, the *poor* strategy selects as target edges those connecting lower degree nodes are deleted first. In addition, three different types

of betweeness are evaluated: Edge betweenees (Coelho et al., 2018), labeled as *between* which is a well established topological measure to identify the participation of the edges for the connectivity of the network; electrical betweeness (Bompard et al., 2012), labeled as *electrical b* in the results works on a combination of betweenees centrality and power transfer distribution factors; and flow betweeness (Z. Wang et al., 2017), labeled as *flow betw* which combines maximum flow and power transfer distribution factors with the network betweenness.

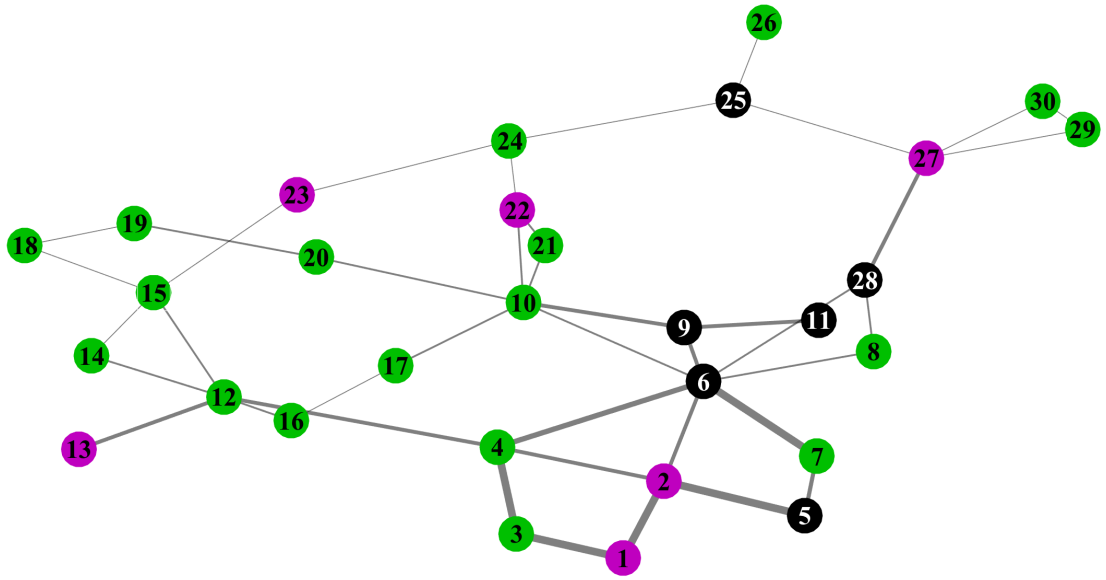
Case study - IEEE 30-bus power network

The network description of the IEEE 30-bus power system, containing 41 edges and 30 nodes is shown in Figure 6.1a. Node color is assigned according to node type: purple color represents supply nodes, $\mathcal{V}_s$; green color represents demand nodes $\mathcal{V}_d$; and black color represents neutral nodes $\mathcal{V}_b$. The initial load is $\lambda_{init} = 179.2\ p.u.$ with base power 100 MVA. By the use of Algorithm 6, the minimum edge cut-set between supply and demand nodes are calculated. Figure 6.1b illustrates the MCS. The cardinality of the minimum cut-set is $s = 15$ and its capacity is $W(\mathcal{S}) = 619\ p.u.$. Targets are sorted according to results in Algorithm 5. Once the targets list is generated, the first target attack is performed. Figure 6.2 summarizes the results of our method of attack as compared to degree-based attacks and random attacks for the IEEE 30-bus system in terms of the residual load.

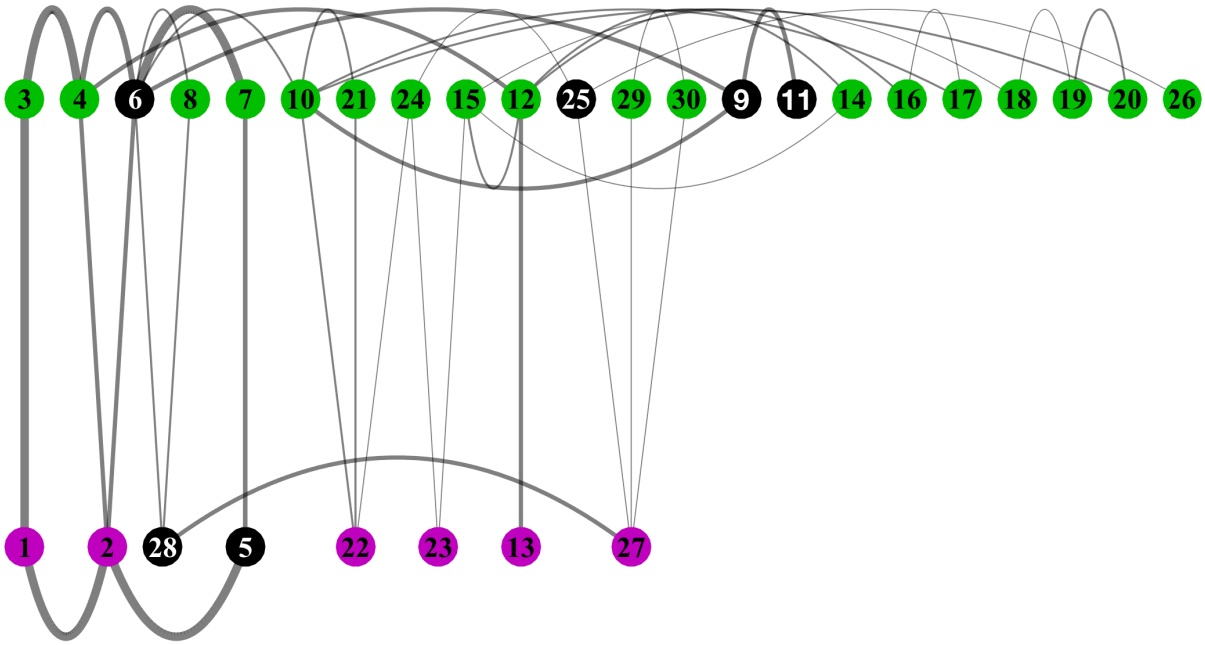
Initially, all methods behave similarly but, for the MCS strategy, as flow bottleneck q^t increases as a result of the reduction of the MCS capacity, the cascading effects of edge overload occurs. After the third attack, bigger cascades occur and the residual load λ^t_{res} is reduced. After a sequence of 4 target attacks the network had lost more than 60% of its demand. By the next attack, the network collapses and $\lambda^{t^*}_{res} = 0$. In the remaining, the final fraction of attacked edges is ρ^{t^*}. Besides, ρ^{t^*} is the lower bound of deleted edges in the network, because additional edges are disconnected by the side effects of the cascading failure process. By comparison, in the rich and poor attack strategy, deleting the same amount of edges, reduce only by 10% of the residual load. Even comparing with the second best strategy, i.e., *electric b*, deleting the same number of edges, reduces 50% the load. Furthermore, it is quite clear that the structure of this network is not simple, and cascading effects are as unpredictable as in real-world cases. The effect of the attack strategy on the cascading failure magnitude is quite critical. A sudden transition between 80% of the load to 0% occurs as an effect of two edge attacks.

Case study - IEEE 300-bus power network

This section presents the IEEE 300-bus power system. The graph representation of the network, containing in total 300 nodes and 411 edges, is shown in Figure 6.3. Initial load is $\lambda_{init} = 23525.8$ $p.u.$ with base power 100 MVA. The parameter $\alpha = 5$ is used to define the capacity of the edges. Using Algorithm 6, the minimum edge cut-set between supply and demand nodes is calculated. Edges highlighted in red represent the elements of the MCS and corresponds to the target edges. The cardinality of the minimum cut-set is $s = 126$ and its capacity is $W(\mathcal{S}) = 124036\ p.u.$. The



(a) Nework graph



(b) Layered network for minimum cut-set

Figure 6.1: a) The IEEE 30-bus power system. The transmission line capacities are represented by the edge width. b) Layered network representation. The elements of the minimum edge cut-set are the links connecting separated node sets.

network structure has regions with a higher density of demand nodes separated from areas with a high density of the supply nodes. In addition, high capacity edges can be targeted inside the

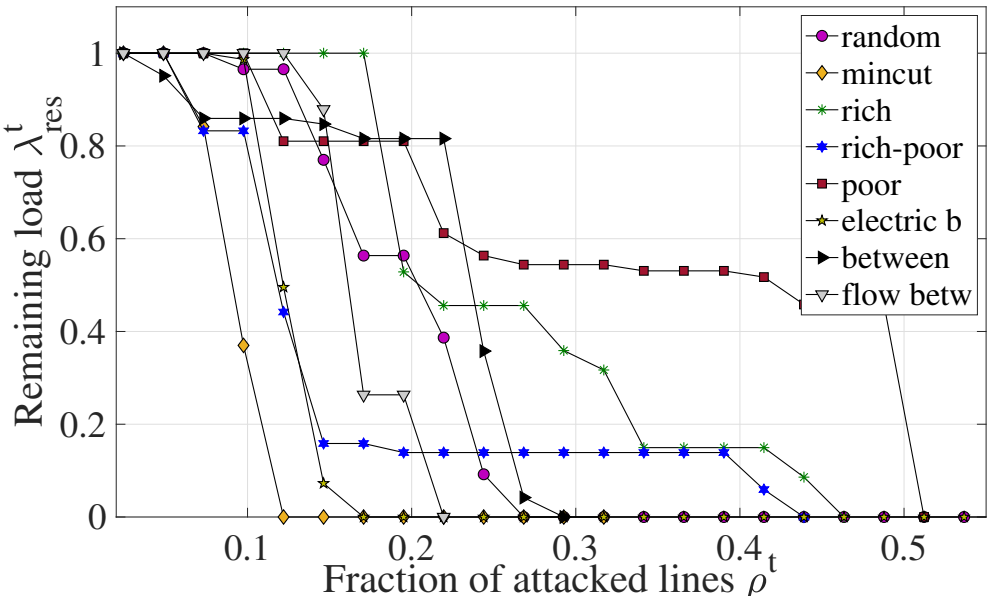


Figure 6.2: Comparison of the effect of degree-based attacks (i.e., rich, rich-poor, poor ranking), random attack, edge betweenness attack, electrical betweenness attack, flow betweenness attack, and MCS attack for the IEEE 30- buses power system.

dense supply nodes regions, disconnecting them easily from demand regions. Intermediate nodes and edges connecting areas are significantly less than interconnections between demand nodes only. The MCS strategy includes in its target, naturally, the connection corridors between highly connected areas that after few attacks affect severally the network flow transfer capacity.

The MCS capacity, according to the Ford-Fulkerson minimum cut theorem, defines a condition for flow feasibility in a network. For a power systems, the feasible power flow between supply and demand exists if it is less or equal than the magnitude of the minimum cut-set $W(\mathcal{S})$. The initial flow bottleneck for the IEEE 300-bus is $q^0 = 5.2720$. This initial flow bottleneck for the studied system is relatively high, which indeed suggests less vulnerability to flow congestion and cascade effects under given operation conditions.

As q^t is reduced, by attacking MCS edges, the flow bottleneck increases and the frontier to infeasible flows is approached. Even if, temporally, bottlenecking appears to be reduced, the general effect of sequential attack is the increasing of the overload risk for all edges in the network. Once the flow congestion is achieved in the network, most of the edges can be potential targets and produce big cascade effects. The power demand operating point establishes a value for q^0 vulnerability. Therefore, what the MCS strategy does is to increase this vulnerability by reducing q^t at every stage t, i.e. $q^t \leq q^0$. Figure 6.4 displays the results of the MCS attack performance in the system. The results indicate that the MCS strategy outperforms the random and degree-based attacks. Initially, the attack increases the flow bottleneck, but the initial performance is less efficient than the performance of degree-based attacks. λ^t_{res} remains stable until the highest flow bottleneck occurs. When it happens, the cascading failures propagate very fast and λ^t_{res} drop suddenly, several

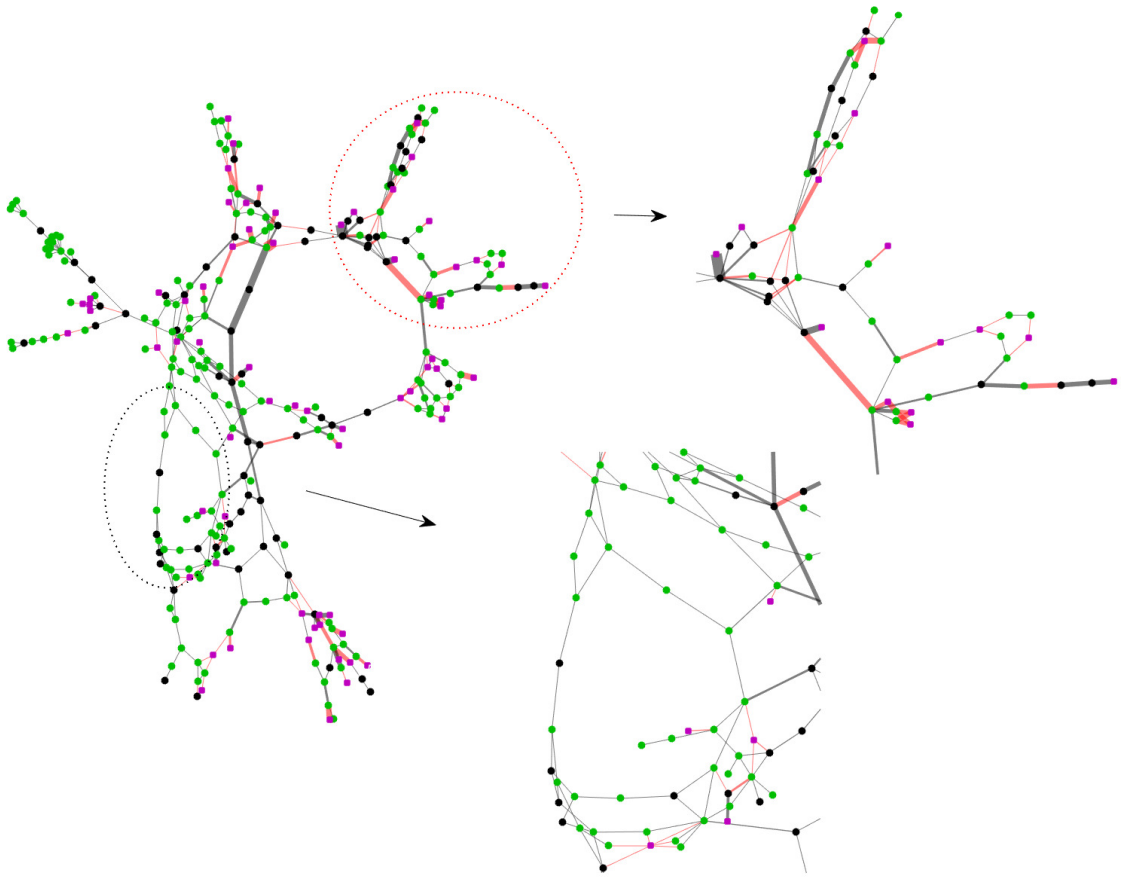


Figure 6.3: The network model of the IEEE 300- buses power system. Edge weights, i.e., transmission line capacities, are represented by the edges' width. The purple color represents supply nodes $\mathcal{V}_s$. The green color represents demand nodes $\mathcal{V}_s$. Black color represents neutral nodes $\mathcal{V}_b$. The edges highlighted in red transmit power flows to serve the entire demand. These red edges correspond to the elements of the minimal edge cut-set. Red zoom depicts the area with the higher density of target elements. Black zoom shows the area with few target elements and clustered demand.

demand nodes are disconnected. By comparison of the MCS collapse attack with rich and poor attack strategies, with the same number of attacked edges, the strategies reduce only by 50% the system load. Even comparing MCS with the second best strategy, i.e., *electric b*, by attacking the same number of edges, the results has a 20% of the lost load difference. Attacks based on edge betweenness *between* performs not quite well because they are not considering flow routing. Flow betweenness, *flow b*, is the third best attack improving the results of the pure topological measures, by considering network maximum flow. The random attack strategy reduces up to 30% of the load with the same number of attacked edges. Interaction between the MCS attack strategy and the cascading failure events in the network is quite critical. For this strategy, a sudden transition of 80% in the load lost occurs as an effect of four edge attacks in a network of more than 400 edges.

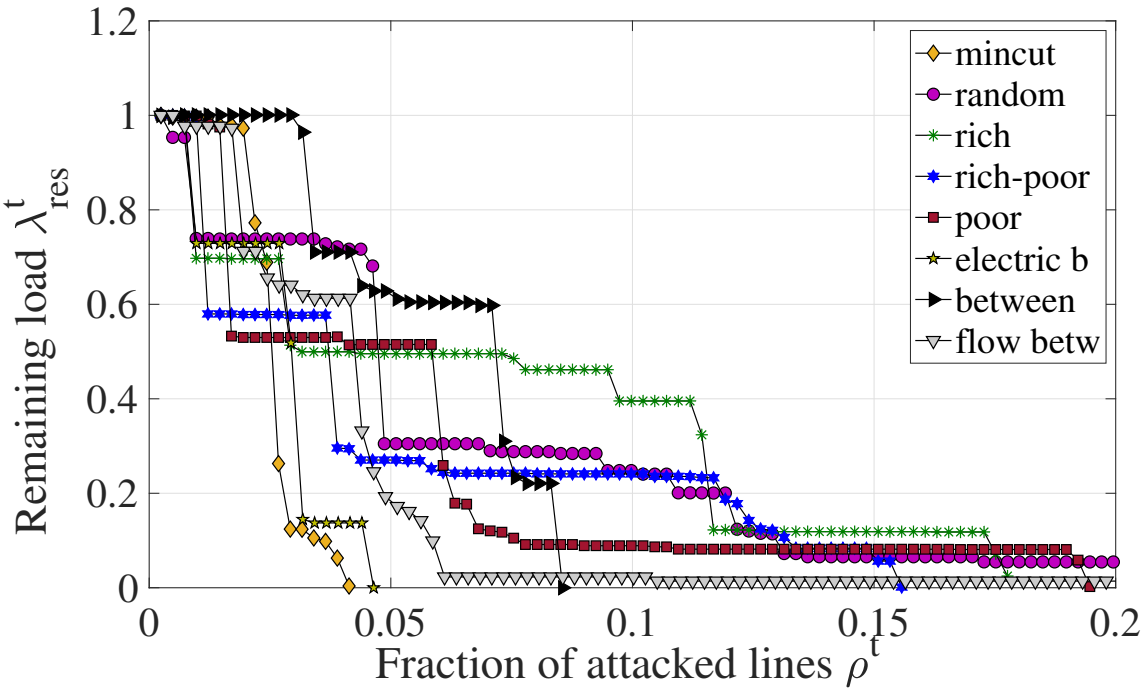


Figure 6.4: Comparison between the effect of degree-based attacks (i.e., rich, rich-poor, poor ranking), random attack, the edge-betweenness attack, the electrical betweenness attack, the flow betweenness attack, and the MCS attack for the IEEE 300- buses power system.

6.4.1 Efficiency Analysis

In this section, attack results are summarized and compared by means of the relationship between overall attack efficiency gain and the network properties of different power networks. The test systems are IEEE 30-bus, IEEE 39-bus, IEEE 57-bus, IEEE 89-bus, IEEE 300-bus networks. Figure 6.5 summarizes the results of the attacks for each network by means of the relation between π^t and ρ^t, i.e., the efficiency gains of MCS attack compared to the null strategy reference which in this case is the random strategy.

With fewer than 15% of edges attacked with the MCS strategy, the results show, more than double of efficiency for all the networks. Even in the worst case (IEEE 300) we obtain efficiency of 4 times with less than 7% edges removed. The best case is IEEE 89 with more than 15 times of gain with less than 9% of edges attacked. Also, It is possible to observe the existence of a threshold value for ρ^t where the attack strategy departs from the null strategy attack. This value corresponds to the minimum fraction of attacked edges needed to collapse a network, which is lower to what can be predicted by the other strategies. Using gain values, the overall efficiency gains η is calculated. The overall efficiency gain measures how fast the MCS attack strategy reaches the end point of collapse in the network in comparison with the reference method.

Figure 6.6 shows the overall efficiency η as a function of network connectivity properties, i.e., connectivity density ν, algebraic connectivity λ_2, network density d, and community measure for demand nodes set μ_d. The information about measures and attack performance for each system is

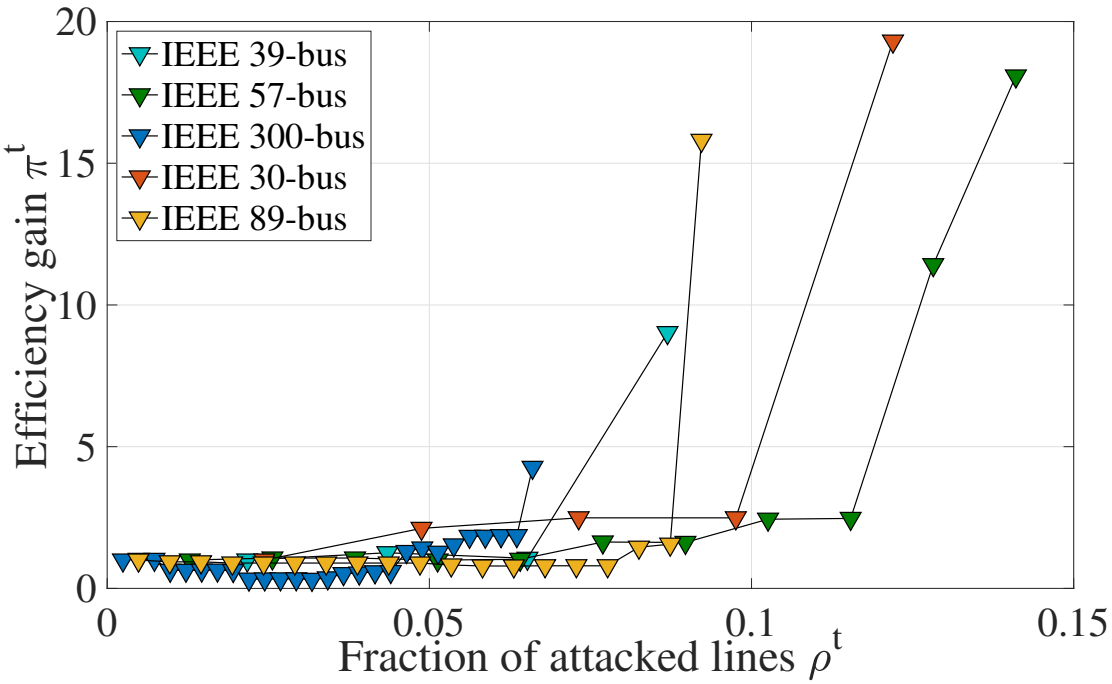


Figure 6.5: Attack strategy efficiency over different power networks.

Table 6.1: Properties and results for for the studied IEEE test cases. Number of nodes ($|\mathcal{V}|$), number of edges, ($|\mathcal{E}|$), mean degree ($\langle k \rangle$), connectivity density (υ), edge density (d), algebraic connectivity (λ_2), generator community (μ_s), load community (μ_d), fraction of attacked edges (ρ^*), and the overall efficiency gain of the MCS attack (η).

	$\|\mathcal{V}\|$	$\|\mathcal{E}\|$	$\langle k \rangle$	υ	d	λ_2	μ_d	ρ^{t^*}	η
IEEE 30	30	41	2.73	0.36	0.09	0.21	0.39	0.12	58.98
IEEE 39	39	46	2.36	0.33	0.06	0.07	0.35	0.08	20.30
IEEE 57	57	78	2.73	0.20	0.05	0.09	0.22	0.14	36.15
IEEE 89	89	206	4.62	0.17	0.05	0.15	0.19	0.09	55.74
IEEE 300	300	409	2.72	0.45	0.01	0.01	0.63	0.06	7.43

summarized in the Table 6.1.

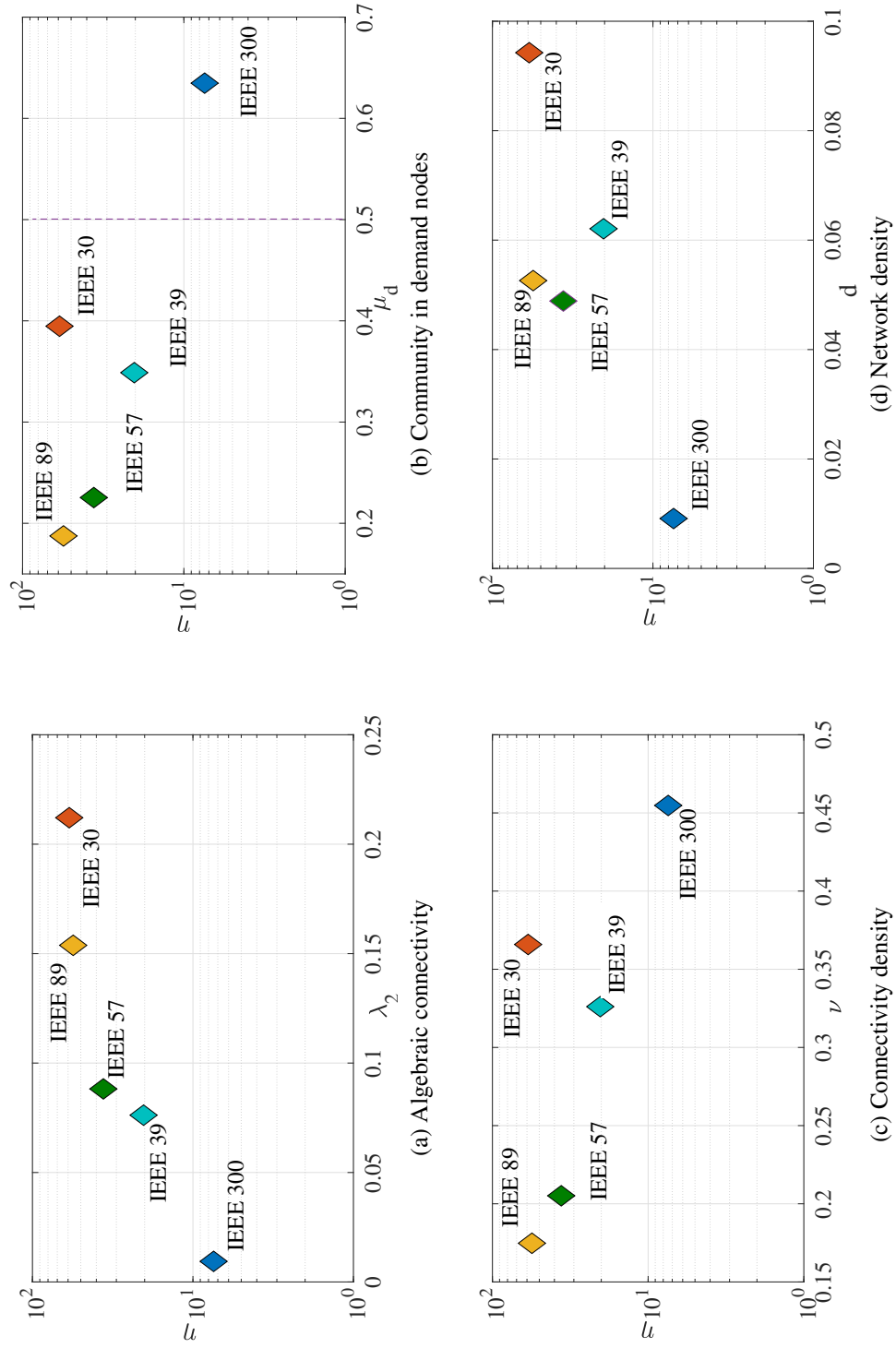
For all the networks, the strategy presents an increase in efficiency. The most vulnerable network to attacks, in general, is the IEEE 300-bus system because it requires the minimum fraction of deleted edges to collapse. This could also be related to the fact that there are kind of power system areas; the lines among areas can be subjected to more constraining power exchanges, then in case of loosing those connecting lines the demand-generation balance is correspondingly compromised. Also, the lower efficiency of the strategy could represent a high vulnerability of the network to any attack strategy. On the other side, the effectiveness of the attack strategy for the other systems is notable.

Figure 6.6a shows a direct relation between algebraic connectivity and the increase in attack efficiency. Networks are actually less robust to this type of combined attacks as the algebraic connectivity increase. Power network effective resistence can be measured in terms of algebraic connectivity. Effective resistence makes reference to how easy is to transmit power between two points in the network. Networks designed to reduce the transmission paths could produce a detriment of network robustness. Also, in terms of real applications planning to increase flow transmission efficiency by adding new lines (higher algebraic connectivity) could result in a more vulnerable network through the emergency of the Braesss paradox (X. Wang, Ko, Kooij, & Mieghem, 2015), (Cetinay, Kuipers, & Mieghem, 2018). Figure 6.6b shows the measure μ_d of the demand nodes community. Values of $\mu_d > 0.5$ represent the existence of a demand node cluster. This means that demand nodes, are more interconnected between them than with supply nodes, implying that few nodes and edges need to be targeted for attack, producing higher impact for the demand nodes isolation. The proposed attack strategy is less efficient in networks where supply and demand nodes are highly connected. The connectivity density ν in Figure 6.6c shows a similar behaviour to μ_d. Networks with a higher number of connections between supply and demand nodes, will be more robust against the proposed attack strategy. IEEE 30-bus system is out of the profile. It could be related to their higher algebraic connectivity. Lower values of network density d, seem to have an inverse impact with the attacks.

Network density for all studied networks in Figure 6.6d is lower that $d = 0.1$. This lower level of density implies that all networks are sparse and have fewer connections than all the possible number of connections between nodes in the network. According to these results, it is evident that is not network density, or network efficiency (i.e., algebraic connectivity) what brings more robustness to a power network considering flows. Instead, a low attack impact appears to be related to distributed placement of supply, closer to points of demand, independency between demand nodes and lower values of algebraic connectivity, implying a trade-off between efficiency and resilience of the grid. Resiliency of future power networks should be improved at future by the increase of the degree at which the system can absorb the impact of system disturbances and using the minimum of the effort to reduce consequences (Francis & Bekera, 2014). In this way, considering the influence that connectivity density and clustering between load or generation can produce to the vulnerability of the network can be a first stage for planning networks where its absorptive capacity is improved. Besides, these hybrid network-electric properties could be included in the design of advanced algorithms for predictive models of failures, resource optimization and placement, stochastic planning and operation, and distributed smart coordination of switches and reclosers.

6.5 Conclusions

In this chapter, we have presented a minimum cut-set-based attack method which consists of attacking the edge cut-set with minimum capacity connecting supply and demand nodes of a given power network, then deleting sequentially the edges in this set to get the smallest attack with higher



(a) Algebraic connectivity

(b) Community in demand nodes

(c) Connectivity density

(d) Network density

Figure 6.6: The impact of network properties on the attack efficiency.

impact. Computational simulations of different power networks showed that the MCS method is more efficient in collapsing the network than traditional procedures based on degree centrality. Therefore, one may notice that most connected nodes and their edges are not necessarily the most important for the cascading failure effect and survival. The edges from the minimum cut-set connecting supply nodes to demand node set are more important and crucial for the power flow transfer capacity than structurally highly connected components. If we attack these edges (or their corresponding nodes on the demand nodes set), the produced damage by cascade effects to the network is greater than using traditional or random methods by eliminating the same number of edges.

The objective of using the proposed MCS attack strategy in the power network is to unveil its structural vulnerability. Measuring this, we can attain the regime where large cascading failure effects and consequent loss of load are presented. Hence we can propose to characterize the vulnerability of the power network by how small a sequence of attacks should be to achieve the network collapse. In other words, how fast the end point of the attack ρ^{t^*} is achieved. As a result, it is shown that the efficiency of the attack increases when the connection between demand-node is denser than the connection to the supply-nodes and the cardinality of the minimum cut-set is low. Besides, the MCS attack efficacy increases with the algebraic connectivity of the network; the higher the network efficiency, the more fragile the network is. In the following chapters, connectivity properties depicted in this work will be used to improve the power network resiliency against cascading collapse by considering them on the design of controlled reinforcement strategies.

Chapter 7

Markov Decision Process based Cascading Failures Attacks

"The inability to predict outliers implies the inability to predict the course of history (Taleb, 2007)."

Nassim Nicholas Taleb
The Black Swan: The Impact of the Highly Improbable

The first stage of the attack is information foraging about system structure an operation. This result in imminent danger if the attacker uses this information to define its targets. Consider an informed attacker who gets information about network topology and network security operation limits. Following previous results, this chapter gives a more general analytical approach to the study of vulnerability in power networks. This chapter aims to integrate network theory and discounted reward Markov decision process in the model of cascading failures attacks. A control strategy is designed to maximize the attack long-term expected reward while reducing attack sequence duration. Attack model identifies the most suitable targets by predicting using a Markov process for predicting the propagation and consequences of the failure. The immediate reward is the expected loss of load due to cascade effects. We estimate the state transition probabilities utilizing a hidden failure model embedded in an Independent edge-dependent network evolution model. Value iteration algorithms are used for identifying targets at every attack stage. Target selection is updated depending on network changes. The results provide an optimal attack strategy with maximum damage considering congestion as a cascade propagation mechanism.

7.1 System Model

The analysis in this chapter is based on the network and the cascading mechanism proposed in Section 6.1. Using this model, we can estimate the risk of cascade during attacks, and long term damage produced by the actions. Please refer to this section to considering model and nomenclature. The following sections present the attacker model, cascading failure risk and damage

estimation and criteria to evaluate expected long-term damage.

7.1.1 Network-based Characteristics

The power system is modeled as a finite undirected weighted flow graph $\mathcal{G}$ such that

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c}), \tag{7.1}$$

where the node set $\mathcal{V}$ and the edge set $\mathcal{E}$, with cardinality $|\mathcal{V}| = n$ and $|\mathcal{E}| = m$, represent buses and transmission lines, respectively. In addition, $\mathbf{c}^t \in \mathbb{R}^m$ is a vector with link flow transmission capacities. In this model, we equate capacities with edge weights. Parallel circuits between buses are represented by a single edge with the sum of their respective capacities.

7.1.2 System-based Characteristics

For the power network in (7.1), let $\mathcal{V}_s \subset \mathcal{V}$ be the set of supply nodes and let $\mathcal{V}_d \subset \mathcal{V} \setminus \mathcal{V}_s$ be the set of demand nodes in the network. Transmission nodes without supply or demand are $\mathcal{V}_b \subset \mathcal{V}$. Consider a node associated with supply/demand vector $\mathbf{p}$ where $\mathbf{p} \in \mathbb{R}^n$; $p_v > 0$ for $v \in \mathcal{V}_s$, $p_v < 0$ for $v \in \mathcal{V}_d$, and $p_v = 0$ for $v \in \mathcal{V}_b$ and $\sum_{v \in \mathcal{V}} p_v = 0$. Consider a flow vector at time t, $\mathbf{f}^t \in \mathbb{R}^m$ where f_e^t is the flow at edge e and satisfies capacity constrain $|f_e^t| < c_e^t$ on every link $e \in \mathcal{E}$ and flow conservation $\sum_{e \in \mathcal{E}_v^t} f_e^t = p_v$ for every node v where $\mathcal{E}_v^t \subseteq \mathcal{E}$ is the set of all incident edges to the node v. The vector flow $\mathbf{f}^t$ is defined by a routing policy $\mathbf{\Xi}^t$. The routing policy defines the magnitude and direction of every edge flow in the network. In this study, we consider a linear routing policy such that

$$\mathbf{f}^t = \mathbf{\Xi}^t \mathbf{p}, \tag{7.2}$$

where $\mathbf{\Xi}^t$ is an $m \times n$. The matrix $\mathbf{\Xi}^t$ maps the supply/demand profile $\mathbf{p}$ onto the power flows going through each edge. The flow routing will depend on the electric and topological properties of the power system. In this study, we use a routing policy based on the DC power flow.

To derive $\mathbf{\Xi}^t$, following (Cetinay, Kuipers, & Mieghem, 2018), consider the DC power flow equations of the power network in terms of the network adjacency matrix $\mathbf{A}$,

$$p_v = \sum_{i=1}^{n} = a_{vi} b_{vi} (\theta_v - \theta_i) = \theta_v \sum_{i=1}^{n} a_{vi} b_{vi} - \sum_{i=1}^{n} a_{vi} b_{vi} \theta_i. \tag{7.3}$$

The terms θ_v and θ_i are the voltage phase angles at bus v and i. b_{ik} is the reciprocal of the transmission line reactance between buses. Then, consider an auxiliary adjacency weighted matrix $\mathbf{H}$, where $h_{vi} = a_{vi} b_{vi}$ is an edge weight associated with the impedance. Then, the corresponding matrix representation of the DC power flow equation in the power network is

$\mathbf{p} = \left\{ \mathbf{diag}\left(\sum_{i=1}^{n} h_{vi} \right) - \mathbf{H} \right\} \mathbf{\Theta} = (\mathbf{D} - \mathbf{H})\, \mathbf{\Theta}$, where $\mathbf{D}$ is a weighted degree diagonal matrix. Introducing the weighted laplacian matrix $\tilde{\mathbf{Q}} = \mathbf{D} - \mathbf{H}$, the equation can be described as $\mathbf{p} = \tilde{\mathbf{Q}}\mathbf{\Theta}$. Calculating a pseudoinverse $\tilde{\mathbf{Q}}^{+}$ of the weighted laplacian it is possible to describe voltage angles of $\mathbf{\Theta}$ as a function of $\mathbf{p}^t$ as $\mathbf{\Theta} = \tilde{\mathbf{Q}}^{+}\mathbf{p}$. The flow f_e at the edge e between node v and node i can be determined as $f_e = b_{vi}\,(\theta_v - \theta_i)$, with its related matrix representation $f^t = \tilde{\mathbf{B}}^{\top}\mathbf{\Theta}$. The term $\tilde{\mathbf{B}}$ is the weighted incidence matrix with $\tilde{b}_{ve} = h_{vi}$ if edge flow f_e goes from v to i, or $\tilde{b}_{ve} = -h_{vi}$ if edge flow f_e goes from i to v and zero otherwise. Then, replacing $\mathbf{\Theta}$ by the matrix equation as a function of the pseudoinverse, we get $\mathbf{f}^t = \tilde{\mathbf{B}}^{\top}\tilde{\mathbf{Q}}^{+}$. As a result the routing policy matrix is $\mathbf{\Xi}^t = \tilde{\mathbf{B}}^{\top}\tilde{\mathbf{Q}}^{+}$ with the element $\xi_{ij}^t = \tilde{b}_{ei}\tilde{q}_{vi}^{+}$.

7.1.3 Network Evolution and Cascading Failures

The network dynamics presented here follows the nomenclature and the model presented in (Savla et al., 2014). Consider the power system modeled as a flow network in (7.1) with supply/demand vector $\mathbf{p}$ and flows in (7.2) evolving in time. Let $\mathcal{G}^t = (\mathcal{V}^t, \mathcal{E}^t, \mathbf{c}^t)$ and $\mathbf{f}^t$ describe the state of the system at every time $t = 0, 1, \ldots$, where $\mathcal{V}^t \subseteq \mathcal{V}$ and $\mathcal{E}^t \subseteq \mathcal{E}$ are the active nodes and links at time t.

For the initial condition of the system $(\mathcal{G}^0, \mathbf{f}^0)$, all the elements of the node and edge set start active, i.e. $\mathcal{V}^0 = \mathcal{V}$, $\mathcal{E}^0 = \mathcal{E}$, and $\mathbf{f}^0$ is the initial flow. At every time t, network $\mathcal{G}^t$ should be connected. Define $\hat{\mathcal{G}}^t$ as the largest connected component in $\mathcal{G}^t$ and $\hat{\mathcal{G}}^0 \equiv \mathcal{G}^0$. The largest connected component of the network refers to the biggest connected part of the entire nodes set where a feasible flow exist. Considering the largest connected component, we are modeling the network in its natural dynamical behavior. Edge disconnection produced by cascade propagation may generate uncontrolled component islanding. Uncontrolled islanding or redispatch is considered during the cascade propagation. In this way, the small connected components could have only load nodes or unbalanced supply-demand nodes that collapse during the cascade evolution. Attack-defender threat models could include controlled actions, but defender actions are out of the scope of this model. The network changes its state as follows. Edges become overloaded when its current flow exceeds the transmission capacity. All the overloaded edges are disconnected along with all the edges in small subcomponents isolated from the largest connected component $\hat{\mathcal{G}}^t$. Accordingly,

$$\mathcal{E}^{t+1} = \mathcal{E}^t \setminus \left\{ e \in \mathcal{E} : f_e^t \geq c_e \right\} \cup \left\{ e \in \mathcal{E}_v^t : v \notin \hat{\mathcal{V}}^t \right\}. \tag{7.4}$$

Next, all active nodes v that have no incident edges, along with all those not included in the large connected component become inactive, i.e.

$$\mathcal{V}^{t+1} = \mathcal{V}^t \setminus \left\{ v \in \mathcal{V}^t : \mathcal{E}_v^t = \emptyset \right\} \cup \left\{ v \notin \hat{\mathcal{V}}^t \right\}. \tag{7.5}$$

Nodes and edges disconnection is irreversible. For each $e \in \mathcal{E}$, the routing policy in (7.2) determines its current flow. In addition, the capacity vector $\mathbf{c}^t$ is changed by a disturbance $\delta^t \in \mathbb{R}^m$,

$$c_e^{t+1} = c_e^t - \delta_e^t, \qquad e \in \mathcal{E}^t. \tag{7.6}$$

Disturbance δ is defined according to the attack strategy (e.g. single line attack or multiple line attacks) as will be described in Section 6.2.2. The initial equilibrium flows $\mathbf{f}^0$ are generated by the given routing policy. The network state does not change as long as $\delta^t = 0$. The initial line transmission capacity $\mathbf{c}^0$ is defined by $\mathbf{c}^0 = \alpha \mathbf{f}^0$, where α is a tolerance parameter and $\alpha \geq 1$.

Modelling the power network and its evolution during failures as a dynamic flow network gives us the advantage to study the influence of the network structure and its interdependency on the physical properties of the power flow. Connectivity analysis can be considered in terms not only of structure but also of flow dynamics at the same time.

7.1.4 Attacker Model

The model assumes a single intruder threatening the network. The attack is repeated in time; for every stage the attacker has to choose an action a^t. Considers the sequence $\Delta =: (a^1, a^2, ...)$ of progressive disturbances representing the external adversary intervention against the power network. At each stage, the disturbance a^t is modeled by $a^t = \Gamma^t \mathbf{c}^t$ where Γ^t is an $m \times m$ matrix and $\Gamma^t = \mathrm{diag}\,(\gamma_1, \gamma_2, ..., \gamma_m)$. Disturbance a^t is applied in (7.6) simulating the lost of line transmission capacity or a severe transmission damage by defining the element γ_e^t as follows

$$\gamma_e^t = \begin{cases} 1, & \text{if edge e is attacked;} \\ 0, & \text{otherwise} \end{cases} \tag{7.7}$$

Denote by $\mathcal{D}$ the set of all feasible attack sequences possible in the network.

7.1.5 Risk Estimation

A standard model of failures estimation due to network congestion is the hidden failures model. We denote $\omega(e)$ as the probability that a functioning edge fails due to congestion mechanism (see Chapter 4).

Each edge in the network has a failure probability function that is modeled as an increasing function of the power flow on edge e,

$$\omega(e) = \begin{cases} 1, & \text{for } f_e^t \geq \alpha f_e^0 \\ \frac{1}{f_e^0(\alpha-1)} f_e^t & \text{for } f_e^0 \leq f_e^t \leq \alpha f_e^0 \\ 0, & \text{otherwise} \end{cases} \tag{7.8}$$

The probability is low initially, well below the line security limit and increases linearly to one when the line flow is α times of the security limit, as shown in Figure 7.1.

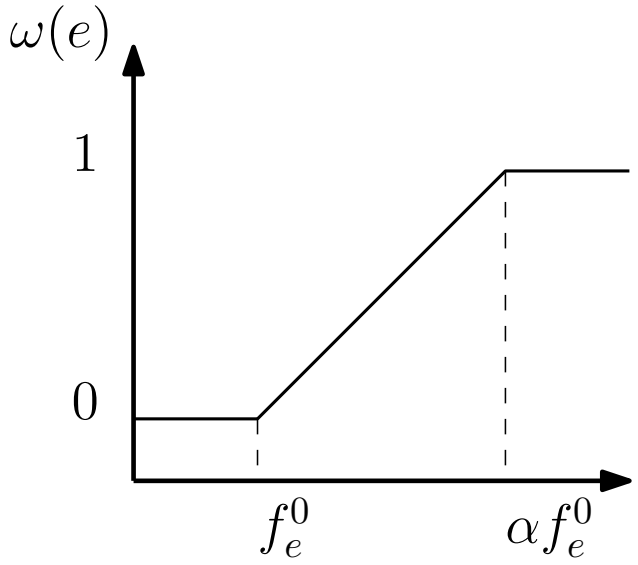


Figure 7.1: Probability distribution of an edge tripping by a cascading failure propagation effect

Probability $\omega(e)$ defines the chance to get a failure in the edge but does not consider the probability of failure related to previous exogenous failures or attacks events. In order to estimate the risk of edge lost triggered by neighboring edges contingency during attacks, an Independent edge-dependent network evolution model is proposed. Assume that the failure of each individual edge is governed by a random process that is independent of all other edges, i.e. $Pr(e_1 \cap e_j) = Pr(e_i)Pr(e_j) = \omega(e_i)\omega(e_j)$. Let $\omega(e)$ denote the probability that any edge , e, that is part of the network at time t will be removed over the next time step by means of cascade propagation. For any pair $\hat{\mathcal{G}}, \hat{\mathcal{G}}' \in S_n$, let $P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}})$ denote the probability that $\hat{\mathcal{G}}_{j+1} = \hat{\mathcal{G}}'$ given that $\hat{\mathcal{G}}_j = \hat{\mathcal{G}}$, and let $\mathcal{E}$ denote the set of edges belonging to $\hat{\mathcal{G}}$. Then the "independent edge-dependent" model yields the graph-to-graph transition probability

$$P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}}) = \prod_{e \notin \mathcal{E}', e \in \mathcal{E}} \omega(e) \prod_{e \in \mathcal{E}', e \in \mathcal{E}} (1 - \omega(e)). \tag{7.9}$$

In the beginning, all the network edges are active, and there are no failures produced by the attacker. Then, when the attacker choose a line to attack a_1^*, the power network probability to move to another state where edge a_1^* and other edges e are down is $P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}})$, the probability that network moves from its initial topology $\hat{\mathcal{G}}$, where $\{a_1^*, e\} \in \mathcal{E}$ to a new topology $\hat{\mathcal{G}}'$ where $\{a_1^*, e\} \notin \bar{\mathcal{E}}'$. Figure 7.2 presents how the transition probability between same states will be different depending on the action taken by the attacker at stage s and the power flow routed through each edge, network topology, and trigger event. Probability changes depending on the action taken by the attacker.

It is also defined $S(a^*, \hat{\mathcal{G}})$ as a measure of severity of the failures proceeding from an arbitrary attack a^* to the network at a particular state $\hat{\mathcal{G}}$. Then the risk of the cascading failure due to attack

a^* is

$$R(a^*, \bar{\mathcal{G}}) = P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}}) S(a^*, \bar{\mathcal{G}}) \tag{7.10}$$

Considers Υ as the set of all possible targets to attack, then the cascading failure network risk under a defined target attack is

$$R(\bar{\mathcal{G}}) = \sum_{\forall a \in \Upsilon} R(a, \bar{\mathcal{G}}) = \sum_{\forall a \in \Upsilon} P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}}) S(a^*, \hat{\mathcal{G}}) \tag{7.11}$$

Therefore, $S(a^*, \hat{\mathcal{G}})$ is a variable that maps an event a^* to its severity and interpret $R(\hat{\mathcal{G}})$ as the expected value of $S(a^*, \hat{\mathcal{G}})$, i.e. $E[S(a^*, \hat{\mathcal{G}})]$.

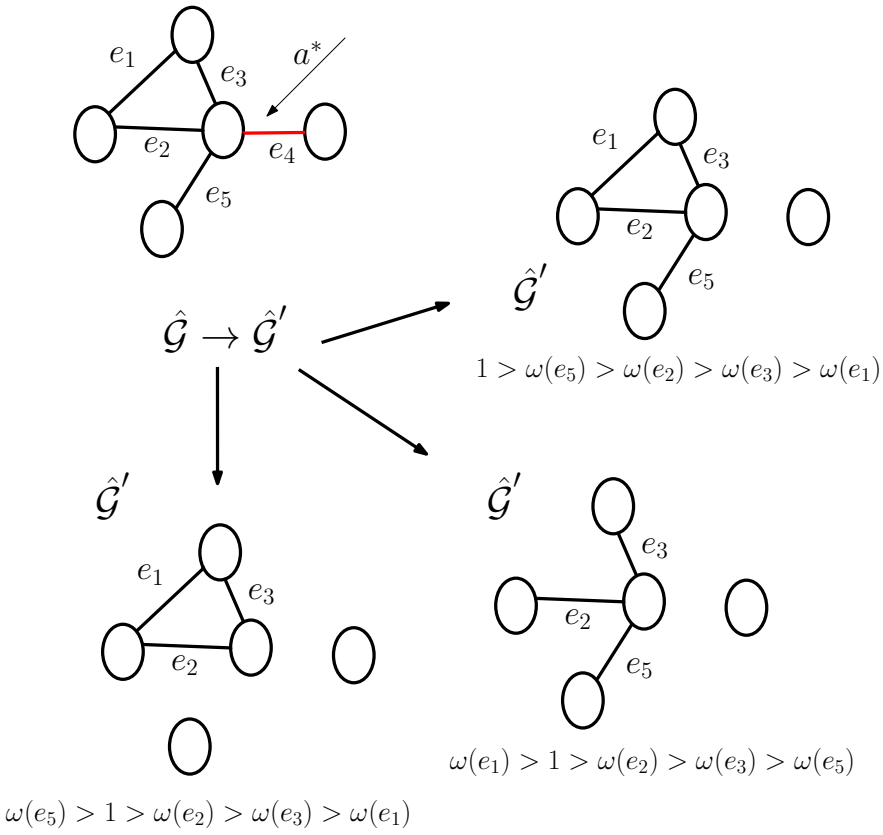


Figure 7.2: Changes in network topology due to different targets for the attacks. Depending on the selected target network will evolve to a new state with an independent probability related to the hidden failures model in

7.1.6 Severity of the Attack

The severity of the attack for the selection of a target a^* at each stage of the attack defined by $S(a^*, \bar{\mathcal{G}})$ is measured considering two parameters: power loss and flow bottleneck. The power lost is used to define the severity of the attack against a^* as

$$S(a^*, \hat{\mathcal{G}}) = \lambda^t = \sum_{v \in \mathcal{I}^s \cap \mathcal{V}_\Gamma} \tag{7.12}$$

where $\mathcal{I}^t$ is the isolated node set resulting from the cascading failures at stage t. On the other side, flow bottleneck (see Section 6.2.1 and 6.2.2) can be used also to measure the severity of an attack by indicating the increase in network congestion due to the target attack against a^*. The severity of the attaks in terms of floww bottleneck is defined as follows

$$S(a^*, \hat{\mathcal{G}}) = \Delta q_e^t = q^t - q_e \tag{7.13}$$

where q_e represents the change in the bottleneck when edge e is attacked and q^t its pre-contingency state.

7.2 Problem Formulation

Following the results shown in Section 6.2.2, we study a strategy that can trigger blackouts with a minimum of sequential attacks. This strategy is accomplished by increasing the estimated risk of network cascading failures. For a given set of attacks actions, a defined supply/demand, network topology, and flow routing strategy over an infinite horizon, the optimal attack sequence that maximizes the damage triggered by the attack with the minimum number of attacks is given by the following optimization problem

$$\begin{aligned} &\max_{a^1,\ldots,a^t} \sum_{t=0}^{\infty} \beta^t E[S(a^*, \hat{\mathcal{G}})] \\ &\text{s. t.} \quad \text{risk estimation } (7.11) \\ &a^t \in \mathcal{E}^t, \end{aligned} \tag{7.14}$$

for $0 < \beta < 1$ being a rate of discount on the risk (Filar & Vrieze, 1996). Risk is higher if attacks damage the networks strongly during the firsts attacks. Maximizing the risk estimation metric implies that target will be selected to increase damage, and produce it fast by minimizing the number of attacks required to achieve maximum damage propagate failures through the network easily. It also implies that maximize the cascading failure risk at each stage minimize the number of required attacks, because of the cumulative sum in the objective function and the proposed rate

of discount. Relevance of (7.14) to evaluate power grid vulnerability had been studied in Chapter 6.4. The impact of an attack that can damage the network and cause a blackout is shown in Figure 6.4. Different target sets are selected and evaluated based on network properties. The severity of the attack depends not only in his duration but also in the risk of producing cascading failures at each stage. As is evident in the previous results, if the attacker manages to increase the cascading failure risk as soon as is possible by using a carefully constructed attack sequence, he can cause, very fast, significant damage in the network. Intuitively, to cause a significant impact, the attack magnitude and damage should be optimized at the same time. Thus the solution of the optimization problem in (7.14) must strick a balance between attack magnitude and damage. In the following section, we solve the optimization problem (7.14) using a Markov Decision Process (MDP) based approach.

7.3 Markov Desicion Process Solution to Multistage Attack

In this section, the optimization problem in (7.14) is cast in an MDP problem and solve it using value iteration.

7.3.1 Markov Decision Process Model

A state s in the MDP corresponds to the network configuration $\hat{\mathcal{G}}^{'}$ and the actions correspond to the attackers target selection a. The set of all the possible actions that the attacker can take at state s is denoted by $A(s)$. The approach is to map the independent - edge-dependent network dynamics modeled by (7.9) to the state transition probabilities, the risk estimation in (7.12) or (7.13)to the MDP immediate reward, and the objective function of (7.14) to the MDP's long term expected reward. Formally the MDP is defined by a tuple $(\mathbf{S}, A, q, R)$ where $\mathbf{S}$ is the set of all possible states, A is the action space of the attacker; $q(s, s^{'}, a)$ is the probability of transiting from state s to state $s^{'}$ under an action $a \in A$ of the attacker; $R(s, s^{'}, a)$ is the immediate expected reward for the attacker when it takes an action $a \in A$ in state $s \in \mathbf{S}$.

MDP state transitions probabilities: We adopt the following approach. Considers an initial state s^0 corresponding to the initial network configuration before attack $\hat{\mathcal{G}}$. States $s^1, ..., s^e, ..., s^m$, where m is the cardinality of $\mathcal{E}$ at time t, correspond to network configurations $\hat{\mathcal{G}}^{'}$ where is asumed to be inactive $e \notin \mathcal{E}$. Then, the state transition probability $q(s, s^{'}, a)$, with $s = s^0$ and $s^{'} = s^e$, is

$$q(s, s^{'}, a) = q(s, s^e, a) = P(\hat{\mathcal{G}}^{'} \mid \hat{\mathcal{G}}) \text{ where} \{e, a\} \notin \hat{\mathcal{E}}^{'} \quad \forall a \in A(s), e \in \mathcal{E}(s). \tag{7.15}$$

The probability of failure for each edge in (7.8) should will depend on the state s and attacker action a, i.e., $\omega(e, s, a)$.

MDP immediate reward: Now, the damage model (either (7.12) or (7.13)) is mapped to the MDP immediate reward function. Accordingly the immediate expected reward of the MDP is

given by $r(s, s^{'}, a) = S(a, \hat{\mathcal{G}})$.

Discounted reward state value function and MDP policy: The solution of the MDP corresponds to a policy π, which is mapping from a state to action. Let $\{R_t\}_{t=0}^{\infty}$ the sequence of random rewards of the attacker, with R_t being the reward of the stage t of the attack. The expectation of R_t is also denoted by $\mathbb{E}_{s\pi}[R_t] := \mathbb{E}_{\pi}[R_t|S_0 = s]$ The overall discounted value of the strategy $\pi = (\pi(1), ..., \pi(s), ..., \pi(N))$ selected by the attacker form the initial state s will be defined by

$$V_{\beta}(s, \pi) := \sum_{t=0}^{\infty} \beta^t \mathbb{E}_{s\pi}\left[R_t\right] \tag{7.16}$$

where β is the discounted factor.

To evaluate the long-term expected reward, the attacker has an immediate expected reward $R(\pi) = (R(1, \pi), R(2, \pi), \ldots, r(N, \pi))^T$ where for each $s \in S$ $r(s, \pi) := \sum_{a \in A(s)} r(s, a)\pi(s, a)$. Considers also the $t-$step transition probability between states as

$$Q^t(\pi) = \left(q_t(s, s^{'}, \pi)\right)_{s,s^{'}=1}^{N} \tag{7.17}$$

Then the value of the strategy f is finaly defined as

$$\mathbf{V}_{\beta}(\pi) = \sum_{t=0}^{\infty} \beta^t Q^t(\pi) r(\pi) \tag{7.18}$$

The previous equation captures the fact that reward output of 1 unit at time $t + 1$is worth only by $\beta < 1$ of what it was worth at time t. Then $\pi(s, a)$ will be the probability that the attacker choose action $a \in A(s)$ in state $s \in S$ whenever s is visited. In this case the strategy will be pure, i.e., $\pi(s, a) \in \{0, 1\}$ for all $a \in A(s), s \in S$.

Optimal policy: The optimal policy maximize the total expected reward, $\pi^* = \text{argmax}_{\pi}\, \mathbf{V}_{\beta}(\pi)$ and the optimal value is V^*. Finally, the attacker strategy at each stage will be the solution of the discounted optimal Markov control problem

$$\begin{aligned} &\max \mathbf{V}_{\beta}(\pi) \\ &\text{s.t.} \quad \pi \in P_s, \end{aligned} \tag{7.19}$$

where P_s is the space of control strategies, $\pi(s) = \pi(s, 1), \pi(s, 2), ..., \pi(s, m(s))$ and

$$\sum_{a=1}^{m(s)} \pi(s, a) = 1 \tag{7.20}$$

7.3.2 Solving the MDP

The attacks problem in (7.19) is solved by dynamic programming. The algorithm storage two arrays indexed by state: Long term reward value V and attack policy π. The algorithm initiates randomly the reward value function V and repeats for each state s the following steps until no further changes take place:

$$\pi(s) := arg\max_{a} \left\{ \sum_{s'} Q(s, s', a) \left(r(s, \pi) + \beta V(s^*) \right) \right\} \tag{7.21}$$

$$V(s) = \sum_{s'} Q(s, s', \pi(s)) \left(r(s, \pi) + \beta V(s') \right) \tag{7.22}$$

The optimal policy π obtained by backward recursion of (7.21) and (7.22) shows the best targets to select for each possible state of the network. Attacks are applied sequentially, then attack with the highest long term reward value is selected and applied to the network. With the new state of the network, the next attack is recalculated and applied. Figure 7.3 shows the flow chart of the MDP cascading failures attack, including the MDP algorithm for target selection.

7.4 Results and Discussion

In this section, we evaluate the performance of the MDP attack in the IEEE 30-bus case study. The immediate reward is evaluated for both, the power loss reward in (7.12) and congestion increase in (7.13). Also, a fixed strategy to reinforce the transmission capacity of some edges as a measure to reduce the impact of cascading failure effects is studied. The use of different criteria selects suitable candidates for reinforcement. The impact of this reinforcement is evaluated by the effect produced in the attack impact. The IEEE 30-bus systems as has been described in other Chapters contains, is composed of 41 lines and 30 nodes, including 6 generator nodes and 18 load nodes. Lines capacity is shown in Table 7.1.

The algorithm shown in Figure 7.3 is used to identify the attacker targets and Algorithm 5 is used to apply the attack and calculate the network power loss. Figure 7.4 presents the results of the MDP attack application against the IEEE 30-bus. The green line presents power loss by selecting the targets randomly. With a 20% of attacked edges, the network only lost 10% of its load. Blackline presents the results of the MDP attack with the immediate reward of equivalent to the loss of power. Close to 12% of attacked edges, the power loss is higher than 50%. First attacks in the sequence do not represent lost for the system. Dotted orange line shows attack results for the MPD attack with immediate reward congestion criteria i.e., $r(s, s', a) = \Delta q$. This attacks strategy presents better results than the other two. After the second attacker action of the sequence, the system has lost 40% of the power. When 12% of the edges are attacked, power lost is two times

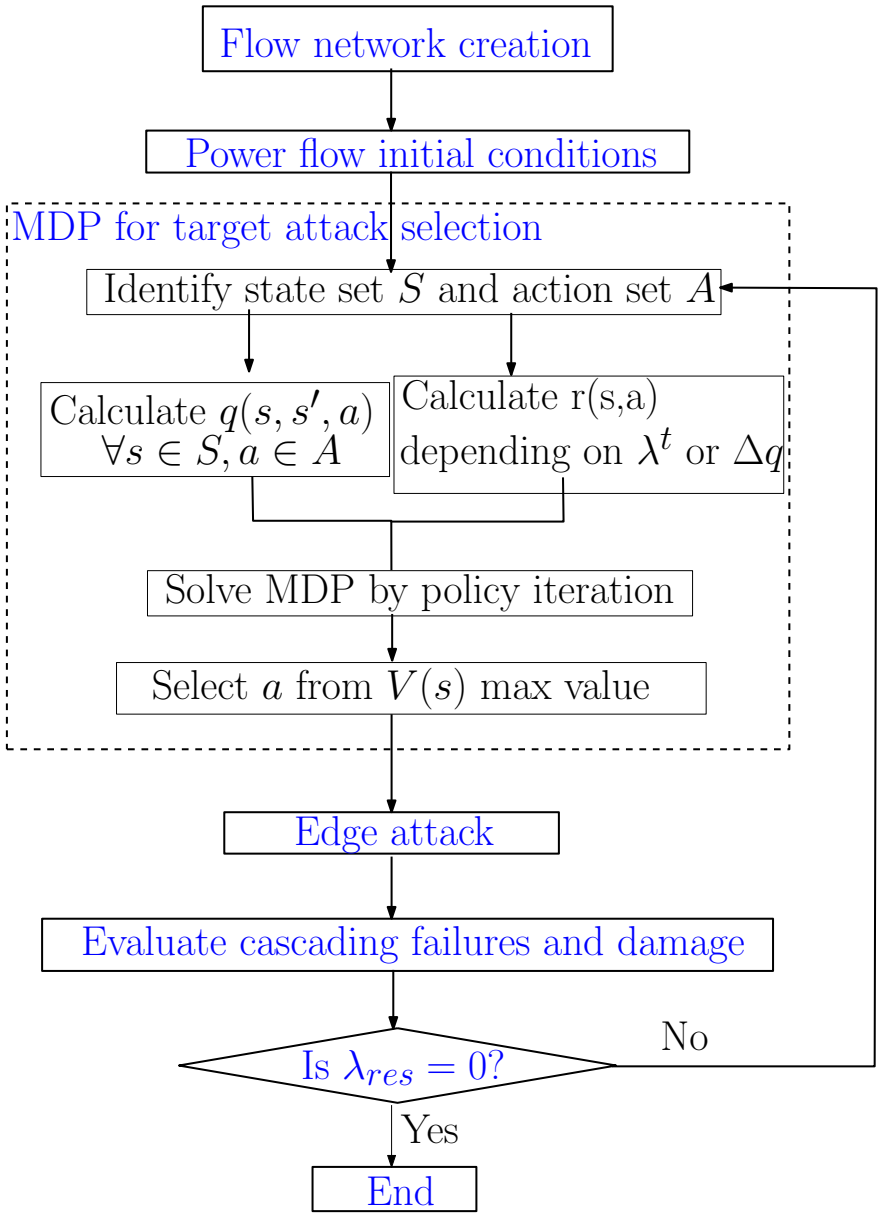


Figure 7.3: Algorithm for the MDP attack strategy.

higher than the lost in MDP with λ^t immediate reward. By the end of the attacks, both behave the same. Therefore as can be observed, attacks based on the increase of congestion result more harmful than attacks focussed on immediate loss of the load. Table 7.2 shows the targets selected for each attack. Attacks in the $MDP_{\Delta q}$ strategy is focused on the edges connecting nodes in the MCS (see Section 6.1) while attacks in the MPD_{λ^t} strategy target edges directly connected to centers of the load. The attack is not successful due to the redundancy of edges connecting the load.

Considering the results of this and previous Chapters, the transmission capacity of edges and network transmission capacity and congestion plays the central role in the vulnerability of the network to different hazard events triggering cascading failures. In this way, it is interesting to

Table 7.1: The values of the transmission capacities of the IEEE-30 bus system.

e	(from-to)	capacity(p.u.)	e	(from-to)	capacity(p.u.)
1	(1, 2)	130	22	(15, 18)	16
2	(1, 3)	130	23	(18, 19)	16
3	(2, 4)	65	24	(19 ,20)	32
4	(3, 4)	130	25	(10, 20)	32
5	(2, 5)	130	26	(10 ,17)	32
6	(2, 6)	65	27	(10, 21)	32
7	(4, 6)	90	28	(10, 22)	32
8	(5, 7)	70	29	(21, 22)	32
9	(6, 7)	130	30	(15, 23)	16
10	(6, 8)	32	31	(22 ,24)	16
11	(6, 9)	65	32	(23, 24)	16
12	(6,10)	32	33	(24, 25)	16
13	(9, 11)	65	34	(25, 26)	16
14	(9, 10)	65	35	(25, 27)	16
15	(4, 12)	65	36	(28, 27)	65
16	(12,13)	65	37	(27 ,29)	16
17	(12,14)	32	38	(27, 30)	16
18	(12, 15)	32	39	(29, 30)	16
19	(12, 16)	32	40	(8, 28)	32
20	(14, 15)	16	41	(6 ,28)	32
21	(16, 17)	16			

Table 7.2: Targets for each attack scenario.

MPD_{λ^t}	$MDP_{\Delta q}$	$MDP^{rand}_{\lambda^t}$ con $50\%+$	$MDP^{electricB}_{\Delta q}$ con 50%	$MDP^{CS}_{\Delta q}$ con $50\%+$
(8,28)	(4,6)	(6-8)	(2,5)	(4,6)
(4,12)	(2,6)	(8-28)	(1,3)	(2,6)
(9,10)	(2,5)	(15-23)	(2,4)	(2,5)
(9,11)	(10,22)	(4-12)	(2,6)	(25,27)
(12,13)	(28,27)	(12-13)	(25,27)	(10,22)
(10,17)	(27,29)	(10-17)	()	
(10,22)	(25,27)	(28-27)	()	
(22,24)		(2-5)	()	

evaluate how by making flexible the capacity value for some edges, the attack impact can be affected. For this, consider a number k of edges selected under determined criteria in order to increase its transmission capacity. The increased capacity will be selected for this example as a minimum required to produce changes in network behavior. In this way, a 10% of the edges had been selected for reinforcement with an increase of 50% of its operational capacity. Three different criteria are used to select suitable candidates for the reinforcement. The first strategy is a random selection of the candidates. The second strategy is the selection of the candidates according to the

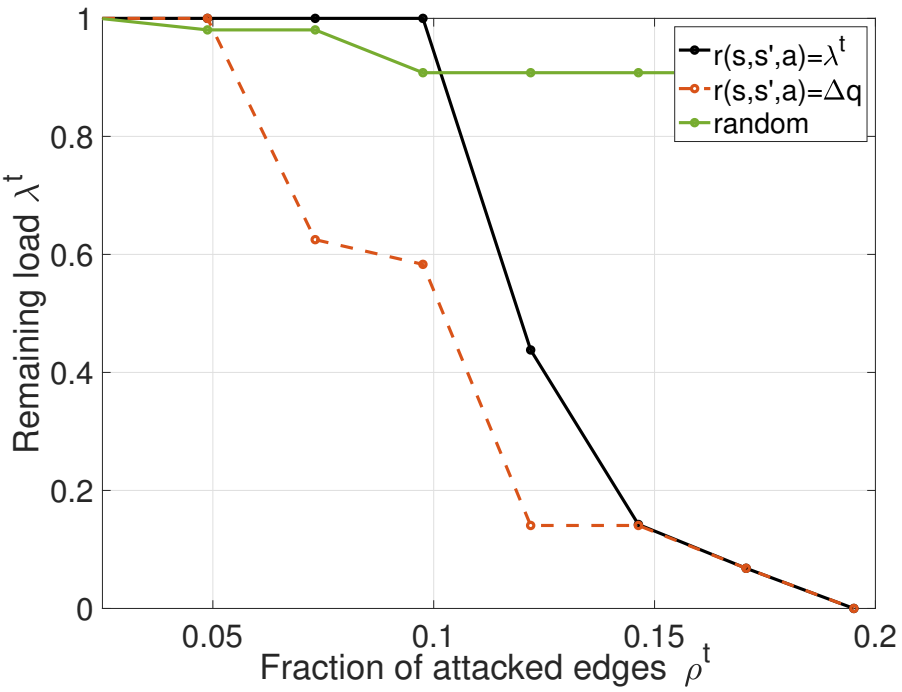


Figure 7.4: Results of the MDP attack application against the IEEE 30-bus without network reinforcement

electric betweenness index. Finally, the last strategy is the selection of candidates according to the cut-set metric for critical links identification described previously.

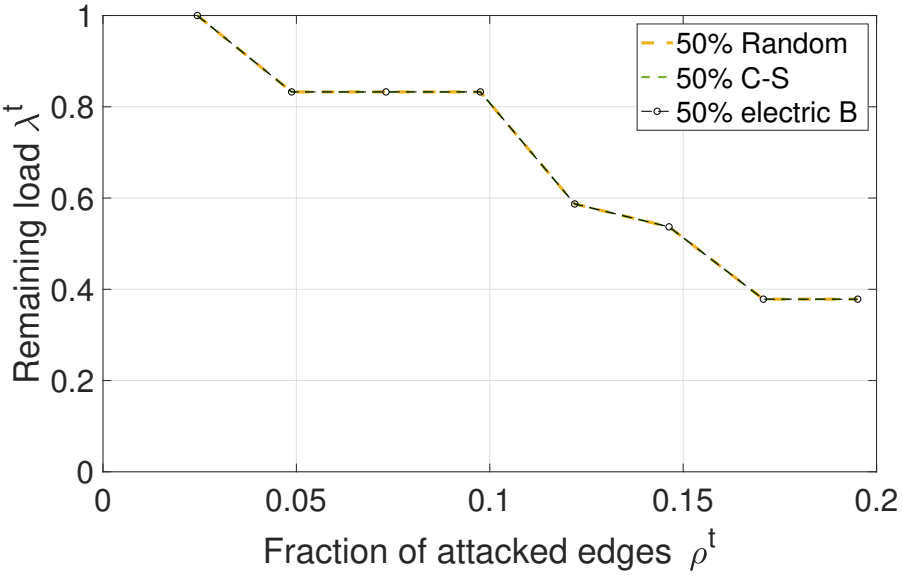


Figure 7.5: Results of the MDP attack with λ^t reward versus the reinforcement strategy

In terms of the Markov Decision Process, the reinforcement of the edges implies the inclusion

of a defender who fixes a pure strategy against the attacker. Results of the MDP are going to be the best response from the attacker to the defender fix strategy. The result will be different for both MDP attacks. Figure 7.5 presents results of the MDP attack with λ^t reward versus the reinforcement strategy. For any strategy to select candidates for the capacity increase, the network vulnerability to the attack is reduced in 50%. All the reinforcement gives the same results. Figure 7.6 presents the results for the MDP attack with Δq reward versus the reinforcement strategy. Random reinforce of capacity does not affect the attack impact, as can be seen in the orange dotted line. On the other side, an increase in capacity of the elements of the CS present a slight decrease in the vulnerability of the network as can be seen in the dotted black line. The most atypical case is the reinforcement of the edges selected by its electric betweenness. Increase of the capacity of these edges impacts the effectivity of the attack in a 90%. Edges with high electric betweenness selected for reinforcement where $(2,5)$, $(2,4)$, $(2,6)$, $(1,3)$. Those edges are edges with the higher capacity in all the network (see Table 7.1). For an increase of 50% on its capacity, the network transmission capacity improves in more than 20% reducing congestion and increasing the resilience of the network in this particular operation point.

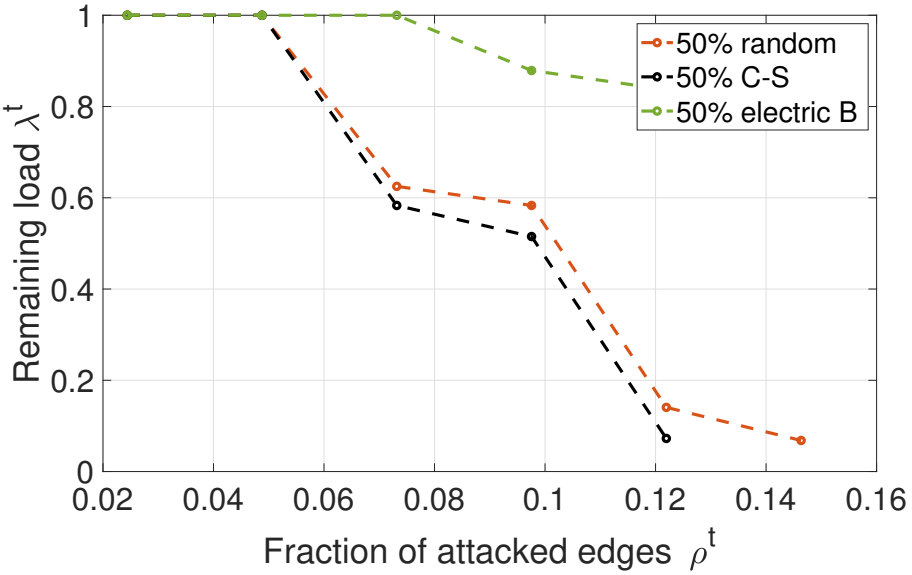


Figure 7.6: Lost of load for the MDP attack with Δq reward versus the reinforcement strategy

By observing these results, it is natural to consider that a possible controlled rating of edges capacities during contingencies could help to reduce the impact that failures and threats against some of their elements can produce. Also, an appropriate strategy should be used to select the best candidates for reinforcement or controlled dynamic capacity rating in order to get the best response against attacks.

Chapter 8

Transmission Capacity Rating as a Strategy to Defend the Network Against Cascading Attacks: A Stochastic Network Game

"The art of war teaches us to rely not on the likelihood of the enemies not coming, but on our readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable (MAIR, 2007)."

Sun Tzu
The Art of War

Resilience against cascading failures and attacks is one of the significant issues to consider in the planning and operation of future energy grids. When looking for ways to improve the future network operation, new defense strategies enriched by the use of network properties information should be established. Following previous attacks-based vulnerability framework, this chapter proposes a defense strategy to control the impact of cascading attacks based on dynamic line rating. A zero-sum Markov game with discounted reward is used to model the cascading attacks-defense problem. State coupled replicator equations are proposed to solve the stochastic games. We obtain candidates lines for transmission capability update from the solution of the attack - defense problem. Case studies are presented to show the effectivity of the defense strategy. By controlling the transmission capacity dynamically as a response to the threats, the resilience of the network is improved significantly.

8.1 Defender Model

The defender is an agent that intends to keep the stable state of the power network defending it from attacks. The available actions for the defender are the set of network edges whose transmission capacity could be dynamically rated. According to Section 7.1.3 the capacity vector $\mathbf{c}^t$ is changed

by a disturbance $\delta^t \in \mathbb{R}^m$, related to the threat model described in Section 7.1.4. In this chapter, Equation (7.6) is modified to include the actions related to the defense strategy. At each stage the network reinforcement ς_e^t is modeled by $\varsigma_e^t = \kappa \Phi^t \mathbf{c}^t$ where κ is the capacity rating value with $1 \leq \kappa \leq 2$, Φ^t is a $m \times m$ matrix and $\Phi^t = \text{diag}(\phi_1, \phi_2, \ldots, \phi_m)$. Reinforcement ς_e^t is used by modifying Equation (7.6) as follows

$$c_e^{t+1} = c_e^t - \delta_e^t + \varsigma_e^t, \qquad e \in \mathcal{E}^t. \tag{8.1}$$

In this way, (8.1) shows the increase of transmission capacity of edge e by defining the element ϕ_e^t as

$$\phi_e = \begin{cases} 1, & \text{if edge e is reinforced;} \\ 0, & \text{otherwise} \end{cases}. \tag{8.2}$$

The network state does not change as long as $\varsigma^t = 0$ and $\delta^t = 0$. Disturbance δ is defined according to the threat model shown in Section 7.1.4. and system model follows the development used in Chapter 6 and 7. The defender of the power network aims to define the best control actions that minimize the cascading failure risk in the long term. Next section defines the problem.

8.2 Problem Formulation

Different from the optimization problem proposed for the attacker in Chapter 7, the defender attempts to reduce the estimated risk of the failures in the network depending on its actions and the attacker strategy. Consider a set of actions for the attacker $\{a_1^1, a_2^1, \ldots, a_m^1\}$ and a set of actions for the defender $\{a_1^2, a_2^2, \ldots, a_m^2\}$. For a given set of attacks actions, a defined supply/demand, network topology, and flow routing strategy over an infinite horizon, the optimal defense sequence that minimizes the damage triggered by the attack. Then, the problem for the defender is the opposite than the proposed model for the attacker in (7.14). Expected risk should be reformulated as $E[S(a^{1,*}, a^{2,*}, \hat{\mathcal{G}})]$ to include the joint actions of defender and attacker.

Also, it should get response according to the best strategies taken by the attacker then the optimal defender strategy will depend on the optimal attacker strategy, and the defender will try to minimize the estimated risk of the cascade as follows

$$\min_{(a^{1,*}, a^{2,t})} \sum_{t=0}^{\infty} \beta \mathbb{E}[S(a^{1,*}, a^{2,*}, \hat{\mathcal{G}})] \tag{8.3}$$

where β is the discounted reward. Defender chooses the best strategy as a response of strategy fixed by an attacker. However, the attacker will be optimizing its strategy, and the defense problem should be recast as an attack-defense problem where both agents are trying to optimize its reward,

for the defender the reduction of risk and the attacker the opposite increase of risk. Next section presents the recast of the problem as a discounted stochastic game.

8.3 Stochastic Game for Cascading Collapse Control

As described in the previous section, the objectives of the attacker and defender under cascading collapse conditions are opposite to each other. By recasting the attacker optimization problem, we can integrate it with the defender problem into a stochastic game of zero-sum played in the power system. The game is played in a sequence of steps. In the beginning, the game is in a given state, and the players select actions independently and at the same time. The selection is based on their information and constraints for the current state. Following, each player receives an immediate reward that results from the chosen actions and the current state. Payoffs and probability transitions between states are defined for each state. The game repeats continuously for new stages by moving between random states depending on the transition probability defined by the strategy played and the previous stage. During the game, each player is going to maximize its long-term expected reward. It is defined as the discounted for all stages of the immediate player rewards.

Due to the competition between the defender and the attacker, the control problem is formulated as a stochastic game G_β with a set of states indicated by S, where each state $s \in S$ is an array denoting the current status of all the network edges. The status of each edge in $\hat{\mathcal{G}}$ is defined by its membership to the edge set $\hat{\mathcal{E}}$. The stochastic game proceeds in a discrete-time sequence. During the game iterations, each player chooses an action to optimize its objective based on the current system state. Let be $A^i(s)$ as the set of all the possible actions that player i, been $i = 1$ for attacker and $i = 2$ for defender, can take at state s individually. As explained in Chapter 7.2 and 8.1, for the attacker each $a^1 \in A^1(s)$ indicates the transmission line to be attacked. On the other hand, for the defender, each $a^2 \in A^2(s)$ indicates the set of edges to be reinforced. Each action $a \in A^i(s)$ is selected by the attacker and defender with a specific probability denoted by $\pi_j^i(s)$. The probability that an edge e fails when attacked, even if it is reinforced or not, is defined by the hidden failures model in (7.8). Normalized probability of failure is defined as

$$\hat{\omega(e)} = \frac{\omega(e)}{\|\omega\|_1} = \frac{\omega(e)}{\sum_{k=1}^{|m-1|} |\omega(e)|} \tag{8.4}$$

where $0 \leq \hat{\omega(e)} \leq 1$. These probabilities included in the independent edge dependent model from (7.9) determine the transition probability between states $q(s^{'}, s, a)$, for $a := (a^1, a^2)$, from state s to $s^{'}$ under the actions a. As mentioned before, agents objectives are opposite: maximizing/minimizing the cascading failures risk in the power network. For each step of the game, both attacker and defender receives an immediate reward defined by the actions taken at state s. Immediate reward will be denoted by $r(s, a)$ and calculated according to attack severity criteria from

(7.12) or (7.13). in Chapter 7.1.6. The general definition of the discounted stochastic game for cascading collapse defense is described as follows

Definition 8.3.1 *The discounted stochastic game $G_\delta(n, S, A, q, r, \pi^1, \ldots, \pi^n)$ has n players and k states. At each time step t, the game is in a state $s \in S = (s_1, s_2, \ldots, s_k)$ and each player i chooses an action a^i from its action set $A^i(s)$ depending on its strategy $\pi^i(s)$ (Liao et al., 2017).*

The payoff function

$$r(s,a) : \prod_{i=1}^{n} A^i(s) \mapsto \mathbb{R}^n \tag{8.5}$$

maps the players joint action $a = (a^1, \ldots, a^n)$ to its immediate payoff value.

The transition probability function

$$q(s,a) : \prod_{i=1}^{n} A^i(s) \mapsto \Delta^{k-1} \tag{8.6}$$

determines the stochastich state change, when Δ^{k-1} is the $(k-1) - simplex$ and $q(s, s^{'}, a)$ is the transition probability from state s to $s^{'}$ under joint action a.

8.4 Optimal Strategies for Defender and Attacker in the Stochastic Game

Here, the stochastic game is presented with the optimal solutions for the zero-sum stochastic game. A method for the solution of the stochastic game, based on population dynamics, is developed in order to find the optimal strategy for the defense of the cascading failures attacks.

8.4.1 Optimal Strategy

The optimal strategy refers to the mixed strategy of all actions chosen by the player that maximize their expected long-term rewards. The optimal strategy is the mixed strategy from all possible actions chosen by the player that maximize its long-term expected reward. First, consider stationary strategies where the probability of selecting a specific action does not change in time, i.e., $\pi^1(s), \pi^2(s)$ do not change over time. In this way, the solution of the problem brings the stationary policies for each player on state s.

The function $R^i(s,a)$ is the expected long term reward for player i selecting actions a^*, for attacker and defender respectively, and $\nu^i_{s'}(\pi)$ the player i expected long-term reward under the

optimal strategy when game starts at stage s. Thus, $\nu^2_{s'}(\pi)$ for the defender will be

$$\nu^2_s(\pi) = \min_{\pi^2(s)} \max_{\pi^1(s)} \sum_{a \in A^2(s)} \sum_{a \in A^1(s)} \pi^2(s) R^2(s,a) \pi^1(s) \tag{8.7}$$

where is a nonnegative row vector $\pi^i(s) = (\pi^i_1(s), \pi^i_2(s), \ldots, \pi^i_{|A^i(s)|}$ with entries that satisfy the simplex $\sum_{a \in A^i(s)} \pi^i_a(s) = 1$ and $\pi^i_a(s) \geq 0$ and

$$R^i(s,a) = r^i(s,a) + \delta \sum_{s' \in S} q(s^{'}, s, a) \nu^i_{s'}(\pi). \tag{8.8}$$

For the attacker, a dual problem exists. Besides, considers that attack-defense cascading failures problem as a zero-sum game where

$$r(s,a) := r^1(s,a) = -r^2(s,a) \tag{8.9}$$

for all $s \in S$, $a^1 \in A^1(s)$ and $a^2 \in A^2(s)$. The optimal reward $\nu^i_s(\pi)$ can be called also the present discount value of the i^{th} player expected future rewards under π with initial stage s.

Furthermore, $\nu^i_{s'}$ is the present discount value of the i^{th} player expected future rewards under π with initial stage $s^{'}$

$$\nu^i_{s'}(\pi) = P^i(s^{'}) + \delta \sum_{z \in S} \nu^i_z(\pi) Q^i(s^{'}) \tag{8.10}$$

where the expected reward for player i resulting from the use of the strategies π^1 and π^2 at state $s^{'}$ define the immediate expected reward $P^i(s^{'})$ where for each $s \in S$

$$P^i(s^{'}) = \sum_{a' \in \prod_{i=1}^n A^i(s')} \left(r(s^{'}, a^{'}) \prod_{i=1}^n \pi^i_{a'_i}(s^{'}) \right) \tag{8.11}$$

with $r(s,a)$ defined in (8.5).

Also, for a fixed pair of stationary strategies π^i and π^2, the Markov probability transition matrix $Q^i(s^{'})$ induced by $(\pi^1(s), \pi^2(s))$ at state s is

$$Q^i(s^{'}) = \sum_{a' \in \prod_{i=1}^n A^i(s')} \left(q(s^{'}, z, a^{'}) \prod_{i=1}^n \pi^i_{a'_i}(s^{'}) \right) \tag{8.12}$$

During each stage, the players consider all possible payoffs obtained for the current strategy.

The current state s is untangled from all other states $s^{'} \neq s$ and the expected payoff shifts to the sum of the expected immediate reward value $P^i(s^{'})$ in the state s for joint action a and the present reward values of other states $\nu_z^i(\pi)$. Hence, if players choose joint action a each time the game is in state s and their fixed strategies for all other states $\pi(s^{'})$ the discounted reward value for players will be defined by (8.13),

$$R^i(s,a) = r^i(s,a) + \delta \sum_{s' \in S} q(s,s^{'},a)\nu_{s'}^{i}(\pi). \tag{8.13}$$

Following, the optimal strategy $(\hat{\pi}^1, \hat{\pi}^2)$, which is understood as the Nash equilibrium of the zero-sum stochastic game is defined.

Definition 8.4.1 *Consider a strategy $\pi^i = (\pi^i(1), \ldots, \pi^i(s), \ldots, \pi^i(N)$ is a block row vector whose s^{th} block is a nonnegative row vector $\pi^i(s) = (\pi_1^i(s), \pi_2^i(s)), \ldots, \pi_{|A^i(s)|}^i$ with entries that satisfy the simplex $\sum_{a \in A^i(s)} \pi_a^i(s) = 1$ and $\pi_a^i(s) \geq 0$. The pair of strategies $(\hat{\pi}^1, \hat{\pi}^2)$ is a Nash equilibrium point of the discounted stochastic game G_β if*

$$\nu_s^1(\pi^1, \hat{\pi}^2) \leq \nu_s^1(\hat{\pi}^1, \hat{\pi}^2), \qquad \forall\, \pi^1 \tag{8.14}$$

and

$$\nu_s^2(\hat{\pi}^1, \pi^2) \leq \nu_s^2(\hat{\pi}^1, \hat{\pi}^2), \qquad \forall\, \pi^2 \tag{8.15}$$

Hence, by getting the Nash equilibrium for each state s, we can obtain an optimal defender strategy against attacker best strategy. This strategy will define the optimal expected long term reward for both players. Due to the zero-sum nature of the game, the present value can be generalized to

$$\nu_s(\pi) := \nu_s^1(\pi) = -\nu_s^2(\pi) \tag{8.16}$$

for all π. Thus the nature of the equilibrium point of the system will be

Definition 8.4.2 *A strategy pair $(\hat{\pi}^1, \hat{\pi}^2)$ constitutes a saddle point for the expected game if and only if for all π^1, π^2*

$$\nu_s^1(\hat{\pi}^1, \pi^2) \leq \nu_s^1(\hat{\pi}^1, \hat{\pi}^2) \leq \nu_s^1(\pi^1, \hat{\pi}^2) \tag{8.17}$$

Then, the cascading failures attack-defense game is a zero-sum game, and the minimax theorem guarantees the existence of a saddle point. Next section presents the development of a multi-population replicator dynamics algorithm designed to determine the optimal solution for the cascading failures stochastic game. Different from population-based algorithms that only focus on the

limit average stochastic game, this algorithm presents a specific solution for the discounted reward stochastic game previously not founded in literature. Also, solution of the population dynamics system is proven to converge to the optimal solution.

8.4.2 State Coupled Replicators for Discounted Reward Stochastic Games

Considers the system of differential equations defining the two-population replicator dynamics as following (Hennes, Tuyls, & Rauterberg, 2009),

$$\begin{aligned} \frac{d\pi_i}{dt} &= \pi_i \left[(A\sigma)_i - \pi^{'} A\sigma \right] \\ \frac{d\sigma_i}{dt} &= \sigma_j \left[(B\pi)_j - \sigma^{'} B\pi \right] \end{aligned} \tag{8.18}$$

where A and B are respectively the game payoff matrices for player 1 and 2. The vector of probabilities π defines the frequency of all puree strategies for player 1. The progress of the replicator i is calculated by the difference between its payoff $(A\sigma)_i$ and the average payoff $\pi^{'} A\sigma$ of the whole population π versus the strategy of player 2.

In the discounted reward stochastic game G_β with discounted payoff reward $R^i(s, a^*)$, the expected payoff of an individual playing a pure strategy i in population π against a population σ is given by

$$P^i(s,\omega) = \sum_{j \in A^i(s)} \left[\omega_j \sum_{a \in \prod_{l \neq i} A^l(s)} \left(R^i(s,a^*) \prod_{l \neq i} \pi^l_{a^*_l}(s) \right) \right] \tag{8.19}$$

where

$$a^* = (a^1 \dots a^{i-1}, j, a^i \dots a^n). \tag{8.20}$$

All possible joint actions a with fixed action j are enumerated in the vector a^*. If population π^i represents a population i, for $i = 1, 2$ respectively as defined in 8.4.1 it is possible to define a system of differential equations similar to (8.18) where the payoff matrix A is replaced by the expected discounted reward game payoff $R^i(s, a^*)$ as follows,

Definition 8.4.3 *The multi-population state-coupled replicator dynamics are defined by the following system of differential equations:*

$$\frac{d\pi^i_j(s)}{dt} = \pi^i_j \left[P^i(s, e_j) - P^i\left(s, \pi^i(s)\right) \right] \tag{8.21}$$

where e_j is the j^{th}-unit vector and $P^i(s,\omega)$ is defined in (8.19) as the expected payoff for an

individual of population i playing some strategy ω in state s.

where $R^i(s, a^*)$ is the discounted reward function of $G_\delta(s, \pi^1, \pi^2)$,

$$R^i(s, a^*) = r^i(s, a^*) + \delta \sum_{s' \in S} q(s, s^{'}, a^*)\nu^i_{s'}(\pi) \tag{8.22}$$

and

$$a^* = (a^1 \dots a^{i-1}, j, a^i ... a^n). \tag{8.23}$$

In total the system has $N = \sum_{s \in S} \sum_{i=1} n|A^i(s)|$ replicator equations.

In order to solve the coupled-state multi population replicator dynamics, a Global Random Start Algorithm is used to define the initial present discount value of the system. The algorithm behaves as follows

1. Randomly selects starting points from the space $\{\pi^i_a(s), \nu^i_s(\pi)\}$ for the replicator equations in 8.21 and solve them until the solution of the system is founded.
2. Given the size of the space the search of the initial point will be inefficient then it is sufficient to search the space of probability vectors to choose the starting $\pi^i_a(s)$.
3. Once the initial probability is chosen, solve the linear system in 8.10to determine the starting $\nu^i_s(\pi)$.

Example: 2-state matching pennies game

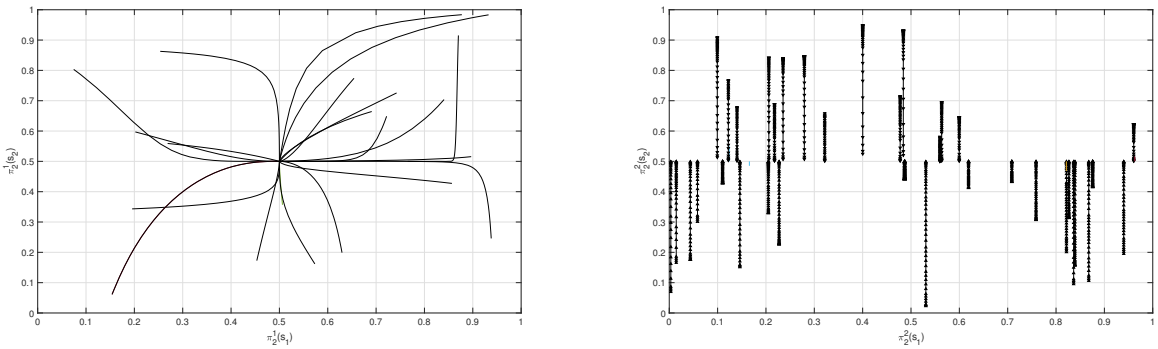
Considers the classic game of "Matching pennies" generalized for a 2-state stochastic game (Hennes, Kaisers, & Tuyls, 2010). Player 1 and 2 both put a penny on a table simultaneously. In state 1, If the two pennies come up the same, then player 1 gets both, otherwise player 2. For state 2, If the two pennies come up the same, then player 2 gets both, otherwise player 1. This game is represented by the reward matrices that follows

$$\left(r^1(s_1), r^2(s_1)\right) = \begin{pmatrix} 1,0 & 0,1 \\ 0,1 & 1,0 \end{pmatrix}, \left(r^1(s_2), r^2(s_2)\right) = \begin{pmatrix} 0,1 & 1,0 \\ 1,0 & 0,1 \end{pmatrix}. \tag{8.24}$$

Similarly, the transition probabilities between states depending on the actions taken are given by the matrices $Q(s_1, s_2)$ and $Q(s_2, s_1)$

$$Q(s_1, s_2) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, Q(s_2, s_1) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \tag{8.25}$$

The probabilities to stay at the same state after a transition occurs are defined by $Q(s_1, s_1) = 1 - Q(s_1, s_2)$ and $Q(s_2, s_2) = 1 - Q(s_2, s_1)$. Coupled state multi-population replicator dynamics in (8.21) is applied to the game and mixed nash equilibrium are founded with joint strategies $\pi^1 = (0.5, 0.5))$, $\pi^2 = (c, 1 - c)$ with c depending on initial conditions.in state 1 and $\pi^1 = (0.5, 0.5))$, $\pi^2 = (0.5, 0.5)$ in state 2. Figure 8.1 presents an overview of the state space for the matching pennies game on each state. A continum of equilibrium points exist in state 1 for player 2 due to linear dependency of the stochastic replicators.

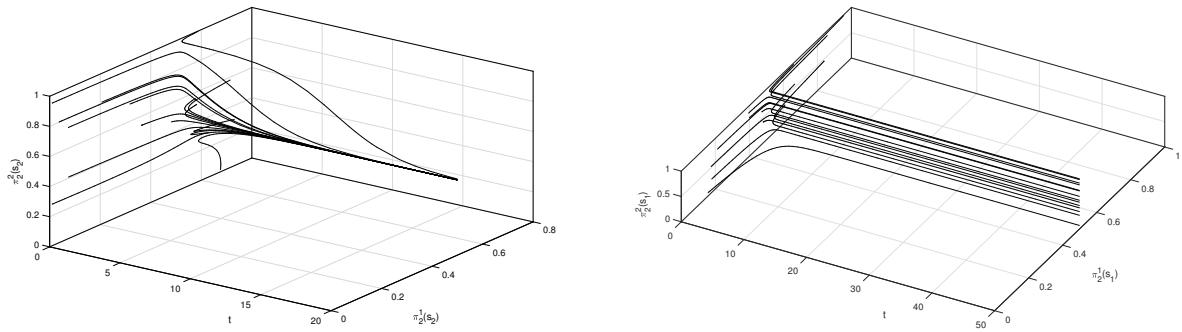


(a) Trajectories for state 1

(b) Trajectories for state 2

Figure 8.1: Overview of the state space for the matching pennies game on each state

Figure 8.2 present multiple trajectory plots for the 2-state matching pennies game departing from random initial conditions in both states. The results show how all the trajectories converge close to the continuum of mixed Nash equilibrium points described before. Results confirm the convergence of the algorithm to the solution of the stochastic game.



(a) Trajectories for state 1

(b) Trajectories for state 2

Figure 8.2: Multiple trajectories for the players in the 2-state matching pennies game.

Figure 8.3 shows the convergence of the discounted value of a strategy pair $\nu_s^1(\pi) = -\nu_s^2(\pi)$ for each state.

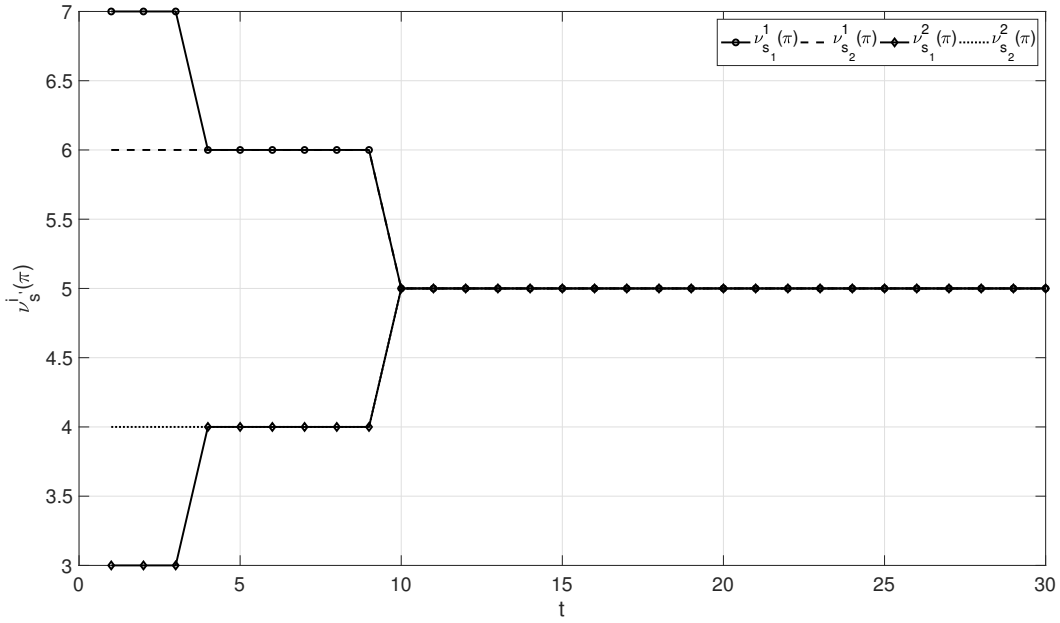


Figure 8.3: Convergence of the discounted value for the matching pennies game

8.5 Simulation Results

In this section, simulations are performed to demonstrate the efficacy of the proposed defense scheme. First, the convergence of the proposed coupled states multi population replicator dynamics algorithm is demonstrated in the IEEE 9 bus system.

Table 8.1: Edge capacity for the studied IEEE 9 -bus system

e	1	2	3	4	5	6	7	8	9
(from-to)	(1, 4)	(4,5)	(5, 6)	(3, 6)	(6, 7)	(7, 8)	(8, 2)	(8, 9)	(9, 4)
capacity (p.u.)	250	250	150	300	150	250	250	250	250

8.5.1 Convergence of CSMP-Replicator Dynamics

This section study the convergence of the proposed coupled multi-population replicator algorithm using the IEEE 9-bus system and the PowerNet toolbox. Transmission capacity limits for each edge of the system following Section 7.1.3. Flow limits are presented in Table 8.1. Figure 8.4 presents the configuration of the system.

To initialize the simulation, we set the probability of actions homogeneously distributed with $\pi^1 = 0.125$ for all actions π^1_j and $\pi^2 = 0.125$ for all actions π^2_j for all the states. Using these initial probabilities we use the Global Random Start Algorithm and calculate the present value initial condition., transition probabilities $q(s, s^{'}, a)$ are calculated and immediate reward for all actions

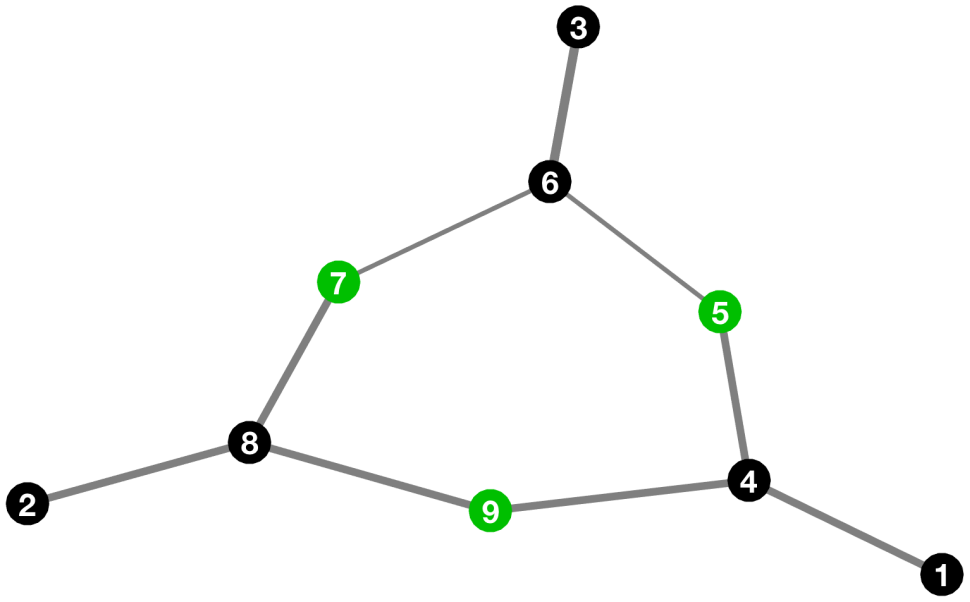


Figure 8.4: Network structure of the IEEE 9-bus system

all states as well. The discount factor is $\beta = 0.9$. Figures 8.5 and 8.6 shows the dynamic of the replicators associated with strategies for attacker and defender.

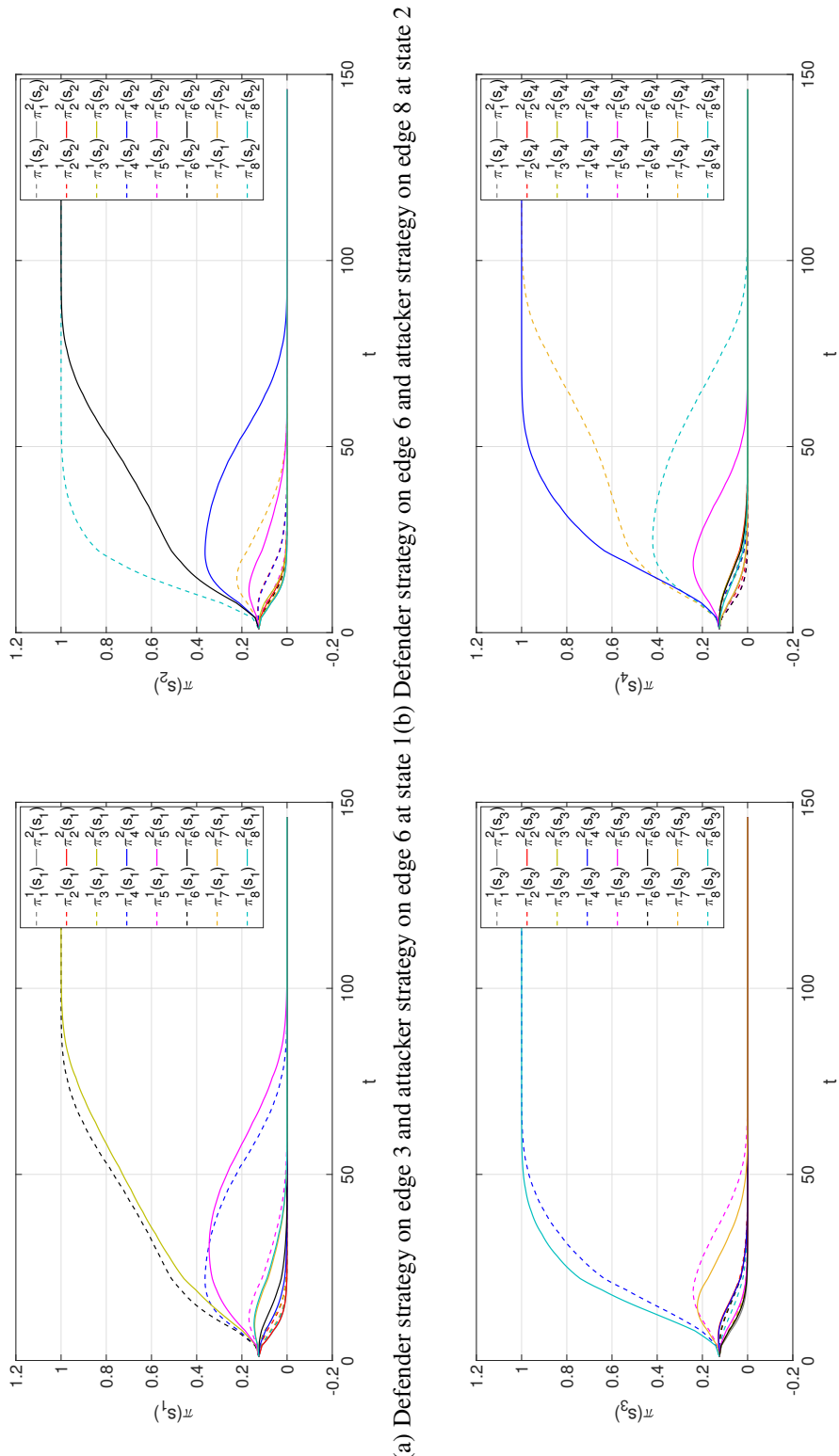
From the results, it is possible to observe for each state a pair of pure strategies for attacker-defender. These become the primary targets for attack and defense, respectively, for each state. In particular, in state 1, the attacker tends to attack edge 6, and the defender will reinforce 3. The probabilities converge to a stationary strategy for both players. A system without control lost all its load by the attack of a single edge, after apply capacity control by the defender, the time of collapse is extended from the first stage to the third stage.

Strategies converge for 150 iterations. Converged strategies achieve a Nash equilibrium point. The strategies obtained can be used as a guide for the defender to select targets for dynamic line rating in order to reduce congestion of the system. By applying this strategy, the system operator will diminish the risk of failure propagation and loss of load. Results in Figure 8.7 show how the present discount changes by employing the action obtained from the replicator method.

The differential equations system integration dictates the complexity of the algorithm. Also, for a higher number of nodes, the time to calculate the reward and transition matrix could increase considerably.

8.6 Conclusions

Stochastic games could be a useful framework to study defense strategies reducing the risk of failure in power networks. Optimal strategies responding to possible damage or failure of components can be studied through this framework. In this chapter, we have investigated defense strategies against cascading failures attacks in power networks. In particular, we built a zero-sum stochastic game whose transition probabilities depends on the network structure and hidden failures model. Different from previous results in the literature, transition probabilities are not estimated constant and homogeneous but are obtained from the network evolution during cascades. Attack defense rewards are calculated through cascading failures models proposed in previous chapters. Different from the results in Chapter 7, this chapter studies the joint actions between attackers and defenders. The strategy enumerates the different network states and the optimal joint strategies achieved in order to reduce the damage in the network or increase the response window. A coupled state multi-population replicator dynamics algorithm has been proposed in order to solve the stochastic game dynamically for each stage. Results extend previous results existing for limit average reward games to discounted long-term reward games. Algorithm complexity could be highly increased by the size of the calculation of transition and immediate rewards. Future works will be mainly focused on the decentralization of the strategy in order to reduce computational times and make it applicable to multiple stage attacks.



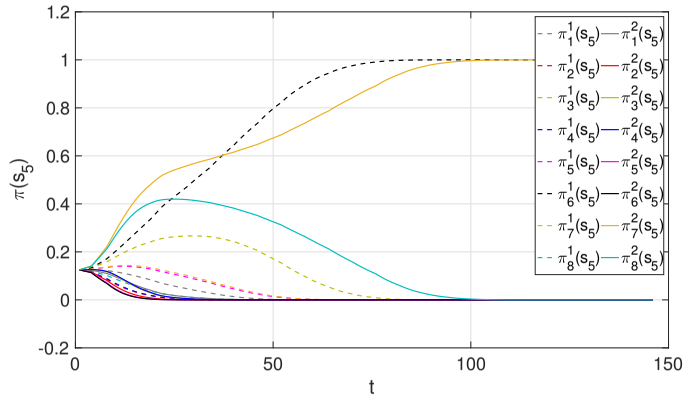
(a) Defender strategy on edge 3 and attacker strategy on edge 6 at state 1

(b) Defender strategy on edge 6 and attacker strategy on edge 8 at state 2

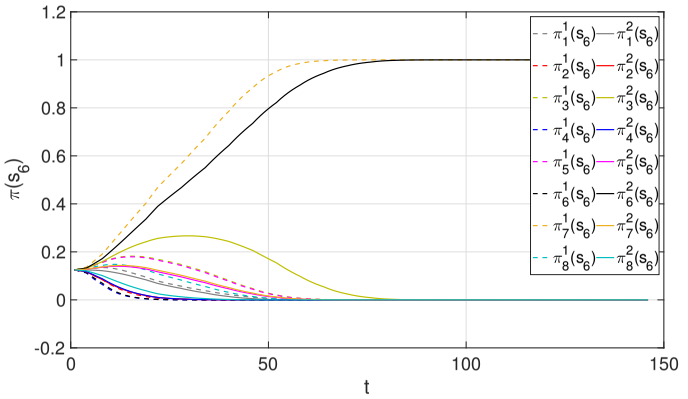
(c) Defender strategy on edge 4 and attacker strategy on edge 8 at state 3

(d) Defender strategy on edge 4 and attacker strategy on edge 7 at state 4

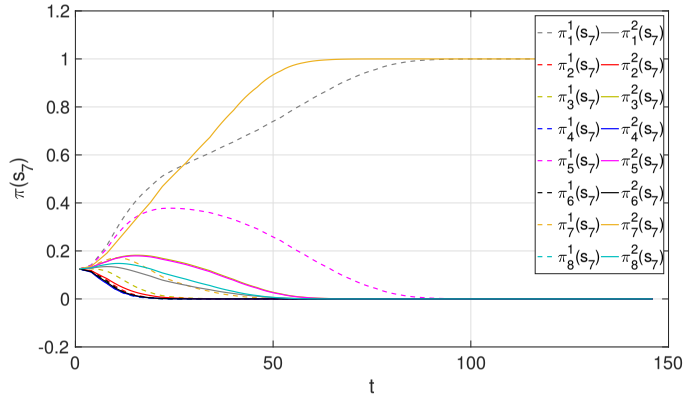
Figure 8.5: Replicator dynamics trajectories converging to the attacker and the defender strategies in the IEEE 9 bus system from state 1 to 4.



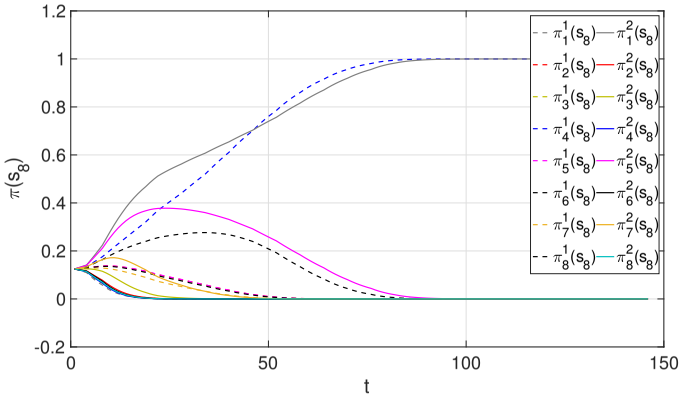
(a) Defender strategy on edge 7 and attacker strategy on edge 6 at state 5



(b) Defender strategy on edge 6 and attacker strategy on edge 7 at state 6

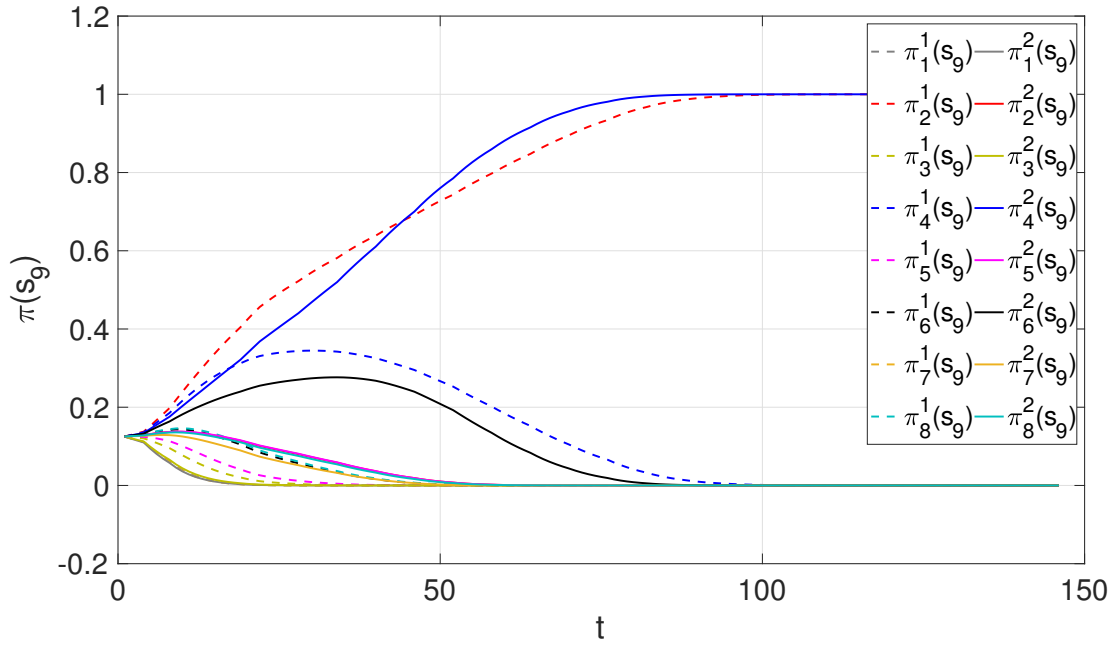


(c) Defender strategy on edge 7 and attacker strategy on edge 1 at state 7

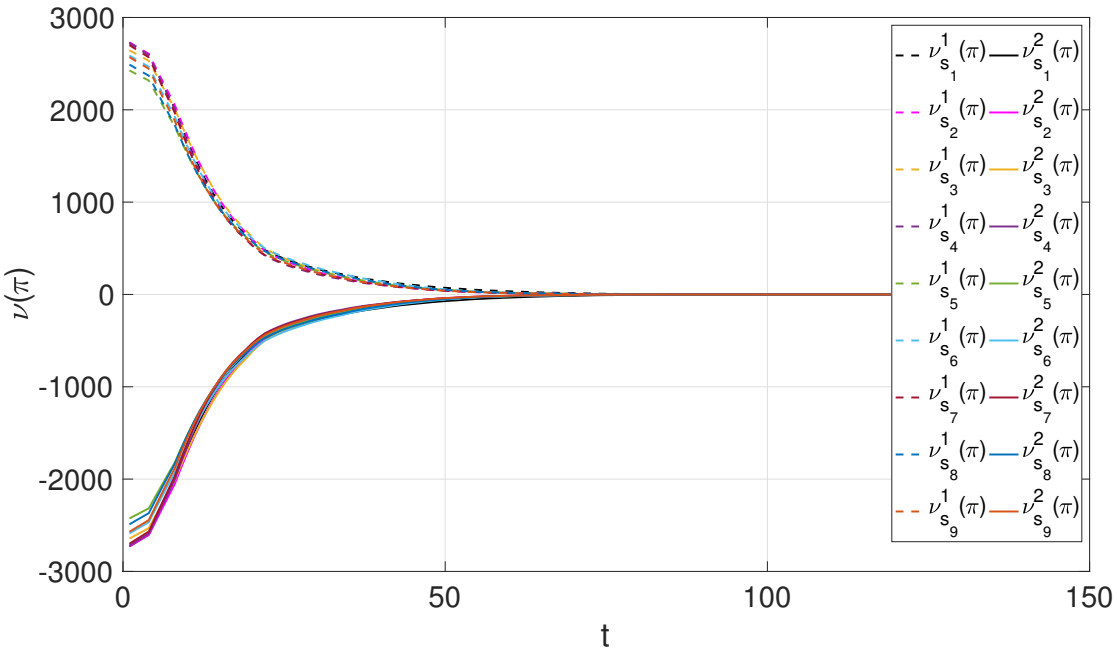


(d) Defender strategy on edge 1 and attacker strategy on edge 4 at state 8

Figure 8.6: Replicator dynamics trajectories converging to the attacker and the defender strategies in the IEEE 9 bus system from state 5 to 8.



(a) Attacker strategy on edge 2 and defender strategy on edge 4 at state 9



(b) Present value for the expected reward for attacker and defender

Figure 8.7: Attack defense strategy at state 9 and present discount value for attacker and defender

Part IV

Summary and Contributions

Chapter 9

Contribution and Concluding Remarks

9.1 Contributions

In this thesis, network-based approaches for the analysis and control of critical transitions in power networks has been presented. It has been introduced how network-based methods had been used during the last decade to approach power systems problems, in particular for cascading failures in chapter 2. *The first contribution of this thesis* studies the connectivity properties of power networks. Chapter 3 demonstrates how functional properties affect structural connectivity is and network congestion. Different from results found in literature properties studied in this chapter are evaluated for the first time in power systems. Network redundancy, bottleneck, and the cut-sets appear to have a significant role in connectivity changes during cascading failures. Computational methods in Chapter 5 demonstrate the influence of the cut-sets during cascading failures.

As a *second contribution of this dissertation*, a new dynamical model of cascading failures integrating networks, hybrid systems, and power systems has been developed in Chapter 4. The main advantage of the model is the integration of node dynamics and network dynamics in a single framework, making more accessible future analysis on the influence of phase compensation for cascading failure defense. A QSS approach of the model is also proposed in Chapter 6 and used in Chapter 7 and 8. The model proposed to have several advantages in order to facilitate the analysis of network properties and its use as design criteria for the attack-defense strategies in power networks.

As a *third contribution of this thesis*, Chapter 6 introduce a new network-based vulnerability analysis of power systems. MCS vulnerability is studied for the first time. The inclusion of multi-step attacks and target selection based on the MCS improves the vulnerability framework. A new metric to compare network vulnerability is presented. MCS attacks are compared to other attacks based on several well-established vulnerability metrics demonstrating its significant role in the vulnerability of the network.

Connectivity impact on network vulnerability during cascading failures is the main issue addressed in this thesis. To this end, the *fourth contribution of this dissertation*, presented in Chapter 7 consist of the logical extension of results in 6 by the modeling and solution of the Markov-based

attack problem. By this strategy, the most successful and efficient attack triggering cascading failures in power networks is presented as a Markov decision process. State transitions are defined based on hidden failures and edge-dependent network evolution. As the *fifth contribution of this thesis*, the Markov-based attack model is extended in a Zero-Sum Stochastic game in Chapter 8, where Nash equilibrium solution is found given the optimal control strategy against cascading failures attacks. Dynamical line rating is integrated into the defender model presenting as a first time this approach as a control strategy against cascading failures. As the *sixth contribution of this dissertation*, state coupled replicators are proposed to solve stochastic games in networks Chapter 8. Lumped Markov chains are used to model state transitions in order to approach the dimensionality problem. State coupled replicators are demonstrated to be useful to select control actions facilitating its extension at future to distributed control strategies.

9.2 Answering the Research Questions

This chapter answers the research questions postulated in Chapter 1.2 summing up the conclusions of this dissertation.

Q1 How do the properties of power networks change during a critical transition? One of the main inconveniences for the control and prevention of critical events in power networks is the lack of understanding of the cascading mechanism and the network structural and functional changes when approaching or crossing these transitions. The main property studied in this dissertation in order to understand this property is network connectivity and its influence on cascade spread. Several issues influencing cascading events have been identified in this dissertation. It has been shown in Chapter 3 how network connectivity changes due to different trigger mechanisms. The influence that trigger failures can have on the generation of the cascading mechanism is highly related to the network properties. Cascading events of different size are triggered depending on the supply/demand operation point and congestion. Power flow paths get congested and spread failures by achieving transmission limits at main connecting elements, i.e., MCS. Supply/demand node placement affects the size of the MCS and at the same time, network congestion. Flow bottleneck increase moving the system through a point of flow unfeasibility. Heavily charged networks can be more vulnerable to failure events that not-loaded networks. Line transmission capacity plays a significant role. Flow unfeasibility due to capacity constraints presents the primary mechanism to node isolation and power loss. Re-dispatch, without considering network-based transmission capacity influence significantly the failure mechanism. Another mechanism is related to state jumps (i.e., voltage angle) occurs during failures. Jumps generate uncontrolled overshoots on node dynamics that cross risk limits causing cascade jumps.

Q2 How to design control actions that can handle critical changes in power network dynamics?

A perturbed power network poses operational challenges for which traditional solutions currently are not efficient. A possible approach to control should create adequate disturbance to evaluate the reaction of the system to worst-case events. Also, identify main components affecting the development of this phenomena in order to control its effect. The possible response of the system should be predicted by inferring transitions of the state and the network. Also, primary triggers and propagation failure precursors should be identified. Mixed stochastic - network approach is demonstrated to be useful in order to count with the unpredictability of failure event and propagation. Also, considering the constraints and influence of connectivity in the development. Defense strategies must be designed by the integration of networks and structural properties as a response of main trigger events. Stochastic dynamics and games have been demonstrated as a useful framework to control the network on this failure regime.

Q3 How to reduce the impact of dynamical changes in power networks under critical transitions? How to modify the distance from the critical point in power networks dynamics trough local control actions? Under which conditions it is possible?

Build a threats framework were systems react in different ways to different stimuli. First, use vulnerability analysis to identify the natural response of the system to cascading failures events. Stablish the worst case scenario consider the design of a strategy to get the best response against a failure scenario like that operation conditions and network structure constraints the possibility to mitigate the failure event. Dynamical line rating can be useful to reduce the impact of cascading effects, controlling the transmission line capacity locally dynamically of elements in the propagation paths identified by vulnerability analysis. Actions should be taken considering long-term consequences that those actions could have in the cascading failure. Stochastic prediction of long-term results of mitigation actions in the zero-sum stochastic games should be analyzed in order to select the line candidates for dynamic control of capacity appropriately.

9.3 Directions for Future Research

Some suggested ideas for future directions are outlined next:

- To design a resilient control strategy for transmission network reconfiguration, considering generation/demand uncertainty and failure events. Network reconfiguration is proposed as a strategy to overcome all possible operating scenarios, voltage violations, and line overload in power networks. The objective of network reconfiguration is to reduce power losses during operation. The primary concern for its application is the possible loss of connectivity and its consequences for network security. During this project, we will propose a control strategy for network reconfiguration where operation under uncertainty of failure events an operation scenario due to unpredictable generation/load profiles (e.g., DERs, demand response). The

strategy will work on stochastic games, where network state transitions will be modeled to include all possible network reconfiguration scenarios, and select better response against possible uncertain failure events. Research results previously obtained on the modeling on cascading failure mechanism and stochastic games for systems vulnerability will be used as main concepts for the proposed research. Case studies will be used to validate the effectivity of the proposed approach.

- To design stochastic transmission network planning strategies considering network vulnerabilities and interdependencies. System operators tend to implement more rapidly resilience-enhancing technical capabilities and operation strategies that are available today and to speed the adoption of new capabilities and new strategies as they become available. In this stage, the idea is to enhance traditional network planning methodologies based on linear programming and stochastic linear programming to include constraint related to connectivity properties that improve network resilience. Stochastic approaches will be considered in order to consider the integration of unpredictable renewable energy resources in the planning and use its variable capacity in favor of network support. Optimization-based approaches combined with network science theory will be used as a framework. As a main result, the transmission planning strategy should be tested on failure scenarios with different conditions of the generation /demand profile.

- To study the influence of network topology and interdependency in system vulnerability from a control systems perspective Enhance operator understanding of interdependency and system vulnerability is a crucial task to deal with the emerging threats and challenges that can only be overcome by integrated risk-management approaches. We are interested in study vulnerability due to interdependency from a control system approach, where metrics will be developed to identify the main elements influencing failures spread and the viability of control responses to reduce the failure impact on the different interdependent infrastructures. Case studies combining communication, transport, and energy infrastructures will be assessed.

References

Awad, A., Chapman, A., Schoof, E., Narang-Siddarth, A., & Mesbahi, M. (2015, Dec). Time-scale separation on networks: Consensus, tracking, and state-dependent interactions. In *2015 54th IEEE Conference on Decision and Control (CDC)* (p. 6172-6177). doi: 10.1109/CDC.2015.7403190

Azzolin, A., Dueñas-Osorio, L., Cadini, F., & Zio, E. (2018). Electrical and topological drivers of the cascading failure dynamics in power transmission networks. *Reliability Engineering & System Safety*, *175*, 196-206.

Ba, Q., & Savla, K. (2016, Dec). A dynamic programming approach to optimal load shedding control of cascading failure in dc power networks. In *2016 IEEE 55th Conference on Decision and Control (CDC)* (p. 3648-3653). doi: 10.1109/CDC.2016.7798818

Ba, Q., & Savla, K. (2017). Computing optimal control of cascading failure in dc networks. *ArXiv*, *abs/1712.06064*.

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

Bak, P. (1996). *How nature works : the science of self-organized criticality / per bak* [Book]. Copernicus New York, NY, USA.

Bak, P., & Sneppen, K. (1993). Punctuated equilibrium and criticality in a simple model of evolution. *Physical review letters*, *71*(24), 4083.

Bak, P., Tang, C., & Wiesenfeld, K. (1988, Jul). Self-organized criticality. *Phys. Rev. A*, *38*, 364–374.

Barabási, A.-L., et al. (2016). *Network science*. Cambridge university press.

Beyza, J., M, J. Y., J, G. C., & F, H. R. (2018, Feb). Vulnerability assessment of a large electrical grid by new graph theory approach. *IEEE Trans. Latin America Transactions*, *16*(2), 527-535.

Bialek, J., Ciapessoni, E., Cirio, D., Cotilla-Sanchez, E., Dent, C., Dobson, I., ... Wu, D. (2016, Nov). Benchmarking and validation of cascading failure analysis tools. *IEEE Transactions on Power Systems*, *31*(6), 4887-4900.

Bienstock, D. (2011, Dec). Optimal control of cascading power grid failures. In *2011 50th IEEE Conference on Decision and Control and European Control Conference* (p. 2166-2173).

Bienstock, D. (2015). *Electrical transmission system cascades and vulnerability*. Philadelphia, PA: Society for Industrial and Applied Mathematics. doi: 10.1137/1.9781611974164

Bilis, E. I., Kröger, W., & Nan, C. (2013, Dec). Performance of electric power systems under physical malicious attacks. *IEEE Systems Journal*, *7*(4), 854-865.

Blanchard, P., Cessac, B., & Krüger, T. (1997). A dynamical system approach to soc models of zhang's type. *Journal of Statistical Physics*, *88*(1), 307–318.

Blanchard, P., Cessac, B., & Krüger, T. (2000). What can one learn about self-organized criticality from dynamical systems theory? *Journal of Statistical Physics*, *98*(1), 375–404.

Bompard, E., Pons, E., & Wu, D. (2012, Sep.). Extended topological metrics for the analysis of power grid vulnerability. *IEEE Systems Journal*, *6*(3), 481-487.

Brummitt, C. D., Barnett, G., & D'Souza, R. M. (2015). Coupled catastrophes: sudden shifts cascade and hop among interdependent systems. *Journal of The Royal Society Interface*, *12*(112).

Brummitt, C. D., D'Souza, R. M., & Leicht, E. A. (2012). Suppressing cascades of load in interdependent networks. *Proceedings of the National Academy of Sciences*, *109*(12), E680-E689.

Campbell, J., C.and Ruths, Ruths, D., Shea, K., & Albert, R. (2015). Topological constraints on network control profiles. *Scientific Reports*, *5*.

Carlson, J., Haffenden, R., Bassett, G., Buehring, W., Collins III, M., Folga, S., ... Whitfield, R. (2012). *Resilience: Theory and application.* (Tech. Rep.). Argonne National Lab.(ANL), Argonne, IL (United States).

Caro-Ruiz, C., Pavas, A., & Mojica-Nava, E. (2016, Sep.). Voltage distributed control for power networks with ders. In *2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (p. 1-5).

Caro-Ruiz, C., Pavas, A., & Mojica-Nava, E. (2017, Oct). Desynchronization of pulse-coupled oscillators in cycle networks: A hybrid systems approach. In *2017 IEEE 3rd Colombian Conference on Automatic Control (CCAC)* (p. 1-5).

Caro-Ruiz, C., Lombardi, P., Richter, M., Pelzer, A., Komarnicki, P., Pavas, A., & Mojica-Nava, E. (2019). Coordination of optimal sizing of energy storage systems and production buffer stocks in a net zero energy factory. *Applied Energy*, *238*, 851 - 862.

Caro-Ruiz, C., & Mojica-Nava, E. (2015a, Oct). Centrality measures for voltage instability analysis in power networks. In *Proceedings of the IEEE 2nd Colombian Conference on Automatic Control (CCAC)* (p. 1-6). doi: 10.1109/CCAC.2015.7345182

Caro-Ruiz, C., & Mojica-Nava, E. (2015b, Oct). Voltage collapse analysis in a graph theoretical framework. In *Proceedings of the IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM)* (p. 667-672).

Caro-Ruiz, C., Pavas, A., & Mojica-Nava, E. (2016). Controllability criterion for random tree networks with application to power systems. In *Proceedings of the 2016 IEEE Conference on Control Applications (CCA)* (pp. 137–142).

Carreras, B. A., Reynolds-Barredo, J. M., Dobson, I., & Newman, D. E. (2019). Validating the opa cascading blackout model on a 19402 bus transmission network with both mesh and tree structures. In *Electrical and Computer Engineering Conference Papers, Posters and Presentations.* (Vol. 64).

Carroll, L., & DAL, S. (2015). *Alice's adventures in wonderland: 150th anniversary edition*. Princeton University Press.

Cetinay, H., Kuipers, F. A., & Mieghem, P. V. (2018, Sept). A topological investigation of power flow. *IEEE Systems Journal*, *12*(3), 2524-2532.

Cetinay, H., Soltan, S., Kuipers, F. A., Zussman, G., & Mieghem, P. V. (2018). Comparing the

effects of failures in power grids under the ac and dc power flow models. *IEEE Transactions on Network Science and Engineering*, 1-1.

Chen, G., Dong, Z. Y., Hill, D. J., Zhang, G. H., & Hua, K. Q. (2010). Attack structural vulnerability of power grids: A hybrid approach based on complex networks. *Physica A: Statistical Mechanics and its Applications*, *389*(3), 595-603.

Chen, Y.-Z., Huang, Z.-G., & Lai, Y.-C. (2014). Controlling extreme events on complex networks. *Scientific reports*, *4*.

Chen, Y.-Z., Huang, Z.-G., Zhang, H.-F., Eisenberg, D., Seager, T. P., & Lai, Y.-C. (2015). Extreme events in multilayer, interdependent complex networks and control. *Scientific reports*, *5*.

Cheng, M. X., Crow, M., & Ye, Q. (2016a). A game theory approach to vulnerability analysis: Integrating power flows with topological analysis. *International Journal of Electrical Power & Energy Systems*, *82*, 29 - 36.

Cheng, M. X., Crow, M., & Ye, Q. (2016b). A game theory approach to vulnerability analysis: Integrating power flows with topological analysis. *International Journal of Electrical Power & Energy Systems*, *82*, 29 - 36.

Chu, C., & Iu, H. H. (2017, June). Complex networks theory for modern smart grid applications: A survey. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *7*(2), 177-191.

Coelho, E. P. R., Paiva, M. H. M., Segatto, M. E. V., & Caporossi, G. (2018). A new approach for contingency analysis based on centrality measures. *IEEE Systems Journal*, 1-9.

Como, G. (2017). On resilient control of dynamical flow networks. *Annual Reviews in Control*, *43*, 80 - 90.

Cornelius, S. P., Kath, W. L., & Motter, A. E. (2013). Realistic control of network dynamics. *Nature communications*, *4*.

Corral, A., & Díaz-Guilera, A. (1997). Symmetries and fixed point stability of stochastic differential equations modeling self-organized criticality. *Physical Review E*, *55*(3), 2434.

Cuffe, P., & Keane, A. (2017, Sept). Visualizing the electrical structure of power systems. *IEEE Systems Journal*, *11*(3), 1810-1821.

Cupac, V., Lizier, J. T., & Prokopenko, M. (2013). Comparing dynamics of cascading failures between network-centric and power flow models. *International Journal of Electrical Power & Energy Systems*, *49*, 369-379.

Dey, P., Mehra, R., Kazi, F., Wagh, S., & Singh, N. M. (2016, July). Impact of topology on the propagation of cascading failure in power grid. *IEEE Transactions on Smart Grid*, *7*(4), 1970-1978.

Díaz-Guilera, A., & Arenas, A. (2008). Phase patterns of coupled oscillators with application to wireless communication. In *Bio-inspired computing and communication* (pp. 184–191). Springer.

Di Muro, M. A., Valdez, L. D., Rêgo, H. A., Buldyrev, S., Stanley, H., & Braunstein, L. A. (2017). Cascading failures in interdependent networks with multiple supply-demand links

and functionality thresholds. *Scientific reports*, *7*(1), 15059.

Dinh, T. N., & Thai, M. T. (2015, June). Network under joint node and link attacks: Vulnerability assessment methods and analysis. *IEEE/ACM Transactions on Networking*, *23*(3), 1001-1011.

Dobson, I., Carreras, B. A., Lynch, V. E., & Newman, D. E. (2001, Jan). An initial model fo complex dynamics in electric power system blackouts. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences* (p. 710-718).

Dobson, I., & Newman, D. E. (2017). Cascading blackout overall structure and some implications for sampling and mitigation. *International Journal of Electrical Power and Energy Systems*.

Dorogovtsev, S. N., Goltsev, A. V., & Mendes, J. F. (2008). Critical phenomena in complex networks. *Reviews of Modern Physics*, *80*(4), 1275.

Dwivedi, A., & Yu, X. (2013, Feb). A maximum-flow-based complex network approach for power system vulnerability analysis. *IEEE Transactions on Industrial Informatics*, *9*(1), 81-88.

Ellens, W., & Kooij, R. E. (2013). Graph measures and network robustness. *CoRR*, *abs/1311.5064*.

Fan, W., Huang, S., & Mei, S. (2016). Invulnerability of power grids based on maximum flow theory. *Physica A: Statistical Mechanics and its Applications*, *462*, 977-985.

Fang, J., Su, C., Chen, Z., Sun, H., & Lund, P. (2018, March). Power system structural vulnerability assessment based on an improved maximum flow approach. *IEEE Transactions on Smart Grid*, *9*(2), 777-785.

Fang, Y., Pedroni, N., & Zio, E. (2017, Sept). Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network. *IEEE Systems Journal*, *11*(3), 1632-1643.

Filar, J., & Vrieze, K. (1996). *Competitive markov decision processes*. Berlin, Heidelberg: Springer-Verlag.

Ford, L., & Fulkerson, D. (1987). Maximal flow through a network. In I. Gessel & G.-C. Rota (Eds.), *Classic papers in combinatorics* (pp. 243–248). Boston MA: Birkhäuser Boston.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, *121*, 90 - 103.

Frank, A. (1994). On the edge-connectivity algorithm of Nagamochi and Ibaraki. *Laboratoire Artemis, IMAG, Université J. Fourier, Grenoble*.

Gao, J., Barzel, B., & Barabási, A.-L. (2016). Universal resilience patterns in complex networks. *Nature*, *530*(7590), 307–312.

Gao, J., Liu, Y.-Y., D'Souza, R. M., & Barabási, A.-L. (2014). Target control of complex networks. *Nature communications*, *5*.

Gates, A. J., & Rocha, L. M. (2016). Control of complex networks requires both structure and dynamics. *Scientific reports*, *6*.

Ghanbari, R., Jalili, M., & Yu, X. (2016, Oct). Analysis of cascaded failures in power networks using maximum flow based complex network approach. In *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society* (p. 4928-4932).

Ghosh, S., & Ruths, J. (2016). Structural control of single-input rank one bilinear systems. *Automatica*, *64*, 8 - 17.

Goebel, R., Sanfelice, R. G., & Teel, A. R. (2012). *Hybrid dynamical systems: modeling, stability, and robustness*. Princeton University Press.

Goh, K.-I., Lee, D.-S., Kahng, B., & Kim, D. (2003). Sandpile on scale-free networks. *Physical review letters*, *91*(14), 148701.

Guo, L., Liang, C., Zocca, A., Low, S. H., & Wierman, A. (2018, Dec). Failure localization in power systems via tree partitions. In *2018 IEEE Conference on Decision and Control (cdc)* (p. 6832-6839).

Henneaux, P., Ciapessoni, E., Cirio, D., Cotilla-Sanchez, E., Diao, R., Dobson, I., ... Yao, R. (2018, June). Benchmarking quasi-steady state cascading outage analysis methodologies. In *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)* (p. 1-6).

Hennes, D., Kaisers, M., & Tuyls, K. (2010). Resq-learning in stochastic games. In *Adaptive and Learning Agents Workshop at AAMAS* (p. 8).

Hennes, D., Tuyls, K., & Rauterberg, M. (2009). State-coupled replicator dynamics. In *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 2* (pp. 789–796).

Hill, D. J., & Chen, G. (2006, May). Power systems as dynamic networks. In *Proceedings of the IEEE International Symposium on Circuits and Systems* (p. 4 pp.-725).

Hines, P., & Blumsack, S. (2008, Jan). A centrality measure for electrical networks. In *Proc. 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (p. 185-185).

Hines, P., Blumsack, S., Sanchez, E. C., & Barrows, C. (2010, Jan). The topological and electrical structure of power grids. In *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS)* (p. 1-10). doi: 10.1109/HICSS.2010.398

Hines, P., Cotilla-Sanchez, E., & Blumsack, S. (2010). Do topological models provide good information about electricity infrastructure vulnerability? *Chaos*, *20*(3).

Hines, P. D. H., Dobson, I., & Rezaei, P. (2017, March). Cascading power outages propagate locally in an influence graph that is not the actual grid topology. *IEEE Transactions on Power Systems*, *32*(2), 958-967.

Hoffmann, H., & Payton, D. W. (2014). Suppressing cascades in a self-organized-critical model with non-contiguous spread of failures. *Chaos, Solitons & Fractals*, *67*, 87 - 93.

Jun, W., Barahona, M., Yue-Jin, T., & Hong-Zhong, D. (2010, jul). Natural connectivity of complex networks. *Chinese Physics Letters*, *27*(7), 078902.

Kim, D. H., Eisenberg, D. A., Chun, Y. H., & Park, J. (2017). Network topology and resilience analysis of south korean power grid. *Physica A: Statistical Mechanics and its Applications*, *465*, 13 - 24.

Kuehn, C. (2011). A mathematical framework for critical transitions: Bifurcations, fast–slow systems and stochastic dynamics. *Physica D: Nonlinear Phenomena*, *240*(12), 1020–1035.

Kuehn, C. (2015). The curse of instability. *Complexity*, *20*(6), 9–14.

Le, A. T., & Sankar, R. (2016). Complex network approach for power grids vulnerability and large area blackout. In H. T. Nguyen & V. Snasel (Eds.), *Computational Social Networks, CSoNet 2016. Lecture Notes in Computer Science* (pp. 206–213). Cham: Springer International Publishing.

Liao, W., Salinas, S., Li, M., Li, P., & Loparo, K. A. (2017, Dec). Cascading failure attacks in the power system: A stochastic game perspective. *IEEE Internet of Things Journal*, *4*(6), 2247-2259.

Liu, S., Chen, B., Zourntos, T., Kundur, D., & Butler-Purry, K. (2014, May). A coordinated multi-switch attack for cascading failures in smart grid. *IEEE Transactions on Smart Grid*, *5*(3), 1183-1195.

Liu, X., & Li, Z. (2017, Nov). Local topology attacks in smart grids. *IEEE Transactions on Smart Grid*, *8*(6), 2617-2626.

Liu, Y.-Y., & Barabási, A.-L. (2016, Sep). Control principles of complex systems. *Rev. Mod. Phys.*, *88*, 035006.

Liu, Y.-Y., Slotine, J.-J., & Barabási, A.-L. (2011). Controllability of complex networks. *Nature*, *473*(7346), 167–173.

Lu, Y.-Z., Chen, Y.-W., Chen, M.-R., Chen, P., & Zeng, G.-Q. (2016). *Extremal optimization: Fundamentals, algorithms, and applications*. CRC Press.

Ma, C. Y. T., Yau, D. K. Y., Lou, X., & Rao, N. S. V. (2013, May). Markov game analysis for attack-defense of power networks under possible misinformation. *IEEE Transactions on Power Systems*, *28*(2), 1676-1686.

MAIR, V. H. (2007). *The art of war: Sun zi's military methods*. Columbia University Press.

Marzo, J. L., Calle, E., Cosgaya, S. G., Rueda, D., & Maosa, A. (2018, Aug). On selecting the relevant metrics of network robustness. In *Proc. 2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM)* (p. 1-7).

Moon, H., & Lu, T.-C. (2015). Network catastrophe: Self-organized patterns reveal both the instability and the structure of complex networks. *Scientific reports*, *5*.

Motter, A. E. (2015). Networkcontrology. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *25*(9), 097621.

Motter, A. E., & Lai, Y.-C. (2002, Dec). Cascade-based attacks on complex networks. *Phys. Rev. E*, *66*, 065102.

Moussa, B., Akaber, P., Debbabi, M., & Assi, C. (2018, Feb). Critical links identification for selective outages in interdependent power-communication networks. *IEEE Transactions on Industrial Informatics*, *14*(2), 472-483.

Nabi-Abdolyousefi, M., & Mesbahi, M. (2013, Dec). On the controllability properties of circulant networks. *IEEE Transactions on Automatic Control*, *58*(12), 3179-3184. doi: 10.1109/TAC.2013.2259992

National Academies of Sciences, E., & Medicine. (2017). *Enhancing the resilience of the nation's electricity system*. Washington, DC: The National Academies Press.

Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Review*, *45*(2),

167-256.

Nicolis, G., Prigogine, I., et al. (1977). *Self-organization in nonequilibrium systems* (Vol. 191977). Wiley, New York.

Nie, T., Guo, Z., Zhao, K., & Lu, Z.-M. (2015). New attack strategies for complex networks. *Physica A: Statistical Mechanics and its Applications*, *424*, 248-253.

Noël, P.-A., Brummitt, C. D., & D'Souza, R. M. (2013). Controlling self-organizing dynamics on networks using models that self-organize. *Physical review letters*, *111*(7), 078701.

Noël, P.-A., Brummitt, C. D., & D'Souza, R. M. (2014, Jan). Bottom-up model of self-organized criticality on networks. *Phys. Rev. E*, *89*, 012807.

Pagani, G. A., & Aiello, M. (2013). The power grid as a complex network: A survey. *Physica A: Statistical Mechanics and its Applications*, *392*(11), 2688 - 2700.

Pasqualetti, F., Zampieri, S., & Bullo, F. (2014, March). Controllability metrics, limitations and algorithms for complex networks. *IEEE Transactions on Control of Network Systems*, *1*(1), 40-52. doi: 10.1109/TCNS.2014.2310254

Phillips, S., & Sanfelice, R. G. (2016). Robust asymptotic stability of desynchronization in impulse-coupled oscillators. *IEEE Transactions on Control of Network Systems*, *3*(2), 127–136.

Pi, R., Cai, Y., Li, Y., & Cao, Y. (2018). Machine learning based on bayes networks to predict the cascading failure propagation. *IEEE Access*, *6*, 44815-44823.

Porter, M. A., & Gleeson, J. P. (2016). Dynamical systems on networks. *Frontiers in Applied Dynamical Systems: Reviews and Tutorials*, *4*.

Poudel, S., Ni, Z., & Sun, W. (2018, July). Electrical distance approach for searching vulnerable branches during contingencies. *IEEE Transactions on Smart Grid*, *9*(4), 3373-3382.

Prignano, L., Sagarra, O., & Díaz-Guilera, A. (2013). Tuning synchronization of integrate-and-fire oscillators through mobility. *Physical review letters*, *110*(11), 114101.

Psaltoglou, A., & Calle, E. (2018). Enhanced connectivity index - a new measure for identifying critical points in urban public transportation networks. *International Journal of Critical Infrastructure Protection*, *21*, 22 - 32.

Qi, J., Sun, K., & Mei, S. (2015). An Interaction Model for Simulation and Mitigation of Cascading Failures. *IEEE Transactions on Power Systems*, *30*(2), 804–819. doi: 10.1109/TPWRS.2014.2337284

Ramírez-Llanos, E., & Martnez, S. (2014, June). A distributed algorithm for virus spread minimization. In *2014 American Control Conference* (p. 184-189). doi: 10.1109/ACC.2014.6859279

Requião da Cunha, B., González-Avella, J. C., & Gonçalves, S. (2015, 11). Fast fragmentation of networks using module-based attacks. *PLOS ONE*, *10*(11), 1-15.

Reynolds-Barredo, J. M., Newman, D. E., Carreras, B. A., & Dobson, I. (2016). The interplay of network structure and dispatch solutions in power grid cascading failures. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *26*(11), 113111.

Rincón, R., Pavas, A., & Mojica-Nava, E. (2016, Oct). Long-term voltage stability analysis

and network topology in power systems. In *Proc. 2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)* (p. 1-6).

Saleh, M., Esa, Y., & Mohamed, A. (2018). Applications of complex network analysis in electric power systems. *Energies*, *11*(6).

Sanchez, J., Caire, R., & Hadjsaid, N. (2013, June). Ict and power distribution modeling using complex networks. In *Proceedings of the IEEE PowerTech (POWERTECH) grenoble* (p. 1-6).

Savla, K., Como, G., & Dahleh, M. A. (2014, Jan). Robust network routing under cascading failures. *IEEE Transactions on Network Science and Engineering*, *1*(1), 53-66.

Scheffer, M., Bascompte, J., Brock, W. A., Brovkin, V., Carpenter, S. R., Dakos, V., ... Sugihara, G. (2009). Early-warning signals for critical transitions. *Nature*, *461*(7260), 53–59.

Seo, J., Mishra, S., Li, X., & Thai, M. T. (2015). Catastrophic cascading failures in power networks. *Theoretical Computer Science*, *607*, 306 - 319. (Combinatorial Optimization and Applications)

Shunkun, Y., Jiaquan, Z., & Dan, L. (2016). Prediction of cascading failures in spatial networks. *PloS one*, *11*(4), e0153904.

Soltan, S., Mazauric, D., & Zussman, G. (2014). Cascading failures in power grids: analysis and algorithms. In *Proceedings of the 5th International Conference on Future Energy Systems* (pp. 195–206).

Soltan, S., Mazauric, D., & Zussman, G. (2017, June). Analysis of failures in power grids. *IEEE Transactions on Control of Network Systems*, *4*(2), 288-300.

Song, J., Cotilla-Sanchez, E., Ghanavati, G., & Hines, P. D. H. (2016, May). Dynamic modeling of cascading failure in power systems. *IEEE Transactions on Power Systems*, *31*(3), 2085-2095. doi: 10.1109/TPWRS.2015.2439237

Summers, T. H., Cortesi, F. L., & Lygeros, J. (2016, March). On submodularity and controllability in complex dynamical networks. *IEEE Transactions on Control of Network Systems*, *3*(1), 91-101. doi: 10.1109/TCNS.2015.2453711

Sun, H., & Hill, D. J. (2008). Master stability equations of complex dynamical networks with general topology. *IFAC Proceedings Volumes*, *41*(2), 1547 - 1552. (17th IFAC World Congress)

Sun, K., Hou, Y., Sun, W., & Qi, J. (2019). *Power system control under cascading failures: Understanding, mitigation, and system restoration*. Wiley-IEEE Press.

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. Random House Group.

Taleb, N. N. (2012). *Antifragile: Things that gain from disorder*. Random House, Inc.

Tang, X., Liu, J., & Hao, X. (2016). Mitigate Cascading Failures on Networks using a Memetic Algorithm. *Scientific Reports*. doi: 10.1038/srep38713

Taylor, J., & Hover, F. (2011). Laplacians for flow networks. *SIAM Journal on Discrete Mathematics*, *25*(3), 1349-1364.

Torres, J. A., & Roy, S. (2014, June). Stabilization and destabilization of network processes by sparse remote feedback: Graph-theoretic approach. In *2014 American Control Conference*

(p. 3984-3989). doi: 10.1109/ACC.2014.6858864

Wang, L.-Z., Su, R.-Q., Huang, Z.-G., Wang, X., Wang, W.-X., Grebogi, C., & Lai, Y.-C. (2016). A geometrical approach to control and controllability of nonlinear dynamical networks. *Nature communications*, *7*.

Wang, X., Ko, Y., Kooij, R. E., & Mieghem, P. V. (2015, Oct). A network approach for power grid robustness against cascading failures. In *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)* (p. 208-214).

Wang, Y., Fan, H., Lin, W., Lai, Y.-C., & Wang, X. (2016). Growth, collapse, and self-organized criticality in complex networks. *Scientific reports*, *6*.

Wang, Z., Chen, G., Hill, D. J., & Dong, Z. Y. (2016). A power flow based model for the analysis of vulnerability in power networks. *Physica A: Statistical Mechanics and its Applications*, *460*, 105-115.

Wang, Z., Hill, D. J., Chen, G., & Dong, Z. Y. (2017). Power system cascading risk assessment based on complex network theory. *Physica A: Statistical Mechanics and its Applications*, *482*, 532-543.

Wei, X., Zhao, J., Huang, T., & Bompard, E. (2018, May). A novel cascading faults graph based transmission network vulnerability assessment method. *IEEE Transactions on Power Systems*, *33*(3), 2995-3000.

Werho, T., Vittal, V., Kolluri, S., & Wong, S. M. (2016, Nov). Power system connectivity monitoring using a graph theory network flow algorithm. *IEEE Transactions on Power Systems*, *31*(6), 4945-4952.

Wildie, M., & Shanahan, M. (2012). Metastability and chimera states in modular delay and pulse-coupled oscillator networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *22*(4), 043131.

Yang, Y., Nishikawa, T., & Motter, A. E. (2017). Small vulnerable sets determine large network cascades in power grids. *Science*, *358*(6365).

Yu, W., Chen, G., & L, J. (2009). On pinning synchronization of complex dynamical networks. *Automatica*, *45*(2), 429 - 435.

Yuan, Z., Zhao, C., Di, Z., Wang, W.-X., & Lai, Y.-C. (2013). Exact controllability of complex networks. *Nature communications*, *4*.

Zhai, C., Zhang, H., Xiao, G., & Pan, T. (2017, Dec). Comparing different models for investigating cascading failures in power systems. In *2017 International Workshop on Complex Systems and Networks (IWCSN)* (p. 230-236).

Zhang, X., Kuehn, C., & Hallerberg, S. (2015, Nov). Predictability of critical transitions. *Phys. Rev. E*, *92*, 052905.

Zhang, X., & Tse, C. K. (2015, Sept). Assessment of robustness of power systems from a network perspective. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *5*(3), 456-464.

Zhao, Y., & Cortes, J. (2016). Gramian-based reachability metrics for bilinear networks. *IEEE Transactions on Control of Network Systems*, *PP*(99), 1-1. doi: 10.1109/TCNS.2016

.2548424

Zhou, D., & Elmokashfi, A. (2018). Network recovery based on system crash early warning in a cascading failure model. *Scientific Reports*, *8*(1), 7443.

List of Symbols

Φ^t	edges index with reinforcement
ϕ_m	edges index for reinforcement
$\mathbf{a}$	index vector of parwise interactions among nodes
$\bar{\lambda}$	natural connectivity
β	rate of discount
Δ^{k-1}	$(k-1)-$simplex
κ	capacity rating value
$\lambda(\mathcal{G})$	edge connectivity
λ_i	eigenvalue i
$\mathcal{N}(i)$	set of node neighbours for node i
$\mu(\mathcal{G})$	a minimum cut of $\mathcal{G}$
$\nu^i_{s'}(\pi)$	expected long-term reward for player i
$\pi^i_j(s)$	probability for selection of action j for player i
$\rho(e)$	probability of failure for edge e
σ_{ij}	number of shortest paths from node i to j
$\sigma_{ij}(e)$	number of shortest paths from node i to j that pass through edge e
ς^t_e	network reinforcement vector
$A^i(s)$	set of actions for player i
$B(e)$	betweenness centrality for edge e
$c(v_x, v_y)$	minimum weight of a cut separating nodes v_x and v_y
$d(\mathcal{V}_{i-1}, v_j)$	edges weight sum for edges connecting $\mathcal{V}_X$ and $\mathcal{V}_Y$
D_{hk}	Jump set
f_e	power flow of edge e
$G(\theta, a, p, u)$	jump map

G_β β-discounted stochastic game

$k_{\min}$ minimum node degree

k_{max} maximum degree

L admittance matrix

l length of a walk in the graph $\mathcal{G}$

$L(a)$ Laplacian matrix

$P^i(s^{'})$ immediate expected reward

$Q^i(s^{'})$ Markov probability transition matrix for player i

RoU_e branches overload

$U(\mathbf{\Theta}, \mathbf{a}, \mathbf{p})$ set of load sheeding control actions

x variable of the state space $\mathbb{X}$

$\mathbf{D}$ weighted degree diagonal matrix, $\mathbf{D} \in \mathbb{R}^{n \times n}$

$\tilde{\mathbf{Q}}^+$ pseudoinverse of the weighted laplacian matrix $\tilde{\mathbf{Q}}$

α tolerance parameter

δ^t element of the disturbance sequence $\Delta = (\delta^t)_{t \in \mathbb{N}}$

η overall attack performance

γ_e^t diagonal element in the e-th row of the disturbance matrix $\Gamma^t \in \mathbb{R}^{m \times m}$

$\hat{\mathcal{V}}^t$ set of nodes in the largest connected component $\hat{\mathcal{G}}^t$ at time t

λ^t lost load

λ_{res}^t residual load

λ_2 algebraic connectivity

λ_{init} system initial load

$\langle k \rangle$ average degree

$\mathcal{A}$ attack sequence

$\mathcal{A}^*$ minimum cardinality attack sequence

$\mathcal{D}^*$ subset of the feasible attack set $\mathcal{D}$

$\mathcal{E}^t$ set of active edges at instant t

$\mathcal{G}$ network graph

$\mathcal{G}^t$ network graph at instant t

$\mathcal{I}^t$ set of isolated nodes at the stage t

$\mathcal{V}^t$ set of active nodes at instant t

$\mathcal{V}_b$ nodes without supply or demand

$\mathcal{V}_d$ set of demand nodes

$\mathcal{V}_s$ set of supply nodes

μ_d demand nodes community detection

ν connectivity density index

π^t attack efficiency

ρ^t cummulative fraction of attacked edges at instant t

θ_v element of the voltage angle vector $\mathbf{\Theta} \in \mathbb{R}^n$

$\tilde{b}_{ve}$ element of the v-th row and e column of the weighted incidence matrix $\tilde{\mathbf{B}} \in \mathbb{R}^{n \times m}$

ξ_{ij}^t element of the i-th row and j-th column of the flow routing policy matrix $\mathbf{\Xi}^t \in \mathbb{R}^{m \times n}$

a_{v_i} element of the v-th row and i-th column of the network adjacency matrix $\mathbf{A}$

b_{vi} reciprocal of the transmission line reactance between buses v and i

c_e e-th element of the flow capacity vector $\mathbf{c}^t \in \mathbb{R}^m$

d network density

e e is an element of the edge set $\mathcal{E}$

f_e^t e-th element of the edges flow vector $\mathbf{f}^t \in \mathbb{R}^m$

$g(\delta^t)$ attack reward function

h_{vi} element of the v-th row and i column of the weighted adjacency matrix $\mathbf{H} \in \mathbb{R}^{n \times n}$

k_v node degree

k_v^{ext} number of edges that connect node v to supply nodes

p_v v-th element of the supply/demand vector $\mathbf{p} \in \mathbb{R}^n$

q^t flow bottleneck at the stage t

s cardinality of the minimum edge cut-set $\mathcal{S}$

v v is an element of the node set $\mathcal{V}$

v_s^{vi}, v_d^{vi} virtual source and demand nodes

W weight of an edge cut-set $\hat{\mathcal{S}}$

Appendices

Appendix A

MATLAB Functions for Network-based Analysis

A.1 Network Model

This section presents a set of MATLAB functions used to work over the MATPOWER case file structure with network-based tools.

A.1.1 getId

Purpose Generate a list of node names for elements of the node-set defined by the attribute `type`

Synopsis `[list] = getId(net,type)`

Description The function `getId` generates a list with the node names for elements in a node-set defined by the attribute `type`. Input `net` is the MATPOWER case file. Nodes names are represented by unique strings assigned in `net`. The type attribute specifies the type of node element in `list`. The list of keywords and states for the type attribute value is

- `nodes`: the list consists of all node names.
- `edges`: two column list with the node names for the nodes that each edge connects.
- `loads`: list including the names of the PQ nodes with nonzero load.
- `gen`: the list consists of all PV node names.
- `nogen`: the list consists of all PQ node names.

A.1.2 getGraph

Purpose Create an undirected graph representation of a power system.

Algorithm 7 Function `getId`

Input: $\mathcal{C} = (B, T, \mathbf{p})$, type
Output: list

switch (the value of type)
case nodes**:**
  Generate a list with the network nodes, $v_{list} \leftarrow B_{id}$, list $\leftarrow v_{list}$.
case edges**:**
  Generate a list with the network nodes, $e_{list} \leftarrow [T_{from}, T_{to}]$, list $\leftarrow e_{list}$.
case gen**:**
  for all b^i **do**
    if b^i is slack or b^i is PV **then**
      Add supply node to the list, $v_{list}^{gen} \leftarrow [v_{list}^{gen}, b_{id}^i]$.
    end if
  end for
  list$\leftarrow v_{list}^{gen}$.
case loads**:**
  for all b^i **do**
    if b^i is PQ and l_i is not zero **then**
      Add demand node to the list, $v_{list}^{loads} \leftarrow [v_{list}^{loads}, b_{id}^i]$.
    end if
  end for
  list $\leftarrow v_{list}^{loads}$.
case nogen**:**
  for b^i **do**
    if b^i is PQ **then**
      Add no supply node to the list, $v_{list}^{nogen} \leftarrow [v_{list}^{nogen}, b_{id}^i]$.
    end if
  end for
  list $\leftarrow v_{list}^{nogen}$.
end switch
return List.

Synopsis `[G,adj] = getGraph(net)`

Description The function `getGraph` generates an object `G` with the attributes: Edges and Nodes. The function identifies multiple edges that are incident to the same two vertices and retains only one of the edges. Also, the function generates the adjacency matrix `A` of the graph. Input `net` is the power system described in MATLAB case file format.

See Also :
`getId`.

Algorithm 8 Function `getGraph`

Input: $\mathcal{C} = (B, T, \mathbf{p})$
Output: $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, A
1: Get v_{list} and e_{list}.
2: $\mathcal{V} \leftarrow v_{list}$, list of buses id in $\mathcal{C}$
3: $\mathcal{E}_0 \leftarrow e_{list}$, list of branches in $\mathcal{C}$
4: $\mathcal{E} \leftarrow \mathcal{E}_0 \setminus \mathcal{S}$, where $\mathcal{S} \subseteq \mathcal{E}_0$ and $\mathcal{S}$ is the set of all repeated edges in $\mathcal{E}_0$
5: $\mathcal{G} \leftarrow (\mathcal{V}, \mathcal{E})$ network topology of $\mathcal{C}$
6: $A \leftarrow [a_{ij}]_{N \times N}$ whose rows i and columns j are indexed by $\mathcal{V}(\mathcal{G})$ and $[a_{ij}] = 1$ if an edge exist. Otherwise $[a_{ij}] = 0$
7: **return** $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, A.

A.1.3 getGraphW

Purpose Create an undirected weighted graph representation of a power system.

Synopsis `[G,adjW] = getGraphW(net)`

Description The function `getGraphW` generates an object `G` with the attributes: Edges, Nodes and Weights. The function identifies multiple edges that are incident to the same two vertices and retains only one of the edges. Also, the function generates the weighted adjacency matrix `adjW` of the graph. Input `net` is the power system described in MATLAB case file format. The edge weights are the MVA emergency ratings in the MATPOWER case file.

See Also :
`getId`.

Algorithm 9 Function `getGraphW`

Input: $\mathcal{C} = (B, T, \mathbf{p})$
Output: $\mathcal{G}, W$

1: $\mathbf{c} \leftarrow T_{cap}$, capacity of branches in net
2: Get v_{list} and e_{list}
3: $\mathcal{V} \leftarrow v_{list}$, list of buses id in net
4: $\mathcal{E}_0 \leftarrow e_{list}$, list of branches in net
5: $\mathcal{E} \leftarrow \mathcal{E}_0 \setminus \mathcal{S}$, where $\mathcal{S} \subseteq \mathcal{E}_0$ and $\mathcal{S}$ is the set of all repeated edges in $\mathcal{E}_0$
6: $\mathcal{G} \leftarrow (\mathcal{V}, \mathcal{E}, \mathbf{c})$ network topology of net
7: $W \leftarrow [w_{ij}]_{N \times N}$ whose rows i and columns j are indexed by $\mathcal{V}(\mathcal{G})$ and $[w_{ij}] = c_{e_{ij}}$ if an edge exist. Otherwise $[w_{ij}] = 0$
8: **return** $\mathcal{G}, W$

A.1.4 getGraphTrans

Purpose Get the undirected weighted graph graph representation of a power system excluding generator nodes.

Synopsis `[G,adjT] = getGraphTrans(net)`

Description The function `getGraphTrans` generates an object `G` with the attributes: Edges, Nodes and Weights. The graph excudes the generation buses. The function identifies multiple edges that are incident to the same two vertices and retains only one of them. Also, the function generates the weighted adjacency matrix of the graph. Input `net` is a power system described in MATLAB case file format. The edge weights are the MVA emergency ratings in the MATPOWER case file.

See Also :
`getId`, `getGraphW`.

Algorithm 10 Function `getGraphTrans`

Input: $\mathcal{C} = (B, T, \mathbf{p})$
Output: $\mathcal{G}, W_{trans}$

1: $\mathbf{c} \leftarrow T_{cap}$, capacity of branches in net
2: Get v_{list} and e_{list}
3: $\mathcal{V} \leftarrow v_{list}^{nogen}$, list of buses id in net without generation
4: $\mathcal{E}_0 \leftarrow e_{list}$, list of branches in net
5: $\mathcal{E} \leftarrow \mathcal{E}_0 \setminus \mathcal{S}$, where $\mathcal{S} \subseteq \mathcal{E}_0$, $\mathcal{S}$ is the set of all repeated edges in $\mathcal{E}_0$
6: $c_{e_{ij}} \leftarrow \sum_{e_{ij} \in S_{e_{ij}}} c_{e_{ij}}$ where $\mathcal{S}_{e_{ij}} \subseteq \mathcal{S}$ is the set of all repeated edges between v_i and v_j
7: $W_{trans} \leftarrow [w_{ij}]_{N \times N}$ whose rows i and columns j are indexed by $\mathcal{V}(\mathcal{G})$ and $[w_{ij}] = c_{ij}$ if an edge exist. Otherwise $[w_{ij}] = 0$
8: **return** $\mathcal{G}, W_{trans}$

A.1.5 plotGraph

Purpose Plot graph nodes and edges of the power system

Synopsis `[] = plotGraph(G,type, gen, loads,  cs, ct)`

Description The function `plotGraph` plots the graph nodes and edges of the power system with a layout defined in the attribute `type`. The function input `G` is the graph object. The type attribute specifies the type of node element to list. The list of keywords and states for the type attribute value is

- `graph`: plot the power network topology identifying, by color labels, the generation, neutral and load nodes-sets. Requires, as input, the list of generator nodes `gen`, and the list of load nodes `loads`.
- `mincut`: plot the edges in the minimumcut set separating the generation and load node-sets. Requires, as input, the node-sets `cs`, `ct` and the augmented graph with source and sink. These can be obtained by the use of the function `sourceSink`.

Function `plotGraph` pseudocode is shown at next.

See Also :
`getId`, `getGraphW`, `sourceSink`.

Algorithm 11 Function `plotGraph`

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{w}), v_{list}^{gen}, v_{list}^{loads}, C_s, C_t$, type
Output: Network figure P

switch (the value of type)
case graph**:**
  Generate plot P of $\mathcal{G}$;
  Highlight in red the supply nodes listed in B_{list}^{gen}
  Highlight in green the demand nodes listed in B_{list}^{loads}
case mincut**:**
  Generate layered plot P of $\mathcal{G}$ for source node set C_s, and sink node set C_t;
  plot edge weights $\mathbf{w}$
  highlight $\mathcal{E}$ in black
  highlight C_s in red
  highlight C_t in green
end switch
return Network figure P

A.1.6 edgeList

Purpose Get an ordered list of edges

Synopsis `[list]= edgeList(G,type)`

Description The function `edgeList` creates an ordered edge list with an attribute `type`. The function input `G` is the graph object. The type attribute specifies the order of the element in `list`. The list of keywords and states for the type attribute value is

- `random`: list of edges in random order.
- `high-high`: list of edges in sorted order by decreasing node degree for each vertices where the edge incides.
- `high-low`: list of edges in sorted order by decreasing node degree and increasing node degree for each vertices where the edge incides, respectively.
- `low-low`: list of edges in sorted order by increasing node degree for each vertices where the edge incides.

Algorithm 12 Function `edgeList`

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, type
Output: $\mathbf{e}_{orden}$

1: **for** all $e_{ij} \in \mathcal{E}$ **do**
2: Get degree of v_i, $\delta_e(v_i) \leftarrow \sum_k a_{ik}$
3: Get degree of v_j, $\delta_e(v_j) \leftarrow \sum_l a_{jl}$
4: Sum the degrees for edge e, $D_e \leftarrow \delta(v_i)_e + \delta(v_k)_e$
5: **end for**
6: **switch** (the value of type)
7: **case** random**:**
8: Assign randomly all elements from $\mathcal{E}$ to $\mathbf{e}_{orden}$
9: **case** high-high**:**
10: Get a sorted list of edges such that $\mathbf{e}_{orden} \leftarrow (e^1, e^2, ...)$ such that $e^1 = e_{ij}$, $e^2 = e_{kl}$ and $\delta_e(v_i) \geq \delta_e(v_k)$, $\delta_e(v_j) \geq \delta_e(v_l)$
11: **case** high-low**:**
12: Get a sorted list of edges such that $\mathbf{e}_{orden} \leftarrow (e^1, e^2, ...)$ such that $e^1 = e_{ij}$, $e^2 = e_{kl}$ and $\delta_e(v_i) \geq \delta_e(v_k)$, $\delta_e(v_j) \leq \delta_e(v_l)$, $D_{e^1} \leq D_{e^2}$
13: **case** low-low**:**
14: Get a sorted list of edges such that $\mathbf{e}_{orden} \leftarrow (e^1, e^2, ...)$ such that $e^1 = e_{ij}$, $e^2 = e_{kl}$ and $\delta_e(v_i) \leq \delta_e(v_k)$, $\delta_e(v_j) \leq \delta_e(v_l)$
15: **end switch**
16: **return** $\mathbf{e}_{orden}$.