

# **Graph Theory Based Protection Method**

**For Smart Grid**

**A Project Report**

*Submitted in partial fulfillment of  
requirements for the  
award of the degree of*

**Bachelor of Technology**

*in*

**Electrical Engineering**

**&**

**Master of Technology**

*in*

**Microelectronics and VLSI Design**

***By***

**Vinay Kumar Meena**

**EE09B063**



**Department of Electrical Engineering  
Indian Institute of Technology, Madras**

**May 2015**

# Thesis Certificate

This is to certify that the project report entitled “**Protection of Smart Grid Using Graph Theory**”, submitted by **Mr. Vinay Kumar Meena (Roll Number: EE09B063)**, to the **Indian Institute of Technology, Madras**, in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Electrical Engineering & Master of Technology in Microelectronics & VLSI Design**, is a bonafide record of work carried by him.

Place: Chennai

Date:06/05/2015

Dr. K. S. Swarup

Department of Electrical Engineering

Indian Institute of Technology Madras

Chennai 600036

# Acknowledgement

I wish to express my deep sense of gratitude and indebtedness to my project guide Dr. K. S. Swarup, Professor in Department of Electrical Engineering, IIT Madras for his most valuable guidance, discussions, suggestions and encouragement, from the conception to the completion of this project. His moral support, unreserved co-operation and generosity, dedication, systematic approach and persistence to scientific research have made a great impact on me. I could not have hoped for a better guide. He stood as constant source of inspiration to me while doing the Project.

I would also like to thank my professors and friends from my undergraduate studies while at Indian Institute of Technology, Madras. The preparation and experience I gained were invaluable.

Finally, I would to like to dedicate my work to my family for their unconditional love and moral support, which has allowed me to achieve what I have and will always do so in future. Special thanks to Girish Ramakrishnan, Hershdeep Singh, Anish Tamse, Jayant Thatte & Ankit Behura for their brilliant co-operation and support, whenever I needed it.

Place: Chennai

Vinay Kumar

Date:06/05/2015

# Abstract

**Key words:** Smart Grid, Graph Theory, Intelligent Electronic Devices, Smart, Power Grid, Management, Protection, Security, Privacy, Protection Zones, Advanced Metering Infrastructure, Automatic Meter Reading, Distributed Energy Resource, Supervisory Control and Data Acquisition, Wide-Area Measurement System

Smart grids are just modern power grids. When we combine power grid with IT technology, we form smart grid. The focus of this project is to detect the fault in a grid network using graph theory method. Graph theory method is going to use a lot of IEDs (Intelligent electronic devices) for detecting fault. For any power network, once we get directed graph of network. We can easily get Adjacency matrix, Reachability matrix and Incidence matrix. When it comes to reachability matrix, we always need to set up reachable steps. We will decide reachable steps on the basis of network and the IEDs. PMU (Phase Measurement Unit) can be used to sample current signals, GPS (Global Position System) can be used to synchronize current signals, and fiber communication network is used to transmit signals. Graph theory based protection zone partitioning reduces IED communication area and increases speed and accuracy of protection system. Through simulation analysis, protection system locates fault accurately when one or more protection devices are out of service. The reliability of protection system is enhanced. Graph theory based protection system has features such as accuracy, quickness, no need to set up and so on. It provides an effective protection system solution for complicated smart grid.

# **Table of Contents**

<b>Thesis Certificate</b>	<b>II</b>
<b>Acknowledgement</b>	<b>III</b>
<b>Table of Contents</b>	<b>IV</b>
<b>Abbreviations</b>	<b>V</b>

## **Abbreviations**

<b>SG</b>	<b>Smart Grid</b>
<b>AC</b>	<b>Alternating current</b>
<b>AP</b>	<b>Access point</b>
<b>DC</b>	<b>Direct current</b>
<b>AMI</b>	<b>Advanced metering infrastructure</b>
<b>AMR</b>	<b>Automatic meter reading</b>
<b>DER</b>	<b>Distributed energy resource</b>
<b>DG</b>	<b>Distributed generation</b>
<b>DOE</b>	<b>Department of energy</b>
<b>DoS</b>	<b>Denial-of-service</b>
<b>EV</b>	<b>Electric vehicles</b>

<b>FNET</b>	<b>Frequency monitoring network</b>
<b>G2V</b>	<b>Grid-to-vehicle</b>
<b>GPS</b>	<b>Global positioning system</b>
<b>IEEE</b>	<b>Institute of electrical and electronics engineers</b>
<b>IETF</b>	<b>Internet engineering task force</b>
<b>IP</b>	<b>Internet protocol</b>
<b>PHEV</b>	<b>Plug-in hybrid electric vehicle</b>
<b>PLC</b>	<b>Powerline communications</b>
<b>PMU</b>	<b>Phasor measurement unit</b>
<b>QoS</b>	<b>Quality of service</b>
<b>RF</b>	<b>Radio frequency</b>
<b>SCADA</b>	<b>Supervisory control and data Acquisition</b>



<b>SEP</b>	<b>Smart energy profile</b>
<b>SG</b>	<b>Smart grid</b>
<b>TCP</b>	<b>Transmission control protocol</b>
<b>V2G</b>	<b>Vehicle-to-grid</b>
<b>VPP</b>	<b>Virtual power plant</b>
<b>WAMS</b>	<b>Wide-area measurement system</b>
<b>WMN</b>	<b>Wireless mesh network</b>
<b>WSN</b>	<b>Wireless sensor network</b>

# **Chapter 1**

## **Introduction**

### **1.1 Introduction to Problem**

Electrical power transmission and distribution systems supply power to dispersed residential customers, commercial and small industrial customers in a safe, reliable and economical fashion. This is achieved by maintaining stable voltage levels, making power factor correction through reactive compensation and offering continuous uninterrupted electric power to meet the demand. Electric power supply interruptions can be planned and unplanned. Planned outages are part of maintenance procedures. However, it is the unplanned outage events which are to be minimized. We will focus our study on detecting and identifying some of those power system faults by some alternative method which does not affect main protection method. This alternative method would play a major role in case main protection method failure.

Relay protection, as “the first defense line” of the power system, undertakes the important responsibility of high quality, stability and reliability of power supply. The establishment of smart grid requires relay protection to adapt to the characteristics of the new type of power grid. The traditional relay protection just uses local electric signal to locate

fault in power network. It uses protection criterion to locate faults accurately. Communication among protection IEDs (Intelligent Electric Device) by optical fiber acquires current signals in different nodes in the power grid. Different level protection zones are partitioned by graph theory. Dynamic online partitioning of the protection zone enhances the adaptability of protection system to the power grid structure.

## 1.2 Motivation

When fault occurs in an electric power system, the effects are often not restricted to the faulty section, but noticeable throughout the whole system. The electric power supply becomes unreliable if faults are not diagnosed as soon as they occur. This protection method is independent with traditional protection. It doesn't clash with traditional main protection. Just like double main protection, the two protection systems have no electric link. When one protection is out of service, the other one can still operate reliably. It uses current differential protection criterion to locate faults accurately. Communication among protection IEDs (Intelligent Electric Device) by optical fiber acquires current signals in different nodes in the power grid. Different level protection zones are partitioned by graph theory. It changes disadvantages of main and backup protection coordinating by time delay and setting values in traditional relay protection and improves reliability and action speed of relay protection effectively. Large funds and resources are being employed by different countries for research and development to modernize power grids. Dynamic online partitioning of the protection zone enhances the adaptability of protection system to the power grid structure. Even if we detect the fault in the system, the restoration after fault occurrence also plays an major role. Here, PMU (Phase Measurement Unit) is going to use to sample current signals, GPS (Global Position System) is going to use to synchronize current signals, and fiber

communication network is used to transmit signals. We must carry it out by putting in place a scheme capable of fault detection and diagnosis; thus maintaining system stability, minimizing customer and network damages, as well as economic losses. Special emphasis has been placed on research in fault detection, isolation and recovery (FDIR) for power systems.

## 1.3 Objective

The objective is to design an algorithm for detecting fault in buses & lines with the help of different IEDs. Each IED will protect a certain portion of network. In principle protection IED can communicate with any node protection component in power network. But unlimited communication is impractical in the communication system structure. Excessive information exchanging and too many programming loops.

## 1.4 Scope

This project will tell you how to detect fault in smart grid network with the help of graph theory. Compared with traditional relay protection which only protects one electrical component, each protection component protects a certain area. One kind of common protection component is protection IED. It collects local electrical signals and communicates with the central processing system and other protection IEDs to obtain electric signals in other nodes through the optical fiber transmission network. It also has signal processing and decision-making abilities.

In principle protection IED can communicate with any node protection component in power network. But unlimited communication is impractical in the communication system

structure. Excessive information exchanging and too many protecting program loops will reduce accuracy and speed of protecting function. The action time of wide-area protection and probability of miss trip or mal-operation will significantly increase. The influence of fault in certain node is finite in the whole power network. Electric signals in long distance nodes do not have much significance. So when the protection system is being set up, the protecting scope of each protection IED namely protection zone must be defined firstly. Protection zone which is partitioned properly could make protection IEDs communicating within it.

## **1.5 Thesis Structure**

Chapter 2 tells us about the introduction of Smart Grid. It also tell us about the three major sections of Smart Grid, Smart Infrastructure System, Smart Management System and Smart Protection System.

Chapter 3 gives us introduction of Intelligent Electronics Devices(IEDs). It defines IEDs and their characteristics.

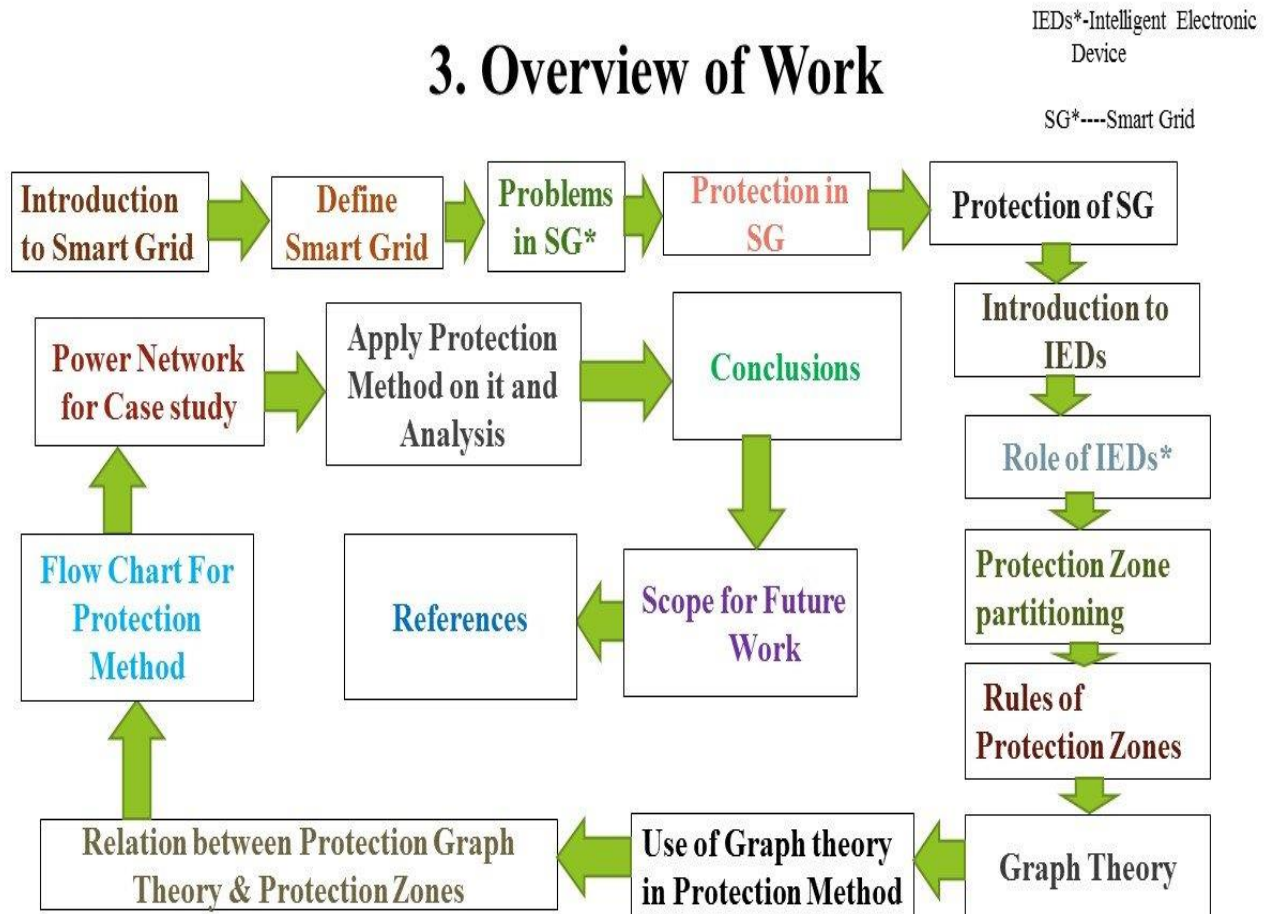
Chapter 4 gives us the introduction of Graph theory. It tells us about the matrices which we are going to use for protection zone partitioning and their definitions. It tells us about the rules of protection zone partitioning. It do comparison with differential protection. It also includes flow chart of graph theory based protection method.

Chapter 5 In this chapter we will do test case study analysis for 220 KV Power Network. It will contain 44 IEDs and 34 nodes.

Chapter 6 In this chapter we will do write of project. We will also look for scope of future work.

## 1.6 Block Diagram of Work Overview

### 3. Overview of Work



## **Chapter 2**

## **Smart Grid**

### **2.1 Introduction**

The term grid is used for an electricity system that may support all or some of the following four operations: electricity generation, transmission, distribution and control. A smart grid, also called smart electrical/power grid, intelligent grid, intelligrid, future grid, inter grid, or intra grid, is an enhancement of the 20th century power grid. The traditional power grids are generally used to carry power from a few central generators to a large number of users or customers. In contrast, the smart grid uses two-way flows of electricity and information to create an automated and distributed advanced energy delivery network.

## SMART GRID

A vision for the future — a network of integrated microgrids that can monitor and heal itself.

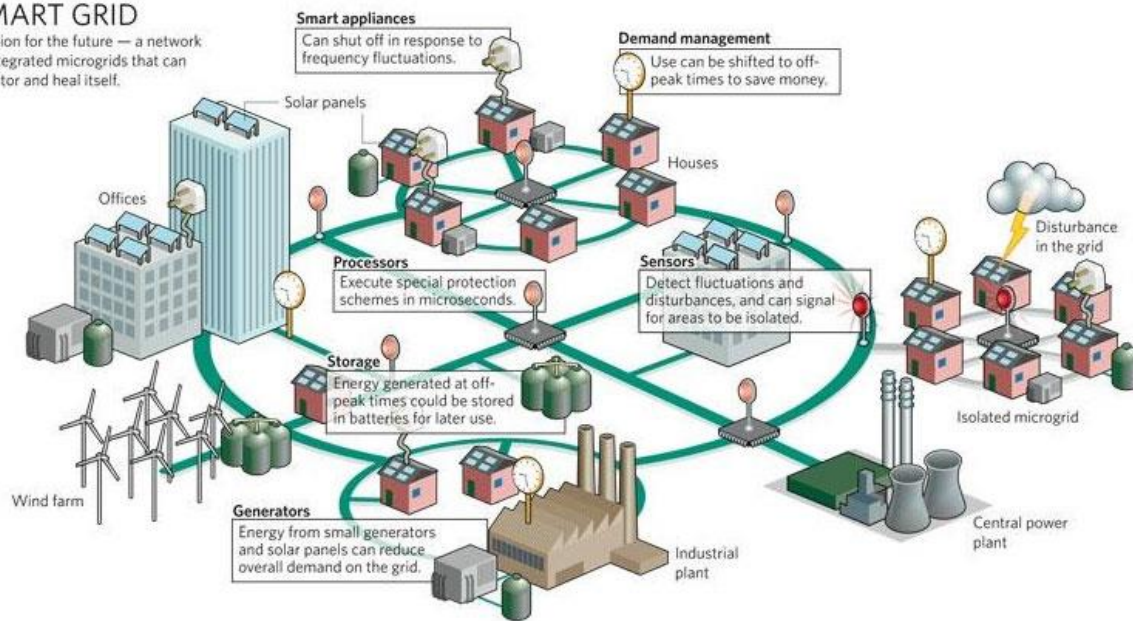


Fig. 1 Smart Grid Network from Generation to Distribution

By utilizing modern information technologies, the SG is capable of delivering power in more efficient ways and responding to wide ranging conditions and events. Broadly stated, the SG could respond to events that occur anywhere in the grid, such as power generation, transmission, distribution, and consumption, and adopt the corresponding strategies. For instance, once a medium voltage transformer failure event occurs in the distribution grid, the SG may automatically change the power flow and recover the power delivery service. Let us consider another example of demand profile shaping. Since lowering peak demand and smoothing demand profile reduces overall plant and capital cost requirements, in the peak period the electric utility can use real-time pricing to convince some users to reduce their power demands, so that the total demand profile full of peaks can be shaped to a nicely smooth demand profile. More specifically, the SG can be regarded as an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion across electricity



generation, transmission, substations, distribution and consumption to achieve system that is clean, safe, secure, reliable, resilient, efficient, and sustainable. This description covers the entire spectrum of the energy system from the generation to the end points of consumption of the electricity. The ultimate SG is a vision. It is a loose integration of complementary components, subsystems, functions, and services under the pervasive control of highly intelligent management-and-control systems. Given the vast landscape of the SG research, different researcher may express different visions for the SG due to different focuses and perspectives.

## 2.2 Comparison between Smart Grid & Power Grid

Power Grid	Smart Grid
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors through out
Manual-monitoring	Self-monitoring
Manual-restoration	Self-restoration
Failures & blackouts	Adaptive & islanding
Limited Control	Pervasive Control
Few customers choice	Many customers choice

## 2.3 Major Systems from Technical Point of View

### 2.3.1 Smart Infrastructure System

The smart infrastructure system is the energy, information, and communication infrastructure underlying of the SG that supports

- 1) Advanced electricity generation, delivery and consumption
- 2) Advanced information metering, monitoring & management
- 3) Advanced communication technologies

The smart infrastructure system is the energy, information, and communication infrastructure underlying the SG. It supports two-way flow of electricity and information. Note that it is straightforward to understand the concept of “two-way flow of information.” “Two-way flow of electricity” implies that the electric energy delivery is not unidirectional anymore. For example, in the traditional power. The smart infrastructure system is the energy, information, and communication infrastructure underlying the SG. It supports two-way flow of electricity and information. Note that it is straightforward to understand the concept of “two-way flow of information.” “Two-way flow of electricity” implies that the electric energy delivery is not unidirectional anymore. For example, in the traditional power grid, the electricity is generated by the generation plant, flow of electricity and information. Note that it is straightforward to understand the concept of “two-way flow of information.” “Two-way flow of electricity” implies that the electric energy delivery is not unidirectional anymore. For example, in the traditional power grid, the electricity is generated by the generation plant, then moved by the transmission grid, the distribution grid, and finally delivered to users. In an SG, electricity can also be put back into the grid by users. For example, users may be able to generate electricity using solar panels at homes and put it back into the grid, or electric vehicles may provide power to help balance loads by “peak shaving” (sending power back to the grid when demand is high). This backward flow

is important. For example, it can be extremely helpful in a microgrid that has been ‘islanded’ due to power failures. We further divide this smart infrastructure into three subsystems: the smart energy subsystem, the smart information subsystem, and the smart communication subsystem.

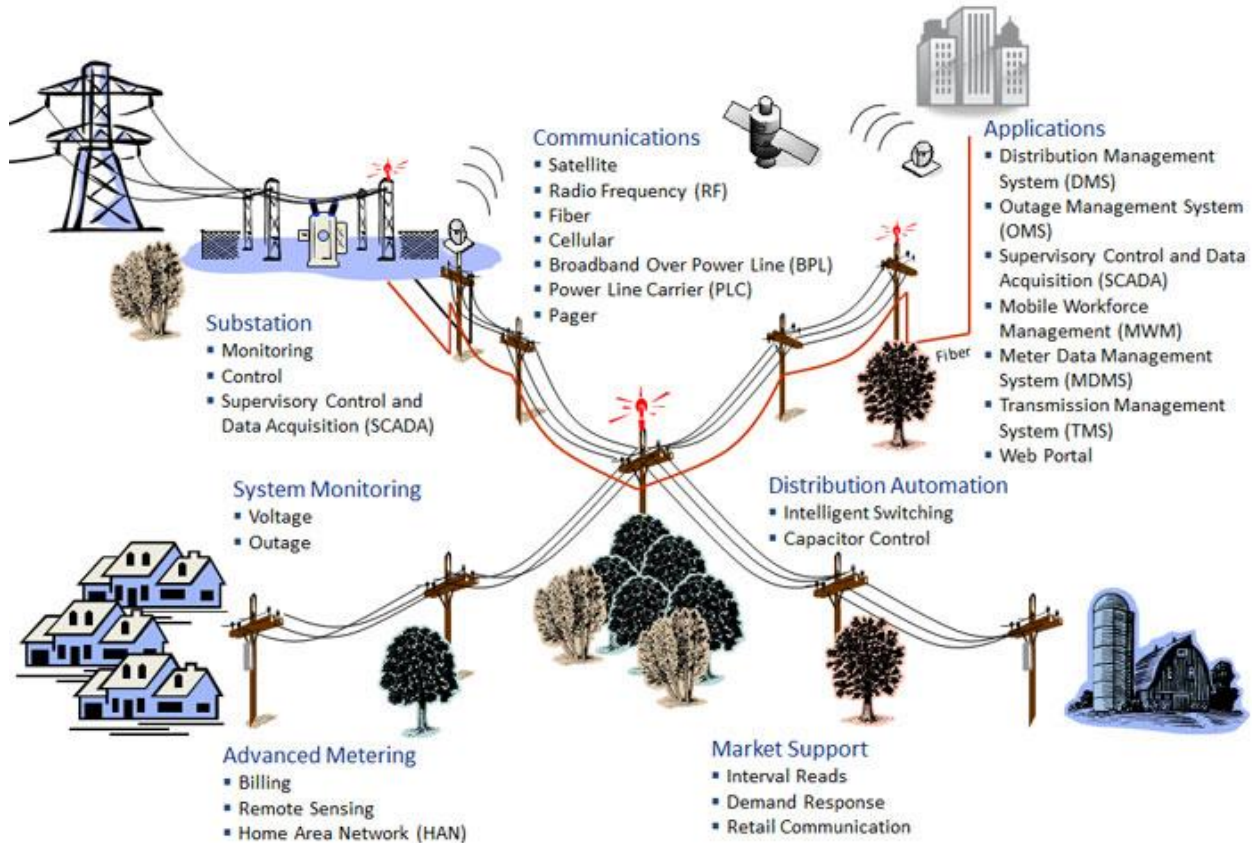


Fig.2 Components of Smart Grid Network

## 2.3.2 Smart Energy Subsystem

Two-way flows of electricity and information lay the infrastructure foundation for the SG. The smart infrastructure can be subdivided into the smart energy subsystem, the smart information subsystem, and the smart communication subsystem, respectively. In this section, we explore existing works on the smart energy subsystem and outline some future research directions and challenges. The traditional

power grid is unidirectional in nature. Electricity is often generated at a few central power plants electromechanical generators, primarily driven by the force of flowing water or heat engines fueled by chemical combustion or nuclear power. In order to take advantage of the economies of scale, the generating plants are usually quite large and located away from heavily populated areas. The generated electric power is stepped up to a higher voltage for transmission on the transmission grid. The transmission grid moves the power over long distances to substations. Upon arrival at a substation, the power will be stepped down from the transmission level voltage to a distribution level voltage. As the power exits the substation, it enters the distribution grid. Finally, upon arrival at the service location, the power is stepped down again from the distribution voltage to the required service voltage. In contrast with the traditional power grid, the electric energy generation and the flow pattern in an SG are more flexible. For example, the distribution grid may also be capable of generating electricity by using solar panels or wind turbines. In this survey, we still divide the energy subsystem into power generation, transmission grid, and distribution grid. We still divide the energy subsystem into power generation, transmission grid, and distribution grid.

### **2.3.2.1 Power Generation**

Electricity generation is the process of generating electricity from other forms of energy, such as natural gas, coal, nuclear power, the sun, and wind. Michael Faraday discovered the fundamental principles of electricity generation: electricity can be generated by the motion of a loop of wire or a disc of copper between the

poles of a magnet, a principle still being used today. There are many energy sources used to generate electric power. As fossil fuels get depleted and generally get more expensive, it is expected that renewable energy will play more important role in the future power generation. In contrast to the power generation in the traditional power grid, smarter power generation becomes possible as the two way flows of electricity and information are supported. A key power generation paradigm enabled by SG will be the distributed generation. DG takes advantage of distributed energy resource systems (e.g. solar panels and small wind turbines), which are often small-scale power generators, in order to improve the power quality and reliability. For example, a microgrid, which is a localized grouping of electricity generators and loads, can disconnect from the microgrid so that distributed generators continue power the users in this microgrid without obtaining power from outside. Thus, the disturbance in the microgrid can be isolated and the study from the International Energy Agency pointed out that a power system based on a large number of reliable small DGs can operate with the same reliability and a lower capacity margin than a system of equally reliable large generators. A review of different distributed energy technologies such as microturbines, photovoltaic, fuel cells, and wind power turbines can be found in. However, implementing DG(s) in practice is not an easy proposition due to several reasons. First DG involves large scale deployments for generation from renewable resources, such as solar and wind, whose yield is, however, subject to wide fluctuations. In general, the generation patterns resulting from these renewables and the electricity demand patterns are far from being equal. Therefore, effective utilization of the DG in a

way that is cognizant of the variability of the yield from renewable sources is important. Considering the DG's potential benefits on power quality, a systematic research on how to balance the high capital costs and the reliable power supplies brought by DG is essential. Although we can only see a limited penetration of DG in today's power system, the future SG is expected to adopt large number distributed generators to form a much more decentralized power system. As predicted, it may evolve from the present system in three stages:

- 1) Accommodating DGs in the current power system
- 2) Introducing a decentralized system of DGs with the centralized generation system
- 3) Supplying most power by DGs and a limited amount by central generation

Note that as DG enables the users to deploy their own generators, the large-scale deployment of DG will also change the traditional power grid design methodology, in which the generators are connected to the transmission grid. The development and deployment of DG further leads to a concept, namely Virtual Power Plant (VPP), which manages a large group of distributed generators with a total capacity comparable to that of a conventional power plant. This cluster of distributed generators is collectively run by a central controller. The concerted operational mode delivers extra benefits such as the ability to deliver peak load electricity or load-aware power generation at short notice. Such a VPP can replace a conventional power plant while providing higher efficiency and more flexibility. Note that more flexibility allows the system to react better to fluctuations. However, a VPP is also a complex system requiring a complicated optimization, control, and secure communication methodology. Now we are aiming to find and

describe a suitable software framework that can be used to help implement the concept of a VPP in future power systems, and emphasized the importance of Service Oriented Architecture in implementing the VPP.

### **2.3.2.2 Transmission Grid**

On the power transmission side, factors such as infrastructure challenges (increasing load demands and quickly aging components) and innovative technologies (new materials, advanced power electronics, and communication technologies) drive the development of smart transmission grids. The smart transmission grid can be regarded as integrated system that functionally consists of three interactive components: smart control centers, smart power transmission networks, and smart substations. Based on the existing control centers, the future smart control centers enable many new features, such as analytical capabilities for analysis, monitoring, and visualization. The smart power transmission networks are conceptually built on the existing electric transmission infrastructure. However, the emergence of new technologies (e.g. new materials, electronics, sensing, communication, computing, and signal processing) can help improve the power utilization, power quality, and system security and reliability, thus drive the development of a new framework architecture for transmission networks. The vision of the smart substation is built on the existing comprehensive automation technologies of substations. Although the basic configurations of high-voltage substations have not changed much over the years, the monitoring, measurement, and control equipment have undergone a sea change in recent years. Major characteristics of a smart substation shall include digitalization, autonomization,



coordination, and self-healing. By supporting these features, a smart substation is able to respond rapidly and provide increased operator safety. In brief, with a common digitalized platform, in the smart transmission grid it is possible to enable more flexibility in control and operation, allow for embedded intelligence, and foster the resilience and sustainability of the grid.

### **2.3.2.3 Distribution Grid**

For the distribution grid, the most important problem is how to deliver power to serve the end users better. However, as many distributed generators will be integrated into the smart distributed grid, this, on one hand, will increase the system flexibility for power generation, and on the other hand, also makes the power flow control much more complicated, in turn, necessitating the investigation of smarter power distribution and delivery mechanisms. One researcher proposed two in-home power distribution systems, in which the information is added to the electric power itself and electricity is distributed according to this information. The first one is a circuit switching system based on alternating current (AC) power distribution, and the other is a direct current (DC) power dispatching system via power packets. Note that the packetization of energy is an interesting but challenging task since it requires high power switching devices. Researchers have shown that silicon carbide junction gate field-effect transistors are able to shape electric energy packets . Hence, the system proposed in has the potential as an intelligent power router. More specifically, supplied electricity from energy sources is divided into several units of payload. A header and a footer are attached to the unit to form an electric energy packet. When the router receives electrical energy packets, they are sorted according to the addresses in the headers and then sent to the corresponding loads. Using energy packet, providing power is easily regulated by controlling the

number of sent packets. In addition, many in-home electric devices are driven by DC power and have built-in conversion circuits to commutate AC input voltage. Thus, DC based power distribution is feasible. These systems will make in-home power distribution systems more efficient and easier to control energy flow.

### **2.3.3 Smart Information Subsystem**

The evolution of SG relies on not only the advancement of power equipment technology, but also the improvement of sophisticated computer monitoring, analysis, optimization, and control from exclusively central utility locations to the distribution and transmission grids. Many of the concerns of distributed automation should be addressed from an information technology perspective, such as interoperability of data exchanges and integration with existing and future devices, systems, and applications. Therefore, a smart information subsystem is used to support information generation, modeling, integration, analysis, and optimization in the context of the SG. In this section, we concentrate on the smart information subsystem. We first explore the information metering and measurement, which generates information from end entities (e.g. smarter meters, sensors, and phasor measurement units) in an SG. This information is often used for billing, grid status monitoring, and user appliance control. We then explore the information management, including data modeling, information analysis, integration, and optimization.

#### **2.3.3.1 Information Metering and Measurement**

Study in information metering and measurement can be classified into smart metering, and smart monitoring and measurement.

Smart metering is the most important mechanism used in the SG for obtaining

information from end users's devices and appliances, while also controlling the behavior of the devices. Automatic metering infrastructure (AMI) systems which are themselves built upon automatic meter reading (AMR) systems, are widely regarded as a logical strategy to realize SG. AMR is the technology of automatically collecting diagnostic, consumption, and status data from energy metering devices and transferring that data to a central database for billing, troubleshooting, and analyzing. AMI differs from traditional AMR in that it enables two-way communications with the meter. Therefore nearly all of this information is available in real time and on demand, allowing for improved system operations and customer power demand management.

On the other hand smart meters which support two-way communications between the meter and the central system, are similar in many aspects to AMI meters, or sometimes are regarded as part of the AMI. A smart meter is usually an electrical meter that records consumption in intervals of an hour or less and sends that information at least daily back to the utility for monitoring and billing purposes. Also, a smart meter has the ability to disconnect-reconnect remotely and control the user appliances and devices to manage loads and demands within the future "smart-buildings." From a consumer's perspective, smart metering offers a number of potential benefits. For example, end users are able to estimate bills and thus manage their energy consumptions to reduce bills. From a utility's perspective, they can use smart meters to realize real-time pricing, which tries to encourage users to reduce their demands in peak load periods, or to optimize power flows according to the information sent from demand sides.

An important function in the vision of SG is monitoring and measurement of grid status. We review the following two major monitoring and measurement approaches, namely sensors and phasor measurement units.

Sensors or sensor networks have already been used as a monitoring and measurement approach for different purposes . In order to detect mechanical failures in power grids such as conductor failures, tower collapses, hot spots, and extreme mechanical conditions, sensor networks should be embedded into the power grid and help to assess the real-time mechanical and electrical conditions of transmission lines, obtain a complete physical and electrical picture of the power system in real time, diagnose imminent as well as permanent faults, and determine appropriate control measures that could be automatically taken and/or suggested to the system operators once an extreme mechanical condition appears in a transmission line. Wireless sensor networks (WSNs) in particular, given their low cost, can provide a feasible and cost-effective sensing and communication platform for remote system monitoring.

Recent developments in the SG have spawned interest in the use of phasor measurement units (PMUs) to help create a reliable power transmission and distribution infrastructure. A PMU measures the electrical waves on an electrical grid to determine the health of the system. Technically speaking, a phasor is a complex number that represents both the magnitude and phase angle of the sine waves found in electricity. Phasor measurements that occur at the same time are called synchrophasors as are the PMU devices that allow their measurement. Typically, PMU readings are obtained from widely dispersed locations in a power system network and synchronized using the global positioning system (GPS) radio clock. With a large number of PMUs and the ability to compare shapes from alternating current (AC) readings everywhere on the grid, system operators can use the sampled data to measure the state of the power system and respond to system conditions in a rapid and dynamic fashion. The frequency monitoring network (FNET) project utilized a network of low cost, high-precision frequency

disturbance recorders to collect synchrophasor data from the power grid . Some of the latest implementations of FNET(frequency monitoring network)'s applications by using PMUs, which are significantly better at observing power system problems than the earlier implementations. The current FNET system hierarchy is suitable for high volume data transfer, processing, storage, and utilization. A variety of applications, especially with regards to real-time dynamic monitoring, have been developed and integrated into the system. FNET is growing into a mature, multifunctional, and low-cost phasor measurement system with stable performance and high accuracy. Early research on the applications of PMU technology was mainly focused on validation of system models and accurate postmortem analysis. However, now with wide-scale realtime PMU data being obtainable, system operators have the capability of deploying system state estimation procedures and system protection functionalities in power grids, with the goal of making the power system immune to catastrophic failures. Several countries, such as Brazil, China, France, Japan, South Korea, Mexico, Norway, and the U.S., have installed PMUs on their power grid systems for research . The installation of PMUs on transmission grids of most major power systems has become an important activity.

## **2.3.4 Smart Protection System**

The smart protection system in SG must address not only inadvertent compromises of the grid infrastructure due to user errors, equipment failures, and natural disasters, but also deliberate cyber attacks, such as from disgruntled employees, industrial spies, and terrorists. In this section, we explore the works targeted the smart protection system in SG. We first review the works related to system reliability analysis and failure protection mechanisms, and then the security and privacy issues in SG.

## 2.3.4.1 System Reliability and Failure Protection

Reliability is the ability of a component or system to perform required functions under stated conditions for a stated period of time. System reliability is an important topic in power grid research and design. Furthermore, cascading blackouts could happen. For example, in the infamous 2003 East Coast blackout, 50 million people in the U.S. and Canada lost power for up to several days. The future SG is expected to provide more reliable system operation and smarter failure protection mechanism.

It is expected that distributed generation (DG) will be widely used in SG. One author proposed to take advantage of new architectures such as microgrid to simplify the impact of DG on the grid. Intuitively, as loads are being served locally within a microgrid, less power flows within the entire grid infrastructure. Thus, the reliability and stability of the SG can be enhanced. They found a very encouraging result that local power generation, even when only introducing a small number of local generators into the grid, can reduce the likelihood of cascading failures dramatically. It is being observed that ideal mix of the SG resources (e.g. distributed renewable sources, demand response, and storage) leads to a flatter net demand that eventually further improves reliability. However, realizing this requires a systematic approach – developing a common vision for cohesive grid wide integration of necessary information technologies. Furthermore, the reliability and stability of an SG also depends on the reliability of the measurement system which is used to monitor the reliability and stability of the SG. Recently, the wide-area measurement system (WAMS) based on phasor measurement units (PMUs) is becoming an important component for the monitoring, control, and protection functions in SG. In order to analyze the reliability of WAMS, a quantified reliability evaluation method by combining Markov modeling and state enumeration techniques. This method can be used for evaluating the reliability

of the backbone communication network in WAMS and the overall WAMS from a hardware reliability viewpoint. Another research topic is using simulation for system reliability analysis. The more accurately a simulation platform can emulate the behavior and performance of an SG architecture, the better we will understand its advantages and potential shortcomings. However, the question is how to build up a simulation system which is accurate, flexible, adaptable, and scalable enough. It is being found that on utilizing an incremental method, beginning with simulating a local microgrid, but with a scalable design that can grow hierarchically into a more complete model. Such a simulator can help us understand SG issues and identify ways to improve the electrical grid. Many people proposed to model both the communication network and the power system in SG using simulation. This model provides means to examine the effect of communication failures as a function of the radio transmission power level.

Failure prediction and prevention play important roles in the smart protection system since they attempt to prevent failures from happening. Second, once the system does fail, failure identification, diagnosis, and recovery are required to make the system recover from the failure and work normally as soon as possible. In addition, since the microgrid is regarded as one of the most important new components in the SG vision, we review the works focused on the microgrid protection. For an SG, one effective approach to preventing failures from happening is predicting the weak points or the region of stability existence in its energy subsystem. An automated process continuously monitors voltage constraints, thermal limits, and steady-state stability simultaneously. This approach can be used to improve the reliability of the transmission grid and to prevent major blackouts.

Now we come to Failure Identification, Diagnosis, and Recovery in a system. Once a failure occurs, the first step must be quickly locating and

identifying the failure to avoid cascading events. Due to the wide deployment of PMUs in SG, many authors have proposed to take advantage of the phasor information for line outage detection and network parameter error identification. Tate and Overbye developed an algorithm which uses known system topology information, together with PMU phasor angle measurements, to detect system line outages. In addition to determining the outaged line, their algorithm also provides an estimate of the pre-outage flow on the outaged line. Later, Tate and Overbye studied how double line outages can be detected using a combination of pre-outage topology information and realtime phase angle measurements that are obtained from PMUs. Cai *et al.* reviewed two popular feature selection methods:

- 1) hypothesis test
- 2) stepwise regression

Those algorithms are used to find out the information that may be buried under the massive data. The ability to “self-heal” in the event of failure is expected to be an important characteristic of SG according to the standards from the National Institute of Standards and Technology (NIST). An effective approach is to divide the power grid into small, autonomous islands (e.g. microgrids) which can work well during normal operations and also continue working during outages. By appropriately controlling the system reconfiguration, the impact of disturbances or failures can be restricted within the islands or can be isolated. Cascading events and further system failures can hence be avoided. Therefore the overall efficiency of system restoration can be improved. Failures could also occur on smart meters so that load data could contain corrupted or missing data. Processing or even recovering such data is important since it contains vital information for day-to-day operations and system analysis. Hence presented B-Spline smoothing and Kernel smoothing based techniques to cope with this issue and



automatically cleanse corrupted and missing data. In addition, for the methodology of making decision on how to process a failure, it is being suggested that the decision-making ability should be distributed to the substation and/or field devices; or at the minimum, to preload these distributed devices with sufficient information such that they can take corresponding automatic actions in the event of a system failure without having to wait for instructions from the central controller. They found that when coupled with a distributed rather than hierarchical communications architecture, preloading substation and field devices with a set of next-actions-to-be-taken instructions can significantly increase grid reliability while simultaneously reducing realtime impact from loss of reliable control.

Protection of microgrids during normal or island operations is also an important research topic since microgrids will be widely used in SG. Note that protection of a microgrid is strongly related to its control and operation issues . For example, traditional protection for distribution grids is designed for high fault-current levels in radial networks. However, during an islanding operation of the microgrid, high fault-currents from the utility grid are not present. Moreover, most of the DG units which will be connected to the low voltage microgrid will be converted/ interfaced with limited fault-current feeding capabilities. This means that the traditional fuse protection of low voltage network is no longer applicable for microgrid, and that new protection methods must be developed. Several protection problems that must be dealt with to successfully operate a microgrid when the utility is experiencing abnormal conditions, and pointed out that there are two distinct sets of problems to solve. The first is how to determine when an islanded microgrid should be formed in the face of abnormal conditions that the utility can experience.

The second is how to provide segments of the microgrid with sufficient coordinated fault

protection while operating as an island separated from the utility. These new issues drive the research on new protection methods.

Two more authors described a relay that uses disturbances in the three phase voltages to provide reliable and fast detection of different types of faults within the microgrid. The choice of an alternative protection scheme for an islanded microgrid is strongly dependent on the type of control implemented.

Security is a never-ending game of wits. SG security is no exception to this paradigm. Cyber security is regarded as one of the biggest challenges in SG. Vulnerabilities may allow an attacker to penetrate a system, obtain user privacy, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. We must note that the advanced infrastructure used in SG on one hand empowers us to realize more powerful mechanisms to defend against attacks and handle failures, but on the other hand opens up many new vulnerabilities. Thus in the following, we also discuss many new security and privacy issues due to the deployment of smart meters, sensors, and PMUs, together with some solutions. Information Metering and Measurement plays an major role when it comes for protecting an system.

One of the security issues comes from the newly deployed smart meters. Smart meters are extremely attractive targets for malicious hackers, since vulnerabilities can easily be monetized. Hackers who compromise a smart meter can immediately manipulate their energy costs or fabricate generated energy meter readings to make money. A common consumer fraud in traditional power grid is that customers turn a traditional physical meter upside down in the electrical socket to cause the internal usage counters to run backward. Due to the use of smart meter, this attack can even be done with remote computers. Moreover,

widespread use of smart meters may provide a potentially large number of opportunities for adversaries. For example, injecting misinformation could mislead the electric utility into making incorrect decisions about local or regional usage and capacity. Let us consider a simple but probably effective Denial-of-Service (DoS) attack. An adversary forges the demand request of a smart meter, and keeps requesting a large amount of energy. Within the framework of SG, it is possible that the electric utility disconnects all the appliances connected to this meter so that all the power services for this user are denied. Widespread deployment of smart meters not only leads to a potentially large number of opportunities for adversaries, but also opens up a door to the cyber attacks which could result in broad effects and even large-scale disasters. An ideal attack on a target country is to interrupt its citizen's electricity supply. Until now, the only possible way to do that involves attacks on critical generation, transmission and distribution assets, which are increasingly well defended. However, the emergence of smart meters changes this game. The nightmare scenario is that a country installs tens of millions of smart meters, controlled by a few central controllers. The attacker can compromise these controllers and send the combination of commands that cause disastrous results. In order to improve the security of smart metering systems, researchers have investigated many possible attacks and proposed some solutions.

Smart meters also have unintended consequences for customer privacy. NIST pointed out that “the major benefit provided by the SG, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its Achilles' heel from a privacy viewpoint”. The obvious privacy concern is that the energy use information stored at the meter acts as an information-rich side channel, and can be repurposed by interested parties to reveal personal information such as individual's habits, behaviors, activities, preferences, and

even beliefs. In order to address the privacy issues of smart meters, some approaches have been proposed. Homomorphic encryption is used to secure the data en route. Hence, intermediate meters do not see any intermediate or final result. The Zero-knowledge proofs are used to ensure that the fee is correct without disclosing any consumption data.

Wide deployment of monitoring and measurement devices (e.g. sensors and PMUs) could also lead to system vulnerabilities. The effective operation of SG depends on the widely-deployed accurate measurement devices. These measurements are typically transmitted to a control center, such as Supervisory Control and Data Acquisition (SCADA) Systems. State estimators in the control center estimate the power grid state through analysis of measurement data and power system models. Therefore, it is very important to guarantee the integrity of the data. A typical attack to compromise data integrity is the stealth attack, also called false-data injection attack. It was shown that an attacker can manipulate the state estimate without triggering bad-data alarms in the control center. Xie *et al.* also showed that with the knowledge of the system configuration, such attacks will circumvent the bad-data measurement detections in present SCADA systems, and may lead to profitable financial misconduct.

. To prevent such attacks, researchers have proposed various approaches. Recall that the control center uses state estimators to estimate the power grid state. In [21], it was shown how one can completely protect a state estimator from these unobservable attacks by encrypting a sufficient number of measurement devices.

It is well-known that the communication technologies we are using are often not secure enough themselves. It is expected that most of the security and privacy issues existing in the general communication networks (e.g. Internet and wireless networks)

could also exist in SG. Particularly, we need to focus more on wireless communication technologies since wireless networks are expected to be the more prevalent networks in SG. For example, wireless mesh networks (WMNs) are considered very reliable because they provide redundant communication paths, but WMNs are vulnerable to attacks by intelligent adversaries. Malicious attacks on information transmission in SG can be categorized into the following three major types based on their goals . Network availability: Malicious attacks targeting network availability can be considered as DoS attacks. They attempt to delay, block, or even corrupt information transmission in order to make network resources unavailable to nodes that need to exchange information in SG. As pointed out by NIST , the design of information transmission networks that are robust to attacks targeting network availability is the top priority, since network unavailability may result in the loss of real-time monitoring of critical power infrastructures and global power system disasters.

Data integrity attacks attempt to deliberately modify or corrupt information shared within the SG and may be extremely damaging in the SG.

Information privacy attacks attempt to eavesdrop on communications in SG to acquire desired information, such as a customer's account number and electricity usage. In order to improve the security and privacy of information transmission, researchers have proposed various solutions. The design principles include explicit names, unique encoding, explicit trust assumptions, use of timestamps, protocol boundaries, release of secrets, and explicit security parameters.

## **2.3.5 Smart Management System**

The smart management system is the subsystem in SG that provides advanced management and control services and functionalities. The key reason why SG can revolutionize the grid is the explosion of functionality based on its smart infrastructure. With the development of new management applications and services that can leverage the technology and capability upgrades enabled by this advanced infrastructure, the grid will keep becoming “smarter.” The smart management system takes advantage of the smart infrastructure to pursue various advanced management objectives. Thus far, most of such objectives are related to energy efficiency improvement, supply and demand balance, emission control, operation cost reduction, and utility maximization.

In SG, a large amount of data and information will be generated from metering, sensing, monitoring, etc. SG must support advanced information management. The task of the information management is data modeling, information analysis, integration, and optimization.

### **2.3.5.1 Data Modeling**

Creating persistent, displayable, compatible, transferable, and editable data representation for use within the emerging SG. In other words, the objective is to make it as interoperable as possible using relevant standards. That is specifically addressing the data that represents state information about the grid and individual items in it. This would include nearly all connected items from generation down to individual consuming devices. They all have state information that may need to be read, stored, transmitted, etc. Let us look at the following two reasons. First, the information exchange between two application elements is meaningful only when both of them can use the information exchanged to perform their respective tasks. Therefore, the structure and

meaning of the exchanged information must be understood by both application elements.

Although within the context of a single application, developers can strive to make the meaning clear in various user interfaces, when data is transferred to another context (another system), the meaning could be lost due to incompatible data representation. Considering that the SG is a complicated system of systems, design of a generally effective data representation is very important. Second, the data modeling is also related to the system forward compatibility and backward compatibility. On one hand, a well-defined data model should make legacy program adjustments easier. We hope that the data representation designed for SG can also be (or at least partially) understood by the current power system, in order to take advantage of the existing infrastructure as much as possible. On the other hand, thus far SG is more like a vision. Its definition and functionality keep evolving. Suppose that in the current implementation, all the data is particularly designed to be stored in an optimized way that can be understood by a current application X. Data modeling is the key to understand the historical data properly and obtain enough information from the historical data. Ontology helps convey knowledge in a formal fashion, just like a programming language conveys mathematics in a formal fashion. With ontology, one speaks of concepts in a subject area, and relationships between them. Like a programming language, it helps define, clarify, and standardize what is being discussed. Another reason that ontology-based strategies are commonly used with success in creating and manipulating data models is that they provide easy export or translation to Extensible Markup Language (XML) or Unified Modeling Language (UML), which provides for a great deal of information interoperability.

## **2.3.5.2 Information Analysis, Integration and Optimization**

Information analysis is needed to support the processing, interpretation, and correlation of the flood of new grid observations, since the widely deployed metering and monitoring systems in SG will generate a large amount of data for the utility. One part of the analytics would be performed by existing applications, and another part of the analytics dimension is with new applications and the ability of engineers to use a workbench to create their customized analytics dashboard in a self-service model. Information integration aims at the merging of information from disparate sources with differing conceptual, contextual, and typographical representations. In SG, a large amount of information has to be integrated. First, the data generated by new components enabled in SG may be integrated into the existing applications, and metadata stored in legacy system may also be used by new applications in SG to provide new interpretations. Data integrity includes verification and cross correlation of information for validity, and designation of authoritative sources. Name service addresses the common issue of an asset having multiple names in multiple systems. Currently most utility companies have limited installed capability for integration across the applications associated with system planning, power delivery, and customer operations. In most cases, this information in each department is not easily accessible by applications and users in other departments or organizations. These “islands of information” correspond to islands of autonomous business activities. Therefore, the emerging SG calls for enterprise level integration of these islands to improve and optimize information utilization throughout the organization. Information optimization is used to improve information effectiveness. The data size in the future SG is expected to be fairly large as a result of the large-scale monitoring, sensing, and measurement. However, the generated data may have



a large amount of redundant or useless data. Therefore, we need to use advanced information technology to improve the information effectiveness, in order to reduce communication burden and store only useful information. In order to compress the size of disturbance signals and reduce sinusoidal and white noise in the signals. The proposed method can be implemented in SG to mitigate data congestion and improve data transmission and quality. It is being applied the singular value decomposition analysis to examine the coupling structure of an electrical power grid in order to highlight opportunities for reducing the network traffic, by identifying what are the salient data that need to be communicated between parts of the infrastructure to apply a control action. They found that typical grid admittance matrices have singular values and vectors with only a small number of strong components.

# **Chapter 3**

## **Intelligent Electronic Devices (IEDs)**

### **3.1 Introduction**

An Intelligent Electronic Device (IED) is a term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks etc.

All the IEDs have their different communication strength. In any smart grid network, it is totally impossible that all the IEDs can communicate with each other. Our requirement is that the IEDs at one substation must communicate with each other. When protection IEDs are used in bus protection, all the IEDs need to be communicated with each other are in the same substation. Communication between the IEDs can be implemented in LAN (Local Area Network). Communication distance of IEDs is much longer when we use it for line protection. Communication can be implemented in fiber-optic network. As we form protection zone on the basis of graph theory. Different IEDs comes under different protection zones. IEDs will command action signal 1 depending on differential criterion is being satisfied or not satisfied by the IEDs.

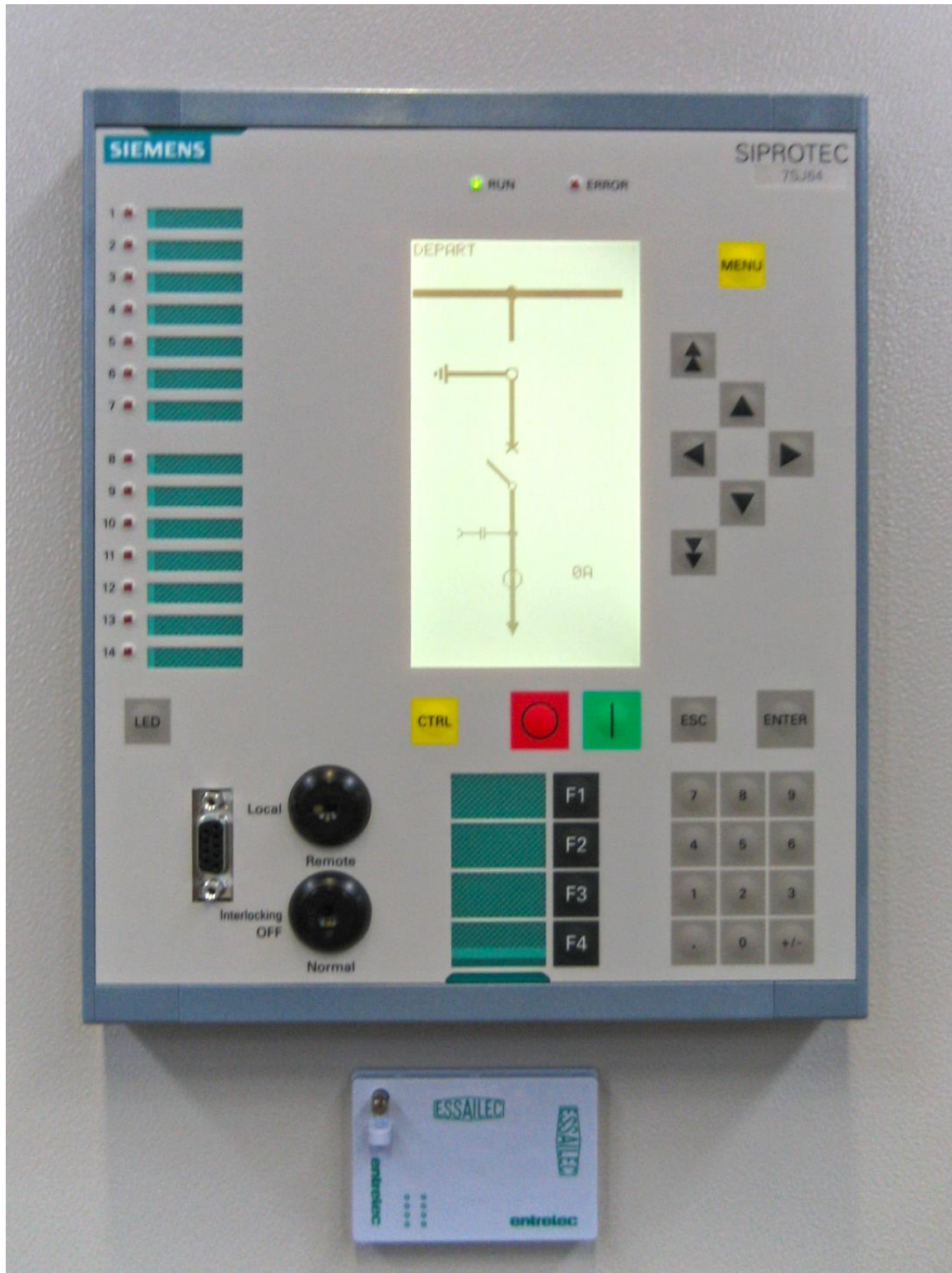


Fig.3 Intelligent Electronic Device

## 3.2 Characteristics of IEDs

- 1) Each IED will protect a certain portion of the network
- 2) All IEDs are connected through optical fiber transmission network
- 3) Communication among protection IEDs by optical fiber acquires current signals in different nodes in the power grid
- 4) It collects local electrical signals and communicates with central processing system and other protection IEDs
- 5) It also has signal processing and decision making abilities
- 6) In theory any IED can communicate with any other IED in any network but unlimited communication is unpractical in all the networks
- 7) Excessive information exchanging and too many programming loops will reduce accuracy and speed of protecting function
- 8) The action time of wide-area protection and the probability of miss trip or mal-operation will significantly increase
- 9) Protection zone which is partitioned properly, could make protection IEDs communicating within it.

# Chapter 4

## Graph Theory

### 4.1 Introduction

A graph is a representation of a set of objects where some pair of objects are connected by link. The interconnected objects are represented by mathematical abstractions called vertices, and the links that connect some pairs of vertices are called edges. A graph may be undirected meaning that there is no distinction between the two vertices associated with each edge, or its edges may be directed from one vertex to another.

Graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. In other words, Graph Theory is a mathematics method which uses graph and theory to describe a certain network structure or some elements and their connections. In graph theory there are two elements, vertexes and edges. Graph is an aggregation of vertexes and edges. In power system, power network structure could be abstracted to a graph.

For better understanding let us take an power network as an example:-

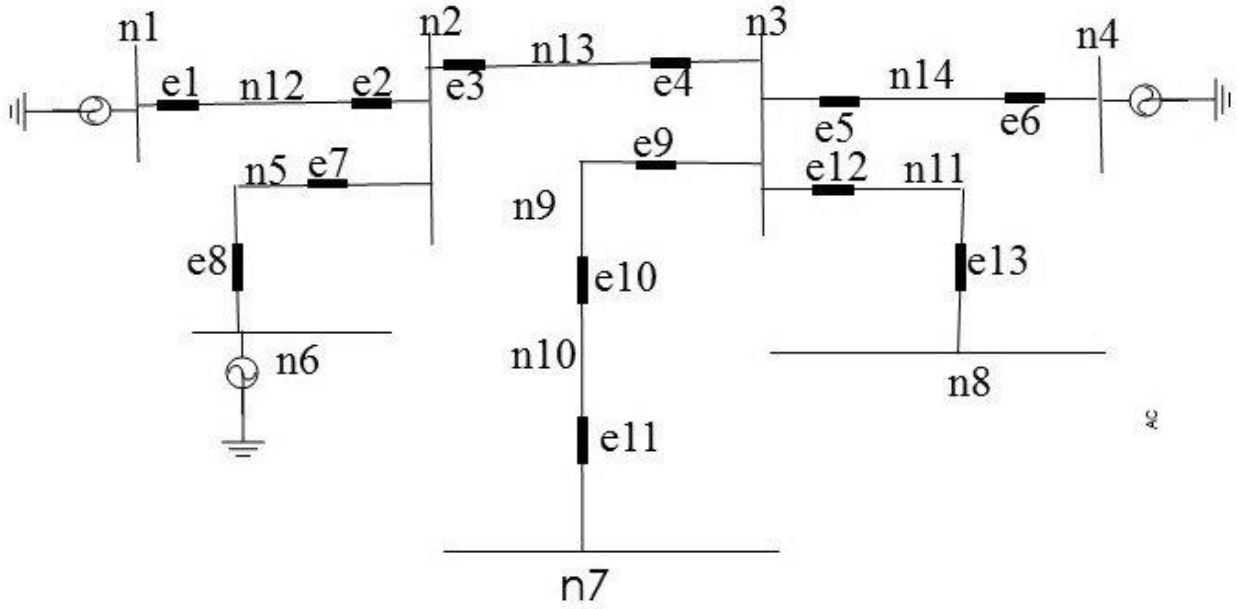


Fig. 4.1 Power Network Representation with Nodes and IEDs

In this figure, all the buses and lines are expressed by n and protection IEDs are expressed by e.

We are treating all electric elements as vertexes and all IEDs as edges. Assuming positive direction from bus to line in directed graph.

A directed graph could be obtained with the help of graph theory. Directed Graph for previous network is as shown below

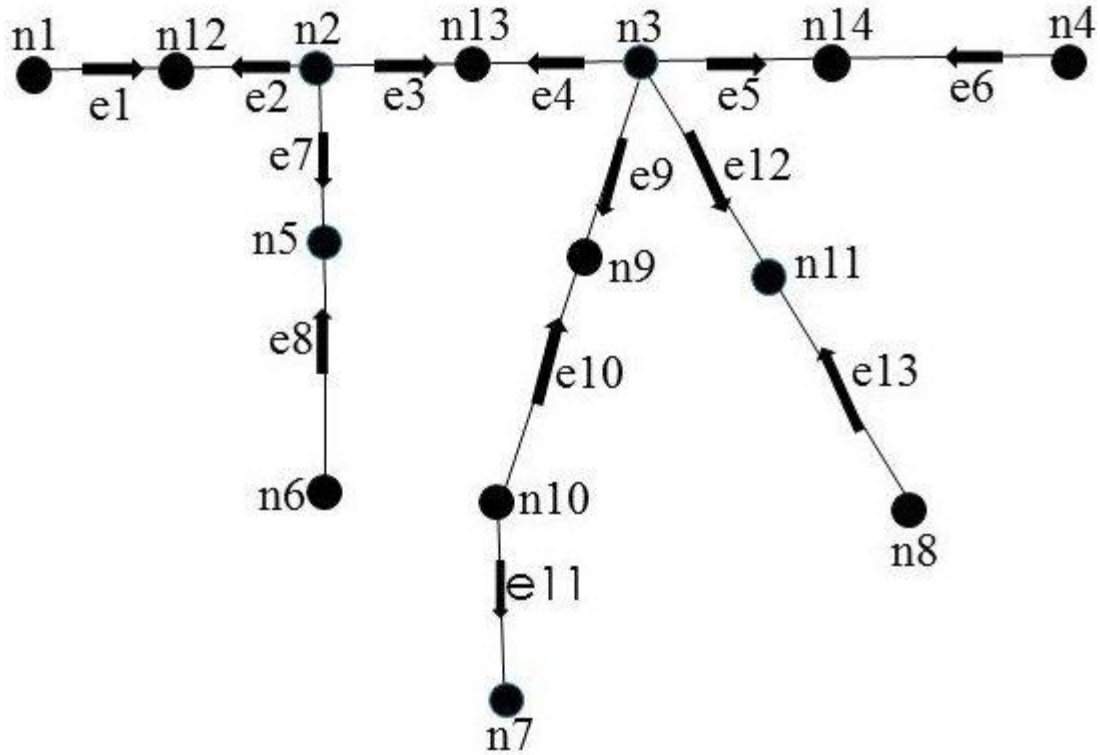


Fig.4.2 Directed Graph for the network in Fig. 4.1

According to Graph Theory, any graph could be described by several matrices. In graph theory generally we have three matrices adjacency matrix  $C$ , reachability matrix  $P$  and complete incidence matrix  $M$ .

### 4.1.1 Adjacency Matrix

It reflects the connecting relationship of vertexes. It is expressed by  $n \times n$  matrix  $C$  if there are  $n$  vertexes. In other words we can say  $C$  is a function of vertex in the power network.  $C$  is defined as follows.

$$C_{ij} = \begin{cases} 1 & \text{node i adjoins node j} \\ 0 & \text{node i doesn't adjoin node j} \end{cases}$$

Adjacency Matrix

### 4.1.2 Reachability Matrix

Reachability matrix P reflects whether there is a connection pathway between two vertexes or whether the connections are less than reachable steps. In other words reachability matrix tells us whether two IEDs in network can communicate with each other or not. P is n×n matrix in the graph including n vertexes. P matrix is also a function of nodes or vertexes in the system. P is defined as follows

$$P_{ij} = \begin{cases} 1 & \text{at least one path from node i to node j} \\ 0 & \text{no path at all from node i to node j} \end{cases}$$

Reachability Matrix

There is a relation between P and C matrix. Matrix P could be directly calculated by matrix C.

The process is shown in equation

$$P = I \cup C \cup C^2 \cup \dots \cup C^{n-1} \quad (1)$$

Relation between Reachability and Adjacency Matrix



Matrix C expresses logic relationship in the equation above, so addition and multiplication in the matrix elements should be logic add and logic multiplication.

### 4.1.3 Complete Incidence Matrix

Complete Incidence Matrix M is  $p \times q$  matrix in a graph with  $p$  vertexes and  $q$  edges. It is a function of both vertexes and edges in a network. The elements are defined as follows

$$m_{ij} = \begin{cases} 1 & \text{node } i \text{ is starting point of edge } j \\ -1 & \text{node } i \text{ is ending point of edge } j \\ 0 & \text{no connection b/w node } i \text{ \& edge } j \end{cases}$$

So, the network structure in Fig. 2 can be expressed by the matrices above. Adjacency matrix C just describes connecting relationship of elements in the network, so the direction could be ignored.

The matrix is obtained as follows

$$C = \begin{matrix} & \begin{matrix} n1 & n2 & n3 & n4 & n5 & n6 & n7 & n8 & n9 & n10 & n11 & n12 & n13 & n14 \end{matrix} \\ \begin{matrix} n1 \\ n2 \\ n3 \\ n4 \\ n5 \\ n6 \\ n7 \\ n8 \\ n9 \\ n10 \\ n11 \\ n12 \\ n13 \\ n14 \end{matrix} & \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (2)$$

If reachable step is 3, matrix P can be calculated by matrix C as follows

$$P = \begin{matrix} & \begin{matrix} n1 & n2 & n3 & n4 & n5 & n6 & n7 & n8 & n9 & n10 & n11 & n12 & n13 & n14 \end{matrix} \\ \begin{matrix} n1 \\ n2 \\ n3 \\ n4 \\ n5 \\ n6 \\ n7 \\ n8 \\ n9 \\ n10 \\ n11 \\ n12 \\ n13 \\ n14 \end{matrix} & \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \end{matrix} \quad (3)$$

Similarly Complete Incidence Matrix could be obtained from the previously defined definition as below. It will depend upon both vertexes and edges in the system.

$$M = \begin{matrix} & \begin{matrix} e1 & e2 & e3 & e4 & e5 & e6 & e7 & e8 & e9 & e10 & e11 & e12 & e13 \end{matrix} \\ \begin{matrix} n1 \\ n2 \\ n3 \\ n4 \\ n5 \\ n6 \\ n7 \\ n8 \\ n9 \\ n10 \\ n11 \\ n12 \\ n13 \\ n14 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (4)$$

## 4.2 Protection Zone Partition by Graph Theory

Take IED e1 as an example for analyzing the network. At first, the protection zone needs to be reduced to an appropriate area. Because e1 belongs to the transformer substation where bus n1 placed, we determine the area according to n1. The first row in matrix P is the area which reachable step from n1 is no more than three. One value elements in the first row correspond with vertexes n1, n12, n2, n13 and n9. They constitute a subgraph of e1 as below:

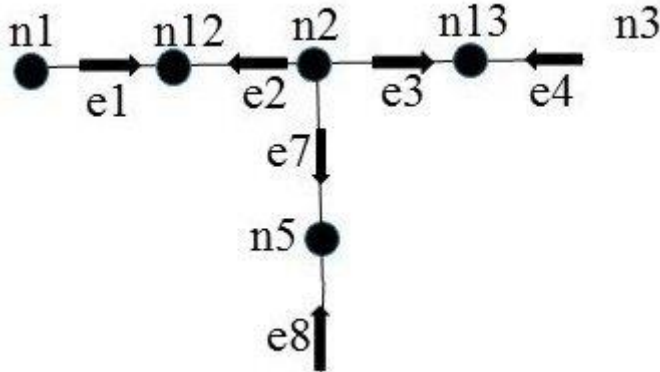


Fig.4. 3 Sub-directed Graph for IED e1

Modify matrix M according to the subgraph as,

$$M = \begin{matrix} & \begin{matrix} e1 & e2 & e3 & e4 & e7 & e8 \end{matrix} \\ \begin{matrix} n1 \\ n2 \\ n13 \\ n5 \\ n12 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 \\ -1 & -1 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (5)$$

## 4.2.1 Rules of Protection Zone Partition

The protection zone is partitioned into three levels as:

- 1) The first level zone protects single element. It protects the line where the protection IED placed or the bus behind the IED.
- 2) As line protection, the second level zone of IED is constituted by the line IED placed and the opposite bus. The second level protection could be the backup protection of the opposite bus.
- 3) The third level zone of line protection is constituted by the line IED placed, the opposite bus and all the outgoing lines of bus.

First, we discuss the line protection. According to the rules above, the first protection zone of e1 is n12. The second protection zone is n12 and n2, and the third protection zone is n12, n2, n5 and n13.

## 4.2.2 Conclusion by Using Graph Theory.

- 1) Observe the column e1. The nonzero elements are correspond with n1 and n12. We know that n1 is a bus and n12 is a line. This is the first level protection zone.

$$M = \begin{matrix} & \begin{matrix} e1 & e2 & e3 & e4 & e7 & e8 \end{matrix} \\ \begin{matrix} n1 \\ n2 \\ n13 \\ n5 \\ n12 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 \\ -1 & -1 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (6)$$

- 2) Observe the row n12 in modified matrix for zone 1. The nonzero elements are correspond with edge e1 and e2. In order to get the second level zone of e1, the edge e2 need to be removed. It means combining n2 and n12 and treating them as a big vertex. Add row n2 and n12 in matrix M and obtain new matrix M1 as below.

$$M1 = \begin{matrix} & \begin{matrix} e1 & e2 & e3 & e4 & e7 & e8 \end{matrix} \\ \begin{matrix} n1 \\ n2,12 \\ n13 \\ n5 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 \end{bmatrix} \end{matrix} \quad (7)$$

- 3) Observe row n2,12 in matrix M1. The nonzero elements are correspond with e1, e3 and e7. The edge e3 and e7 need to be removed in order to obtain the third level zone of e1. The method is the same with obtaining the second level zone. The matrix M2 is showing as below after removing e3 and e7.

$$M2 = \begin{matrix} & \begin{matrix} e1 & e2 & e3 & e4 & e7 & e8 \end{matrix} \\ \begin{matrix} n1 \\ n2,5,12,13 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 & -1 \end{bmatrix} \end{matrix} \quad (8)$$

Observe the column e1 in matrix M2. Obviously the third level zone is n2, n12, n5 and n13.

## **4.3 Comparison with Differential Arithmetic Protection**

### **4.3.1 Differential Protection Arithmetic**

Differential protection arithmetic is based on KCL (Kirchhoff Current Law). The principle is the sum of current inflowing and outflowing one node equals to zero. If fault occurs on the node, short current will break the balance of the sum of inflow and outflow current. According to sampling all current values inflowing and outflowing, the condition of the elements could be monitored and the elements could be protected by protection device in real time. The principle of differential protection arithmetic is simple, reliable, sensitive and easy to implement. It can be used in line protection to protect overall length of transmission line and can be used in bus protection. It is widely used in traditional relay protection and its operation effect is favorable. In wide-area protection system, PMU (Phase Measurement Unit) can be used to sample current signals, GPS (Global Position System) can be used to synchronize current signals, and fiber communication network is used to transmit signals. The advantages of differential protection arithmetic could be fully embodied on those bases.

### **4.3.2 Protection Method based on Graph Theory**

As backup protection system, wide-area differential protection system which is designed in this paper can operate separately and independently with tradition protection. It doesn't clash with traditional main protection. Just like double main protection, the two protection systems have no electric link. When one protection is out of service, the other one can still operate reliably. When protection IEDs are used in bus protection, all IEDs need to be communicated with each other are

in the same substation. Communication can be implemented in LAN (Local Area Network). When protection IEDs are used in line protection, communication distance of IEDs is much longer. Communication can be implemented in fiber-optic network. Specific IED's selection is implemented by protection zone partitioning method based on graph theory. For example in equation 8, e1 needs to protect n12, it needs to communicate with e2 which depends on searching protection IEDs which the nonzero elements of row n12 correspond to. When current values of these two nodes obtained, add them. If the sum is close to zero, the line n12 is normal. Otherwise n6 is considered to breakdown, and breaker of e1 will be tripped off.

If n12 has no fault, protection zone needs to be enlarged.

Through equation 9, we need e1 communicating with e3 and e7 to protect zone n2,12. The sum of current sampling values can be used to judge whether fault occurs inside the node n2,6. If n2,12 is judged to be no fault, protection zone is further enlarged. Through equation 10, e1 needs to communicate with e4 and e8. If fault occurs, breaker of e1 will be tripped off, otherwise protection returns. Before each differential calculating in the whole workflow, IED needs to detect sampling current values of other IEDs inside protection zone. If one of them equals to zero, the protection in that node can be considered to have already acted and breaker in that node can be considered to have already tripped off. Fault can be considered to have already removed and protection should return.

## 4.4 Flow Chart of Protection Method

The flow chart of Graph theory Based protection method is shown as below:-

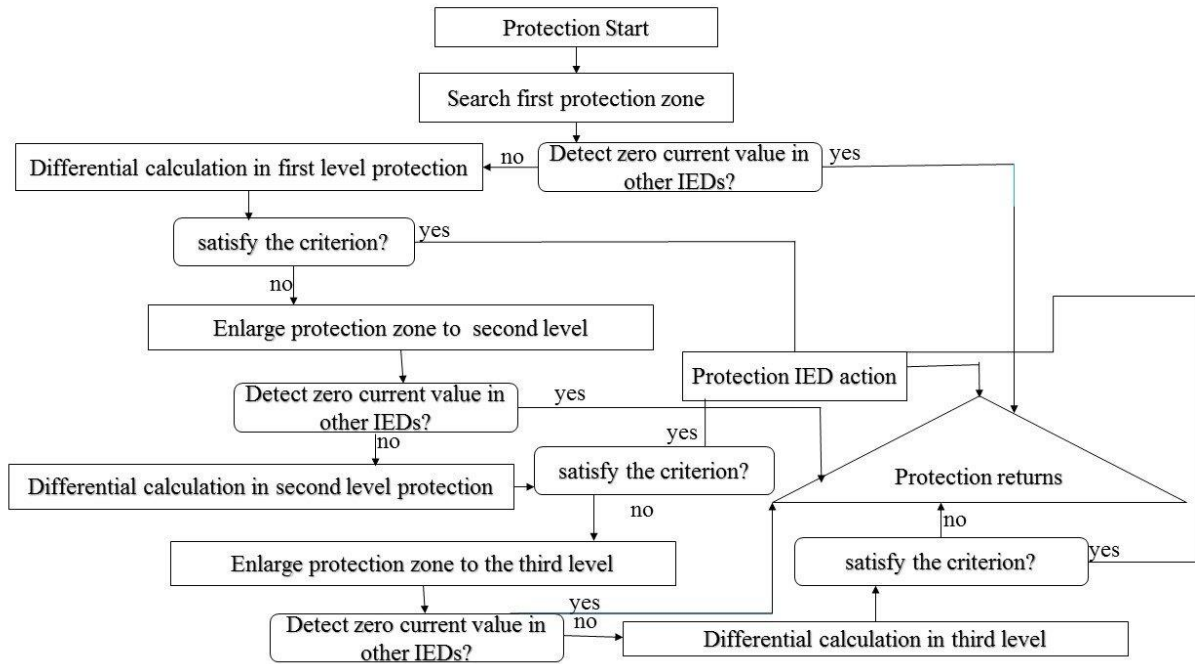


Fig.4. 4 Flow Chart of Graph theory based Protection Method

## 4.5 Self -Healing Cases

In the cases mentioned below IED itself will heal without any external change.

- 1) If IED fails to communicate with other protection device, protection is locked.
- 2) If IED successfully cuts off fault, communication will still maintain until new protection zone formed.
- 3) If IED detects unbalanced current without low voltage or over current, protection is locked.

Bus protection needs current values in different nodes when buses have different operation mode.

## 4.6 Case Study

For case study analysis taking 220kV Power Network as simulation object. PSASP (Power System Analysis Software Package) is used to sample current values in each IED node and



MATLAB is used to write graph theory based protection program. These two pieces of software are combined to implement differential protect function. 220kV power network is shown as

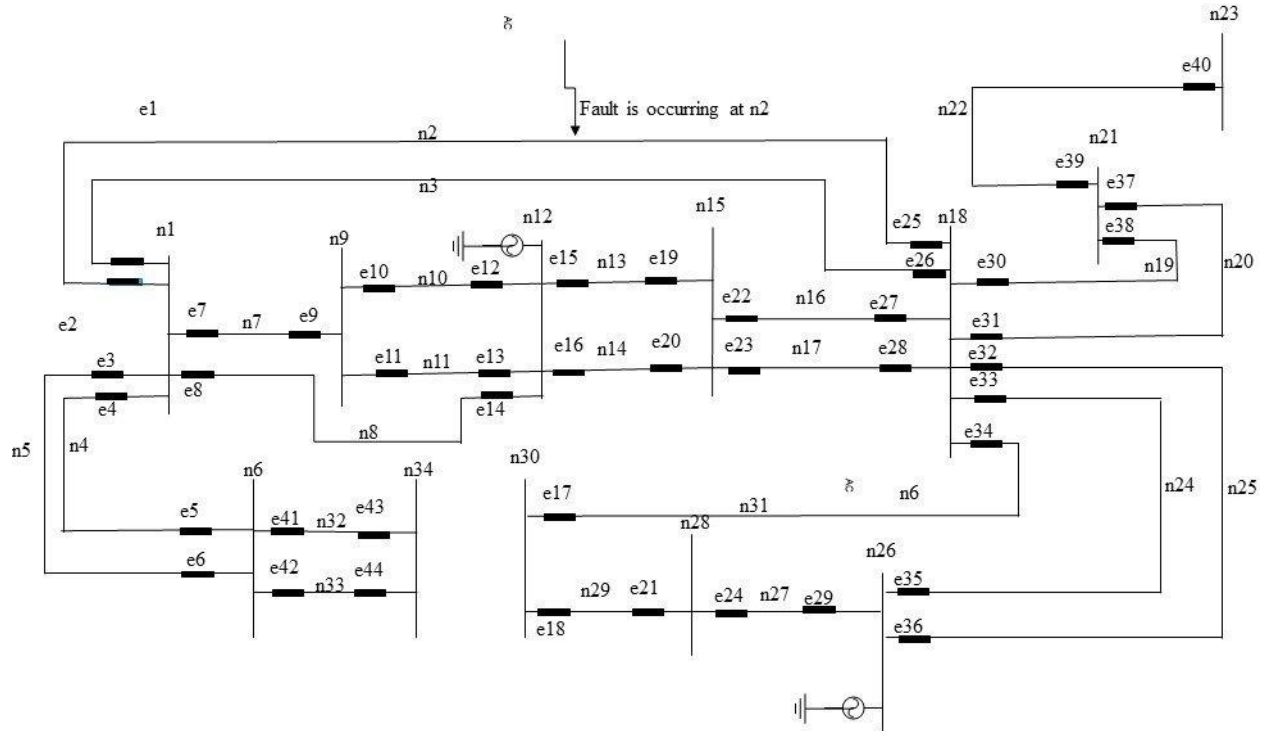


Fig.4.5 220 KV Power Network

Simulation operating time is 5 seconds and current sampling frequency is 100Hz. Transmission n2 is supposed to occur three-phase short circuit at 2s. We take IED e2 as researching object, other IEDs have a similar analytical method. First the protection zone of e2 needs to be known. The power network is transformed into directed graph by using graph theory which is shown in Fig. 6.



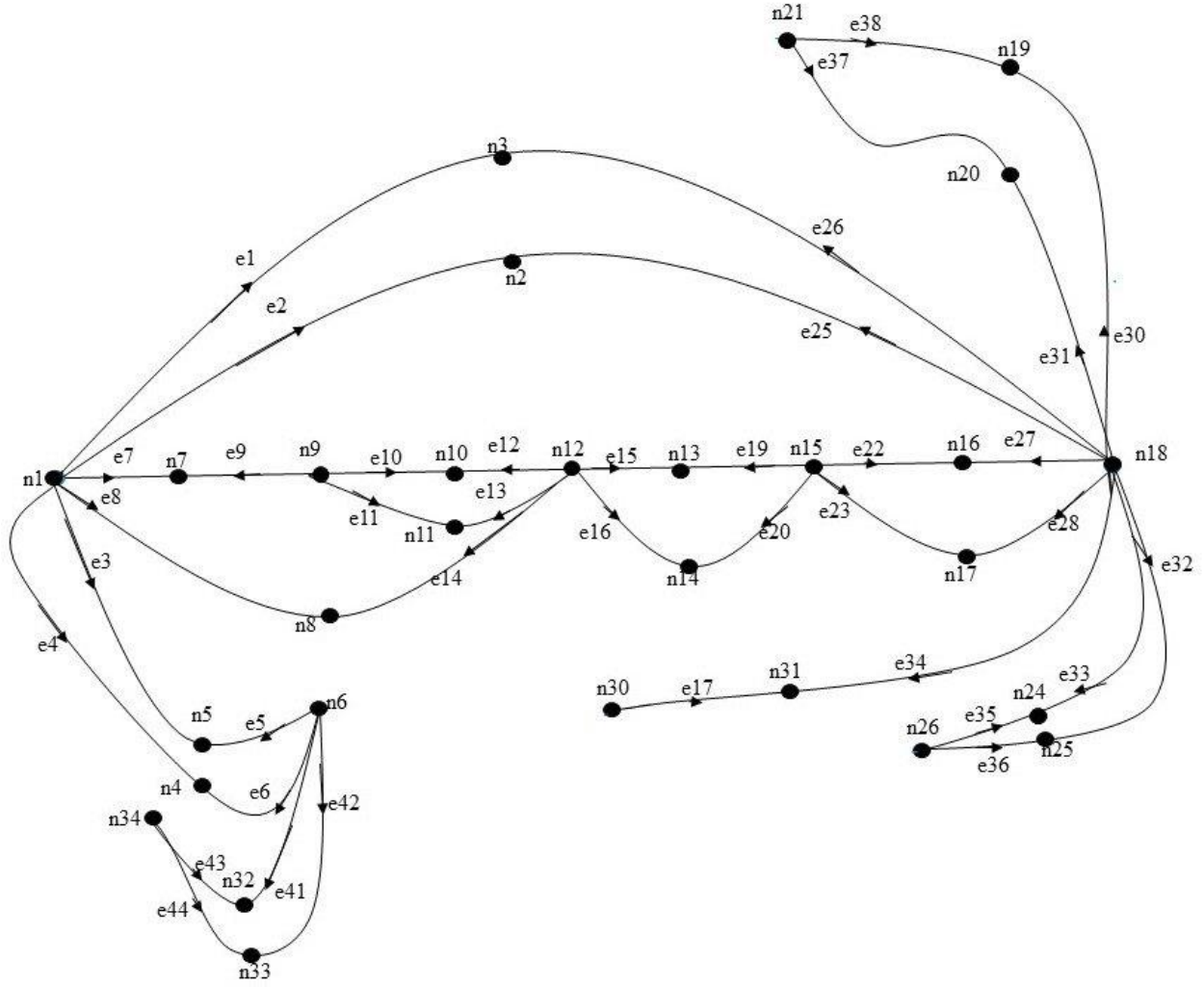


Fig.4. 7 Subdirected Graph for IED e2

We sample related node current values and implement differential calculation in each level protection zone to judge if there is a fault in protection zone. If calculation value is close to zero, the protection zone is normal. Otherwise there are some elements in the zone breaking down. The method to judge is designing a threshold value. As long as absolute value of differential calculation is more than the threshold value, protection device will act immediately and export action signal 1 to breaker.

According to matrix M, e2 communicates with e25 in the first level protection zone, with e2, e27, e28, e30, e31, e32, e33, e34 in the second level and with e1, e17, e22, e23,

e35 , e36 , e37 , e38 in the third level. The sampling current values from moment 3.00 to 3.04s are shown in table II. All current values are expressed as p.u.(per unit).

Table 4.1: Representing currents in IEDs comes under Protection Zone 1

Time	e2	e25
3.00	2.36712	-2.35312
3.01	2.36712	-2.35312
3.02	2.36841	-2.35312
3.03	32.93132	37.69784
3.04	35.84963	33.69023

Table 4.2: Representing currents in IEDs comes under Protection Zone 2

Time	e2	e26	e27	e28	e30	e31	e32	e33	e34
3.00	2.36712	1.18542	0.41886	0.42361	0.29842	0.26275	-0.68483	-0.78867	0.9774
3.01	2.36712	1.18542	0.41886	0.42362	0.26842	0.26275	-0.68483	-0.78867	0.9774
3.02	2.36841	1.98613	0.41882	0.42362	0.26814	0.26275	-0.68483	-0.78867	0.8774
3.03	32.9312	-7.35984	-3.37295	-1.41443	-6.86457	-5.86744	-5.27637	-5.31889	-3.22167
3.04	35.8493	-8.11525	-3.8972	-2.93274	-8.68645	-5.68918	-6.76811	-4.80653	-3.79676

Table 4.3: Representing the currents in IEDs comes under Protection Zone 3

Time	e2	e1	e17	e22	e23	e35	e36	e37	e38
3.00	2.36712	-1.1949	-0.7923	-0.42229	-0.42742	0.48227	0.47836	-0.27819	-0.27116
3.01	2.36712	-1.1949	-0.7923	-0.42229	-0.42742	0.48227	0.47836	-0.27819	-0.27116
3.02	2.36841	-1.1949	-0.7923	-0.42229	-0.42742	0.48227	0.47836	-0.27819	-0.27116
3.03	32.9312	7.3625	3.21489	3.37066	3.41206	5.31117	5.26861	5.85711	5.86256
3.04	35.8493	7.11776	2.79044	2.89504	2.93061	-2.79676	4.76092	5.67931	5.68453

At the moment 3.00s, e2 and e25 proceed to the first level differential calculation.

$$\text{Sum} = 2.36964 + (-2.35142)$$

$$= 0.01822 \quad (9)$$

Because of  $|\text{Sum}| < 1$ , differential criterion is dissatisfied

There is no fault in the first level protection zone.

Enlarge protection zone to protection zone 2 or second level protection zone and start differential calculation by e2 and e26, e27, e28, e30, e31, e32, e33, e34.

$$\begin{aligned} \text{Sum} &= 2.36712 + [-(1.18542 + 0.41886 + 0.42361 + 0.26842 + 0.26275 - 0.68483 - 0.78867 + 0.9774)] \\ &= 0.00672 \quad (10) \end{aligned}$$

Because of  $|\text{Sum}| < 1$ , differential criterion is dissatisfied.

There is no fault in the second level protection zone.

Enlarge protection zone again to third level protection zone and start differential calculation third time by e2 and e1, e17, e22, e23, e35, e36, e37, e38.

$$\begin{aligned} \text{Sum} &= 2.36712 + [(-1.1949 - 0.7923 - 0.42229 - 0.42742 + 0.48227 + 0.47836 - 0.27819 - 0.27116)] \\ &= -0.0566 \quad (11) \end{aligned}$$

Because of  $|\text{Sum}| < 1$ , differential criterion is dissatisfied.

Three levels of protection all dissatisfy differential criterion at 3.00 s. No fault occurs in the protection zones at 3.00 s.

So e2 exports action signal 0 at 3.00 s. Sign symbol in the differential calculation above could be obtained by products that corresponding elements in matrix M multiply by current sampling values.

Similarly, action signals 0 are exported at moment 3.01s and 3.02s.

Sampling current obviously increases in IED e2 at moment 3.03s due to occurrence of fault.

Differential calculation in first level protection zone

$$\text{Sum} = 32.93132 + 37.69784$$

$$= 73.62916 \quad (12)$$

Because of  $|\text{Sum}| \gg 1$ , differential criterion is satisfied.

Over current and differential calculation satisfy criterion at the same time.

Protection IED e2 acts immediately exports action signal 1.

Fault criterions can be obtained as well at the moment 3.04s.

Suppose communication failure occur in fiber network between e2 and e25 at moment 3.03s.

It leads the first level differential calculation to be locked.

Now again protection zone enlarges to the second level.

Differential calculation is shown below.

$$\begin{aligned} \text{Sum} &= 33.93132 + [(-7.35984 - 3.37295 - 3.41433 - 5.86457 - 5.86744 - 5.27637 - 5.31889 - 3.22167)] \\ &= 73.62738 \quad (13) \end{aligned}$$

Because of  $|\text{Sum}| \gg 1$ , differential criterion is satisfied.

So criterion is satisfied in the second level zone. e2 exports action signal 1 to breaker.

If there are one or several protection devices are out of order in the second level protection zone, it will be enlarge to the third zone.

$$\begin{aligned} \text{Sum} &= 33.93132 + [(7.3625 + 3.21489 + 3.37066 + 3.41206 + 5.31117 + 5.26861 + 5.85711 + 5.86256)] \\ &= 73.59088 \quad (14) \end{aligned}$$

Because of  $|\text{Sum}| \gg 1$ , differential criterion is satisfied.

IED e2 acts immediately and export action signal 1.

## **4.7 Results**

### **4.7.1 In Matlab**

```
>> ps1
Enter value of e2
2.35964
Enter value of e25
-2.35142
Export actiona signal 0
Enter value of e2
2.35964
Enter value of e25
-2.35142
Export actiona signal 0
Enter value of e2
2.35963
Enter value of e25
-2.35141
Export actiona signal 0
Enter value of e2
33.93132
Enter value of e25
39.69784
Export actiona signal 1
Enter value of e2
31.84963
Enter value of e25
36.69023
Export actiona signal 1
>>
```

Fig 4.8 Matlab Code results for Protection zone 1



```
>> pz2
Enter value of e2
2.35954
Enter value of e25
1.18513
Enter value of e27
0.41842
Enter value of e28
0.42351
Enter value of e30
0.25814
Enter value of e31
0.25272
Enter value of e32
-0.48483
Enter value of e33
-0.48857
Enter value of e34
0.7774
Export action signal 0
Enter value of e2
2.35954
Enter value of e25
1.18513
Enter value of e27
0.41843
Enter value of e28
0.42352
Enter value of e30
0.25814
Enter value of e31
0.25272
Enter value of e32
-0.48483
Enter value of e33
-0.48857
Enter value of e34
0.7774
Export action signal 0
Enter value of e2
2.235953
Enter value of e25
1.18513
Enter value of e27
0.41843
Enter value of e28
0.42352
Enter value of e30
0.25814
Enter value of e31
0.25272
```

Fig 4.9 Matlab Code results for Protection zone 2

```
>> pz3
Enter value of e2
2.35964
Enter value of e1
-1.1949
Enter value of e17
-0.7923
Enter value of e22
-0.42229
Enter value of e23
-0.42742
Enter value of e35
0.48227
Enter value of e36
0.47836
Enter value of e37
-.27819
Enter value of e38
-.27116
Export action signal 0
Enter value of e2
2.35964
Enter value of e1
-1.1949
Enter value of e17
-0.7923
Enter value of e22
-0.42229
Enter value of e23
-0.42742
Enter value of e35
0.48227
Enter value of e36
0.47836
Enter value of e37
-.27819
Enter value of e38
-.27116
Export action signal 0
Enter value of e2
2.35963
Enter value of e1
-1.1949
Enter value of e17
-0.7923
Enter value of e22
-0.42229
Enter value of e23
-0.42742
Enter value of e35
0.48227
```

Fig 4.10 Matlab Code results for Protection zone 3

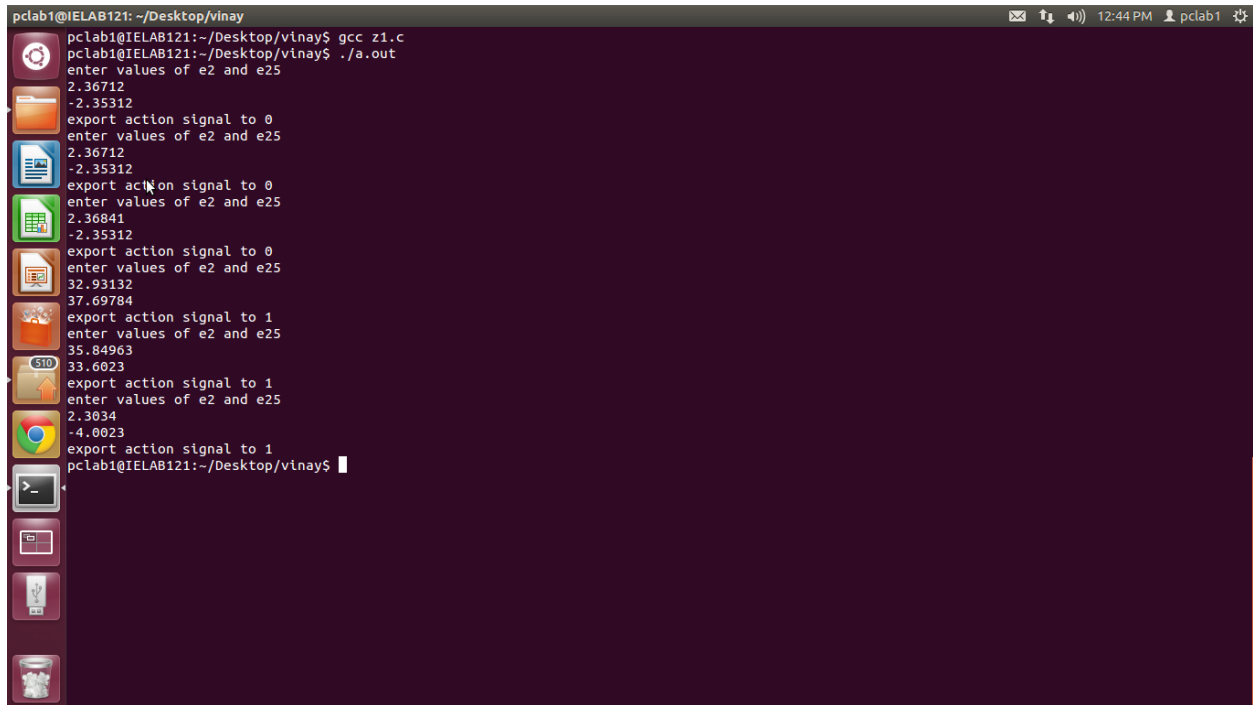
```

>> allps
Enter value of e2
2.236712
Enter value of e25
-2.35312
Export actional signal to 0
Enter value of e2
2.236712
Enter value of e25
-2.35312
Export actional signal to 0
Enter value of e2
2.236841
Enter value of e25
-2.35312
Export actional signal to 0
Enter value of e2
32.93132
Enter value of e25
37.69784
Export actional signal to 0
Enter value of e2
35.84963
Enter value of e25
33.6023
Export actional signal to 0
Enter value of e2
0.00013
Enter value of e26
0.06752
Enter value of e27
0.41886
Enter value of e28
0.42361
Enter value of e30
0.29842
Enter value of e31
0.26275
Enter value of e32
-0.68483
Enter value of e33
-0.78867
Enter value of e34
0.9774
Export actional signal to 0
Enter value of e2
2.236842
Enter value of e26
1.18542
Enter value of e27
0.41886

```

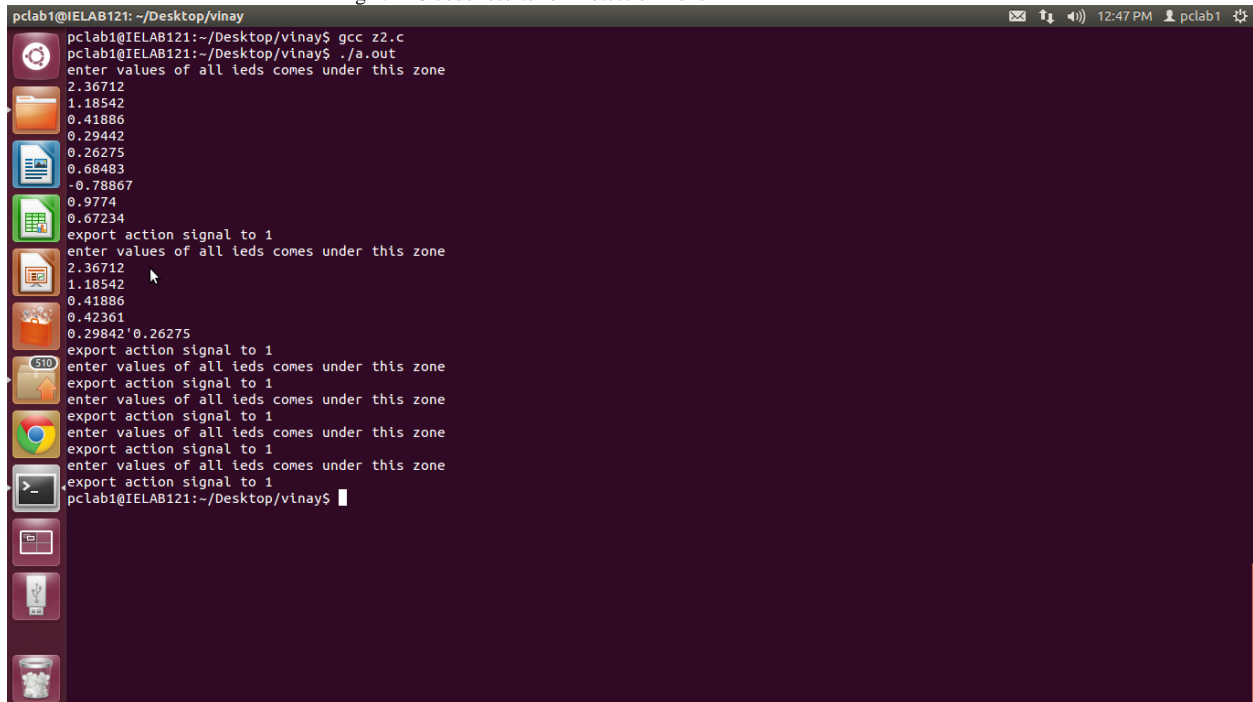
Fig 4.11 Matlab Code results for all Protection zones

## 4.7.2 In C Language



```
pclab1@IELAB121: ~/Desktop/vinay
pclab1@IELAB121:~/Desktop/vinay$ gcc z1.c
pclab1@IELAB121:~/Desktop/vinay$ ./a.out
enter values of e2 and e25
2.36712
-2.35312
export action signal to 0
enter values of e2 and e25
2.36712
-2.35312
export action signal to 0
enter values of e2 and e25
2.36841
-2.35312
export action signal to 0
enter values of e2 and e25
32.93132
37.69784
export action signal to 1
enter values of e2 and e25
35.84963
33.6023
export action signal to 1
enter values of e2 and e25
2.3034
-4.0023
export action signal to 1
pclab1@IELAB121:~/Desktop/vinay$
```

Fig 4.12 C code results for Protection Zone 1



```
pclab1@IELAB121: ~/Desktop/vinay
pclab1@IELAB121:~/Desktop/vinay$ gcc z2.c
pclab1@IELAB121:~/Desktop/vinay$ ./a.out
enter values of all leds comes under this zone
2.36712
1.18542
0.41886
0.29442
0.26275
0.68483
-0.78867
0.9774
0.67234
export action signal to 1
enter values of all leds comes under this zone
2.36712
1.18542
0.41886
0.42361
0.29842'0.26275
export action signal to 1
enter values of all leds comes under this zone
export action signal to 1
enter values of all leds comes under this zone
export action signal to 1
enter values of all leds comes under this zone
export action signal to 1
enter values of all leds comes under this zone
export action signal to 1
pclab1@IELAB121:~/Desktop/vinay$
```

Fig 4.13 C code results for Protection Zone 1

```
pclab1@IELAB121: ~/Desktop/vinay
pclab1@IELAB121:~/Desktop/vinay$ gcc z3.c
pclab1@IELAB121:~/Desktop/vinay$ ./a.out
enter values of all leds comes under this zone
2.36712
-1.1949
-0.7923
-0.42229
-0.42742
0.48227
0.47836
-0.27819
-0.27116
export action signal to 0
enter values of all leds comes under this zone
32.9312
7.3625
3.21489
3.37066
3.41206
5.31117
5.26861
5.85711
5.86256
export action signal to 1
enter values of all leds comes under this zone
```

Fig 4.14 C code results for Protection Zone 3

```
pclab1@IELAB121: ~/Desktop/vinay
pclab1@IELAB121:~/Desktop/vinay$ gcc allz.c
pclab1@IELAB121:~/Desktop/vinay$ ./a.out
enter values of leds current corresponding to protection zone 1
2.36712
1.18542
export action signal to 1
enter leds corresponding to protection zone 2
2.236712
1.18542
0.41886
0.42362
0.26814
0.27275
0.68483
-0.78867
export action signal to 1
enter leds current corresponding to protection zone 3
2.36712
-1.1949
-0.7923
-0.42229
-0.42742
0.48227
0.47836
-0.27819
export action signal to 1
enter values of leds current corresponding to protection zone 1
```

Fig 4.15 C code results for All Protection Zones

# **Chapter 6**

## **Conclusion**

### **6.1 Summary**

Graph theory based protection method is totally independent of main protection method. We can also use it along with main protection method just like two protection systems are totally independent of each other. We can also call it as back up protection method. This is the main advantage of this method over other protection methods. IED plays an major role in this method. IED collects local electric signals and communicates with central processing system and other IEDs. It also have signal processing and decision making abilities. These abilities come into picture in case of self- healing process during fault occurrence. PMU (Phase Measurement Unit) can be used to sample current signals, GPS (Global Position System) can be used to synchronize current signals, and fiber communication network is used to transmit signals. Graph theory based protection zone partitioning reduces IED communication area and increases speed and accuracy of protection system. Through simulation analysis, protection system locates fault accurately when one or more protection devices are out of service. The reliability of protection system is enhanced. Graph theory based protection system has features such as accuracy, quickness, no need to set up and so on. It provides an effective protection system solution for more complicated smart grid.

## 6.2 Scope For Future Work

Graph theory plays vital role in the protection of Smart Grid. For any power network, once we get directed graph of network. We can easily get Adjacency matrix, Reachability matrix and Incidence matrix. When it comes to reachability matrix, we always need to set up reachable steps. We will decide reachable steps on the basis of network and the IEDs. So we could do something about it to fix the number of steps so that it will become independent of IEDs in the network. I have already told how to detect fault in smart grid network with the help of graph theory. Compared with traditional relay protection which only protects one electrical component, each IED is protecting certain area. We can optimize this area or portion of power network. We are using electric signals to collect local electrical signals and communicates with the central processing system and other protection IEDs to obtain electric signals in other nodes through the optical fiber transmission network. Even we could use some other network in place of optic fiber network. I choose three levels of protection zones. When it comes to multi level protection zone, we could optimize number of protection zone levels.

# Appendix A

## A.1 Tables Containing Different IED's Current in the Corresponding Protection Zones

Table A.1.1 Showing the IEDs currents corresponding to Protection Zone 1

Time	e2	e25
3.00	2.36712	-2.35312
3.01	2.36712	-2.35312
3.02	2.36841	-2.35312
3.03	32.93132	37.69784
3.04	35.84963	33.69023

Table A.1.2 Showing the IEDs currents corresponding to Protection Zone 2

Time	e2	e26	e27	e28	e30	e31	e32	e33	e34
3.00	2.36712	1.18542	0.41886	0.42361	0.29842	0.26275	-0.68483	-0.78867	0.9774
3.01	2.36712	1.18542	0.41886	0.42362	0.26842	0.26275	-0.68483	-0.78867	0.9774
3.02	2.36841	1.98613	0.41882	0.42362	0.26814	0.26275	-0.68483	-0.78867	0.8774
3.03	32.9312	-7.35984	-3.37295	-1.41443	-6.86457	-5.86744	-5.27637	-5.31889	-3.22167
3.04	35.8493	-8.11525	-3.8972	-2.93274	-8.68645	-5.68918	-6.76811	-4.80653	-3.79676



Table A.1.3 Showing the IEDs currents corresponding to Protection Zone 3

Time	e2	e1	e17	e22	e23	e35	e36	e37	e38
3.00	2.36712	-1.1949	-0.7923	-0.42229	-0.42742	0.48227	0.47836	-0.27819	-0.27116
3.01	2.36712	-1.1949	-0.7923	-0.42229	-0.42742	0.48227	0.47836	-0.27819	-0.27116
3.02	2.36841	-1.1949	-0.7923	-0.42229	-0.42742	0.48227	0.47836	-0.27819	-0.27116
3.03	32.9312	7.3625	3.21489	3.37066	3.41206	5.31117	5.26861	5.85711	5.86256
3.04	35.8493	7.11776	2.79044	2.89504	2.93061	-2.79676	4.76092	5.67931	5.68453

## A.2 All the Matrices for Case Study Network

Adjacency Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
n1	1	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n3	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n4	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n5	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n6	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
n7	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n8	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n9	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n10	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n11	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n12	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n13	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n14	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n15	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Adjacency Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34	
n17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
n18	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0	0	0	1	0	0	0	
n19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	
n20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	
n21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	
n22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	
n23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	
n24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	
n25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	
n26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	
n27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	
n28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	
n29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
n30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	
n31	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	
n32																																			

Adjacency Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
n33	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	
n34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	

Matrix A.2.1 Adjacency Matrix for case study 220 KV Power Network

Reachability Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
n1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	0	0	0	1	1	1	1	1
n2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	0
n3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	1	1	0	0	1	1	1	0	0	1	1	1	0	0	0
n4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
n5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
n6	1	1	1	1	1	1	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
n7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	0
n8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	0
n9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n10	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n11	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n12	1	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n13	0	1	1	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	0	0	1	0	0	0
n14	0	1	1	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	0	0	1	0	0	0
n15	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	0	0	0	1	1	0	0	0
n16	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	0	1	1	1	0	0	0

Reachability Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34	
n17	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	0	0	
n18	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	
n19	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	0	0	0
n20	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	0	0	0
n21	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	0	0
n22	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	
n23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
n24	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	0	0	0
n25	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	0	0	0
n26	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	0	0	0
n27	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	0	0	0
n28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
n29	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	0	0	0
n30	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0
n31	1	1	1	1	1	0	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	0	0
n32	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	

Reachability Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	

Matrix A.2.2 Reachability Matrix for Case Study 220 KV Power Network

Complete Incidence Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
e1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e3	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e4	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e5	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e6	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e7	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e8	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e9	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e10	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e11	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e12	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e13	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e14	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e15	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e16	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Complete Incidence Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
e17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0
e18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
e19	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e20	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
e22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
e25	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e26	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
e30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0

### Complete Incidence Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
e33	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
e34	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
e35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0
e36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
e37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
e40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
e41	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
e42	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
e43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
e44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1

### Matrix A.2.3 Complete Incidence Matrix for Case Study 220 KV Power Network

#### Modified Incidence Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
e1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e3	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e4	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e5	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e6	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e7	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e8	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e9	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e10	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e11	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e12	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e13	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e14	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e15	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e16	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Modified Incidence Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
e17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0
e19	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e20	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e25	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e26	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
e32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
e33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
e34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
e35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
e36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0

Modified Incidence Matrix Contd....

	n1	n2	n3	n4	n5	n6	n7	n8	n9	n10	n11	n12	n13	n14	n15	n16	n17	n18	n19	n20	n21	n22	n23	n24	n25	n26	n27	n28	n29	n30	n31	n32	n33	n34
e37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0
e38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
e41	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
e42	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
e43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
e44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1

Matrix A.2.4 Modified Incidence Matrix for Case Study 220 KV Power Network

# References

- [1] Lu Kaicheng, Lu Huaming. *Graph Theory and its application[M]*. Beijing: Tsinghua University Press, 1995.
- [2] Xinfeng ZHANG, Yunyong ZHANG, Fengqiang DENG, Xiangliang ZHANG. *On-line Fault Locating Method for Wide Area Back-up Protection*
- [3] Chen Heng, Wang Yanping. *Technical Discussion of Relay Protection in Smart Grid[J]*. Science & Technology Information, 2010, (27).
- [4] Ding Wei, He BenTeng, Wang HuiFang. *Discuss of wide-area relay protection based on wide-area information*
- [5] Dongyuan Shi, and Xianzhong Duan, *Member, IEEE*. *Adaptive Agent-Based Wide-Area Current Differential Protection System*
- [6] Y. Serizawa, H. Imamura, N. Sugaya, M. Hori, A. Takeuchi, M. Inukai, H. Sugiura, T. Kagami. *Experimental Examination of Wide-area Current Differential Backup Protection Employing Broadband Communications and Time Transfer Systems*
- [7] Bertil I, Per-Olof L, Dnaiel K, et al. *Wide-aera protection against voltage collapse[J]*. IEEE ComPuter Application in Power, 1997, 10(4):30~35.
- [8] K. Kangvansaichol, *Member, IEEE*, and P. A. Crossley, *Member, IEEE*. *Multi-zone Current Differential Protection for Transmision Networks*
- [9] Li Yingchuan. *Research and Design of Power System Transmission-Line Protection IED Based on IEC 61850[D]*. Chengdu: Southwest Jiaotong University, 2005.
- [10] Su Sheng, Duan Xianzhong, Zeng Xiangjun, K.K.Li, W.L.Chan. A
- [11] A. Armenia and J. H. Chow. *A flexible phasor data concentrator design leveraging existing software technologies. IEEE Trans. Smart Grid*, 1(1):73–81, 2010.



- [12] Y. M. Atwa, E. F. El-Saadany, M. M. A. Salama, and R. Seethapathy. *Optimal renewable resources mix for distribution system energy loss minimization. IEEE Trans. Power Syst.*, 25(1):360–370, 2010.
- [13] Austin Energy. *Austin Energy Smart Grid Program*, <http://www.austinenergy.com/About%20Us/Company%20Profile/smartGrid/index.htm>.
- [14] V. Bakker, M. Bosman, A. Molderink, J. Hurink, and G. Smit. *Demand side load management using a three step optimization methodology. IEEE SmartGridComm '10*, pages 431–436, 2010.
- [15] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, F. Li, J. Li, Z. Li, C.-C. Liu, L. Mili, S. Miller, R. Podmore, K. Schneider, K. Sun, D. Wang, Z. Wu, P. Zhang, W. Zhang, and X. Zhang. *Initial review of methods for cascading failure analysis in electric power transmission systems. IEEE Power and Energy Society General Meeting '08*, pages 1–8, 2008.
- [16] S. Barmada, A. Musolino, M. Raugi, R. Rizzo, and M. Tucci. *A wavelet based method for the analysis of impulsive noise due to switch commutations in power line communication (PLC) systems. IEEE Trans. Smart Grid*, 2(1):92–101, 2011.
- [17] T. Baumeister. *Literature review on smart grid cyber security, Technical Report*, <http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf>. 2010.
- [18] C. Bennett and D. Highfill. *Networking AMI smart meters. IEEE Energy 2030 Conference '08*, pages 1–8, 2008.
- [19] R. Berthier, W. H. Sanders, and H. Khurana. *Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. IEEE SmartGridComm '10*, pages

350–355, 2010.

[20] R. J. Best, D. J. Morrow, D. M. Lavery, and P. A. Crossley. *Synchrophasor broadcast over Internet protocol for distributed generator synchronization*. *IEEE Trans. Power Del.*, 25(4):2835–2841, 2010.

[21] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. *Detecting false data injection attacks on DC state estimation*. *the First Workshop on Secure Control Systems'10*, pages 1–9, 2010.

[22] P. Bonanomi. *Phase angle measurements with synchronized clocks principle and applications*. *IEEE Trans. Power App. Syst.*, 100(12):5036– 5043, 1981.

[23] A. Borghetti, C. A. Nucci, M. Paolone, G. Ciappi, and A. Solari. *Synchronized phasors monitoring during the islanding maneuver of an active distribution network*. *IEEE Trans. Smart Grid*, 2(1):82–91, 2011.

[24] A. Bose. *Smart transmission grid applications and their supporting infrastructure*. *IEEE Trans. Smart Grid*, 1(1):11–19, 2010.

[25] S. Bou Ghosn, P. Ranganathan, S. Salem, J. Tang, D. Loegering, and K. E. Nygard. *Agent-oriented designs for a self healing smart grid*. *IEEE SmartGridComm'10*, pages 461–466, 2010.

[26] N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi. *The deployment of a smart monitoring system using wireless sensors and actuators networks*. *IEEE SmartGridComm'10*, pages 49–54, 2010.

[27] D. M. Britz and R. R. Miller. *Mesh free space optical systems: A IEEE Workshop on Local & Metropolitan Area Networks*, pages 37–42, 2007.

[28] A. N. Brooks and S. H. Thesen. PG&E and Tesla Motors: *Vehicle to grid demonstration and evaluation program*, <http://spinnovation.com/sn/Articles on V2G/PG and E and Tesla>

Motors – Vehicle to Grid Demonstration and Evaluation Program.pdf.

- [29] H. E. Brown and S. Suryanarayanan. *A survey seeking a definition of a smart distribution system. North American Power Symposium '09*, pages 1–7, 2009.
- [30] R. E. Brown. *Impact of smart grid on distribution system design. IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–4, 2008.
- [31] M. Brucoli and T. C. Green. *Fault behaviour in islanded microgrids. 19th International Conference on Electricity Distribution*, pages 1–4, 2007.
- [32] S. Bu, F. R. Yu, and P. X. Liu. *Stochastic unit commitment in smart grid communications. IEEE INFOCOM 2011 Workshop on Green Communications and Networking*, pages 307–312, 2011.
- [33] S. Bu, F. R. Yu, P. X. Liu, and P. Zhang. *Distributed scheduling in smart grid communications with dynamic power demands and intermittent renewable energy resources. IEEE ICC'11 Workshop on Smart Grid Communications*, 2011.
- [34] Y. Cai, M.-Y. Chow, W. Lu, and L. Li. *Statistical feature selection from massive data in distribution fault diagnosis. IEEE Trans. Power Syst.*, 25(2):642–648, 2010.
- [35] V. Calderaro, C. N. Hadjicostis, A. Piccolo, and P. Siano. *Failure identification in smart grids based on Petri Net modeling. IEEE Trans. Ind. Electron.*, 58(10):4613–4623, 2011.
- [36] R. Caldon, A. R. Patria, and R. Turri. *Optimal control of a distribution system with a virtual power plant. Bulk Power System Dynamics and Control Conference*, pages 278–284, 2004.
- [37] S. Caron and G. Kesidis. *Incentive-based energy consumption scheduling algorithms for the smart grid. IEEE SmartGridComm'10*, pages 391–396, 2010.
- [38] A. Carta, N. Locci, and C. Muscas. *GPS-based system for the measurement of synchronized*

*harmonic phasors. IEEE Trans. Instrum. Meas.*, 58(3):586–593, 2009.

[39] J. Chen, W. Li, A. Lau, J. Cao, and K. Wang. *Automated load curve data cleansing in power system. IEEE Trans. Smart Grid*, 1(2):213–221, 2010.

[40] L. Chen, N. Li, S. H. Low, and J. C. Doyle. *Two market models for demand response in power networks. IEEE SmartGridComm'10*, pages 397–402, 2010.

[41] S. Chen, S. Song, L. Li, and J. Shen. *Survey on smart grid technology (in Chinese). Power System Technology*, 33(8):1–7, April 2009.

[42] T. M. Chen. *Survey of cyber security issues in smart grids. Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II (part of SPIE DSS 2010)*, pages 77090D–1–77090D–11, 2010.

[43] X. Chen, H. Dinh, and B. Wang. *Cascading failures in smart grid - benefits of distributed generation. IEEE SmartGridComm'10*, pages 73–78, 2010.

[44] M. Chertkov, F. Pan, and M. G. Stepanov. *Predicting failures in power grids: The case of static overloads. IEEE Trans. Smart Grid*, 2(1):162–172, 2011.

[45] H. S. Cho, T. Yamazaki, and M. Hahn. Aero: *Extraction of user's activities from electric power consumption data. IEEE Trans. Consum. Electron.*, 56(3):2011–2018, 2010.

[46] Cisco Systems. *Internet protocol architecture for the smart grid, white paper*, [http://www.cisco.com/web/strategy/docs/energy/CISCO\\_IP\\_INTEROP\\_STDS\\_PPR\\_TO\\_NIST\\_WP.pdf](http://www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf). July 2009.

[47] E. H. Clarke. *Multipart pricing of public goods. Public Choice*, 11(1):17–33, 1971.

[48] K. Clement, E. Haesen, and J. Driesen. *Coordinated charging of multiple plug-in hybrid electric vehicles in residential distribution grids. IEEE PSCE'09*, pages 1–7.

[49] K. Clement-Nyns, E. Haesen, and J. Driesen. *The impact of charging plug-in hybrid electric*

- vehicles on a residential distribution grid. IEEE Trans. Power Syst.*, 25(1):371–380, 2010.
- [50] F. M. Cleveland. *Cyber security issues for advanced metering infrastructure (AMI). IEEE Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–5, 2008.
- [51] D. Coll-Mayor, M. Paget, and E. Lightner. *Future intelligent power grids: Analysis of the vision in the European Union and the United States. Energy Policy*, pages 2453–2465, 2007.
- [52] C. M. Colson and M. H. Nehrir. *A review of challenges to real-time power management of microgrids. IEEE Power & Energy Society General Meeting*, pages 1–8, 2009.
- [53] A. J. Conejo, J. M. Morales, and L. Baringo. *Real-time demand response model. IEEE Trans. Smart Grid*, 1(3):236–242, 2010.
- [54] F. J. C. Corripio, J. A. C. Arrabal, L. D. del R'io, and J. T. E. Munoz. *Analysis of the cyclic short-term variation of indoor power line channels. IEEE J. Sel. Areas Commun.*, 24(7):1327–1338, 2006.
- [55] G. D'an and H. Sandberg. *Stealth attacks and protection schemes for state estimators in power systems. IEEE SmartGridComm'10*, pages 214–219, 2010.
- [56] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke. *Synchronized phasor measurement applications in power systems. IEEE Trans. Smart Grid*, 1(1):20–27, 2010.
- [57] U. D. Deep, B. R. Petersen, and J. Meng. *A smart microcontrollerbased iridium satellite-communication architecture for a remote renewable energy source. IEEE Trans. Power Del.*, 24(4):1869–1875, 2009.
- [58] Department of Energy. [http://www.eia.doe.gov/cneaf/electricity/epm/table1\\_1.html](http://www.eia.doe.gov/cneaf/electricity/epm/table1_1.html).
- [59] Department of Energy, Office of Electricity Delivery and Energy Reliability. *Study of security attributes of smart grid systems – current cyber security issues 2009*,

[http://www.inl.gov/scada/publications/d/securing\\_the\\_smart\\_grid\\_current\\_issues.pdf](http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf).

[60] P. Donegan. *Ethernet backhaul: Mobile operator strategies & market opportunities*. *Heavy Reading*, 5(8), 2007.