Dynamic improvement of robustness of power transmission grids in decentralized and distributed environments

Master's Thesis in Computer Science

by

Medya Amidi, BSc

2nd July 2012

Delft University of Technology

Computer Science, Information Architecture
Faculty of EEMCS, Faculty of TPM
Delft University of Technology
Delft,The Netherlands
www.ewi.tudelft.nl

Toegepast Natuurwetenschappelijk Onderzoek
Schoemakerstraat 97
Delft, The Netherlands
www.tno.nl

Author
Candidate: Medya Amidi, BSc
Study number: 1289780
Email: medyamidi@gmail.com

Title
Dynamic improvement of robustness of power transmission grids
in decentralized and distributed environments

MSc presentation
12th July 2012

Graduation Committee

Prof. dr. ir. J.L.G. Dietz (chair)	Section Information Architecture, EEMCS Delft University of Technology
Prof.Dr.ir. R.E. Kooij (external supervisor)	TNO, EEMCS
Prof.Dr. F.M. Brazier (daily supervisor)	System Engineering, TPM Delft University of Technology
Dr. E.F.Y. Ogston (daily supervisor)	System Engineering, TPM Delft University of Technology

Abstract

Power transmission networks are large scale complex distributed and networked systems, situated in dynamic environments. Managing such systems is essentially decentralized and distributed. The main function of power transmission grids is to assure the security and reliability of the network and to avoid blackouts. Key elements that can determine the security and reliability in transmitting power are the grids topological structures as well as their physical and operational behaviors and states. The capacity of a network to cope with disturbance imposed on it defines its degree of robustness. In assessing power grids reliability, their robustness and vulnerability against failures (both random failures and intentional attacks) must be taken into account. The secure delivery of power as well as the ability to protect and react to power outage and failures must be done in a distributed environment. Improving the robustness of the grids in distributed environment with no centralized control and management is a challenge. This work propose an effective theoretical method based on complex network approaches for improving robustness of power transmission networks dynamically by reducing their vulnerability in a decentralized and distributed environment. The method is applied to test a grid system to demonstrate its effectiveness on improving the networks robustness.

Contents

List of Figures

List of Tables

Executive Summary

Power transmission networks are large scale complex distributed and networked systems, situated in dynamic environments. Managing such systems is essentially decentralized and distributed. The main function of power transmission grids, aside from proper delivery of power, is to assure the security of the network and to avoid blackouts. This is an essential requirement for today's modern society in which a slightly disturbance in power can cause a disastrous loss in business. Random failures and intentional attacks are two major causes for blackouts to occur. The level of network reliability can thus be assessed based on its tolerance against these failures. Key elements that can determine the security and reliability in transmitting power are the grid's topological structures as well as their physical and operational behaviors and states. The capacity of a network to cope with disturbance imposed on it refers to the grid's level of tolerance. This ability can be determined in terms of network robustness against failures. Therefore measuring robustness of power grid networks can provide strong indications on the level of network's reliability and security.

This work proposes a method based on complex network approaches for dynamically improving robustness of power transmission networks in a decentralized and distributed environment.

There has been extensive research done on robustness of power grids using the theory of complex networks. The reasons for choosing such approaches are that firstly power grids show similar behavior as observed in scale-free and small-world network models introduced in CN theory. Secondly, a complete and detailed analysis and security assessments that takes into account all features of power transmission grids both dynamic of the system as well as structure and their states is almost impossible in a reasonable computational time due to massive size and complex interaction among the network components. And finally CN approaches deal with security problems from more general perspectives.

There are two types of CN approaches in assessing the robustness of power transmission grids: one group is based on purely topological approaches in which important physical properties of electrical power systems are neglected. For this reason, these methods fail to capture the real behavior of power systems and therefore the results they provide are inaccurate in assessing the robustness of the grids. The second group, which includes extended versions of purely topological approaches, takes the power system properties and characteristics into account and thus provides more realistic models to analyze the robustness. However most of these methods studied the performance of transmission grids in terms of their robustness and vulnerability using global metrics and techniques. The problem with such approaches is that in order to assess the robustness, the method needs to have a global picture of the systems: all information about the topology of the network with the associated properties must be known in the first place in order to let the metric to assess the robustness of the network.

Moreover while measuring the robustness of power grids is important, it just provides us descriptive knowledge about the state and structure of the network. There are other concerns related to actions that need to be taken if failures occur. The main questions are how the robustness of the network can be improved so that in case of failures, the performance of the network is less affected and how such improvement can be brought about in a decentralized and distributed environment.

Improving the robustness of the grids in distributed environment with no centralized control and management is a challenge. First of all, since robustness of the network is a global concept, metrics introduced to measure and assess it are global. The challenge here is how to use such global metrics when dealing with distributed systems to improve robustness locally. Secondly, power transmission networks are distributed networks. They need to be designed in such a way that they can adapt changes automatically and manages themselves autonomously. Self-management techniques are needed to let these autonomous entities to operate in such distributed environment. Therefore for these autonomous entities to make local decisions to provide changes, they need to communicate with each other to coordinate their actions. Coordination in distributed environment is challenging since the information these entities base their decision on, is limited to their local knowledge of the environment they are operating in.

To address challenges mentioned above, an effective theoretical method is porposed based on CN approaches for improving robustness of power transmission networks dynamically by reducing their vulnerability in a decentralized and distributed environment.

To improve robustness a distributed algorithm called Weighting Scheme is developed which enables autonomous entities (software agents) to bring local changes at nodes in the network which result in a homogeneous network. In the theory of complex networks, homogeneous networks have a high degree of robustness against failures. Power transmission grids are heterogeneous weighted networks by nature. Thus Weighting Scheme method tries to create a homogeneous network from the original heterogeneous network by means of local manipulations at nodes.

This way it is excepted that the robustness of the obtained network after manipulation imposed by Weighting Scheme algorithm is greater than that of the original network. It is importnant to note that homogeneity is not the optimal criterion for robustness but is a property that can be more easily determined with only local information and it is an indicator of overall robustness.

To examine the reuslt and evaluate the effectiveness of WS algorithm, an extended topological metric called net-ability is used. Net-ability is an extended version of topological global efficiency introduced in complex network theroy which deteremines the global performance of power transmission networks. To assess the robustness of the network the relative drop in net-ability is calculated when network components are failed ((links or nodes are removed).
The results of the experiment show that Weighting Scheme algorithm has indeed improved the robustness of the network: relative drops in net-ability after applying Weighting Scheme algorithm is indeed reduced by each link removal (simulating failures) compared to relative drops in net-ability of the original network. Relative drop in net-ability is a metric to define the network vulnerability. Hence in other words the experiment shows that the vulnerability of the resulted homogeneous network after applying our method is reduced and therefore the robustness of the network is improved. And finally all is done in distributed and decentralized settings. It is important to note that the resulting network is not an optimal homogeneous network (in its absolute sense) where all nodes are topologically equivalent but each node has its local homogeneous topology. Creating a pure homogeneous network is not an objective here.

The method proposed here is applied to a sample power transmission network to demonstrate WS effectiveness on improving the network's robustness in decentralized and distributed environments.

Chapter 1

Introduction to the Problem Statement

1.1 Introduction

Electricity grid is an interconnected network that delivers electricity from producers to the consumers. In industry, the electrical grid is composed of three main components: electricity generation, power transmission and power distribution. The existing grid is strictly a hierarchical system with power plants at the top generating electricity and ensuring that the electricity is delivered to the consumers at the bottom of the hierarchy see 1.1.

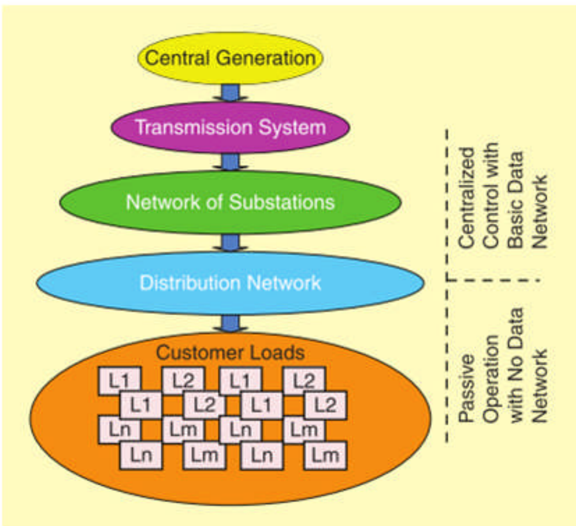

Figure 1.1: Existing grid

Electrical power transmission transfers electrical energy through transmission lines from power plants to electrical substations which are located near demand centers. Most of the transmission lines carry electricity in a long distances and thus to reduce the energy loss they transfer the electricity in high-voltage (110 kV or more). Transmission lines when interconnected with each other, form transmission networks.

The main function of substations is to transfer voltage from high to low or reverse. There are transmission substations which connect transmission lines together and distribution substations which transfer power from the transmission system to the distribution system reducing the voltage to the values that are suitable for local distribution.

A major limitation of distributing power is that electrical power (currently) cannot be stored therefore there must be a sophisticated control system that can match power generation with the demand of energy. If demands exceed the supplies, power plants and transmission lines and equipment can shut down which in turn can cause cascading failures and eventually lead to blackouts. Other reasons of cascading failures are random failures of the (transmission) lines or as a result of intentional attacks. Living in a digital era, even a slightly disturbance in power quality can cause loss of information which can have a disastrous impact on business and economy.

Power transmission grids therefore play a crucial role by assuring the proper functioning of power systems. The main function of transmission grids aside from transferring power is to secure the loads supplied by power generation plants and try to avoid blackouts.

1.2 Plan of Future Grid

As it will be more elaborated in the coming Chapters, there are various concerns and drivers that forces the power grid to move toward a more intelligent grid which can address criteria such as energy reliability, security, efficiency etc. The plan is that every node in the next generation of power grid network (from supplying to transmission and distribution of electricity) will be smart, adaptive, self- healer, proactive, responsive, eco-sensitive, real-time, flexible, and can be interconnected with everything else.

1.3 How to Make Power Grids Smart

The intelligence applied to the current power transmission grid is local and is done by central control and protection systems. The central control systems are most of the time too slow and the protection systems are limited to protection of specific components [38]. To add intelligent to power transmission grids, there is a need for autonomous, smart entities such as software agents than can make decisions, act independently and can communicate and cooperate with others, forming a large distributed computing platform.

1.4 Introduction to The Problem

As mentioned earlier power transmission grids play a critical role in the electricity network. Their main role is to secure delivery and help avoiding failures and blackouts. Power system security assessment deals with system's capability to provide it services under unpredictable circumstances. A key element that can determine the security and reliability in transmitting power is the grid's robustness and its vulnerability since they can determine the impact of failures on the network. Because of the importance of these two concepts, many research and efforts have been devoted to their analysis. This work tries to find a way to improve the robustness of power transmission grids.

1.4.1 Definition of robustness and vulnerability

There are different definitions for network robustness and vulnerability in the literature. Here we adopt the definition provided in [8, 7]. System vulnerability is defined as *"the system inadequacy to withstand a negative situation, limit its consequences, recover and stabilize after the occurrence of the situation."* Generally, *"robustness refers to the ability of a network to avoid malfunctioning when a fraction of its constituents is damaged"*[7].

Robustness is defined as the extent to which the complex network is able to cope with disturbance imposed on it while vulnerability is defined as the extent to which the complex network is unable or inadequate to cope with disturbances imposed on it. Studies have shown that power transmission grids show patterns of reaction to outages and failure similar to complex networks[5, 22].

By definition Complex network is a network that has certain non-trivial topological features that do not occur in simple networks [7]. Therefore a wide range of research in complex network theory in evaluating the vulnerability and robustness of network has been applied to power transmission grids.

Power transmission networks are complex, distributed networks situated in dynamic environments. They are distributed because they are made up of many geographically dispersed components. In assessing their security and reliability, their robustness and vulnerability against failure and outages must be taken into account. The secure delivery of power as well as the ability to protect and react to power outage and failures must be done a distributed environment. The current control and protection systems in transmission networks are central which can be too slow and thus not effective enough to respond to the high demand of reliability and security in a modern society. Many researches have been studied the performance of transmission grids in terms of their robustness and vulnerability using global metrics and techniques. However, the study of how these measurement techniques can be used to improve the robustness or reduce the vulnerability of the grid in distributed environment can provide solutions to these centralized approaches.

> This thesis is therefore to study how to improve the robustness of the transmission grids dynamically by reducing their vulnerability in a decentralized and distributed environment.

1.5 Research Approach

To tackle the problem the first step is to define robustness and vulnerability properly and further find a way to measure them so that it can reflect the properties and characteristics of power transmission networks.

The major thread in transmission network is whether a large blackout occurs. This can happen by either accidental failure of lines due to overload or some other faults but also by intentional attacks. The latter case is usually not random but rather specifically to the most sensitive or critical components of the system. Looking into literature, particularly in the theory of complex networks, there is extensive research done in addressing these failure issues in order to understand the behavior of power grids both in terms of random failure and malicious attacks [5]. Since determining robustness and/or vulnerability of the network can say a lot about the impact of these failures (intentional and random) various measurement techniques have been developed (are being developed) to determine critical components of the network to which network is vulnerable or to define the degree of robustness of the network [41, 46, 48, 7, 2]. However, most of these works use the purely topological approaches which undermine the real behavior and characteristics of power grids. Among metrics and measurement techniques in the literature, [8] introduces a metric to define and measure the global efficiency of the power transmission grids with which the most critical lines can be identified that make the network vulnerable if they are failed. The metric is called Net-ability. The advantage of this metric is that it incorporates real physical properties and characteristics of power grid that are not fully considered in most of the purely topological approaches. However, Net-ability is a metric to define the global efficiency of the network. This means in order to measure the net-ability of the network, one needs to have a whole picture of the network topology.

The next step is how to define improvement in robustness or reduce in vulnerability in terms of Net-ability metric and how to incorporate it as a global performance indicator for local decision making to bring about the improvement. And finally how to do all these works in a distributed setting.

The questions mentioned above form the core of this thesis. Through the following Chapters these questions and relating challenges are elaborated, addressed and answered see Section 1.6.

1.6 Document Outline

Chapter 2 provides a back ground on the Smart Grid: how it evolves, what the forces and drivers are that lead existing power grid to move towards an intelligent grid; what are the characteristics of Smart Grid and finally the state of current development in this domain is explained.

The goal of Chapter 3 is to find out to what extent topological approaches in the field of complex network theory can help to understand power grid networks and their behaviors. To do so, first, we give background knowledge on the theory of complex networks, the types of CNs, their properties and dynamics with particular attention on network robustness and its topological characteristics. Second we explain what makes power grid network a complex network and whether applying approaches in Complex Network Theory can fully capture the characteristics of power grids. To answer this fundamental question the strength and shortcomings of CN field of research are discussed.

In order to understand the behavior of power transmission grids, one should know how the electrical systems work. Chapter 4 provides knowledge on electrical system and power flow study. The concepts such as network impedance and admittance, power flow equations AC and DC models are described in detail. If you have already enough knowledge on this field you may skip this part.

Chapter 5 presents the algorithm approach to address the problem statement mentioned in the Introduction Chapter. Questions such as what and why we want to achieve doing this research will be answered. More elaborated definition of the problem is given. The importance of the problem is clarified. The method and expecting results are explained. After this Chapter, the reader should fully understand the problem, its importance and the method that has been developed to address the problem.

Implementation and experimental design are explained in Chapter 6. Subjects such as how to cast the experiment, what needs to be tested and implemented, the issues encountered during the experiments and the challenges are described.

In Chapter 7 the experimental results are illustrated, interpreted. The findings are discussed and evaluated with what it was expected at the first place. And finally Chapter 8 concludes by discussing the benefits the proposed approach would have for solving the problem of robustness and vulnerability in the distributed decentralized setting and suggestions for future work are provided.

Chapter 2

Smart Grid

2.1 Introduction

This chapter provides a back ground on the Smart Grid. It starts with describing the traditional power grid by explaining its structure, its capacity, and its shortcomings from different economical, technical and operational perspectives. Further the trend is analyzed to clarify the forces and drivers causing the traditional grid move towards an intelligent grid. The concept of Smart Grid is elaborated and important criteria and requirements necessary to realize it are discussed. And finally the current state of developments and research are discussed.

2.2 Traditional Power Grid

The existing electricity grid is unidirectional. It covers only one third of fuel energy to electricity. It has a hierarchical topology of its assets and thus tends to suffer from domino effect failure [25]. It suffers from the loss of energy during transmission and cannot recover the waste heat. To meet the demand peak only 20% of its capacity is used [25]. These are some of the major shortcomings of the existing grid from operational and technical perspectives. From management perspective, the existing Grid has a centralized generation; it is not equipped with self-healing and self-management techniques and if failure occurs manual restoration is the only way to recover. Therefore the grid is vulnerable to failure and as a consequence blackouts can happen.

From the economical perspective, electricity sectors almost everywhere evolved with vertically integrated monopolies and their primary components of electricity supply were integrated within individual firms [33, 27]. Traditional Power Grid is designed as a hierarchical system, managed by monopolist or an oligarchy of actors with a large generating facilities and the network of cables for distributing power to end users [33, 27]. Traditional power grid management systems are limited in scales because of the nature of their centralized decision making. Reducing electricity price paid by consumers is the first reason to introduce competitive power market [34]. In this setting, however, consumers have a little influence on the power market since most consumers have little financial incentive and expertise required in participating into such complex market. Most actors currently contributing in the market are committees composed of trailers, distribution companies, representative for transmission and generators, regulators who are making the decision [34]. Traditionally, increasing demand in energy, increasing in peakiness of energy, or any other pressures are solved by investing in expanding centralized generating capacity and the associated infrastructure [40].

Wholesales markets uses clearinghouse to calculate and distribute prices and to inform participants of winning or losing bids [51]. In such setting only large utilities can participate in the electricity market. Consumers are hence treated as loads requiring energy and thus not as an actor on demand site capable of decision making. Study has shown introducing competitive market only from the supply side and shielding the demand from price liberalization has had serious negative impacts on the market [12, 34]. Enhancing the ability of demand to respond to price signals could benefit both consumers who choose to be actively involved in the market and the market to operate more efficiently. Moreover introducing new resources of energy and power (renewable energy resources); and advanced technologies at hand to address the major shortcomings of the existing grid are the main drivers to push the market to change and power grid to a more intelligent and sophisticated grid.

2.3 Trend

The move from the traditional monopolistic electricity sector towards more competitive wholesale market because of high operation and retailing costs, the development of new technologies, new facilities etc. was the early stage of new evolving trend. Market unbundling in distribution and production of energy is emerging [14, 33, 27]. Entering new players into the energy sector with the ability of producing, distributing and selling energy changes the management and control of the energy market. Form the technological perspectives, new energy generating facilities based on renewable energy resources are developing and becoming widely accessible. The improvement in solar panel technologies, domestic-sized wind turbines, and micro-CHP [51] changes the traditional vision on energy market in which the players where only large utility participants such as wholesales since these technologies provide possibilities for even households to participate in the market. However, to incorporate larger number of participants the decentralization of power grid management systems is essentially required. Thanks to the technological advancement in communications, control systems etc., possibilities for improving power grid management are plausible. Other concerns and drivers that force the current power production and delivery systems to evolve [49] are improvement in reliability and efficiency of electric systems: ”in an increasingly

digital world, even the slightly disturbance in power quality and reliability cause loss of information, processes and productivity...” [26].
As mentioned earlier a strong motivation to move towards an improved, reliable power grid is the impact of grid on business: the business losses caused by grid problems cannot be compromised anymore. Figure 2.1[31] illustrates the annual business losses from grid problems in USA.

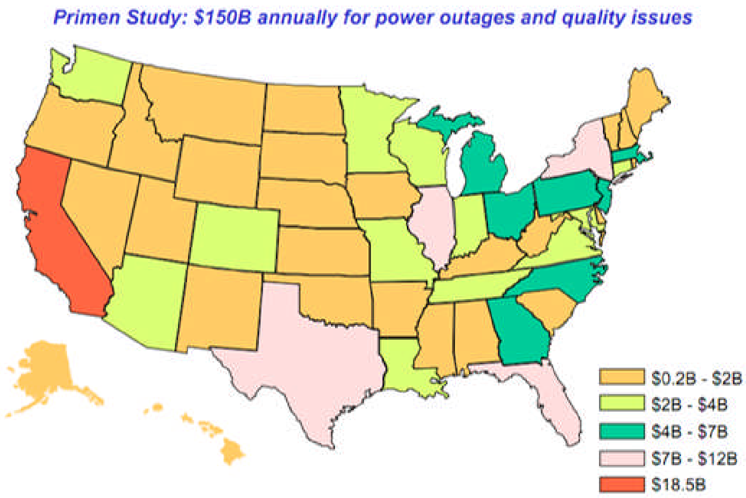

Figure 2.1: Annual Business Losses from Grid Problem

Growing trend in society awareness of more efficient use of energy and desirability of using more sustainable energy; replacement of oil or gas fuel with electricity or other sources of energy [18]; growing demand of energy; aging current infrastructure [18]; and many other forces all demand a changes in the existing power Grid and necessitate the introduction of a more sophisticated and intelligent grid.

2.4 Smart Grid

There is no unique definition of the term Smart Grid. But it sometimes refers to a new scenario of a Grid with the high degree of decentralization in the production of the energy [27], changing the power market in which different actors called prosumers (both producer and consumers) will participate and thus will demand a market with freedom of energy trading [44, 27]. Smart Grid refers to the future of transmission and distribution, systems. The first step in the power grid evolution starts at the distribution side, enabling new applications and operational efficiencies to be introduced into the system. The distribution system of the past is radial and dumb but the future distribution system is meshed and intelligent [38, 11].

A long side of distribution part the infrastructure of transmission grid is quickly

aging. The pressure of increasing demands and insufficient investment for improvement, aging components, environmental challenges (CO2 emission sources, natural catastrophes, lack of space for grid expansion etc.) and market changes, incompatibility of existing infrastructure of grid to accommodate new technologies all emphasize the need of an intelligent, reliable transmission grid. The new transmission grid must be capable of self-healing techniques, advanced control, sensing and monitoring systems to provide the reliability that is needed.
As the system is required to be intelligent, communication and data management will play an important role in realization of this intelligence.

From functional perspective the introduction of Smart Grid is the result of required new generation of power grid being able to, among others, self-healing, high reliability and scalability, real-time pricing, energy management, power quality [11]. It needs to provide utility companies to have full control and monitoring on their services.

From the technical perspectives, in the future grid, very large number of distributed (renewable) energy sources will be connected to the existing grid. There will be physically distributed generation installations (e.g., gas turbines, micro turbines, fuel cells, solar panels, wind turbines) connected to existing infrastructure. Since these distributed renewable energy resources are intermittent (they enter and leave the grid due to their availability), the new generation of power grid must address the dynamic behavior of both distribution and transmission networks. The Smart Grid should be capable of incorporating new technologies such as advanced metering, distribution automation, low-cost communication and distributed energy resources.

Aforementioned requirements explain why distribution grid and network infrastructure become highly important and why they require major updates. The main role of the high voltage grid will change and since the grid involves prosumers at rather local level, medium and low voltage grids will be also involved [27]. The realization of (functional and constructional) requirements of Smart Grid depends on how to incorporate new technologies. There have been many attempts to make use of these technologies for the future grid, however these project are more tend to use technologies in isolation rather than create an integrated Smart Grid which make use of variety of technologies [11].

In short a new generation of grid, Smart Grid, is needed to address these requirements: Energy Efficiency, Reliability, Renewables, Security, Dynamic behavior, Economy, Cost Reduction, Consumer Choice, Energy Independence, and Climate Change.

2.5 Current Development on Smart Grid

There are many research and development activities going on focusing on different aspects of the new generation grid from economic to functional and technical characteristics. Projects have been conducted in distribution area to investigate the impact of Smart Grid on the existing distribution systems and to understand how the changes can be implemented so that existing distribution systems can be transformed into the Smart Grid in the future. Some of these projects are summarized in the subsections here below.

2.5.1 EPRI IntelliGrid

The Electric Power Research Institute (EPRI's) IntelliGrid initiative founded in 2001 started its vision by linking communication advancement to the infrastructure of power grid to create reliable, automated, resilient electricity delivery systems with advanced costumer services. The aim of the project is to develop, apply, and integrate technology advances to facilitate power grid to meet requirements mentioned earlier. The intelligent self-healing grid is able to do so by, for instance, sending, receiving and processing data on the systems conditions using health metrics, power flows, and further communicating these information among intelligent devices, generators, systems operator and customers. The key projects held by EPRI IntelliGrid are Fast Simulation and Modeling (FSM) developing a software system to simulate and model the power grid dynamics; communication for Distributed Energy Resources (DER) to encompass highly automated distribution systems with flexible electrical system architecture operated via open architecture communication systems; Consumer Portal and monitoring systems.

2.5.2 Modern Grid Initiative

The modern Grid Initiative established by the U.S. Department of Energy (DOE) in 2005 through the Office of Electricity Delivery and Energy Reliability (OE) and the National Energy Technology Laboratory (NETL). Their program is to modify the traditional approach of developing today's grid. Each project will involve national and regional stake- holders and multiple funding parties. Benefiting by blending both traditional centralized approach and distributed resource, demands response, networked distribution systems, and advanced operational tools they try to minimize the negative aspects of centralized and distributed approaches. Their focus is on six key goals:

- **Reliability** - a grid that withstands disturbance, failure and provides a quality that is acceptable for today's need.
- **Security** - a grid that withstands physical and cyber-attack.
- **Efficiency** - more efficient power production, transmission and improved asset utilization, cost and power flow control.

- And finally the modern grid should be **safe**, **harmless**, and **environmental friendly**.

2.5.3 CSIRO

Commonwealth Scientific and Industrial Research Organization is the national government body for scientific research in Australia. It was founded in 1926 originally as the Advisory Council of Science and Industry. The project focusing on Smart Grid is aimed at utilizing ICT technological advancements to increase efficiency in energy use and renewable energy resources. CSIRO's smart energy technologies are aimed for use in the home, in commercial buildings and in the energy distribution system. The project includes:

- **A smart grid**: management of electricity supply and demand by coupling advanced communication and sensing technology with smart metering infrastructure.
- **An open-access demand management service**: cost effective and efficient use of energy for small consumers such as householders and small businesses as it is for large industries.
- **A virtual power station**: developing virtual power stations grouping together renewable energy sources such as solar panels and wind farms and integrate them with the grid by using advanced control systems and artificial intelligence.
- **Smoothing out renewables**: one of the characteristics of renewable energy resources is that they are intermittent. The project goal is to overcome such complication by using Ultrabattery and further developing algorithms to optimize the battery to store and release energy produced by renewable energy resources such a wind farm to meet demand.
- **Intelligent air-conditioning**: control and management of air-conditioning systems in buildings.
- **Utility simulation tools**: allowing energy utilities to predict effect of their decisions in managing their network on energy use, consumer comfort and customer satisfaction.

There are other programs founded by different institutions and collaborations such as WiseGrid, Advanced Grid Applications Consortium, California Energy Commission- Public Interest Energy Research (PIER) Program, GridWorks focusing on different aspects of Smart Grid, holding various ongoing projects for realization of aforementioned goals for the future grid.

Various ongoing research and development activities in both industry and academia study different aspects of smart grid. [34] explains how consumers and retailers

can actively and effectively participate in the electricity market (from the demand side). In [25] challenges and important aspects in transition path from existing grid towards smart grid are discussed. References [38] presented smart grids for future power delivery. [51] discusses the possibilities that virtual organizations, autonomous systems (represented by software agents or peers capable of self-management) and overlay structures can provide in order to have a self-managing grid that is able to adapt when necessary in the decentralized manner. References [14, 33, 27] study the trend that is emerging in the electrical market. Concepts of cell, MicroGrid, E-market and Virtual Power Plants are introduced and studied in [10, 32, 35, 43]. A wide range of research studies the domain of distributed energy resource management (DER). What the effects of connecting these resources are to the existing grid. How reconfiguration techniques can result in more efficient and effective ways of power supply and matching it with demand site. What the market mechanisms are to coordinate price. How we can deal with the dynamic behavior of the grid. Self-healing techniques, Management structures (centralized versus decentralized and hybrid structures) overlay systems and many other fields of research are used and studied to address different aspects of future grid.
Aforementioned fields and subjects were examples to provide a picture of current state of development of Smart Grid.

Chapter 3

Introduction to Complex Networks

3.1 Introduction

Power systems show behavior similar to small-world networks [19] and scale-free [4, 29]. There have been extensive studies using complex network theory to model, analyze and understand power system networks. A complete and detailed analysis and security assessments that takes into account all features of power transmission grids both dynamic of the system as well as steady state is almost impossible in a reasonable computational time due to massive size and complex interaction among the network components. Therefore topological approaches based on CN are used as alternatives to detailed analyses. This is because they deal with security problems from more general perspectives. For these reasons it is necessary to understand what the theory of complex networks have to offer in analyzing power grid system. Therefore the material of this Chapter is intended to serve a brief overview on the theory of complex network and to answer questions such as: what makes a network a complex network? What are the important properties of such networks? What are different CN models that can be used to study power grids? Network models such as random networks, scale-free networks are introduced. And finally how the theory of complex network can help us to understand power grid and to what extent it can represent the behavior of the grid.

3.2 Complex Networks

The rapidly evolving of complex network theory study has been witnessed in the past few years. Its wide range of applications in different domains includes oil and gas productions, electrical power grids, biological and chemical systems, neural networks, social interacting species, telecommunication, World Wide Web, water supply, public health, transportation systems, financial and security systems [5]. All these networks are examples of systems composed of a large number

of highly interconnected dynamic units. With the advances in complex network field many natural phenomena and complex systems in real world can be modeled and analyzed to solve large scale practical problems. Before, these systems were considered to be completely regular networks but the models based on regular networks couldn't describe and analyze the behavior of these real world networks [22].
There are two aspects of complex networks needed to be considered when studying them: their structures and topologies, and their dynamics. The first addresses issues such as the network's components and their interconnectivity. Moreover it describes the relation between its components and helps us to understand how to model a real world phenomenon and how to mimic its infrastructure and its properties. The latter one concerns the behavior of the network. For instance how the system would interact with its environment or react on changes imposed on it.

Generally speaking, a network can be defined as a set of interconnected nodes. Nodes are fundamental elements of the network. They are connected to each other based on a particular relation in the context they are used. For instance in social network, nodes represent people and their relations are represented by the links connecting them. The relation can be friendship (such as in Facebook) or professional relation (such as in LinkedIn). Nodes can be routers in the Internet, which are connected by physical links such as optical fibers [54]. They can be webpages in the World Wide Web, joined by the so-called hyper-links.

A complex network has non-trivial topological features, i.e., features that do not occur in simple networks. Graph theory is a branch of discrete mathematics in which complex networks have been studied. Formally, a complex network can be represented as a graph. An undirected graph $G = (N, L)$ consists of two sets N (nodes) and L (links) where $N = \emptyset$ and L is a set of unordered (ordered in case of directed graph) pairs of elements of N. In directed graph Links have directions. In undirected graph each link is defined by two nodes i and j it connects and it is denoted as $l_{i,j}$. If the graph is directed the order of i and j in representing the link is important ($l_{i,j} \neq l_{j,i}$). Two nodes joined by a link are referred to as adjacent or neighboring nodes. A weighted graph consists of three sets. Next to nodes and links sets, the third one is a set of values (weights) that are real number attached to the links. Weights represent the strength of the links. If two nodes are not adjacent or neighbors, they still can be reachable from one to the other. A *walk* from node i to node j is an alternating sequence of nodes and edges (a sequence of adjacent nodes) that begins with i and ends with j. The length of the walk is defined as the number of edges in the sequence. A *trail* is a walk in which no edge is repeated. A *path* is a walk in which no node is visited more than once. In an unweighted and undirected graph, the length of a path is the number of edges in a path connecting nodes i and j. The walk of minimal length between two nodes is known as *shortest* or *geodesic* path.
A graph is said to be *connected* if, for every pair of distinct nodes i and j, there is a

path from i to j, otherwise it is said *unconnected* or *disconnected*. A *component* of the graph is a maximally connected subgraph. A *giant* component is a component whose size is of the same order as N (number of nodes in the graph).
Graphs can also be represented in matrix format. A graph $G = (N, L)$ can be completely described by its *adjacency (connectivity)* matrix A, a $N \times N$ matrix, whose entry $a_{i,j}$ ($i, j = 1,..., N$) is equal 1 when the link $l_{i,j}$ exists, and zero otherwise.
The degree (or connectivity) k_i of a node i (in un-weighted/undirected graphs) is the number of edges incident with the node, and is defined in terms of the adjacency matrix A as:

$$k_i = \sum_j a_{i,j} \tag{3.1}$$

In case of weighted graph, connectivity or the degree of the node i is measured by its strength:

$$s_i = \sum_j w_{i,j} \tag{3.2}$$

Where $w_{i,j}$ represents the weight of the link connecting i and j.
If the graph is directed, the degree of the node has two components: the number of outgoing links $k_{i,out}$ and the number of ingoing links $k_{i,in}$. And the total degree will be the sum of these two components.
Degree distribution $P(k)$ is a basic topological property of a graph G, and it is defined as the probability that a node chosen uniformly at random has degree k. It shows basically the fraction of nodes in the graph having the degree k. Note that in the case of directed networks one needs to consider two distributions, $P(k_{in})$ and $P(k_{out})$.
Average shortest path length or characteristic path length is a measure of the typical separation between two nodes in the graph [7].

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} d_{i,j} \tag{3.3}$$

Where N is the number of nodes and $d_{i,j}$ is the length of the shortest path from node i and j. There is one problem with this formula: if there exists a pair of nodes in the graph that are not reachable (there is no path connecting them), the formula above will diverge. To solve the problem of divergence, there is an alternative approach that considers the harmonic mean of shortest lengths [7] which is called *Graph Efficiency*:

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{i,j}} \tag{3.4}$$

E is an indicator of traffic capacity of the network, or an indicator to define global performance of the network [17, 50, 36, 8]. The concept of Graph efficiency is used in many research domains one of which is power grid networks(see ref. 32 and 36 of [7]).

Another important node characterization is the centrality of a node. The communication of two non-neighboring nodes depends on the nodes belonging to the path that connects those two nodes therefore there is a measure called node betweenness that defines the relevance of a given node. It is equal to the number of shortest paths from all nodes to all others that pass through that node. That is why it is also called node centrality. Node betweenness or centrality can be used to define the node's importance to the network as well as indicating the connectivity. Using node's centrality as to define the node's importance to the network is a global effect. Node centrality is originally introduced in study of social networks. See ref. 18 and 19 of [7].
Formally, the betweenness b_i of a node i, sometimes referred to also as load, is defined as:

$$b_i = \sum_{j \neq k} \frac{n_{jk}(i)}{n_{jk}} \tag{3.5}$$

where n_{jk} is the number of shortest paths connecting j and k, while $n_{jk}(i)$ is the number of shortest paths connecting j and k and passing through i.
These are some important network characterizations that we are going to come across in the rest of this document. There are many other important properties such as transitivity, Motifs, community structure etc., which are excluded here because of their irrelevance to this study. For more information please see [7].

3.2.1 Topology of real networks

As mentioned earlier, to study complex real systems such as social networks, World Wide Web, power grids, neural networks etc., we need to model them first: models that can represent their structures and dynamics. The theory of Complex Networks provides us such facilitation. Due to computational advances, powerful and reliable data analysis tools, as well as availability of large databases during last few decades, today we are able to analyze the properties, topologies and the behavior of several networked systems in the real world more accurately. Studies have revealed that most of the real networks share the same topological characteristics and properties despite their inherent differences (see ref. 8,25,80, 28,81-84, 85-88 of [7]). For instance most of real world networks have high clustering coefficients, small characteristic path lengths, fat tailed shapes in the degree distributions and so forth. These features are the ones that distinguish real networks radically from regular and random networks (the standard models studied in mathematical graph theory). This has led to developing new models that can capture the most significant properties of real network empirically observed. Such models are random networks [23, 22] small-world [52, 53, 37, 22] and scale-free networks [6, 22].

3.2.2 Random networks

Erdös and Rényi in 1959 have initiated a study of random graphs by means of probabilistic methods. These methods are intended to study the properties of graphs as a function of the increasing number of random connections. The random refers to the arrangement of node and connection in a random way. The model that Erds and Rnyi had proposed to generate random graph consist of N node and K links and it is called ER random graphs. It starts with N disconnected nodes and then the model starts connecting some randomly selected nodes, prohibiting multiple connections until the number of links is equal to K [7]. Another model of random graphs as an alternative to ER models is connecting some nodes with a probability $0 < p < 1$. For more information about random graphs see [23, 7, 22]. ER random graphs are good models among graphs model but they do not capture most of the real networks properties such as power grids discussed earlier. There are other models found in the literature that tried to extend the ER models which can give a better representation of real networks (see 121, 122, 123, 4, 124 of [7]).

3.2.3 Small-world networks

Small-world property has been observed in many real networks such as biological networks, social networks and technological networks [7]. Studies have shown that power grids, as complex networks, show properties observed in small world networks [52, 8, 27] and thus small-world network models can be good candidates to model power grids and study their topological structures.
In real networks small-world property is related to the presence of clustering with high values of clustering coefficient. Simply, a small-world network is a type of graph model in which most nodes are not neighbors but most nodes are reachable from each other by a small number of hops. Mathematically, small-world network is defined by an average shortest path length L that depends at most logarithmically on the network size N. In other words it is defined to be a network where the distance L between two randomly chosen nodes depends logarithmically on the number of nodes $N : L \approx LogN$.
Watts and Strogatz [7], proposed a model to construct small-world networks as networks that have both small size of L (as in random graph) and high clustering coefficient C (as in regular lattices). Alternative methods to construct small-world networks can be found in (see 126-128 of [7]).

3.2.4 Scale-free networks

Another CN model used widely in power grids studies is scale-free network models since power systems show behavior similar to scale-free networks [4, 29]. Before the introduction of scale-free networks, networks were considered homogeneous. Homogeneity refers to networks in which almost of the nodes are topologically equivalent [7]. For instance in random graph and regular lattices, each of the possible $N(N-2)/2$ links have the same probability and thus the degree distribution is binomial or Poisson in the limit of large graph size. In contrary to these networks, real networks tend to have different degree distributions. Study has shown that most of the real networks display degree distribution followed the power law

$P(k) \approx Ak^{-\gamma}$ with $2 < \gamma < 3$ with the different average degree than that of random and regular lattices. Such networks are called Scale-free networks [7]. In a scale-free network, hence, most nodes have low connectivity but few of them are highly connected to the rest of the network.

3.3 Robustness in complex network

In assessing the security and reliability of power networks the grid's topological structures and their physical and operational behaviors are key elements. The concept of robustness of transmission networks as well as their vulnerability to random failure and attacks can be used as promising indicators in determining the network's security.
Robustness is defined as the extent to which the complex network is able to cope with disturbance imposed on it. Generally, robustness refers to the ability of a network to avoid malfunctioning when a fraction of its constituents is damaged. Here we will give a brief review on issues regarding robustness of the network in both random failure and intentional attack cases. There are two different variant of robustness: static and dynamic robustness. Static robustness refers to topological structure of the network. A network is called robust if disconnecting its components is difficult. For instance in social network when a relationship link is removed, the robustness of the network structure is changed but there is no quantity that needs to be redistributed in the network. Dynamic robustness, however, refers to cases where changes occur in the network, the redistribution of flows needs to be taken into account. For instance, in power grids, when a generation node is failed, we need to redistribute the power flow through other lines and nodes in the grids. Other example is the Internet: when a router is failed, packets passing through it should be redirected and redistributed through other routers in the network. [48] is an example that introduces a metric to measure and determine the dynamic robustness of communication networks. While the static robustness can be treated analytically, dynamic robustness almost relies on the numerical simulations [7].

3.4 Network tolerance to errors and attacks

The ability of the network to withstand random failures and targeted attack refer to the network tolerance to error and attack respectively. By withstand in the context of complex network we mean, the ability (and the extent to which) the network preserves its connectivity properties in case of failure. And thus preventing it to become disconnected and decomposed to isolated islands. Failures (random or targeted) are nodes and/or links deletions or removal. Different types of network illustrate different reactions to such failures. How the network reacts to the failures and what the impacts are (on topological structure or the dynamic of the network) can be explained, determined and measured by network's robustness.
Many complex systems (compared to simple or regular networks) illustrate a high

degree of tolerance against errors. For instance scale-free networks such as power grids [4, 29], World Wide Web [1, 30, 2], Internet [24], social networks are robust against a very high degree of error rates (random failures). This is due to the topological properties of these networks. In scale-free networks a few number of nodes are highly connected to the rest of the network acting as hubs; while most of them have a low connectivity. Thus the probability that random failures cause the network to disconnect is very low. However, these networks are vulnerable against intentional attacks. By targeting those few hubs, the network can easily become disconnected. In contrast random graphs are affected by errors while they are robust against targeted attacks. This is because all nodes in such networks have more or less the same degree of connectivity [2]. Therefore randomly removal of nodes or links can have a greater impact on network connectivity. On the other hand, these networks are robust against intentional attacks since there are no highly connected nodes (hubs) in the network by removing which, network becomes disconnected. Studies have shown that power transmission grids show behavior similar to scale-free and small-world networks. Thus for measuring their robustness and their vulnerability, using complex network models can be a good starting point.

3.5 Power Grid as a complex network

Power systems show behavior similar to small-world networks [19] and scale-free [4, 29]. There have been extensive studies using complex network theory to model, analyze and understand power system networks [19, 47, 56, 58, 28] and see reference 14,15 [4, 29]. Many of them study the issue of cascading failures; analyzing the structural vulnerabilities and robustness of power systems. For instance [15] have analyzed the Italian power grid based on the cascading failure model introduced in [16]. Some of the characterizations of complex network such as betweenness, global efficiency (based on shortest path) are used to study the vulnerability of power systems by identifying the critical links and nodes in power system [21], [13]. However most of these models fail to fully capture the behavior of power systems. The reason is that these models neglect some important physical and operational aspects of the power transmission grids. Here we will list the important properties of power grids that need to be considered when using complex network characterizations to model them as complex networks.

- In power grids electricity does not necessarily flow along the shortest path from node i to node j but along all the paths connecting node i and j.
- Electricity does not flow between all node combinations but only from generators to loads.
- For each pair of generation and load, the network has different transfer capacity when transmitting power.

- Physical properties such as impedance and maximum capacity of lines, operational states must be taken into account.
- Nodes and lines are not identical.
- It is not possible to guide flow of power through a specific path. Almost all lines between source and destination will take part with different contributions.

When studying power transmission grids, one must take two important aspects into account: (1) physical and operational state of the grid, and (2) the topology of the network. The first aspect relates mainly to the dynamic of the system and deals with the flow of power, matching supply and demand and such. The second one relates to the structure and the topology of the transmission networks. Moreover, components in transmission grids such as nodes and lines have each specific attributes and properties both quantitative and qualitative. For instance, nodes which are called buses in power grids can be categorized in three groups: generators, loads and transmission buses. Generators provide (inject) power to the network while loads consume (withdraw) power from the grid. Transmission buses act as intermediate nodes, transmitting power from generators to loads. Each of these nodes has their own properties and hence need to be treated differently. Further Links (branches), too, have their own properties and characteristics:
Transmission lines are characterized by their power flow limit. There are three different types of flow limitations: thermal, voltage drop and steady state stability. Due to their characteristics, transmission lines are not identical too. Therefore approaches that treat power grids as graphs in which nodes and lines are identical tend to be inaccurate to capture the real behavior of the grids and might provide misleading interpretations and results. Another property of transmission lines is impedance of the line. Impedance, as well as flow limits of lines play important role in calculating distance between two nodes. As a consequence the concept of shortest path defined in complex network theory see equation 3.3 will be inaccurate method to measure the distance between nodes.

In general, most of the purely topological models of power transmission grids consider nodes and lines as identical elements. Further they model the network as an unweighted undirected graph. Therefore in these models connectivity of nodes is measured exclusively as the nodes' degree. Moreover to measure network performance and identify critical components some apply metrics such as global efficiency and betweenness [17, 50, 36] assuming that transmitting power can happen from any node to another. All these approaches neglect the physical properties of the grid components and therefore cannot provide accurate models to study power grids' topologies as well as their dynamics.

Some recent developments have tried to incorporate physical and operational features of the grid in their study. In the field of grids' security and studying their robustness and vulnerability we have found [8, 22] that address issues mentioned above. [8] proposes an extended topological approach that includes the definitions of traditional topological metrics (e.g., degrees of nodes and global efficiency) as well as the physical/operational behavior of power grids in terms of real power-flow allocation over lines and line flow limits. The approach proposes new metrics (net ability and entropic degree) to assess grids' vulnerability. Our purpose of this research is to improve robustness of power grids in a decentralized, distributed setting. For this end, we have decided to use these metrics proposed in [8]. But before we explain why these metrics are chosen and how we could use them in our research, we will provide an overview of how exactly electrical power systems function. Next chapter, hence, will provide a summary of electrical power flow study and the concepts such as impedance, admittance, power flow equations will be explained.

Chapter 4

Power Transmission Grids

4.1 Introduction

To define a suitable metric for measuring robustness and vulnerability of power transmission networks, one needs to understand how electrical power systems work and how important properties of power system can be included in the topological approaches for studying power grids. Many studies of power grids vulnerability using complex network approaches haven't included fundamental principles of power system theory and thus have failed to develop accurate models of these systems. Therefore, this Chapter is intended to give a summary of electrical power flow study: a technical background on how power systems work. It can be used as a reference for clarifying some technical terms throughout the documents. It is intended primarily to explain briefly in a very simple way for non-electrical engineers (specially computer scientists) to understand electrical components and their properties as well as power flow studies. Those who have some knowledge about power flow study may skip this Chapter. For more information please see [20].

4.2 Electric Power

Simply speaking, electric power is the mathematical product of two quantities, namely current and voltage. If these tow quantities vary over time then we have AC power and if they are kept in constant level then we have DC power. Digital devices such as computer use DC power while for instance, refrigerators use AC. From economical perspective, DC power will be transmitted over long distance in very high voltages. AC power on the other hand can be easily transform between voltages. This is a very important feature since in transmitting power over long distances at high voltages there would be less loss in energy. Further it is more economical to produce power in high voltages. Since AC power can easily transform for high to low and reverse, it is easier and more manageable to produce power in high voltage at generation and step-down the power near the load.
In power grid system multiple generators and loads are connected that are oper-

ating at the same frequency and number of phases. Loads are nodes or buses to which power is delivered (such as household appliances). Depending on whether they use AC or DC they operate in different voltages and certain frequencies and phases (in case of AC).
At any time the amount of power consumed by loads must be equal to the (net) amount that is supplied by generators. Therefore matching supply and demand is a very important issue and one of the greatest challenges in power systems. Electric power consists of two parts: real or active power (P) and reactive power (Q). In matching power supply and demand both real and reactive power supply must be in line with the consumption (i.e. reactive power just like real power must balance). Real power is the part that is used in load (does useful work) while reactive power heats the wire and cause waste of energy. Therefore engineers take both parts into account and measure them as the magnitude of the vector sum of real and reactive power which is called apparent power.

4.3 Power System Components

Roughly speaking, there are two main components in transmitting power in power systems: buses, and branches. Buses in power systems can be classified in three types: load bus, generation bus and slack bus.

4.3.1 Load bus (PQ bus)

Load bus is a bus at which the real and reactive power are specified and for which the bus voltage is calculated. This is because voltage on a load bus can change with changing loads and that is why they have specified values for P and Q while V varies with load conditions.

4.3.2 Generator bus (PV bus)

Generator bus is a bus at which the magnitude of the voltage is kept constant. Generator buses work efficiently at full load and that is why it is preferred to have them run at their 100% capacities. Most generator buses supply fixed amount of power and their voltage magnitude is kept constant and that is why they have specific P and $\mid V_i \mid$.

4.3.3 Slack bus (swing bus)

Slack bus is a special generator bus which serves as the reference bus in the power system. Its function is to make power flows in the system balanced. It does so by supplying real and reactive power in the system whenever is needed. Therefore these buses (can be only one or more in the power system) won't work at their full capacities as other generator buses do since they need to handle increase and decrease in demand.

4.3.4 Electrical impedance

In electrical engineering the concept of impedance is to measure the opposition of the circuit (in AC system) to the current when voltage is applied. In other words, it is to measure how much the circuit is resisting against the flow of power. Formally, impedance (Z) is a complex ratio of voltage (V) to the current (I) and it is measured in ohms:

$$Z = V/I \tag{4.1}$$

Impedance has magnitude (real part) and phase (imaginary part). Impedance extends the concept of resistance in DC systems. Impedance with zero phase is resistance. In AC system, there are two other elements next to the DC resistance that oppose the flow of power. These two other elements (inductance and capacitance) are referred to as reactance. Reactance forms the imaginary part and resistance forms the real part of complex impedance:

$$Z = R + jX \tag{4.2}$$

where R represents resistance (measured in ohms) and X reactance (measured in ohms). There is another concept called electrical admittance (Y) which is the measure of how easily the circuit will allow a current to flow. Formally, it is the inverse of impedance (Z) and it is defined:

$$Y = Z^{-1} = 1/z \tag{4.3}$$

While impedance is measured in ohms, admittance is measured in siemens. Likewise impedance, admittance is measured in both DC and AC system. In AC system, next to a measure of the ease with which a steady current can flow (DC part represented in the real part), it also measure the dynamic effects (known as susceptance represented as the imaginary part):

$$Y = G + jB \tag{4.4}$$

where Y is admittance, G is the conductance (measured in siemens) and B is the susceptance (measured in siemens).

4.3.5 Branch impedance and admittance

In study of power flow, Transmission lines are represented by their equivalent pi models (impedance in p.u.) with series impedance

$$Z_s = r_s + jx_s \tag{4.5}$$

The equivalent admittance of the line is therefore:

$$Y_s = \frac{1}{z_s} = \frac{1}{r_s + jx_s} \tag{4.6}$$

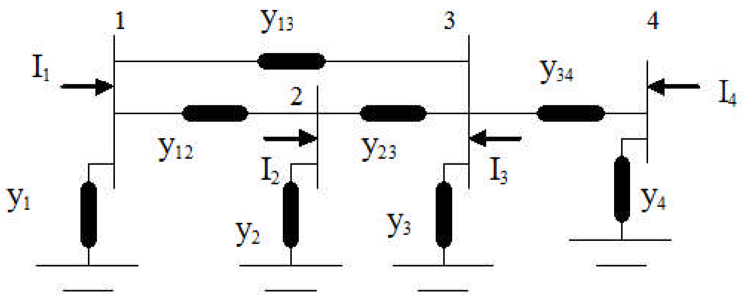

Figure 4.1: Circuit of four nodes and branches

Figure 4.1 below shows a circuit of four nodes (buses) and branches connecting buses and branches to the ground.

The vertical lines with the number above them represent the buses or nodes in the network and lines connecting these nodes are branches with their corresponding admittance values. Y_{ij} represents admittance of the branch connecting node i to node j. The branches to the ground represent shunt elements. A shunt element can be a capacitor or inductor and is modeled as fixed admittance to ground at a bus. It is represented by Y_i at node. $I_1, I_2, I_{3,}$ and I_4 are current injections at buses 1, 2, 3 and 4 respectively. Current injection at a bus is equivalent to power injection. These current injections can be either positive (into a bus) or negative (out of the bus). Current or power flow injection is a nodal quantity (unlike current flow through the branches which is a branch quantity).

4.3.6 Network admittance (Bus admittance) matrix

In calculating power flow, bus admittance matrix (Y_{bus}) is used (in some case bus impedance matrix is considered but in our work we have used bus admittance matrix). One should bear in mind that there is a difference between branch impedance matrix and bus impedance matrix. As said earlier power flow injection at buses is a nodal quantity unlike current flow through the branches which is a branch quantity. The network admittance matrix relates nodal quantities. To understand this relation, consider the network depicted in Figure 4.1. According to Kirchoff's Current Law (KCL), the sum of incoming current (current injections to a bus) must be equal to the sum of outgoing current from that bus, connecting a bus to other buses. Recalling Ohm's Law, $I = V/z = Vy$, the current injection to the bus 1 can be written as: the imaginary part):

$$I_1 = (V_1 - V_2)y_{12} + (V_1 - V_3)y_{13} + (V_1 - V_4)y_{14} + V_1 y_1 \tag{4.7}$$

Note that bus 1 is not connected to bus 4 in this network but it can be represented by a branch whose impedance is infinity and hence whose admittance will be zero therefore the third term in the equation 4.7 will be zero. The reason for doing so is that it allows us to consider that bus 1 could be connected to the bus 4.

Rearranging equation 4.7 will give us:

$$I_1 = V_1(y_1 + y_{12} + y_{13} + y_{14}) + V_2(-y_{12}) + V_3(-y_{13}) + V_4(-y_{14}) \tag{4.8}$$

By doing the same for all the buses in the network (here only bus 2 is illustrated):

$$I_2 = V_1(-y_{21}) + V_2(y_2 + y_{21} + y_{23} + y_{24}) + V_3(-y_{23}) + V_4(-y_{24}) \tag{4.9}$$

we will see that the current injections are linear function of the nodal voltage. Therefore we can write the equations in matrix format. The matrix obtained from all terms of admittances will form the network or bus admittance. This matrix is called Y_{bus}. And for the given network its elements are:

$$\underline{Y} = \begin{bmatrix} y_1 + y_{12} + y_{13} + y_{14} & -y_{12} & -y_{13} & -y_{14} \\ y_{21} & y_2 + y_{21} + y_{23} + y_{24} & -y_{23} & -y_{24} \\ -y_{31} & -y_{32} & y_3 + y_{31} + y_{32} + y_{34} & -y_{34} \\ -y_{41} & -y_{42} & -y_{43} & y_4 + y_{41} + y_{42} + y_{44} \end{bmatrix}$$

Denoting the element in row i, column j, as Y, we rewrite the network admittance matrix given above as:

$$\underline{Y} = \begin{bmatrix} Y_{11} & Y_{12} & Y_{13} & Y_{14} \\ Y_{21} & Y_{22} & Y_{23} & Y_{24} \\ Y_{31} & Y_{32} & Y_{33} & Y_{34} \\ Y_{41} & Y_{42} & Y_{43} & Y_{44} \end{bmatrix}$$

4.4 Power Flow Study

Power flow or load flow studies are tools (involving numerical analysis) to determine the steady-state operation of electric power system and to plan the future

of power system expansion (additional generation, capacitive/inductive VAR supports etc.). They are used to determine if the system remains within specified limits (by for instance, placing capacitors and/or reactors to maintain system voltage within limits) or whether equipment (such as transformers and conductors) are overloaded. Primarily power flow studies calculate: (1) the voltage at each bus (angle θ, and magnitude $\mid V \mid$), (2) power flow (both real P and reactive Q) on all branches, and (3) losses in each branch as well as total system losses. In studying power flow, we make an assumption about either a voltage of a bus or the power supplied to the bus for each bus, and then determine the magnitude, phase angle of bus voltages, and power (current) of lines (which would result from the assumed combination of voltages and power flows).
Power flow study usually uses simplified notion such as per-unit system.
Per unit system is used in power system to express values for voltage, current, impedance, admittance, torque, etc. It is the expression of systems quantities as fractions of a defined base unit quantity (see equation below). Examples of base values can be base power as nominal power of the equipment or base voltage as the nominal voltage of the equipment.

$$Base\ value\ in\ p.u. = \frac{quantity\ expressed\ in\ SI\ units}{Base\ value} \tag{4.10}$$

A simplest way to perform the flow calculation is by iteration:

1. Create bus impedance matrix (Y_{bus}).
2. Make initial estimation for bus voltage for each bus.
3. Update the bus voltage estimate for each bus (one at a time) based on voltage estimate and power flow at every other buses and the values of bus admittance matrix.
4. Repeat the process to make the voltages at each bus approaching the correct answers.

Buses in power systems can be classified in three types: load bus, generation bus and slack bus. To update the estimates for each of these types of bus, different equations are used. As described earlier, load buses have a specified real and reactive power (P_D and Q_D respectively). In the power flow problem these values are assumed to be known and that is why load buses are called PQ buses. On the other hand, generation buses have specified real power (P_G) and the voltage magnitude $\mid V \mid$. And finally slack buses have specified voltage magnitude $\mid V \mid$ and phase θ. These values are assumed to be known in determining the power flow equations as known variables. The values that are unknown and hence need to be calculated are voltage magnitude and angle for each Load buses and the voltage angle for generation bus. In a system with N buses and R generators, there are then $2(N-1)-(R-1)$ unknowns. To solve this we need $2(N-1)-(R-1)$ equations with no more unknown variable. This approach is not computationally possible in system with a large number of buses (for each bus there are two unknown variables out of four: $P, Q, \mid V \mid$ and θ thus we need two equations for each bus). This is a non-linear system of equations problem. Therefore other techniques are used to solve the power flow problem. The famous and most used one is called Newton-Raphson method which is an iterative process. The summary given in this Chapter (on electrical power system; its main components with their properties; power flow problem and basic concepts used to solve it) is intended to provide some primary knowledge on how power systems work. However for detailed elaboration on electrical systems and power flow equations please refer to [20].

Chapter 5

Algorithm Approach

5.1 Introduction

The main function of power transmission grids is to assure the security of the network and to avoid blackouts. Living in a digital era, even a slightly disturbance in power quality can cause loss of information which can have a disastrous impact on business and economy as have been observed in both US (see 291,292, 293 of [7]) and Europe caused by accidental failures. The severe consequences of power networks' failures have indicated possible threads for intentional attacks. Power transmission grids play a crucial role in preventing such disastrous loss by assuring proper functioning of transmission grids. Power system security assessment deals with system's capability to provide it services under unpredictable circumstances. This project aims at finding a method to improve robustness of the transmission grids dynamically (by reducing its vulnerability) in a decentralized and distributed environment.

Key elements that can determine the security and reliability in transmitting power are the grid's topological structures as well as their physical and operational behaviors and states. Due to the importance of transmission network security, there have been extensive research and studies devoted (both in industry and in academia) to find methods and techniques to measure their level of reliability and security. The concept of robustness of transmission networks as well as their vulnerability to random failure and attacks can be used as promising indicators in determining the network's security and reliability.
To determine and measure network robustness and vulnerability the theory of complex network has been applied recently in studying power systems. The reason is that power systems show behavior similar to complex networks (small-world networks and scale-free networks). Moreover, a complete and detailed analysis and security assessments that takes into account all features of power transmission grids both dynamic of the system as well as steady state is almost impossible in a reasonable computational time due to massive size and complex interaction among the

network components. Therefore topological approaches based on CN are used as alternatives to detailed analyses. This is because they deal with security problems from more general perspectives.
The wide range of studies using complex network theory in power system domain is a witness of their applicability in this field [19, 47, 56, 58, 28, 15, 3]. However most of these models fail to fully capture the behavior of power systems. The reason is that these models neglect some important physical and operational aspects of the power transmission grids. In Chapter 3 we have pointed out important characteristics of power grids that need to be considered when using complex network characterizations to model them as complex networks.

While determining and measuring robustness and vulnerability of power grids is important, it just provides us a descriptive knowledge about the state and structure of the network. There are other concerns that are related to actions that need to be taken if failures occur. Questions such as: what can be done if a failure happens; how the robustness of the network can be improved so that (in case of failures), the performance of the network can be less affected; how the cascading effects of these failures can be prevented; how such effects can be controlled; central control approaches are more effective or decentralized approaches; how the network can be less vulnerable towards intentional attacks or accidental failures; how robustness of the network might be affected in a changing and dynamic environment; what can be done to address the distributed nature of power grids and many other concerns need to be discussed and analyzed.

Aforementioned questions relate to the fact that power systems are large scale distributed and networked systems that operate in changing and dynamic environment. Such systems need to be designed in such a way that they can adapt changes automatically and manages themselves autonomously. To adapt changes, self-management techniques can be used which are essentially distributed. This project aims at finding a method to improve robustness of the transmission grids (by reducing its vulnerability) in a decentralized, distributed, and dynamic environment.
To tackle the problem the approached used here consists of three steps:
The first step is to define robustness and vulnerability properly.
The second step is to find or define a metric to measure robustness and vulnerability so that they can reflect the properties and characteristics of power transmission networks.
And finally, the third step is to develop a method (an algorithm) to bring about any improvement dynamically in decentralized and distributed settings.

5.2 Robustness/Vulnerability of Power Transmission Grids

To assess power transmission grids (PTGs) vulnerability and robustness, a suitable metric is needed which takes into account two important aspects: structural and operational robustness. Structural robustness or vulnerability relates to the structure of the power systems (type of nodes and links) and operational relates to the state of the system (for instance load and generation level and distribution). Here we consider only the structural robustness of PTG networks. Generally robustness refers to the ability of the network to cope with negative changes impose on it. Vulnerability however is defined as system inadequacy to tolerate negative changes imposed on it. In general the tolerance of the network to failures refers to the ability of the network to maintain its connectivity after deletion of a fraction of its nodes or lines [7]. However, connectivity properties of the network when defining the robustness is perfectly suitable for network such as World Wide Web (WWW) or Internet.

In general PTG networks can suffer severely without having being disconnected. There are also cases that PTG network performance is not strongly affected when some fraction of the network is indeed disconnected [5]. Therefore, connectivity property would not be a good criterion to define the robustness of PTG networks. Recall from the fact that purely topological CN approaches in assessing the power grids' robustness are not accurate enough, we need to find a metric that takes into account topological as well as physical properties of the power systems. As mentioned earlier:

- In power grids electricity does not necessarily flow along the shortest path from node i to node j but along all the paths connecting node i and j.
- Electricity does not flow between all node combinations but only from generations to loads.
- For each pair of generation and load, the network has different transfer capacity when transmitting power.
- Physical properties such as impedance and maximum capacity of lines, operational states must be taken into account.
- Nodes and lines are not identical.
- It is not possible to guide flow of power through a specific path. Almost all lines between source and destination will take part in transmitting power with different level of contributions.

Metrics for measuring network robustness and vulnerability defined in CN approaches, usually determine robustness of the network by trying to find critical components in the network. This is because by identifying these components, one can assess the vulnerability in case these components are failed.

To find critical components, most CN metrics deal with concepts such as distance between two nodes, the path lengths, network efficiency, average shortest path, centrality of nodes and so on (see Chapter 3). These concepts need to be extended or redefined in such a way that they can represent the behavior of power grids. For instance, distance between two nodes, a generator and a load, in power grids is related more to the links' characteristics such as impedance, voltage drop, transmission losses than the shortest path length. Therefore it is necessary to utilize such properties when identifying critical components in the context of electrical power systems in order to define a proper robustness and vulnerability metric.

5.3 Topological Metrics Applied in PTG

The second step in our approach is to define or choose a suitable metric for measuring PTG robustness. Metrics such as *global efficiency*, *betweenness*, are widely applied in studying PTG. In [22] the concept of betweenness (centrality) is used to define a metric (called centrality index) to calculate the vulnerability of PTG networks. The model is a weighted graph and weights given to the links are based on the maximum power flow through the edges in power grids. Links (branches) which carry more portion of power from the source (generator) to sink (load) are given a higher weight in this analysis. The approach proposed in [22] for defining PTG network vulnerability deals with the state (flow of power) of the network. In [8] the extended version of global efficiency is used to calculate PTG vulnerability which deals with the topological structure of PGT networks. In CN approaches, global efficiency (see ref. 47 of [5]) is used as a metric to evaluate the tolerance of complex networks to outages. The metric is given in Equation 5.1:

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{i,j}} \tag{5.1}$$

Where N is the number of nodes and d_{ij} is the geodesic distance between i and j. The sum is taken over all pairs of nodes of the network. E is used to locate the critical components of the grid. Recall from Chapter 3, geodestic or shortest path between two given nodes is defined (in an un-weighted graph) as the path with minimum length connecting those two nodes. And geodestic distance (d_{ij}) is the length of the shortest path.

Global efficiency E is a metric to measure the performance of the network with the assumption that efficiency for sending any quantities (for instance information) between two nodes i and j is proportional inversely to their distance. By locating critical components in the network using efficiency, (see ref. 49 of [5]) defines vulnerability metric of the network as the amount of drop in network efficiency E when a component (a link or a node) is removed from the network. Equation 5.2 calculates the vulnerability $V_E(l)$ of a line l as the drop in network performance (efficiency) after the removal of l.

$$V_E(l) = \frac{E - E_l}{E} \tag{5.2}$$

Where E is the network global efficiency of the network and E_l is the global efficiency after removal of l. In [8, 9] the definition of global efficiency given in Equation 5.1 is extended to include important physical properties and characteristics of PTG networks. The paper proposes a new metric called *net-ability* (extended version of global efficiency metric used in CN purely topological approaches) to calculate and evaluate network performance and further uses this net-ability to define the extended version of vulnerability given in Equation 5.2.

The three main problems of efficiency E metric given in Equation 5.1 when applied in PTG are:

- In power grids electricity does not necessarily flow along the shortest path from node i to node j but along all the paths connecting node i and j. Therefore the classical idea of shortest distance is not suitable for PTG and hence a new concept of distance needs to be used.
- Electricity does not flow between all node combinations but only from generations to loads. Therefore only the distance between pairs of loads and generators should be taken into account.
- For each pair of generation and load, the network has different transfer capacity when transmitting power. Increase the power injection at node i until the first line reaches its line flow limit determines the transfer capacity of the network at that moment.

[8] argues that net-ability takes into account all three points mentioned above in defining network performance and further vulnerability of PTG. This can be seen in the next part, where the metric and its components as well as structural vulnerability are explained in detail. For more detail please refer to [8, 5, 9].

5.4 Net-ability

5.4.1 Definition

[8] defines net-ability as follows:

> "The net-ability of a transmission grid is a measure of its ability to function properly under normal operating conditions. The ability to function properly depends on the maximum (real or apparent) power that can be allowed to flow over lines, the distribution of power flow among lines and the impedance of lines (technical and economic considerations)."

The first line gives the definition of net-ability as: *"the ability of network to function properly under normal operational conditions"*. In other words, it is a measure of network's global performance under normal operational conditions. Operational conditions relate to load and generation level and distribution; voltage modules and angles, line flows, etc. These elements relate to the dynamic of the power grid systems. They are continuously changing.
The second line in the definition relates to topological structure (nodes and links) as well as physical characteristics of network's elements such as impedance and power flow limits of lines, etc. Power flow paths depend on various physical system parameters (resistance, inductance, conductance and capacitance) that impose limits on flow when transferring power to and from different locations. The impedances of lines quantify the electrical distance in power grids. They affect power distribution over various lines in the grid when power is injected at a bus (generator bus) and withdrawn at another bus (load bus).
The function of power transmission networks is to transmit power flow from generator to load nodes in a most efficient way with respect to both technical and economical perspectives. The economic issues are related to transmission cost and economic efficiency of the market. And technical issues related to voltage drop, power losses and stability issues.
To summarized, net-ability metric is the extended version of the concept global efficiency from CN approaches (explained in the previous part) that includes physical and topological features of power transmission networks to calculate the network performance. The main reason that we have chosen net-ability for our purpose is that in the definition of this metric the main properties of power transmission networks are carefully considered while other metrics in CN approaches neglected to include them. This will be fully understood in the detail explanation of net-ability and its components in the following part.

5.4.2 Net-ability metric and its components

Power Transmission Distribution Factor (PTDF)

In electrical circuits power does not flow along a single path from nodes i to j. It rather flows along all the paths connecting i to j according to power flow study. It is of course of importance to know which one of these links carries bigger portion of power in transmitting it form node i to j. To address this property, there is a concept used in power flow study called power transmission distribution factors (PTDF). It is sometimes called injection shift factors (ISF) or generation shift factors. This concept is related to each line and it describes different contributions of lines in transmitting power from a generator to a load. It is also used to compute the sensitivities of link flows to changes in nodal real power injections at buses and withdrawal at a reference bus. In linear model of power system PTDF can be represented in the matrix format. If H is used to denote PTDF matrix, for a network with N nodes and Y lines then the element in row i and column j, h_{ij} represents the change in the real power flow in line i given a unit increase in the power injected at bus j.

$$H = \begin{bmatrix} h_{11} & ... & h_{1N} \\ ... & ... & ... \\ h_{Y1} & ... & h_{YN} \end{bmatrix}$$

As we repeatedly said, power is transmitted from generators to loads and, hence not through all possible combinations of nodes. And further transmission of power from generator g to load d is not simply through the shortest path between these two nodes but rather involves all lines with different contributions. To calculate the distribution factor for a line i, when transmitting power from a generator g to a load d, we can use matrix H as follows:

The columns corresponding to node g and node d are denoted by $\{h_{ig}\}_{i=1,...,Y}$ and $\{h_{id}\}_{i=1,...,Y}$ respectively. The distribution factor h_i^{gd} of ith line corresponding to power injection at node g and withdrawal at node d is calculated as follows:

$$h_i^{gd} = h_{ig} - h_{id}(i = 1, ..., Y) \tag{5.3}$$

Using PTDF matrix in defining net-ability metric for calculating the network performance makes sure that two main properties of electrical power systems are considered. First power flows from generators to loads (thus not through all combinations of nodes) and power does not flow through a single path (shortest path) when transmitted from a generator i to a load j but rather along all lines connecting i to j with different contribution factors.

The electrical distance

The second concept included in defining net-ability metric is the concept of distance in the context of electrical power systems. The concept of distance can be explained as the difficulty to transfer quantity between two nodes in the network. In general, distance depends on the path that the quantity (here power) passes through. Therefore the concept of distance should contain the property of lines in that path. Recall that in the electrical power systems, the difficulty or cost of transmission through a path depends on both power flow through the lines and on their impedance.

This new concept of distance is called *electrical distance* in [8, 7]. It is defined (in DC power flow model of distance) as the equivalent impedance Z^{gd} from a generation bus g to a load bus d as the impedance between the two buses. Z^{gd} is equal to the voltage V_{gd} between the two buses when $I_g = 1$ (see the definition of impedance in Chapter 4). [8, 5] define Z^{gd} as follows:

$$Z^{gd} = \frac{V_{gd}}{I_g} = V_{gd} \Rightarrow Z^{gd} = (Z_{gg} - Z_{gd}) - (Z_{gd} - Z_{dd}) \tag{5.4}$$

where Z_{gd} is the g-row, d-column term of the impedance matrix of the network impedance (see also the definition of network impedance in Chapter 4).

The transfer capacity

[8] defines transfer capacity of the network from generator g to load d as the power injection at bus g when the first of the lines reaches its maximum power flow limit:

$$C_g^d = MIN_{l\epsilon L}[P_l^{max} / \mid h_l^{gd} \mid] \tag{5.5}$$

Where L is the set of lines in the network, P_l^{max} is the power flow limit of the line l, and h_l^{gd} is the PTDF of line l for power injection at generator bus g and withdrawal at load bus d. Power flow limits of lines are physical property of cables (lines) in transmission network. As we see, transfer capacity of the network when power is transmitted from a generator g to a load d can be calculated by taking into account the power distribution factors of all lines in the network (set of all lines: L) as well as their capacities for carrying power. One of these lines reaches its maximum implies that the network transfer capacity for that specific pair of load and generator reaches its maximum too (when a unit power is injected at g). Thus the network transfer capacity for a specific pair of load and generator can be defined by taking the minimum value of this set.
[8] defines net-ability metric based on the three components mentioned above as follows:

$$A(J) = \frac{1}{N_g N_d} \sum_{g\epsilon G_g} \sum_{d\epsilon D_d} C_g^d \frac{1}{Z_{gd}} \tag{5.6}$$

Where N_g is the number of generators in the network (= dimG_g where G_g is the set of generators) and N_d is the number of loads in the network (= dimD_d where D_d is the set of loads).

The unit for net-ability is MW/V, which indicates with one unit of cost (V) how many benefits (power transmission) can be achieved through the considered network from any generator to any load. This meaning is consistent with the concept of efficiency in CN approaches (see Equation 5.1).
Theoretically, three cases are possible:

1. All generator and load nodes are connected by an ideal channel (bus) with no impedance and infinite power flow capacity. In this case, intuitively, net-ability must be infinite too. According to the definition, net-ability will be infinite.

2. The other extreme is all loads and generators are disconnected and form isolated nodes. Here the net-ability of the network must be zero. All nodes are disconnected implies that they are connected through a channel with infinite impedance and zero power capacity. Thus in the formula terms C_g^d and $\frac{1}{Z_{gd}}$ will be zero and therefore net-ability will zero too.

3. In the real model, loads and generators are connected through lines with different impedances and power flow capacities. Therefore net-ability will be a value between zero and infinity.

5.5 Extended Vulnerability Metric

Similar to CN topological approaches [17, 50, 36] which identify critical components of the network according to relative drop in global efficiency caused by components failure, here the critical components in PTG can be identified by relative drop in net-ability caused by failure of its components. The vulnerability of the network when one of its components is failed is thus defined as:

$$\Delta A^{\gamma} = \frac{A(J) - A(J-1)}{A(J)} \tag{5.7}$$

Where $A(J)$ in the net-ability of the network before removal of any links l, and $A(J-1)$ is the net-ability after line l is removed. ΔA^{γ} calculates the relative drop in net-ability after link removal and hence it indicates the vulnerability of the network towards line l removal. By calculating relative drops in net-ability after each line failure, one can identify the critical lines in the network: the line whose failure causes the greatest drop in net-ability is the most critical line for that specific network.

Now that it is explained what net-ability is and how it is defined and used to determine the vulnerability of power transmission networks, it is the time to move to the next step of our project: how to use net-ability metric to bring about any improvement in robustness of PTG dynamically in decentralized and distributed settings.

5.6 How to Use Net-ability

Previous part discussed the advantages of net-ability metric in applying to power transmission networks. Further it is explained how this metric is used to identify the critical components of the network which in turn can determine the vulnerability of the networks in case of any failures. Although acquiring knowledge about critical components and the structure vulnerability of the network is of high importance (descriptive approach) but there are still important questions which this approach is unable to answer to: ”what can we do with this structural vulnerability?” ”How can we reduce this vulnerability and thus obtain a more robust network against failures?” And recall that power systems are large scale distributed and networked systems that operate in changing and dynamic environment, ”how does the process of robustness improvement (if there is any) proceed dynamically in such distributed and decentralized environments?”

Moreover net-ability is a global metric, i.e., in order to calculate the performance

of the network, it needs to have the whole picture of the network topology. Net-ability is intended to give indications of network vulnerability only for the static topological structure of power grids. Given a network, it can identify the structural vulnerability of the network. Thus it does not provide any solution for the dynamic of power transmission networks.
The purpose of our project is to improve robustness (by reducing the vulnerability) of PTG in decentralized and distributed settings using net-ability as a metric for robustness of the network.
To make this happen, first, there is a need for autonomous, smart entities such as software agents than can make decisions, act independently and can communicate and cooperate with others, forming a large distributed computing platform.
To address decentralized control mechanism, there is a need to develop an algorithm that enables agents (operating in distributed platform) to bring about local changes that lead to a more robust network through local decision making process. And finally to address dynamic improvement of robustness, this algorithm needs to provide local decision making process in real time.
But as we mentioned net-ability is a global metric. The question is: "how can we use this global metric for our local changes provided by software agents?" The solution is we can use net-ability to validate that our local distributed algorithm indeed improves the robustness of the network. In other words, if we can develop a method using which software agents can provide some local changes and manipulation in the system which can result in a network that is more robust compared with that of before manipulation, we have reached our goal. To show that the robustness is indeed improved we can use net-ability to validate our method by illustrating that the relative drop in net-ability is decreased after local manipulation when failures occur.

5.7 Algorithm Approach

Before starting to design our method, we need to build up the hypothesis. The hypothesis is that homogeneous networks are robust against failure. Scale-free network such as power transmission grids are heterogeneous weighted networks by nature. The idea is if we can find a way to obtain a homogeneous weighted network, we can improve the robustness. The expecting result is that "if we have a homogeneous weighted graph we must have less relative drop in net-ability caused by components failure. This implies that the network becomes less vulnerable against failures and therefore the robustness of the network is improved." If the actual results show what is expected we have not only improved the robustness of the grid but also the importance of critical components are reduced accordingly (recall that the critical components in PTG can be identified by relative drop in net-ability caused by failure of its components). But first we need to answer these questions:

- What does homogeneity mean?

- What are the properties of a homogeneous network? And how it is related to power transmission networks?
- And finally how can we build homogeneous PTGs?

In the theory of complex network homogeneity means that almost all nodes are topologically equivalent. This does not mean that nodes are identical but rather their topologies (for instance their degree in un-weighted graphs) are almost equivalent. The degree distribution of random graphs, for instance, is binomial or Poisson. This means that each of the $\frac{N(N-2)}{2}$ links is presented with equal probability. However, scale-free networks on the other hand are highly inhomogeneous with respect to their degree distribution. According to CN approaches power transmission networks can be modeled as scale-free networks. These networks are inhomogeneous in nature: a few ”hubs” in a scale-free network play a similar role as a single center in a star network [54]. While homogeneity in un-weighted graphs means that nodes have more or less the same degree, in weighted graphs it means that links to which a node is connected have more or less the same weights. Recall from chapter 3, in weighted graphs, connectivity or the degree of the node i is measured by its *strength*:

$$s_i = \sum_j w_{i,j} \tag{5.8}$$

Where w_{ij} represents the weight of the link connecting i and j.
[7] argues homogeneous graphs are resistant to failures (both random and intentional attack) and cascading of which. Since scale-free networks are heterogeneous, when studying the dynamic behavior of such systems, they are subjected to an external pressure or load. These systems (as it can be seen in power transmission networks) exhibit a critical point which depends on both the network architecture and the heterogeneity of the nodes' capacities [7]. When a failure occurs (for instance a node or a link is removed), the redistribution of load will happen, for instance power will flow through other available lines and nodes. In such situations, there is a chance that other lines become overloaded (the amount of power willing to flow through them exceeds their capacities). As a result, these lines and nodes will not be able to function anymore and thus cascading failure will happen. There are many defensive strategies to prevent cascading failures. One strategy proposed in (see ref. 299 of [7]) is by selectively removing nodes or links to reduce the size of cascading and to prevent the propagating failure to the rest of the network. Although results show that this method is an efficient strategy defense, but removal always increases the immediate damage on the network. Another strategy is rewiring or adding extra nodes in the network. These strategies have shown improvement in robustness of networks against cascading failure but they change networks' topologies. As mentioned earlier in this part, homogeneous networks have high degree of robustness against failures. Scale-free network such as power transmission grids are heterogeneous weighted networks by nature. Thus

the idea is if we can find a way to obtain a homogeneous weighted network, we can improve the robustness.

5.7.1 Hypothesis

From the discussion above, we know that homogeneous weighted graphs are robust against failure. By homogeneous weighted graph here is meant *a weighted network whose weights are (more or less) evenly distributed*. It is importnant to note that homogeneity is not the optimal criterion for robustness but is a property that can be more easily determined with only local information and it is an indicator of overall robustness. The idea to be tested is if we could obtain a homogeneous power transmission network in which weights of the lines are evenly distributed, we can acquire a more robust network. The main question here is "How can we obtain a homogeneous network in distributed setting?"

One might ask what actually redistribution of weights in power transmission networks means. Weights are physical power flow limits of lines. Manipulation of these capacities means that in some cases they are increased and in others they are decreased. Increasing transmission capacity of transmission lines is a challenging topic in research. There are technologies in development to increase transmission capacities of lines. There are methods for dynamic and static increase technologies proposed in the literature [55]. Real-time Ratings of Transmission Lines is another use of advanced information technologies to expand the capacity of existing transmission systems. Special devices can measure the real-time tension in transmission lines, ambient temperature, wind speed, and/or conductor sag. The drawback with this technology is the high cost relative to the incremental potential increase in capacity [42]. In [45] a method is proposed to increase the thermal capacity of transmission lines. In [42] an online dynamic capacity increase technology of transmission lines is designed.
By increasing and decreasing of capacities in this project is meant, there are control systems that are able to control power flow passing lines. Decreasing (increasing) capacities in PTG or their corresponding weights in the modeled network means reducing (increasing) the maximum amount of power flow that can pass through that line. In practical sense, to be able to control power flow of lines, there is a need for power flow control systems attached to nodes (generators, loads, transmission substations etc.). Other methods are backup-line facilities. Adding backup lines equipped with switches for turning on/off can provide the same effect as increasing and decreasing transmission capacities. New technologies for capacity increase mostly fall into two categories - new materials that may increase the amount of power that can be safely transferred and devices that more finely *control the flow of power*. The disadvantage of many of these new facilities and systems is that they are still being researched and their cost is very high [42].

Now that the idea of the algorithm is explained, we need to answer the question

of ”how can we obtain such homogeneous network by redistributing capacities in distributed setting?”
The next part will answer this question by describing the algorithm. After we will explain what the expected results would be.

5.7.2 Algorithm Design

To design the algorithm, first an abstract topological model of the power transmission networks is made. The model is weighted undirected network consisting of nodes represent buses (generators, loads etc.) and links represent branches in the power transmission network. To each link a weight is assigned representing the power flow capacity of the line. Recall that these weights (capacities) are power flow limits of lines as explained in [5].The model is undirected graph. The reason for this choice is, first of all, net-ability deals with structural vulnerability of the network and thus does not consider the power flow of lines. Secondly our algorithm manipulates the weights which are the capacities of lines, thus including the direction of power flows is not necessary at this point.
Each node further is equipped with a software agent which is able to act and decide autonomously. Further these agents are able to communicate and coordinate with each other for actions they want to take. Since these agents operate in distributed environment, they do not have any global information about the topology and the state of the network. They only have knowledge about their own state and topology: information such as node’s degree (number of links to which they are connected), distribution of weights among these links, and the flow passes through them. Further these agents can only communicate and coordinate with their neighbors by means of sending messages.

WeightingScheme Algorithm

To obtain a homogeneous network in distributed way, we propose an algorithm that enable nodes to redistributes weights among links to which they are connected one node at the time. Each node can readjust its links’ weights by redistributing them *evenly* among those links. The resulting network is not an optimal homogeneous network (in its absolute sense) where all nodes are topologically equivalent but each node has its local homogeneous topology. The algorithm is called WeightingScheme and its mechanism is as follows:
The algorithm will be initiated by a node in the network. Weight adjustment is done sequentially and thus not concurrently, meaning that at a given time only one node will be able to do weight adjustment. The agent at work runs configuration method for weight redistribution. This method calculates the total weights distributed at all links incident to the node at work and further it divides the total weights equally among those links. This way weights are redistributed among links. Note that again one node at the time does redistribution of weights. By doing so, we make sure that no weight adjustment will take place concurrently. This issue is one

of the typical problems in developing distributed algorithm. This situation occurs in distributed environment since agents act autonomously and have no global picture of the system. Further, to make sure no simultaneous manipulation happens, agents will coordinate with each other by means of messaging mechanism: upon receiving messages from neighbors, each agent makes sure whether the incoming message is a duplicate or not. Since each agent must run the algorithm only once, it must react on only one incoming massage and discard other messages. Duplication will happen since each agent will send message to all its neighbors, and therefore there would be cases that agents receive multiple massages from their different neighbors. If so, the message will be discarded, otherwise agent will start the algorithm for weight redistribution. After finishing weight adjustment, the agent will forward message to its neighbors except to the node it has received the message from. The algorithm will finish when all agents run the algorithm once in response to initiation.
Any node in the network can randomly initiate the algorithm. The idea is that in practice a node that is under stress can initiate the algorithm from any point of the network. If so since actions are coordinated by sending and receiving messages, all nodes are guaranteed to run the algorithm once in response to the initiation.
WeightingScheme algorithm consists of four main parts:

- Massage ID to determine who has initiated the message,
- Weight adjustment,
- Message Queuing to keep track of duplicate messages,
- Send and receive mechanism.

Algorithm for each node consists of two parts: Initiate and Respond

Initiate:
Any node can initiate the algorithm–In practice a node can initiate the algorithm if under too much stress.

1. Adjust own weights
2. Add Message to history queue
3. Forward message to neighbors

Respond:
1. Check not duplicate message
2. If not duplicate
   Add message to history
   Adjust weights
   Forward message to all neighbors except the neighbor from which the message is arrived.
3. if duplicate message
   Discard.

Termination criteria:
If all connected nodes have responded to the message.

Figure 5.1: Weighting Scheme Algorithm

Once the algorithm has run by all nodes, it is the time to calculate network's net-ability and further to validate whether the robustness of the network has indeed improved when failures happen. The expecting result is that "if we have a homogeneous weighted graph we must have less relative drop in net-ability caused by components failure. This implies that the network becomes less vulnerable against failures and therefore the robustness of the network is improved." This can be tested by comparing the network's net-ability before and after weights adjustment. Further we can test reduction of the network's vulnerability by comparing the relative drop in net-ability before and after adjustment when components failed one by one. If the actual results show what is expected we have not only improved the robustness of the grid but also the importance of critical components are reduced accordingly (recall that the critical components in PTG can be identified by relative drop in net-ability caused by failure of its components).
Next chapter will describe the experimental design, the platforms and simulation environments used/developed to perform the experiment.

Chapter 6

Experimental Design

6.1 Introduction

Weighting Scheme algorithm is intended to create a homogeneous network in which weights of nodes are evenly distributed. The resulting homogeneous network to be obtained is not an optimal homogeneous network (in its absolute sense) where all nodes are topologically equivalent but rather each node has its local homogeneous topology. The expected result is that the network obtained after algorithm run, is a more robust against components failure.
To develop the Weighting Scheme algorithm and examine its effects on network net-ability we need to cast the experiment and further test it by means of available data set for power transmission grids.
This Chapter is intended to explain briefly the experimental design and its setup. The simulation tools and input data set used are explained as well as important challenged encountered during the design process.

6.2 Experiment

In this section we present the experiment to examine the following questions:

- How is the net-ability of the network affected?
- To what extent is the robustness of the network affected?
- How effective is Weighting Scheme algorithm?
- What are other methods for weight adjustments?
- What are the advantages and disadvantages of other methods compare to Weighting Scheme?
- Does adding communication between agents improve on non-communicative agents?

To cast, develop and implement the experiment, we need two simulation environment (1) an environment in which we can simulate and model physical properties and characteristics of power transmission networks as well as their fundamental objects, features, components to mimic their topologies and behavior. And (2) an environment in which we can simulate the communication between power transmission components for regulating, coordinating and managing changes. Further these two simulation platforms need to be integrated to provide a setting for experimental works.

The first step is to construct a CN model of power transmission networks as well as the features and components that are needed to mimic their topologies and behaviors. In Chapter 5 we have explained the metric net-ability and its components (PTDF matrix, transfer capacity and electrical distance) that we are going to use for measuring the vulnerability and robustness of the network. In Chapter 4 we have explained the main concepts in studying power systems (which is needed to model power transmission networks). Elements such as capacities of transmission lines and network impedance are described. Further AC and DC model of power systems are explained. The experimental model used in [8] is DC model of power system for simulating power transmission networks. Most of the studies use DC model of power system because DC model is a simplified model of AC and thus it reduces the efforts and complexity of calculations. For the same reason we will adopt the DC model in our experiment. To model the power transmission networks we need to have access to power network dataset. Using power system data we need to build an environment to simulate power systems behavior or use the existing tools. And finally for doing experiment in distributed and decentralized setting, we will cast and develop our experiment in a distributed multi-agent simulation environment called AgentScope.

The scenario we consider here is to set up a network representing a real power transmission grid with dynamic links using power system data set available. The topological model of the network (generator and load buses as well as their connections through transmission lines) is made based on CN models: generator and load buses are represented by nodes, transmission lines by links and power flow limits of lines as weights assigned to links.
During the experiment the Weighting Scheme algorithm brings about changes on these links (weight redistribution). These changes will be recorded, and at the end of the experiment net-ability of the network is calculated and graphed over time. Further each link will be removed (simulating failure) one by one, and each time the net-ability will be calculated and displayed in a table. Further generator and load buses each are represented by an agent enabling them to send and receive messages and communicate with other agent nodes for further coordination and manipulation. Production and supply of the energy is not included in this scenario.

Any node in the network can randomly initiate the algorithm. The idea is that in practice a node that is under stress can initiate the algorithm from any point of the network. If so, since actions are coordinated by sending and receiving messages, all nodes are guaranteed to run the algorithm once in response to the initiation. To make sure that the method initiated from any point in the network works correctly, the algorithm is run several times (equal to the number of nodes in the systems), with each time one specific node as an initiator.

6.3 Simulation Tools

In this section we will explain the simulation tools used to build the experiment.

6.3.1 AgentScope

As said in the Section 6.2 to set up the experiment in a distributed and decentralized environment we will use AgentScope interface. AgentScope [39] is a tool (written in JAVA) that supports the experimental stages of multi-agent systems development. It consists of a small set of generic interfaces for:

- Networked communication between agents (such as coordination, negotiation, collaboration, and coalition formation),
- Measurement and analysis of agent behavior,
- The setup of experimental scenarios.

In nutshell AgentScope is a set of generic interfaces designed to make it easy to write, reuse experiments (and their components such as scenarios and metrics). Experiments are divided into three main components: (1) Agent behaviors which are things to be tested and designed, (2) Logs which are things to be recorded, and (3) experimental setup which is the environment agents operate in.

Agent behavior is separated into components called protocols. A protocol is a distributed set of components that collectively provide a specific distributed service. A protocol consists of two parts: the abstract *algorithm* and the *implementation* of that algorithm that provides a particular service to ”agents” located on nodes in a distributed system. Each participating agent runs an instance of the protocol, and collectively these protocol instances provide the service to their agents. A protocol is a distributed service that may have many different implementations. Distributed tasks such as sampling, aggregation, clustering can be seen as services from a higher-level applications. This approach views multi-agent systems as both collection of entities that act autonomously and make decision based on information they can acquire from their environments, and as distributed systems. An agent is made of a set of interacting protocols (distributed services).

The Network Interface provides the methods and classes needed for agent protocol instances to communicate with each other. Each protocol instance has an individual ”address” for communicating with other protocol instances. Communication happens through message exchanges. Upon receiving message, protocol instances are triggered into action in response to ”events” or in response to the request from their agents. Events are set to occur at a particular time.

The Measurement and Analysis Interface defines a generic method of recording protocol behavior during an experiment. This interface provides classes to define which data should be recorded about the protocol's behavior during experimental run and how this data should be manipulated to provide the final output of the experiment.

The Experimental Control interface defines a generic method of setting up experiments so that an experimental scenario can be easily reused, or ported between platforms. A full experimental scenario is an ”experiment” while trials are single runs of that scenario.

In our experiment the protocols used are:

- *GraphGrid* protocol –a subclass of *Grid* protocol, which is used to model the power grid as a network. GraphGrid represents agent node (and its topology) of the grid network. Agent node has information only about its own links. In case of changing weights of links, this protocol makes sure that the agent node on the other side of the link knows about the updated weight value.

- *WeightingSchemeManager* –a subclass of *GridManager* protocol, which is used to bring changes on links (a behavior to test). The Weighting Scheme algorithm is implemented in this class overriding *checkConfiguration* method that is created to bring changes. For each new behavior that we want to test, a new subclass of GridManager must be created that overrides the checkConfiguration method.

To each protocol a Log is attached to record the behavior. In our experiment, *GridLinksLog* class is used to record each change made to a link. This list of changes is then available for analysis. *DynamicGridInitializer* class is used to specify what logs should be created. Since agents are assumed to be distributed (on many machines) each agent has its local Logbook which is used to record data during the experiment run. The AgentScope makes sure that these individual logs are combined to form a single global log at the end of the experiment.

For message to be sent and received by agents in our experiment, *AdjustWeightMessage* class is used (which is a subclass of *Message*). It contains addresses of agent from which message is received and agent to which message is to be sent.

Further it contains messageID which indicates which node is the initiator. messageID is used to check whether the message is a duplicate one: if an agent receives a message of type *AdjustWeightMessage*, it checks in its message history list whether there exists (already) a message of type *AdjustWeightMessage* with the same messageID field. If so, the message will be discarded. Otherwise agent will add it to its message history. messageID has further a counter to keep track of messages forwarded.

As said earlier, a *Trial* is a single run of the full experimental scenario. In our experiment, *BasicRiliabilityTrial* is a Trial that specifies parameters that change between runs and *ReliabilityExperiment* is a full experiment giving the list of all trials. *DynamicGridInitializer* takes *BasicRiliabilityTrial* as input to record changes.

Weighting Scheme algorithm redistributes weights evenly among links. If we want to try out another method (for instance instead of equal redistribution of weights among all links to which a node is connected, we want to develop an algorithm that takes only weights of links with maximum and minimum values and balance their weights) we need to create a subclass of *GridManager*, say *MinMaxManager*, and override the *checkConfiguration* method of this class putting the new algorithm there. Further create a new subclass of Trial, say *MinMaxTrial*, and override the *getGridManager* method of this class to specify the new *GridManager (MinMaxManager)*. And finally add this new trial to the method run in *ReliabilityExperiment* class.

So far we have explained how our experiment can be built using AgentScope tool for simulating the power grid as a multi-agent system operating is a distributed and decentralized environment.
For the second part of the experiment, we need to find a tool for simulating power transmission behavior; physical properties and characteristics of power systems. Further we need to have a real data set of power networks to do the experiment and examine our proposed method.

Most of real power transmission network data are highly confidential. Searching for public data, we came across a simulating software package for power system study with public input data sets of power transmission networks. The simulation tool is called MATPOWER. The tool, however, is written in MATLAB.
We had basically two options: (1) we could generate a series of network configurations from JAVA code of power grid model we have implemented in AgentScope tool and plug in to MATLAB for calculating net-ability and other physical components using MATPOWER tool. Or (2) we could try to develop a simulating tool for power system study in JAVA including calculation of net-ability based on MATPOWER and further integrate this new tool with AgentScope.
The second option requires much more effort to develop and deeper knowledge about how power systems work. However, developing such tool in JAVA and fur-

ther integrate it with AgentScope interface will enhance and extend the AgentScope interface integrating physical and communication networks and provide possibilities for future projects. For these reason we have decided to develop software package for simulating power system study in JAVA based on MATPOWER simulation tool.
To do so, first we need to understand MATPOWER tool. In the next section we will explain MATPOWER software package, its functions and the structure of the input data set that we will be using in our experiment.

6.3.2 MATPOWER

Matpower is a package of MATLAB M-files (An M-file can be either a function with input and output variables or a list of commands). It is a simulation tool for calculating and solving power flow and optimal power flow problems. It employs all standard steady-state models used for power flow analysis. It includes AC as well as DC models. All magnitudes of all values are expressed in per unit.

In Matpower, all branches and buses that are off-line are removed before forming the models used to solve (optimal) power flow problems. All buses are numbered successively starting from 1. All generators are reordered by bus number. Solving (optimal) power flow problems, all generators and branches are assumed to be in-service. Since Matpower is written in Matlab, the models and equations are presented in vector and matrix forms.
To solve (optimal) power flow problems Matpower functionality involves:

1. Preparing the input data
2. Invoking the function to run the simulation
3. Viewing and accessing the results-either printed on the screen or saved in output data structure or files.

Input Data sets

In the input data set, all relevant power system parameters are defined. There are different cases to be simulated and the input data set for each of these cases are specified as a set of data matrices packaged as the *fields* of a Matlab struct, referred to as a "Matpower case" struct and denoted by the variable *mpc*.
In other words, a MATPOWER case file is an M-file or MAT-file that defines or returns a *struct* named mpc, referred to as a "MATPOWER case struct" and the input data for Matpower are specified in a set of data matrices packaged as the *fields* of this struct.
For those not familiar with Matlab, Struct in Matlab is a class of structures. Structure is a data type that groups related data using data containers called fields. Each field can contain data of any type or size. For instance, if we have a struct A with

two fields, namely: fieldName1 and fieldName2, we can assign values to these fields as follows: A.fieldName1 = aValue or A.fieldName2= otherValue. ”aValue” and ”otherValue” can be anything: matrices, vectors, strings, scalar or even other structs.

The input fields in the Matpower struct (mpc struct) are **baseMVA, bus, branch, gen** and, optionally, **gencost**. The baseMVA field’s value is a scalar and it is for specifying the system MVA base used for converting power into per unit quantities. Other data variable for the fields: bus, gen, branch and gencost are matrices, where a row corresponds to a single bus, branch, gen, etc. and the columns are different parameters and properties for them. The mpc struct also has a version field whose value is a string set to the current Matpower case version, currently ”2” by default. For convenience and code portability, **idx_bus** defines a set of constants to be used as named indices into the columns of the bus matrix. Similarly **idx_brch, idx_gen** and textbfidx_cost define names for the columns of branch, gen and gencost, respectively. These constants are defined in a script called `define_constants`. Other additional fields are allowed to be included in case struct. The function OPT for instance is designed to recognized other fields next to the input fields (baseMVA, bus, branch, gen). User defined fields may also be included.

To make it easier to understand, below are the detailed Matpower caseformat given in tables for each input matrix (bus data in Figure 6.1, generator data in Figure 6.2, branch data in Figure 6.3, and generator cost data in Figure 6.4). Note that the ”name” column contains the constant names given for columns of each data matrix which are defined in `define_constants`.

name	column	description
BUS_I	1	bus number (positive integer)
BUS_TYPE	2	bus type (1 = PQ, 2 = PV, 3 = ref, 4 = isolated)
PD	3	real power demand (MW)
QD	4	reactive power demand (MVAr)
GS	5	shunt conductance (MW demanded at $V = 1.0$ p.u.)
BS	6	shunt susceptance (MVAr injected at $V = 1.0$ p.u.)
BUS_AREA	7	area number (positive integer)
VM	8	voltage magnitude (p.u.)
VA	9	voltage angle (degrees)
BASE_KV	10	base voltage (kV)
ZONE	11	loss zone (positive integer)
VMAX	12	maximum voltage magnitude (p.u.)
VMIN	13	minimum voltage magnitude (p.u.)
LAM_P†	14	Lagrange multiplier on real power mismatch (u/MW)
LAM_Q†	15	Lagrange multiplier on reactive power mismatch (u/MVAr)
MU_VMAX†	16	Kuhn-Tucker multiplier on upper voltage limit (u/p.u.)
MU_VMIN†	17	Kuhn-Tucker multiplier on lower voltage limit (u/p.u.)

† Included in OPF output, typically not included (or ignored) in input matrix. Here we assume the objective function has units u.

Figure 6.1: Bus Data (mpc.bus) table

There are other fields that are allowed to be included in the structure (mpc struct)

name	column	description
GEN_BUS	1	bus number
PG	2	real power output (MW)
QG	3	reactive power output (MVAr)
QMAX	4	maximum reactive power output (MVAr)
QMIN	5	minimum reactive power output (MVAr)
VG	6	voltage magnitude setpoint (p.u.)
MBASE	7	total MVA base of machine, defaults to baseMVA
GEN_STATUS	8	machine status, > 0 = machine in-service; ≤ 0 = machine out-of-service
PMAX	9	maximum real power output (MW)
PMIN	10	minimum real power output (MW)
PC1*	11	lower real power output of PQ capability curve (MW)
PC2*	12	upper real power output of PQ capability curve (MW)
QC1MIN*	13	minimum reactive power output at PC1 (MVAr)
QC1MAX*	14	maximum reactive power output at PC1 (MVAr)
QC2MIN*	15	minimum reactive power output at PC2 (MVAr)
QC2MAX*	16	maximum reactive power output at PC2 (MVAr)
RAMP_AGC*	17	ramp rate for load following/AGC (MW/min)
RAMP_10*	18	ramp rate for 10 minute reserves (MW)
RAMP_30*	19	ramp rate for 30 minute reserves (MW)
RAMP_Q*	20	ramp rate for reactive power (2 sec timescale) (MVAr/min)
APF*	21	area participation factor
MU_PMAX†	22	Kuhn-Tucker multiplier on upper P_g limit (u/MW)
MU_PMIN†	23	Kuhn-Tucker multiplier on lower P_g limit (u/MW)
MU_QMAX†	24	Kuhn-Tucker multiplier on upper Q_g limit (u/MVAr)
MU_QMIN†	25	Kuhn-Tucker multiplier on lower Q_g limit (u/MVAr)

* Not included in version 1 case format.
† Included in OPF output, typically not included (or ignored) in input matrix. Here we assume the objective function has units u.

Figure 6.2: Generator Data (mpc.gen) table

such as user-defined fields or fields used as parameters to directly extend the OPF (optimal power flow) formulation.

name	column	description
F_BUS	1	"from" bus number
T_BUS	2	"to" bus number
BR_R	3	resistance (p.u.)
BR_X	4	reactance (p.u.)
BR_B	5	total line charging susceptance (p.u.)
RATE_A	6	MVA rating A (long term rating)
RATE_B	7	MVA rating B (short term rating)
RATE_C	8	MVA rating C (emergency rating)
TAP	9	transformer off nominal turns ratio, (taps at "from" bus, impedance at "to" bus, i.e. if $r = x = 0$, $tap = \frac{\lvert V_f \rvert}{\lvert V_t \rvert}$)
SHIFT	10	transformer phase shift angle (degrees), positive ⇒ delay
BR_STATUS	11	initial branch status, 1 = in-service, 0 = out-of-service
ANGMIN*	12	minimum angle difference, $\theta_f - \theta_t$ (degrees)
ANGMAX*	13	maximum angle difference, $\theta_f - \theta_t$ (degrees)
PF†	14	real power injected at "from" bus end (MW)
QF†	15	reactive power injected at "from" bus end (MVAr)
PT†	16	real power injected at "to" bus end (MW)
QT†	17	reactive power injected at "to" bus end (MVAr)
MU_SF‡	18	Kuhn-Tucker multiplier on MVA limit at "from" bus (u/MVA)
MU_ST‡	19	Kuhn-Tucker multiplier on MVA limit at "to" bus (u/MVA)
MU_ANGMIN‡	20	Kuhn-Tucker multiplier lower angle difference limit (u/degree)
MU_ANGMAX‡	21	Kuhn-Tucker multiplier upper angle difference limit (u/degree)

* Not included in version 1 case format.
† Included in power flow and OPF output, ignored on input.
‡ Included in OPF output, typically not included (or ignored) in input matrix. Here we assume the objective function has units u.

Figure 6.3: Branch Data (mpc.branch) table

name	column	description
MODEL	1	cost model, 1 = piecewise linear, 2 = polynomial
STARTUP	2	startup cost in US dollars*
SHUTDOWN	3	shutdown cost in US dollars*
NCOST	4	number of cost coefficients for polynomial cost function, or number of data points for piecewise linear
COST	5	parameters defining total cost function $f(p)$ begin in this column, units of f and p are \$/hr and MW (or MVAr), respectively (MODEL = 1) ⇒ $p_0, f_0, p_1, f_1, \ldots, p_n, f_n$ where $p_0 < p_1 < \cdots < p_n$ and the cost $f(p)$ is defined by the coordinates (p_0, f_0), (p_1, f_1), …, (p_n, f_n) of the end/break-points of the piecewise linear cost (MODEL = 2) ⇒ $c_n, \ldots, c_1, c_0$ $n+1$ coefficients of n-th order polynomial cost, starting with highest order, where cost is $f(p) = c_n p^n + \cdots + c_1 p + c_0$

† If gen has n_g rows, then the first n_g rows of gencost contain the costs for active power produced by the corresponding generators. If gencost has $2n_g$ rows, then rows $n_g + 1$ through $2n_g$ contain the reactive power costs in the same format.
* Not currently used by any MATPOWER functions.

Figure 6.4: Generator Cost Data (mpc.gencost) table

As mentioned earlier Matpower package provides numerous examples for simulation listed in case files. Figure 6.5 is the table containing all casefiles available in Matpower.

name	description
`caseformat`	help file documenting MATPOWER case format
`case_ieee30`	IEEE 30-bus case
`case24_ieee_rts`	IEEE RTS 24-bus case
`case4gs`	4-bus example case from Grainger & Stevenson
`case6ww`	6-bus example case from Wood & Wollenberg
`case9`	9-bus example case from Chow
`case9Q`	`case9` with reactive power costs
`case14`	IEEE 14-bus case
`case30`	30-bus case, based on IEEE 30-bus case
`case30pwl`	`case30` with piecewise linear costs
`case30Q`	`case30` with reactive power costs
`case39`	39-bus New England case
`case57`	IEEE 57-bus case
`case118`	IEEE 118-bus case
`case300`	IEEE 300-bus case
`case2383wp`	Polish system - winter 1999-2000 peak
`case2736sp`	Polish system - summer 2004 peak
`case2737sop`	Polish system - summer 2004 off-peak
`case2746wop`	Polish system - winter 2003-04 off-peak
`case2746wp`	Polish system - winter 2003-04 evening peak
`case3012wp`	Polish system - winter 2007-08 evening peak
`case3120sp`	Polish system - summer 2008 morning peak
`case3375wp`	Polish system plus - winter 2007-08 evening peak

Figure 6.5: Example Cases table

Each of these case files contains the data values for data matrix fields (BaseMV, bus, gen, branch..) as well as version fields and another field called ”Area Data”. The main simulation routines in Matpower, whose names begin with run (e.g. **runpf**, **runopf**), accept either a file name or a case struct as an input. Figure 6.6 lists main functions of Matpower:

Results as are said are pretty-printed to the screen, displaying a system summary, bus data, branch data and, for the OPF, binding constraint information. The bus data includes the voltage, angle and total generation and load at each bus. It also includes nodal prices in the case of the OPF. The branch data shows the flows and losses in each branch. For further detail about the electrical model of data (branch, generator, and load models) as well as AC and DC power flow equations please refer to [57].

name	description
`runpf`	power flow†
`runopf`	optimal power flow†
`runuopf`	optimal power flow with unit-decommitment†
`rundcpf`	DC power flow‡
`rundcopf`	DC optimal power flow‡
`runduopf`	DC optimal power flow with unit-decommitment‡
`runopf_w_res`	optimal power flow with fixed reserve requirements†

† Uses AC model by default.
‡ Simple wrapper function to set option to use DC model before calling the corresponding general function above.

Figure 6.6: Top level simulation functions

6.3.3 9-bus system as input data set

For our experimental purpose, we need to develop several Matpower functions such as `makePTDF.m` and `makeYbus.m` to calculate net-ability and its components. The input data set we have chosen for our experiment is case9.m: a 9-bus system. This input data set is chosen basically for three main reasons:

- Since we have developed JAVA version of power flow systems, we needed to validate whether our codes work correctly particularly whether the result obtained for the net-ability are correct using a specific input data set. Since we didn't have access to codes, we needed to contact the author of [8] paper each time to validate our results. This process cost a lot of time and effort for both parties and therefore choosing a small input data set could accelerate this process.

- Our purpose in this project is to show whether our method works. Thus computational performance is not a big concern at this stage. Using a bigger input data set simply requires extra time and space to calculate and manipulate bigger matrices.

- Matpower is written in Matlab and Matlab is built for matrix manipulation. Therefore the computational performance of manipulating and working with huge matrices in Matlab is better than that of in JAVA.

In the future it is necessary though to test the method for bigger data set and enhance the code to obtain better performance (if needed). The 9-bus system used in this experiment depicted in figure 6.7.

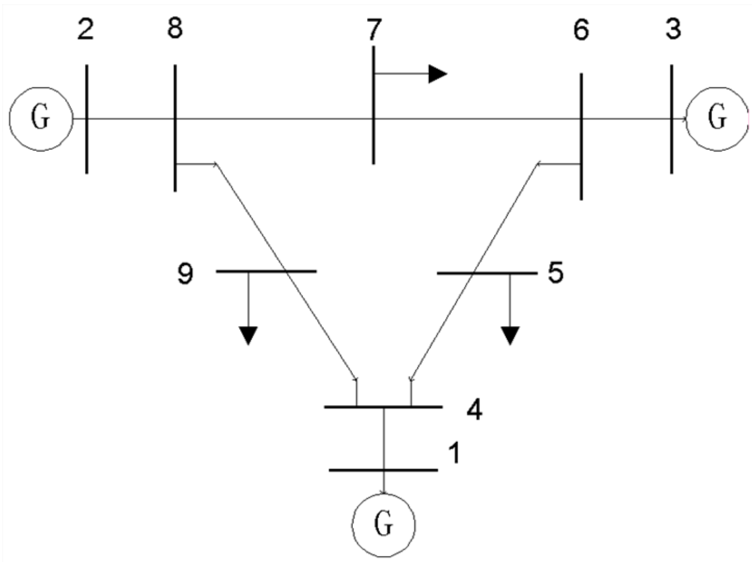

Figure 6.7: 9-bus system

The vertical lines to which an arrow is attached represent load buses and those to which a circle is attached represent generator buses. Generators and loads can be specified in the input data set from their PD (real power demand (MW)) and PG(real power supply (MW)) values. Load buses have non-zero values for PD while generator buses have non-zero values for PG (except for the slack bus). The weights corresponding to maximum power flow capacities of lines can be obtained from branch RATE_A parameter values in data set. These values for 9-bus system data set are given in Tables 6.1 and 6.2.

Table 6.1: The generator and load data for 9-bus system

Bus number	Generation(MW)	Load(MW)
1	0	0
2	163	0
3	85	0
4	0	0
5	0	90
6	0	0
7	0	100
8	0	0
9	0	125

Table 6.2: The line data for 9-bus system

Branch number	From bus	To bus	Reactance	S_{ij}^{max}(MW)
1	1	4	0,0576	250
2	4	5	0,092	250
3	5	6	0,17	150
4	3	6	0,0586	300
5	6	7	0,1008	150
6	7	8	0,072	250
7	8	2	0,0625	250
8	8	9	0,161	250
9	9	4	0,085	250

From the tables, bus number 1, 2, and 3 are generators (bus number 1 is a slack bus (see definition of slack bus in Chapter 4)) and bus number 5, 7, and 9 are load buses. The power flow limit of lines are given in the last column (S_{ij}^{max}MW) of the branch table above. To compute net-ability, transfer capacities, PTDF values and electrical distances need to be calculated. According to the formula given in Equation 5.5 transfer capacity is calculated for each pair of generator and load. In 9-bus network we have 9 pairs of generator-load. PTDF values for each line and electrical distance are calculated accordingly. The corresponding abstract network model of 9-bus system is depicted in the figure 6.8

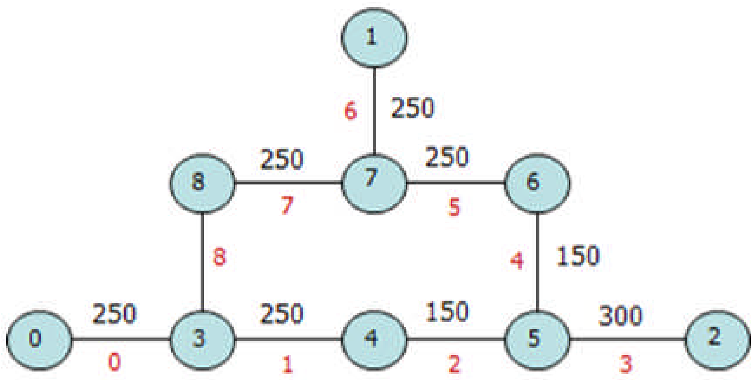

Figure 6.8: Network model of 9-bus system

Numbers in vertices correspond to the bus number given in the data set; weights correspond to the rateA column given in the branch matrix in the data set. And finally red numbers are links' IDs.

This Chapter was intended to explain briefly the experimental design and setup as well as important challenged encountered during this process. In the next Chapter the result are discussed to answer the questions brought up at the beginning of this Chapter. Further alternative methods are explained in comparison with Weighting Scheme algorithm.

Chapter 7

Result and Discussion

The questions stated at the beginning of Chapter 6 form the core of project's experiment. In Chapter 6 the experimental design is described to let us strat the test and evaluate the results. In this Chapter, results of the experiment are discussed to answer the questions mentioned in Chapter 6.
The data required analyzing the effect of the Weighting Scheme algorithm on topological vulnerability and robustness of the network includes the number of buses and their types (generators, loads and transmissions), the number of lines and their connection to buses with their associate power flow limits, and finally the network impedance. Having this information, PTDF, transfer capacities and electrical distance of the network are calculated. As a result the net-ability of the network (and the related drop associated with line failures) is obtained. Having net-ability and the related drop associated with line failures, the performance of WS algorithm in improving the robustness of the network can be examined. The method is applied to a 9-bus system. To make sure the method works correctly, WS algorithm is run serveral times (equals to the number of nodes in the network), each time one specific node as the initiator of the algorithm. The result for all runs are shown in the tables. One specific run is elaborated, the rest are just illustrated.
The results of the experiment show that Weighting Scheme algorithm has indeed improved the robustness of the network: relative drops in net-ability after applying Weighting Scheme algorithm is indeed decreased by each link removal (simulating failures) compared to relative drops in net-ability of the original network.
The experiment shows that the vulnerability of the resulted homogeneous network after applying our method is reduced and therefore the robustness of the network is improved. Another finding is that the net-ability of the network after applying Weighting Scheme algorithm is worsened: the net-ability is decreased after the weight adjustment compared to the original value of net-ability before weight adjustment. This implies that based on the definition of net-ability the global performance of a homogeneous network is less than that of a heterogeneous network. Note that decrease in net-ability means decrease in the global performance of the network which is undesirable while decrease in relative drop in net-ability means

the performance of the network is less affected by changes imposed on it (failure of its components) and thus is a desirable affect.

7.1 The Effects on Net-ability

Recall from Chapter 6, the first question to answer is

How is the net-ability (global performance of the network) affected?

To answer this question we first apply Equation 5.7 to the 9-bus system depicted in Figure 7.1 to obtain net-ability value of the network before applying Weighting Scheme algorithm. We call this value as ”original net-ability”.

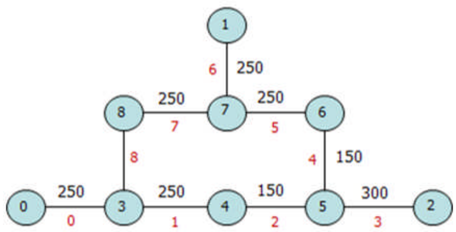

Figure 7.1: Network model of 9-bus system

In the next step the Weighting Scheme algorithm is run by nodes in the graph. In each run, one of the node is initiated the algorithm. Recall from the previous Chapter that any node in the network can randomly initiate the algorithm. To make sure that the method initiated from any point in the network works correctly, the algorithm is run several times with each time one specific node as an initiator. In this experiment the algorithm is run 9 times. Each time the new value of net-ability after weight adjustment is recorded and graphed.
Below is an example of one run starting from node with ID zero (see Figure 7.1) to show how Weighting Scheme algorithm works:

Table 7.1: Weighting Scheme algorithm initiated at nodeID = 0

# of run	Node ID	Link ID	Weight after WS	Net-ability after WS
1	node 0	0	250	1421 (no change)
2	node 3	0	250	1421
		1	250	1421
		8	250	1421
3	node 4	1	200	1405(decreased)
		2	200	1445 (increased)
4	node 8	8	250	1445
		7	250	1445
5	node 5	3	216.67	1378 (decreased)
		2	216.67	1378
		4	216.67	1409 (increased)
6	node 7	6	250	1409
		5	250	1409
		7	250	1409
7	node 2	3	216.67	1409
8	node 6	5	233.34	1409
		4	233.34	1409
9	node 1	6	250	1409

The sequence of nodes running the algorithm initiated by nodeID zero is (second column of the table):

$$0 \rightarrow 3 \rightarrow 4 \rightarrow 8 \rightarrow 5 \rightarrow 7 \rightarrow 2 \rightarrow 6 \rightarrow 1 \tag{7.1}$$

and the sequence of changes in net-ability values caused by links' weight changes is (the last column):

$$1421 \rightarrow 1405 \rightarrow 1445 \rightarrow 1378 \rightarrow 1409 \tag{7.2}$$

The net-ability graph after Weighting Scheme run by node0 is depicted in the Figure 7.2

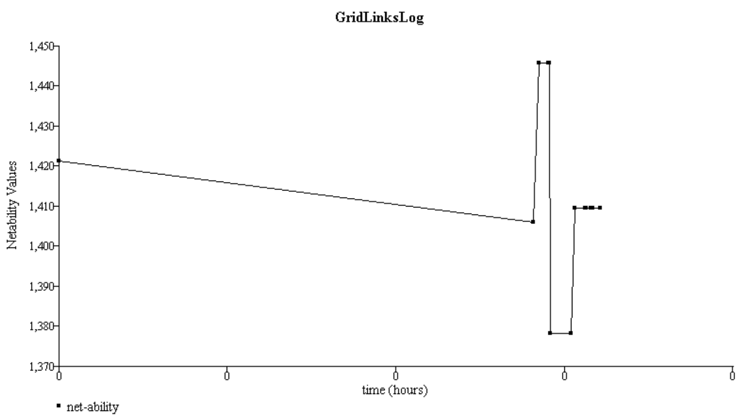

Figure 7.2: Net-ability for node 0

Figure 7.2 indicates that net-ability is decreased after weight adjustment. As explained in the Chapter 6 each time a change occurs, GridLinksLog records the change and at the end of the experiment all changes is graphed. Running the algorithm for eight other cases showed the same result: in all cases values of net-ability was decreased compared to the original value. The reason that at some point we have increase in net-ability and at some other points decrease, depends on the values of transfer capacities. In the 9-bus system there are three generator buses (1, 2, and 3) and three load buses (5, 7, and 9) (see the table 6.1 in Chapter 6). Since in the abstract model of the 9-bus system (see Figure 7.1), IDs of nodes (generators and buses) begin from zero instead of one, the corresponding bus numbers are 0, 1, and 2 for generators and 4, 6, 8 for loads . For each pair of generator-load, PTDF and transfer capacity is calculated. For instance PTDF and transfer capacity from generator 0 to load 4 is calculated as follows:

The PTDF from generator 0 to load 4 is taken from the column 0 of PTDF matrix minus the column 4 of PTDF matrix (see Equation 5.3)

Table 7.2: PTDF from generator 0 to load 4

Branch	0-3	3-4	4-5	2-5	5-6	6-7	7-1	7-8	8-3
p	1.000	0.8649	-0.1351	0	-0.1351	-0.1351	0	-0.1351	-0.1351

The corresponding transfer capacity of generator 0 to load 4 is calculated as follows:

$$C_0^4 = \{\frac{S_{03}}{p_{03}}, \frac{S_{34}}{p_{34}}, \frac{S_{45}}{p_{45}}, \frac{S_{25}}{p_{25}}, \frac{S_{56}}{p_{56}}, \frac{S_{67}}{p_{67}}, \frac{S_{71}}{p_{71}}, \frac{S_{78}}{p_{78}}, \frac{S_{83}}{p_{83}}\}$$
$$= min\{\frac{250}{1.000}, \frac{250}{0.8649}, \frac{150}{0.1351}, \frac{300}{0}, \frac{150}{0.1351}, \frac{250}{0.1351}, \frac{250}{0}, \frac{250}{0.1351}, \frac{250}{0.1351}\} = 250$$

Where S_{ij} is the power flow limit of line connecting nodes i and j. It is obtained from RATE_A column of branch data matrix in the data set (see Chapter 6, Table 6.2). And p_{ij} values are the PTDF factors explained above.

Running Weighting Scheme algorithm, the values of PTDF remains unchanged while the weights are adjusting. This means that in calculating transfer capacity, the numerators are changing while denominators remain unchanged. According to Equation 5.6, net-ability is calculated over the sum of all minimum values of transfer capacities of generator-load pairs. In 9-bus system case, the sum is taken over min values for each generator-load pair transfer capacity:

$$C_0^4, C_1^2, C_2^4, C_0^6, C_1^6, C_2^6, C_0^8, C_1^8, C_2^8$$

If changing weights causes one of these "minimum" values to change, then net-ability value will be changed accordingly. In case of increase in one these minimum values, net-ability will be increased and in case of decrease, net-ability will be decreased. However, if changing weights does not affect these minimum values, the net-ability value will remain unchanged. Therefore it does not necessarily mean that the value of net-ability will be increased if the weight of a specific link is increased after running the algorithm. This can also be derived from the transfer capacity formula given in Equation 5.5. It can be concluded that in order to have increase in net-ability (global performance) of the network, one needs to search through paths connecting pairs of generators and loads to find minimum capacities and increase those values. This method requires nodes to have a global picture of the network and hence it will be difficult or even computationally impossible for hundreds of thousands nodes operating in a distributed environment. Another interesting question is why in this experiment the value of net-ability is decreased in all nine cases? Answering to this question requires examination of different networks. But one possible answer could be since in applying Weighting Scheme algorithm the total weights remain unchanged, adjusting weights means in some links there are increase in weights and in other decrease. Even though increase in some links' weights might increase the min value of transfer capacity of a specific pair, for the same reason decrease in other links' weights might affect transfer capacity for other pairs. Since net-ability is calculated for all pairs, the probability of having either decrease in net-ability or no change is not small. An interesting future work could be to find a method to manipulate weights in such a way that the net-ability, in other words, the global performance of the network remains unaffected but at the same time the robustness of the network is improved.

Results of net-ability after 9 runs of Weighting Scheme algorithm initiated by all nodes are given in graphs below:

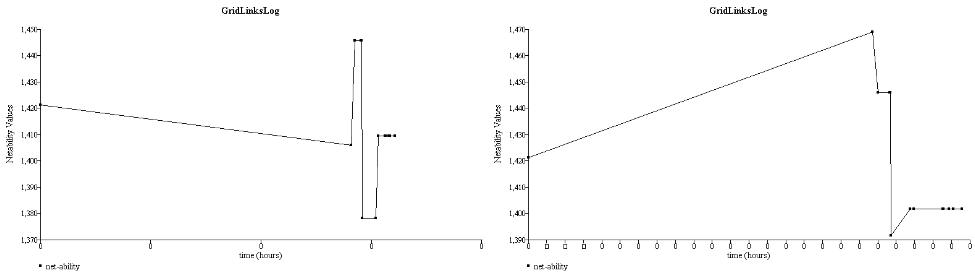

Figure 7.3: Net-ability for node 0 and 1

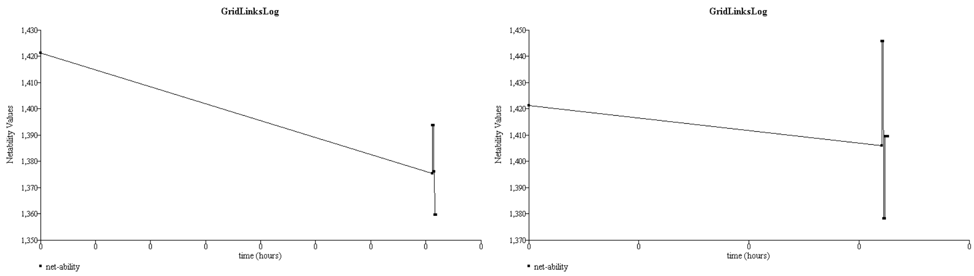

Figure 7.4: Net-ability for node 2 and 3

w

And net-ability values for nine runs of Weighting Scheme algorithm initiating from node i where $i = (0, ..., 8)$ are given in Table 7.3:

Table 7.3: Net-ability values after weight adjustment

Node-ID	0	1	2	3	4	5	6	7	8
Net-ability	1409.4	1401.5	1359.6	1409.4	1383.5	1359.6	1379.8	1401.5	1386.3

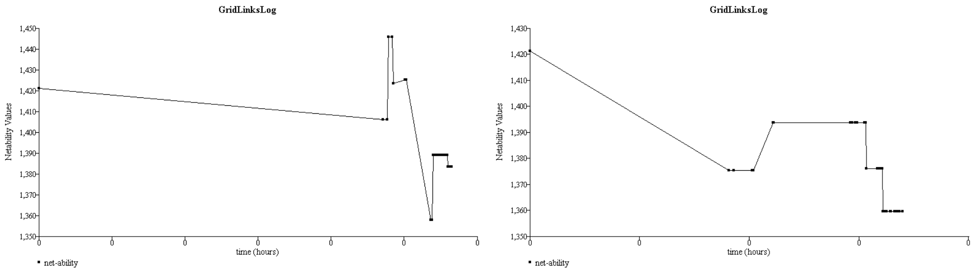

Figure 7.5: Net-ability for node 4 and 5

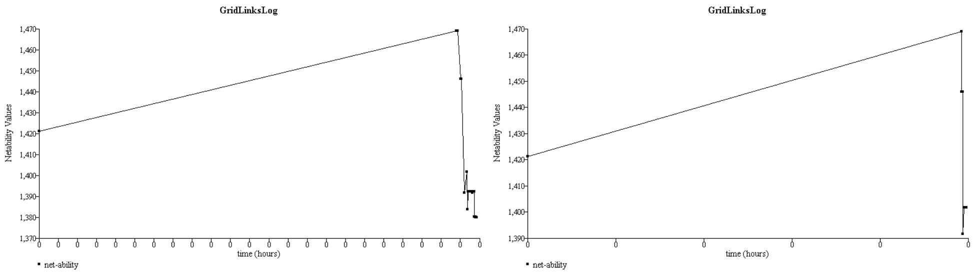

Figure 7.6: Net-ability for node 6 and 7

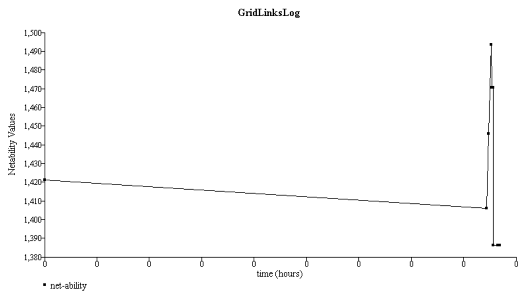

Figure 7.7: Net-ability for node 8

7.2 The Effects on Robustness

The second question mentioned in Chapter chp:ChapterSix is:

to what extent is the robustness of the network affected after applying WS algorithm?

To examine the effect of Weighting Scheme on the robustness of the network, we apply the relative drop in net-ability defined in Equation 5.7 on lines failure. First on the original graph (before weight adjustment) the relative drops in original net-ability are calculated and recorded for each removal of lines to see to what ex-

tent the original network is vulnerable against line failure and thus how robust is the network.
In the next step, the Weighting Scheme algorithm is applied. Again, here, to examine the behavior of Weighting Scheme started from any point of network, the algorithm is run several times, each time one of the nodes considered to be a initiator. Further after each run a line is removed and net-ability is recalculated to determine the relative drop. The results are recorded and compared with the result of the original network to see the effect of Weighting Scheme algorithm on robustness of the network. The algorithm is run 9 times for each of the buses in the network. The results for before and after Weighting Scheme algorithm are given in tables below with the corresponding relative drop in net-ability after links removal.

Table 7.4 illustrates new values of net-ability after each link removal and corresponding relative drop of the original network (before WS algorithm applied).

Table 7.4: Relative drop in original network after link removal

original Net-ability	1421,1	
Branch ID removed	Net-ability after removal	% drop
branch 1	886,41	37,63
branch 2	1030,9	27,46
branch 4	994,7	30
branch 5	857,15	39,69
branch 7	914,95	35,62
branch 8	842,71	40,7

Table 7.5: Relative drop before and after WS run initiated at node 0

Node 0			
Net-ability after WS	1409,42		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	995,2	29,39	37,63
branch 2	1036,3	26,479	27,46
branch 4	993,56	29,509	30
branch 5	920,2	34,719	39,69
branch 7	997,65	29,22	35,62
branch 8	929,55	34,05	40,7

Table 7.6: Relative drop before and after WS run initiated at node 1

Node 1			
Net-ability after WS	1401,54		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	945,644	32,53	37,63
branch 2	1028,19	26,64	27,46
branch 4	1022,279	27,06	30
branch 5	965,94	31,08	39,69
branch 7	999,27	28,7	35,62
branch 8	921,88	34,22	40,7

Table 7.7: Relative drop before and after WS run initiated at node 2

Node 2			
Net-ability after WS	1359,63419		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	973,19	28,42	37,63
branch 2	1061,18	21,95	27,46
branch 4	1012,91	25,5	30
branch 5	943,1	30,63	39,69
branch 7	1022,93	24,76	35,62
branch 8	954,01	29,83	40,7

Table 7.8: Relative drop before and after WS run initiated at node 3

Node 3			
Net-ability after WS	1409,42		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	995,2	29,39	37,63
branch 2	1036,3	26,48	27,45
branch 4	993,56	29,51	30
branch 5	920,2	34,71	39,69
branch 7	997,65	29,21	35,62
branch 8	929,55	34,05	40,7

Table 7.9: Relative drop before and after WS run initiated at node 4

Node 4			
Net-ability after WS	1383,5		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	992,3	28,28	37,63
branch 2	1053,66	23,84	27,46
branch 4	1001,36	27,62	30
branch 5	934,57	32,45	39,69
branch 7	1020,663568	26,22	35,62
branch 8	959,2571019	30,66	40,7

Table 7.10: Relative drop before and after WS run initiated at node 5

Node 5			
Net-ability after WS	1359,63		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	973,19	28,42	37,63
branch 2	1061,18	21,95	27,46
branch 4	1012,91	25,5	30
branch 5	943,1	30,63	39,69
branch 7	1022,93	24,76	35,62
branch 8	954,01	29,83	40,7

Table 7.11: Relative drop before and after WS run initiated at node 6

Node 6			
Net-ability after WS	1379,86		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	942,65	31,69	37,63
branch 2	1031,35	25,26	27,46
branch 4	1008,05	26,94	30
branch 5	952,18	30,1	39,69
branch 7	1005,94	27,1	35,62
branch 8	930,93	32,53	40,7

Table 7.12: Relative drop before and after WS run initiated at node 7

Node 7			
Net-ability after WS	1401,54		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	945,65	32,53	37,63
branch 2	1028,18	26,64	27,46
branch 4	1022,27	27,06	30
branch 5	965,94	31,08	39,68
branch 7	999,27	28,7	35,62
branch 8	921,88	34,22	40,7

Table 7.13: Relative drop before and after WS run initiated at node 8

Node 8			
Net-ability after WS	1386,35		
Branch ID removed	Net-ability after removal	% drop after	% drop before
branch 1	945,6453102	31,79	37,63
branch 2	994,184792	28,29	27,46
branch 4	983,6994936	29,04	30
branch 5	920,2026242	33,62	39,69
branch 7	965,5406958	30,35	35,62
branch 8	892,7213124	35,6	40,7

Tables 7.5 to 7.13 show new values of net-ability as well as their corresponding relative drop by each link removal after running WS algorithm by each node.

To make tables easier to compare, relative drops column of the original network is placed next to relative drops columns of the network after weight adjustment. The results show that in all cases, the relative drops in net-ability are reduced. Each of these table (Tables 7.5 to 7.13) corresponds to one particular run of WS initiating by the node given on top of the table. The first colum of these tables are the link IDs of the removed links. The global net-ability after WS run is given in the second rows (for instance the value of net-ability for nodeID zero reduces to 1409.42 after WS run). Further the second columns state the values of net-ability after links removal and in the third column the relative drops in net-ability (the network vulnerability) is calculated for each link removal. The last column (which is identical for all these tables) indicates the relative drop in net-ability of the 'original network (before weight adjustment)'. The results given in these tables show that in all cases the relative drops in net-ability is reduced after applying WS compared to the original network.
Although the WS algorithm decreases the global net-ability of the network, as one observes, the network vulnerabilty is reduced in all cases. Note that decrease in net-ability means decrease in the global performance of the network which is an undesirable effect while decrease in relative drop in net-ability means the performance of the network is less affected by changes imposed on it (failure of its components) and thus is a desirable effect. These result illustrate that WS algorithm has indeed reduced the vulnerability of the network and thus the robustness of the network is improved.

> In other words, we have shown that Weighting Scheme algorithm has indeed improved the robustness of the network by creating a more homogeneous network in a decentralized and distributed environment when failures occur.

As mentioned earlier, any node in the network can randomly initiate the algorithm. The idea is that in practice a node that is under stress can initiate the algorithm from any point of the network. If so, since actions are coordinated by sending and receiving messages, all nodes are guaranteed to run the algorithm once in response to the initiation. Adjusting weights can be interpreted as imposing control on the amount power that can flow over lines. This interpretation engages the network dynamics and relates the static to dynamic robustness of the network. When a node is under stress the node can impose control on the power flow passes through its lines and thus reduces the risk of failure. However, another mechanism is required to detect that the node is under stress at the first place. The advantage of weight readjustment is that it can be done dynamically: at any point of the network and at any time node can decide to run the algorithm. Further since nodes coordinate with each other through message passing, it is guaranteed that everyone has run the algorithm. Another advantage of proposed method is that nodes can apply this method using only their own local information about their topologies. In this sense it can be used in distributed environment where no central control and extra management is needed.

7.3 Challenges

The neighboring nodes in the network run the algorithm when one has initiated it. In practice we are dealing with a network in which actual power is flowing through the lines and in which direction of the flow matters at a given time. Therefore incoming and outgoing links must be identified. The amount of flow coming into a node through incoming links must be equal the amount of flow going out of the node through outgoing links (for transmission nods) except for source and sink nodes.

Now assume a node, say node m, receives a message and is unable to redistribute its weights. Assume the weight of a link, say link k, from which node m has received a message is increased. Assume further that link k is an incoming link to the node (power is coming through that link). Increase in weight of link k allows a flow of more portion of power through it. If this is the case (the actual power flow passing link k, is indeed increased) and If node m is unable to redistribute its weights (the control system on the node doesn't work or there is no back-up lines available) and if the outgoing links from node m cannot handle the increase in power (the sum of their capacities is less that the incoming flow), the node becomes overloaded and cascading failure might occur. If on the other hand, node m (unable to adjust its weight) sends the message to its neighbors anyhow, the neighboring agents can continue the weight adjustment and the failure might not cascade further. These situation must be tested and examine when the actual dynamic of the network is considered.

A solution for such situation is to apply a rather less aggressive weight adjustment. Weighting Scheme algorithm, as shown, is an effective theoretical method to improve the robustness. It is primarily intended to show whether such approaches can improve the robustness. It adjusts and redistributes weights in a rather aggressive way: weights are *evenly* redistributed to create a homogeneous network. The resulting network is not an optimal homogeneous network where all nodes are topologically equivalent but at each node has its local homogeneous topology. Another rather less aggressive approach could try to create a network which is *"close"* to a nodal homogeneous topology. This can be done by adjusting weights to specific limits based on some constrains instead of even redistribution of weights. An example could be a *gradual increment/decrement* in weights: in each run, a fraction of weight's value is added to or subtracted from the original value in case of increase or decrease in weights respectively.

In the next section, alternative approaches are discussed and compared with Weighting Scheme method.

7.4 Alternative Approaches

The third question mentioned in Chapter chp:ChapterSix is:

What are other alternatives to weight adjustment?

This section discusses other alternative methods to WS as well as their advantages and disadvantages. One approach for weigh redistribution is already mentioned in the previous part: incremental adjustment. Another approach is to add extra communication among neighboring nodes before they adjust their weights: before weight adjustment, the agent at work can ask the outgoing capacities of its neighbors in order to send power after adjustment no more than the total outgoing capacity of its neighbor. If a neighbor cannot handle, the node can adjust its weights on other links except the one connecting it to the neighbor with problem. This method can reduce the possibility of cascading failure explained above since it tries to prevent overloading phenomenon by putting extra coordination among nodes.
Another alternative is to cut the coordination among agents (resembling a pure distributed environment) where nodes randomly adjust their weights (using for instance incremental weighting adjustment) without coordinating with each other. This method, as said, resembles a pure distributed case. The advantage of this approach is that there is no concern about communication overhead issues. An important issue here is that nodes might apply changes on weights simultaneously. To overcome this issue, one approach could be that nodes wait a random amount of time before they start weight adjustments. By doing so, the probability that nodes collide will be reduced.

7.5 Communicative Versus Non-communicative Agents

The final question mentioned in Chapter chp:ChapterSix is:
Does adding communication between agents improve on less or non-communicative agents?

The latter case in which agents are non-communicative is already discussed in the previous section. WS algorithm, when initiated at a node, is run by the rest of nodes through messaging mechanism. Adding communication and extra coordination may help better control on weight adjustment to reduce a risk of cascading failures. Further, it can provide a possibility that weigh adjustment happens only in some nodes (for instance nodes with high degree both in their number of neighbors and in their weight distribution on their links) instead of all. The idea is that links to and from hub nodes tend to be used more frequently than other links in the network. The weight of a link can thus be assumed to depend on the degrees of the two nodes that it connects. Moreover, these links might become critical to the network since they might have a higher centrality index compared to other links. Therefore, instead of running WS algorithm on all nodes, each two neighboring agents can communicate with each other to know about each other's degrees. Then the one with a higher degree is chosen to adjust its weights. This way the number of algorithm runs is reduced in cost of adding extra communication and coordination. The choice of cutting the number of times that WS algorithm is run versus adding extra communication depends on both the result and performance of this method in comparison with WS.

Chapter 8

Conclusion and Future Work

This thesis is to study how to improve the robustness of transmission grids dynamically (by reducing their vulnerability) in a decentralized and distributed environment.

The work proposes an effective theoretical method based on complex network approaches taking into account the physical and behavioral properties of electrical systems to improve the robustness. An abstract model of the network is made based on complex network theory where components of the transmission networks (generator, load and transmission buses and transmission lines) are presented as nodes and links respectively. To each link a weight is assigned representing the power flow capacity of the line. These weights (capacities) are power flow limits of lines. All nodes are further modeled as autonomous entities called agents that can act independently and make decision based on the local knowledge they can acquire from their environment. A distributed algorithm called Weighting Scheme is developed which enables these autonomous agents to bring about changes in local settings which results in a more robust network.

Why power transmission grid?

The main function of power transmission grids, aside from proper delivery of power, is to assure the security of the network and to avoid blackouts. This is an essential requirement for today's modern society in which a slightly disturbance in power can cause a disastrous loss in business. Random failures and intentional attacks are two major causes for blackouts to occur. The level of network reliability can thus be assessed based on its tolerance against the failures.

Why robustness of the power grid must be examine and improved?

Key elements that can determine the security and reliability in transmitting power are the grid's topological structures as well as their physical and operational behaviors and states. By topological structure is meant the number of nodes (generator, load and transmission buses) and their connections through links (transmission lines). By operational behavior and state of the networks is meant their electrical properties and characteristics (impedance of lines, voltage drops and losses etc.) as well as electrical dynamics of the network (the actual flow of power through the lines in a given time). Power grids tolerance to failures (both random and intentional attacks) is referred to the network ability to withstand such failures. This ability can be determined in terms of network robustness against failure and outages. Therefore measuring robustness of power grid networks can provide strong indications on the level of network's reliability and security. By robustness is meant, the extent to which a power transmission network is able to cope with changes imposed on it.

Why complex network theory is a good starting point in assessing and improving the grids' robustness?

There has been extensive research done on robustness of power grids using the theory of complex networks. First of all power grids show similar behavior as observed in scale-free and small-world network models introduced in CN theory. Secondly, a complete and detailed analysis and security assessments that takes into account all features of power transmission grids both dynamic of the system as well as structure and their states is almost impossible in a reasonable computational time due to massive size and complex interaction among the network components. And finally CN approaches deal with security problems from more general perspectives. Therefore topological approaches based on CN theory are used as alternatives to detailed analyses of reliability and security of grids.

What do CN approaches have to offer in assessing robustness of grids and what are their shortcomings?

Much research based on CN approaches has done to study, model and analyze power grid networks. There are two categories of such approaches: one group is based on purely topological approaches in which some important physical and operational aspects of the power transmission grids in terms of different types of nodes, power flows distribution among lines and line flow limits, impedance etc. are neglected. These methods thus fail to capture the real behavior of power systems and the results they provide are inaccurate in assessing the robustness of the grids.

The other group, which includes extended versions of purely topological approaches, takes the power system properties and characteristics into account in the topological model of power grids and thus provides more realistic models to analyze the robustness. However most of these methods studied the performance of transmission grids in terms of their robustness and vulnerability using global metrics and techniques. The problem with such approaches is that in order to assess the robustness, the method needs to have a global picture of the systems: all information about the topology of the network with the associated properties must be known in the first place in order to let the metric to assess the global performance of the network in assessing its robustness when failures occur. These methods therefore do not address the decentralized and distributed nature of power grid networks.

Moreover while determining and measuring robustness and vulnerability of power grids is important, it just provides us a descriptive knowledge about the state and structure of the network. There are other concerns related to actions that need to be taken if failures occur. The main questions are how the robustness of the network can be improved so that in case of failures, the performance of the network is less affected and how such improvement can be brought about in a decentralized and distributed environment.

Why assessing the net work's robustness must be done in decentralized and distributed way?

Power transmission networks are large scale complex distributed and networked systems, situated in dynamic environments. Such systems need to be designed in such a way that they can adapt changes automatically and manages themselves autonomously. To adapt changes, self-management techniques can be used which are essentially distributed. Therefore the secure delivery of power as well as the ability to protect and react to power outage and failures must be done in a decentralized and distributed environment. However improving robustness of the grids in a decentralized and distributed environment is a challenge.

Why is improving robustness of the grids in a decentralized and distributed environment a challenge?

First of all, since robustness of the network is a global concept, metrics introduced to measure and assess it are global. The challenge here is how to use such global metrics when dealing with distributed systems where decisions to make changes to improve robustness, are made locally. To overcome this challenge, the solution is to use the metric to evaluate the effects of local changes on the global performance of the network.
Secondly, in order for autonomous agents to make local decisions to provide changes, they need to communicate with each other to coordinate their actions. Coordination in distributed environment is challenging since the information agents base their decision on, is limited to agents' local knowledge of the environment they are operating in. This brings up questions such as to what extent should agents coordinate their acts? Or how can we prevent agents to make invalid changes? (Invalid changes refers to decisions that agents might make based on invalid information).
Thirdly, the CN metrics proposed to assess robustness of power grids do not provide

methods for actions to improve robustness in distributed settings.

How these challenges can be addressed and how is the robustness of the network improved?

To overcome the challenges mentioned above, a distributed algorithm called Weighting Scheme is developed which enables nodes equipped with software agents to bring about changes in local settings which results in a more robust network.

To improve the robustness, the method tries to create a homogeneous network. Homogeneous networks have high degree of robustness against failures. In the theory of complex networks homogeneity means that almost all nodes are topologically equivalent. This does not mean that nodes are identical but rather their topologies (for instance their degree) are almost equivalent. By homogeneous weighted graph here is meant a weighted network whose weights are (more or less) evenly distributed. Scale-free network such as power transmission grids are heterogeneous weighted networks by nature. It is importnant to note that homogeneity is not the optimal criterion for robustness but is a property that can be more easily determined with only local information and it is an indicator of overall robustness.

Our Weighting Scheme algorithm tries to create a homogeneous network by enabling nodes to adjust the weights of their links by redistributing weights evenly among those links. Any node in the network can randomly initiate the algorithm. The idea is that in practice a node that is under stress can initiate the algorithm from any point of the network. Further nodes adjust their weights one by one in response to the initiation. Since actions are coordinated by sending and receiving messages between agents, all nodes are guaranteed to run the algorithm once in response to the initiation. Once all nodes run the algorithm, the network obtained is a homogeneous network.

How to evaluate whether Weighting Scheme algorithm has indeed improved the robustness of the network when failure occurs?

To evaluate our method net-ability metric for assessing the vulnerability of the power grid is used. Net-ability is an extended topological metric based on CN approaches to measure the global performance of the network. It incorporates the physical properties of electrical power system in terms of different types of nodes, power flows distribution among lines and line flow limits, impedance of line and transfer capacity of the network. To determine the network vulnerability, the relative drop in net-ability is calculated after links removal (simulating failures). This way one can identify the critical lines in the network: the line whose failure causes the greatest drop in net-ability is the most critical line for that specific network.

The expecting result after applying Weighting Scheme algorithm is that "if we obtain a homogeneous weighted graph, the relative drop in net-ability caused by components failure is decreased. This implies that the network becomes less vulnerable against failures and therefore the robustness of the network is improved." Note that decrease in net-ability means decrease in the global performance of the network which is undesirable while decrease in relative drop in net-ability means the performance of the network is less affected by changes imposed on it (failure of its components) and thus is a desirable affect.

Experimental results

The results of the experiment show that Weighting Scheme algorithm has indeed improved the robustness of the network: relative drops in net-ability after applying Weighting Scheme algorithm is indeed decreased by each link removal (simulating failures) compared to relative drops in net-ability of the original network. The experiment shows that the vulnerability of the resulted homogeneous network after applying our method is reduced and therefore the robustness of the network is improved.

Another finding is that the net-ability of the network after applying Weighting Scheme algorithm is worsened: the net-ability is decreased after weight adjustment compared to the original value of net-ability before weight adjustment. This implies that based on the definition of net-ability the global performance of a rather homogeneous network is less than that of a heterogeneous network. This can be explained by referring to the definition of the net-ability and how it is calculated. Weighting Scheme algorithm manipulates weights of links. Weights of links correspond to the maximum power flow of lines. These values are used to define the transfer capacities (one of the net-ability component) of the network for all pairs of generators and loads in the network. Net-ability is calculated over the sum of all minimum values of transfer capacities of generator-load pairs. If changing weights causes one of these "minimum" values to change, then net-ability value will be changed accordingly. In case of increase in one of these minimum values, net-ability will be increased and in case of decrease, net-ability will be decreased. However, if changing weights does not affect these minimum values, the net-ability value will remain unchanged. Therefore it does not necessarily mean that the value of net-ability will be increased if the weight of a specific link is increased after running the algorithm. Moreover, in applying Weighting Scheme algorithm the total weights remains unchanged. Therefore adjusting weights means in some links there are increase in weights and in other decrease. Even though increase in some links' weights might increase the min value of transfer capacity of a specific pair, for the same reason decrease in other links' weights might decrease the min values of transfer capacity for other pairs. Since net-ability is calculated for all pairs, the probability of having either decrease in net-ability or no change is not small.

Is net-ability a suitable metric to evaluate the robustness of power grids?

Net-ability as mentioned before is a metric to measure the global efficiency (performance) of power grid networks. Therefore it does not directly reflect the degree of robustness of the network. It is its relative drop which is called extended vulnerability metric that indicates the level of network's robustness against failures. Further since the vulnerability metric reflects the robustness of the network based on the relative drop in net-ability, it is not a quantitative metric for measuring the robustness (it does not quantify the robustness or vulnerability).

Another shortcoming of net-ability metric is that it only includes the topological information about the network. Its relative drop (vulnerability metric) only reflects the static robustness of the network. The electrical dynamics of power system (actual power flows on lines) are not included in assessing the vulnerability of the network and thus dynamic robustness of power transmission grid is not addressed. The Method proposed in this work however, tries to relate the static topological robustness of power grid to their dynamic robustness: the WS algorithm can be interpreted as a control mechanism imposed by local nodes to manage maximum actual power flow passing through their lines. This is an interesting achievement since it opens the door to a new field of how the static and dynamic robustness of the network can be related. Form practical point of view, there are advanced technologies that provide control on actual power flow passing through transmission lines. However, these technologies are still in their research phase and are costly methods. Our goal was to show whether in theory such mechanism as Weighting Scheme can indeed improve the robustness of power grids. The feasibility of such mechanism depends on the availability of the future technologies.

Weighting Scheme versus other method for improving robustness

Many methods and mechanisms for improving robustness proposed in the literature require structural changes in the network. When dynamic of the power system is considered (the actual power flow over the lines), in case of a failure (for instance a node or a link is removed), the redistribution of power flow will happen. Power will flow through other available lines and nodes. In such situations, there is a chance that other lines become overloaded (the amount of power willing to flow through them exceeds their capacities). As a result, these lines and nodes will not be able to function anymore and thus cascading failure will happen. There are many defensive strategies to prevent cascading failures. One strategy proposed in the literature is by selectively removing nodes or links to reduce the size of cascading and to prevent the propagating failure to the rest of the network. Although results show that this method is an efficient strategy defense, but removal always increases the immediate damage on the network. Another strategy is rewiring or adding extra nodes in the network. These strategies have shown improvement in robustness of networks against cascading failure but they change networks' topologies in a rather extreme way.

In contrast to methods mentioned above, Weighting Scheme method proposed here improve the robustness of the network by applying less extreme changes in the topology of the network. Weighting Scheme improves robustness by adjusting weights of links. In other words, it brings changes by adjusting line flow capacities to improve the robustness. Since the total weights remain unchanged, it means that weights of some links are increased while others are decreased. Adjusting power flow capacities can be interpreted as controlling the flow of power over the lines. In some cases increasing in weights of links can be done by switching on some extra backup lines installed and decreasing may be done by reducing the flow passing the lines by control systems. Once backup lines are installed, it is a matter of turning them on when the capacity of a line needs to be increased. In this sense, our method could be more feasible in practice (compared to the method that needs rewiring and/or adding extra nodes in the network) while at the same time it improves robustness of the network in distributed and decentralized environment dynamically.
Further, in the future grid, very large number of distributed (renewable) energy sources will be connected to the existing grid. Since these distributed renewable energy resources are intermittent (they enter and leave the grid due to their availability), the new generation of power grid must address the dynamic behavior of both distribution and transmission networks. In such dynamic environments since the generators and loads are changing the changes already made to improve robustness by adding extra nodes or rewiring might be useless when topology is dynamic (such as in distributed networks). In contrast our method can easily cope with such dynamic environment: since the method is run by nodes based on the nodal topology (not the network topology), entering a node requires that node to do its adjustment.

In the future the method must be further analyzed including the dynamic of power system to examine its effect on cascading failure: under which condition and situation the method can prevent or reduce the risk of cascading failure and under which circumstances it might increase the risk of such problems. Further optimization methods can be analyzed in fine tuning Weighting Scheme algorithm to achieve better and more realistic results by including the dynamic of power system networks. As an example, one can consider a rather less aggressive weight adjustment to reduce the possibility of cascading failure effects. Weighting Scheme proposed here adjusts weights by trying to redistribute weights evenly. The resulting network is not an optimal homogeneous network (in its absolute sense) where all nodes are topologically equivalent but each node has its local homogeneous topology. The reason to choose such approach was to examine whether in theory such adjustment improves the robustness. Therefore to what extent the method is realistic was not our primary concern. A less aggressive method could be an incremental approach in which weights are adjusted as a fraction of their original values each time the algorithm is run. Another alternative can be to let some nodes adjusts their weights in the network instead of having all of them run the algorithm. For this latter case, more communication and coordination between nodes are needed to let them choose who is going to do adjustment. To wrap up, the approach proposed here can be a start of upcoming projects addressing the problem of how the static and dynamic robustness of the network can be related.

8.1 List of Contribution

The major contribtutions of this thesis can be listed as follows:

- Developing a power system simulation tool in JAVA
- Integrating AgentScope with power system simulation tool
- Building an experimental environment on top of AgentScope and power system simulation environment
- Proposing and developing a distributed algorithm called Weighting Scheme
- Applying Net-ability and its related structural vulnerability metrics to evaluate the robustess of PTGs
- Testing and examining the behavior and the effectiveness of WS algorithm by doing an experiment

Acknowledgement

This work was supported by the faculty of EEMCS department of Computer Science (Information Architecture) and the faculties of TPM department of service system engineering of Delft University of technology, the Netherlands, TNO, the Netherlands and Dipartimento di Ingegneria Elettrica, Politecnico di torino, Torino, Italy.

This research project would not have been possible without the support, encouragement of many people. The author wishes to express her gratitude to her supervisors, Prof. Dr. R. Kooij and Dr. E. Ogston who were not only helpful and offered invaluable assistance, support and guidance but also have encouraged and challenged her throughout the process. Gratitude is also due to the members of the supervisory committee, Prof. Dr. J. Dietz and Prof. Dr. F. Brazier without whom and their supports this study would not have been successful. Special thanks to Luo Lingen (PhD student at Politecnico di torino) for his collaboration and supports and to Yakup and Arman for their valuable comments and discussions.

My deepest gratitude and respect to my dearest mom and dad for supporting and loving me unconditionally and for the sacrifices they made to let me follow my dreams. To my dearest sister, Maryam, who has always supported, encouraged and loved me in all aspects and has been always there whenever I needed her.

I would like to thank my dearest friend, Golara, without whose priceless emotional supports and the fun we have had together during the entire study, I wouldn't be writing this acknowledgment now. And finally to Jos who has always believed in me, for his encouragement and valuable supports.

Bibliography

[1] R Albert. The diameter of the world wide web. *Arxiv preprint cond-mat/9907038*, 1999.

[2] R Albert. Error and attack tolerance of complex networks. *Arxiv preprint cond-mat/0008064*, 2000.

[3] R Albert. Structural vulnerability of the North American power grid. *Physical Review E*, 2004.

[4] LAN Amaral. Classes of small-world networks. *Proceedings of the ...*, 2000.

[5] S. Arianos, E. Bompard, A. Carbone, and F. Xue. Power grids vulnerability: a complex network approach. *Arxiv preprint arXiv:0810.5278*, 2008.

[6] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *science*, 1999.

[7] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.U. Hwang. Complex networks: Structure and dynamics. *Physics reports*, 424(4-5):175–308, 2006.

[8] E Bompard. Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure ...*, 2009.

[9] E Bompard. Extended topological approach for the assessment of structural vulnerability in transmission networks. *... Transmission & Distribution, IET*, 2010.

[10] M. Braun and P. Strauss. A review on aggregation approaches of controllable distributed energy units in electrical power systems. *International Journal of Distributed Energy Resources*, 4(4):297–319, 2008.

[11] RE Brown. Impact of Smart Grid on distribution system design. *... and Delivery of Electrical Energy in the 21st ...*, 2008.

[12] D Caves. Mitigating price spikes in wholesale markets through market-based pricing in retail markets. *The Electricity Journal*, 2000.

[13] G Chen and ZY Dong. An improved model for structural vulnerability analysis of power networks. *Physica A: Statistical Mechanics ...*, 2009.

[14] R Cossent. Towards a future with large penetration of distributed generation: Is the current regulation of electricity distribution ready? Regulatory recommendations under a. *Energy Policy*, 2009.

[15] P Crucitti. A topological analysis of the Italian electric power grid. *Physica A: Statistical Mechanics and its* ..., 2004.

[16] P Crucitti. Model for cascading failures in complex networks. *Physical Review E*, 2004.

[17] P Crucitti. Locating critical lines in high-voltage electrical power grids. *Fluctuation and Noise Letters*, 2005.

[18] D-Cision. Smart Grid in de toekomstbeelden uit het Energierapport. Technical report, 2010.

[19] M Ding. Reliability assessment to large-scale power grid based on small-world topological model. *Power System Technology, 2006. PowerCon* ..., 2006.

[20] Italy. Dipartimento di Ingegneria Elettrica, Politecnico di torino, Torino. Power Flow Study - Unpublished.

[21] A Dwivedi. Identifying vulnerable lines in a power network using complex network theory. *Industrial Electronics, 2009.* ..., 2009.

[22] A Dwivedi. Analyzing power network vulnerability with maximum flow based centrality approach. *Industrial Informatics (INDIN),* ..., 2010.

[23] P. ERDS and A . RÉNYI. On the evolution of random graphs. 1960.

[24] M Faloutsos. On power-law relationships of the internet topology. *ACM SIGCOMM Computer* ..., 1999.

[25] H Farhangi. The path of the smart grid. *Power and Energy Magazine, IEEE*, 2010.

[26] Galvin Electricity Initiative. Fact Sheet: The Electric Power System in Unreliable. Technical report, 2008.

[27] Marco Giuliano Andrea Pagani and Aiello. Towards Decentralized Trading: A Topological Investigation of the Dutch Medium and Low Voltage Grids. *CoRR*, abs/1101.1, 2011.

[28] Z Guohua and W Ce. Vulnerability assessment of bulk power grid based on complex network theory. ... *and Power* ..., 2008.

[29] P Hines. A centrality measure for electrical networks. *Hawaii International Conference on* ..., 2008.

[30] Bernardo A. Huberman and Lada A. Adamic. Growth dynamics of the world-Wide web. *J. Reprod. Fertil*, 1993.

[31] Modern Grid Initiative. Annual program and peer review meeting, 2006.

[32] H. Akkermans J.G. Schaeffer. CRISP Final Summary Report. Technical report, 2006.

[33] P Joskow. Lessons learned from electricity market liberalization. *The Energy Journal*, 2008.

[34] DS Kirschen. Demand-side view of electricity markets. *Power Systems, IEEE Transactions on*, 2003.

[35] R.H. Lasseter and P. Paigi. Microgrid: A conceptual solution. In *Power Electronics Specialists Conference, 2004. PESC 04. 2004 IEEE 35th Annual*, volume 6, pages 4285–4290. IEEE, 2004.

[36] V. Latora. How the science of complex networks can help developing strategies against terrorism. *Chaos, Solitons & Fractals*, 2004.

[37] Vito Latora and Massimo Marchiori. Efficient behavior of small-world networks. *Physical Review Letters*, 2001.

[38] B.F. Massoud Amin, S. and Wollenberg. Toward a smart grid: power delivery for the 21st century. *Power and Energy Magazine, IEEE*, 3:34–41, 2005.

[39] Elth Ogston and Frances Brazier. AgentScope: multi-agent systems development in focus. *The 10th International Conference on ...*, 2011.

[40] Elth Ogston, Astrid Zeman, Mikhail Prokopenko, and Geoff James. Clustering Distributed Energy Resources for Large-Scale Demand Management. *First International Conference on SelfAdaptive and SelfOrganizing Systems SASO 2007*, pages(Saso):97–108, 2007.

[41] G. Paul, T. Tanizawa, S. Havlin, and HE Stanley. Optimization of robustness of complex networks. *The European Physical Journal B-Condensed Matter and Complex Systems*, 38(2):187–191, 2004.

[42] Public Service Commission of Wisconsin. Electric Transmission Lines. pages 1–13.

[43] D Pudjianto. Virtual power plant and system integration of distributed energy resources. *Renewable Power ...*, 2007.

[44] C Robinson. Power to the People by Vijay V. Vaitheeswaren. *Energy & Environment*, 2005.

[45] TO Seppa. A practical approach for increasing the thermal capabilities of transmission lines. *Power Delivery, IEEE Transactions on*, 1993.

[46] B. Shargel, H. Sayama, I.R. Epstein, and Y. Bar-Yam. Optimization of robustness and connectivity in complex networks. *Physical Review Letters*, 90(6):68701, 2003.

[47] K Sun. Complex networks theory: A new method of research in power grid. *... and Distribution Conference and Exhibition: Asia and ...*, 2005.

[48] A Sydney and C Scoglio. Elasticity: topological characterization of robustness in complex networks. *Proceedings of the 3rd ...*, 2008.

[49] U.S. Department of Energy. The Smart Grid: An Introduction, 2008.

[50] Massimo Marchiori2 Vito Latora. Vulnerability and protection of infrastructure networks. *Physical Review E*, 2005.

[51] FBEOM Warnier. The Future of Energy Markets and the Challenge of Decentralized Self-Management. *homepage.tudelft.nl*.

[52] Duncan J. Watt and Steven H. Strogatz. Collective dynamics of 'small-world'networks. *nature*, 1998.

[53] DJ Watts. Small worlds: the dynamics of networks between order and randomness. 2003.

[54] F.A.N.W. XIAO. Complex networks: topology, dynamics and synchronization. *International Journal of Bifurcation and Chaos*, 12(5):885–916, 2002.

[55] Huang Xinbo and Cheng Ronggui. Theoretical study on dynamic capacity-increase of transmission lines. *Condition Monitoring and Diagnosis, ...*, 2008.

[56] H Zhao. Power transmission network vulnerable region identifying based on complex network theory. *... and Restructuring and Power ...*, 2008.

[57] Ray D Zimmerman and Carlos E Murillo-s. User s Manual. *Power*, pages 1–116, 2011.

[58] L Zongxiang. Cascading failure analysis of bulk power system using small-world network model. *... Applied to Power ...*, 2004.