AN ABSTRACT OF THE THESIS OF

Panini Sai Patapanchala for the degree of Master of Science in Computer Science presented on June 15, 2016.

Title: Exploring Security Metrics for Electric Grid Infrastructure Leveraging Attack Graphs

Abstract approved: _____

Rakesh Bobba

Electric grid is a critical cyber-physical infrastructure that serves as lifeline for modern society. With the increasing trend of cyber-attacks, electric grid security has become a significant concern. Electric grid operators are working hard to reduce the risk of these attacks towards the system. Having security metrics for monitoring the risk to the cyber-physical power grid infrastructures would be very helpful to grid operators. However, security metrics to assess the security posture or risk to enterprise networks have been a long standing challenge. Cyber-physical systems (CPS) that have interconnected cyber and physical infrastructure add an additional layer of complexity. In this thesis work, we explore some security metrics that can be used to monitor the security posture and risk to CPS. These metrics take both the cyber security posture and physical impact of an attack in to account. We focused on both individual and coordinated attacks that can cause cascading outages. To evaluate

these metrics, we created cyber physical models for 9-bus, 39-bus and RTS-96 power system models using the previously developed Cyber Physical Security Assessment (CyPSA) framework. Our metrics provide a novel way to identify and prioritize assets critical to the system and help operators take steps to improve the overall security posture of the system.

Exploring Security Metrics for Electric Grid Infrastructure Leveraging Attack Graphs

by

Panini Sai Patapanchala

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Master of Science

Presented June 15, 2016
Commencement June 2017

Master of Science thesis of Panini Sai Patapanchala presented on June 15, 2016.

APPROVED:

Major Professor, representing Computer Science

Director of the School of Electrical Engineering and Computer Science

---

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Panini Sai Patapanchala, Author

ACKNOWLEDGEMENTS

Firstly, I would like to thank Dr. Rakesh Bobba for being the best mentor I could have ever hoped for. Thank you for supporting my graduate studies, teaching me the craft of scientific research, and helping me shape my life and professional career. You have been one of the most influential people in my life and I shall be eternally grateful to you. I also wish to thank CyPSA team. I could never forget the assistance and help I got from you people. A very special thanks to Dr. Eduardo Cotilla-Sanchez, Dr. Jinsub Kim and Dr. Margaret Niess for agreeing to be in my committee. My heart felt thanks to Dr. Bella Bose and Nicole Thompson for the initial support they have provided.

Finally, I would like to thank my parents and brother for encouraging me to challenge myself by pursuing Masters. More importantly, I thank them for providing me with all the opportunities that have enabled me to accomplish this and more. Annayya, your constructive criticism always makes me to achieve goals I set for. Last but not the least, I would like to thank my besties Vishnu Priya, Bharath Sunchu and friends in Corvallis for all the fun, memories and help. My stay in Corvallis would not have been half as enjoyable if you were not around. Thank you for being my family away from home. I could not have done this without you guys.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF TABLES

LIST OF ALGORITHMS

LIST OF APPENDIX FIGURES

Chapter 1: Introduction

Electrical energy is a key commodity for todays modern society. In most cases, electric power is not generated at the same location as it is consumed. It is produced by power plants at remote locations and is delivered to the end users by a power grid. It is a network of transmission and distribution systems maintaining different levels of voltage, depending on the amount of electricity needed. Substations are used to connect these voltage levels using transformers, circuit breakers etc.

Any kind of damage to these physical infrastructure elements is catastrophic during disasters. Thus, delivering efficient and reliable supply of energy has become the main concern of electrical companies. Since the evolution of power grid, it has undergone many improvements through each decade. Today, it consists over 10,000 electric generating units and 1 million MW of generating capacity connected to more than 300,000 miles of transmission lines. Although the power grid is considered as engineering marvel, many works have been proposed to still improve its capacity.

To move forward with technology advancements, we need a new kind of power grid, that incorporates computerized equipment and technology. In this way it would be easy for operators to automate and manage the increasing complexity and meet the needs of electricity in this century. To serve this purpose, supervisory control and data acquisition (SCADA) systems are currently in use to collect and analyze

data in various industries. These kind of upgrades to power grids are being carried out as a part of smart grid initiative. This initiative brings a lot of affect on the SCADA system. In addition to that, it widens the communication medium between all entities of a power grid including power plants, control centers, transmission and distribution substations, and even customer homes. As a result of this, the cyber components in the power grid has been significantly increased. These cyber components like controller, relays and sensors are generally connected by Ethernet or radio communication modules along with configuration functionalities such as embedded web servers.

This increases the communication elements and their cyber connectivity in the infrastructure and the interdependency between cyber and physical components introduces a greater level of complexity. Thus, to secure the operations of power system from attackers becomes more challenging. Electric grid operators are working hard to reduce the risk of these attacks towards the system. Control Systems. NERCC reliability standards were proposed to be followed by entire United States Power Companies. Even following such standards, there is no guarantee that power systems are secure.

Over the time, events like North east blackout of 2003 and a terrorist threat of russion cyberwarfare in one way or other are the outcomes of cyber communication network failures. In addition to these, the recent cyber attack on Ukrainian Critical Infrastructure has proved that cyber threats are real and they can cause huge damage not only to power grid but also to society. Public reports say that BlackEnergy (BE) malware was discovered on the Ukrainian power companies computer networks but it

is still under investigation. Thus, with the increasing trend of cyber-attacks, security of electric grid has become a significant concern. To overcome these situations a metric for cyber induced contingencies risk assessment would be helpful. Having security metrics will make grid operators a way to identify and prioritize critical assets. However, security metrics to assess the security posture or risk of cyber induced physical contingencies to electric grid networks have been a long standing challenge. Some important reasons are –

- interconnected cyber and physical infrastructure adds an additional layer of complexity to the network
- hard to identify attack dependency and coordinated attacks
- hard to capture inter dependency of cyber physical factors while ranking

Thus, in my thesis work, an effort has been made to find a metric that can measure the security of system.

We explored some security metrics that can be used to monitor the security posture and risk to CPS. These metrics take both the cyber security posture and physical impact of an attack in to account. We focused on both individual and coordinated attacks that can cause cascading outages.

To evaluate these metrics, we created cyber physical models for 9-bus, 39-bus and RTS-96 power system models using the previously developed Cyber Physical Security Assessment (CyPSA) framework. Our metrics provide a novel way to identify and prioritize assets critical to the system and help operators take steps to improve the overall security posture of the system.

Rest of the document is organized as follows: In the Chanpter 2 we will discuss the background details required for understanding the cyber physical modelling and measurements used in the metrics. In Chapter 3 we will discuss how to create a cyber physical model using the CyPSA framework. Electric grid security metrics will be presented with examples in Chanpter 4. Result and Summary with future scope is presented in Chapter 5 and 6 respectively.

Chapter 2: Background

Before moving to Cyber Physical Modeling, one needs to understand a power system model and how a protected system on it works to overcome the disruptions and make the system reliable. With the inclusion of cyber elements for communication in power grid, a wide range of attacks are possible in cyber communication networks. Thus, we will have a brief discussion on cyber communication involved for control in SCADA. Later, we will look in detail on how an attack can happen in certain networks, how to represent different attacks in a attack graph and scoring the attack related to their criticality. Finally, we will look at related work that has been carried out in cyber physical modeling and security metrics for risk asssesment in CPS.

Rest of this chapter is organised as follows: the power system architecture, Cyber Communication involvement and the Downside of the cyber elements will be discussed. Later I will be presenting related work that has been carried out in security metrics for risk assessment in power grid.

2.1 Power System Architecture- Physical Characteristics

Power system contains generation transmission distribution. Huge power. Machinery costly. In this section, we will discuss on how to represent a power grid through one-line diagrams. We also look in to how the reliability of the system is improved by using node breaker models. These models help to minimize the damage to the

physical components during disasters. Finally, different protection systems that help in monitoring and controlling physical components are discussed.

2.1.1 One line diagram

One-line diagrams are very well known notions to represent a power system in power flow studies. It is the graphical representation of power flow paths between the entities of the system. For example we use one-line diagram or single-line diagram (SLD) for depicting a three-phase power system [14]. All the electric elements like circuit breakers, transformers, capacitors, bus, and conductors are represented as standard symbols. A single conductor is used to represent all the lines or terminal of a three-phase power system. The elements in the diagram do not actually represent the size or location of the actual equipment, but it is a standard convention to organize the elements as left-to-right or top-to-bottom. For a PLC control system, we can use a one-line diagram to to show a high-level view of the conduit.

2.1.2 Node-breaker model

The power system networks are usually represent using the bus-branch models. Each substation is represented by single bus operating at a nominal voltage level. Without external sources, it is difficult to obtain the substation breaker information. As a result, it is not possible to know how it operates during contingencies and a large number of contingencies have to be manually created to replicate bus and breaker failure contingencies. This would often lead to human errors and a lot of time is

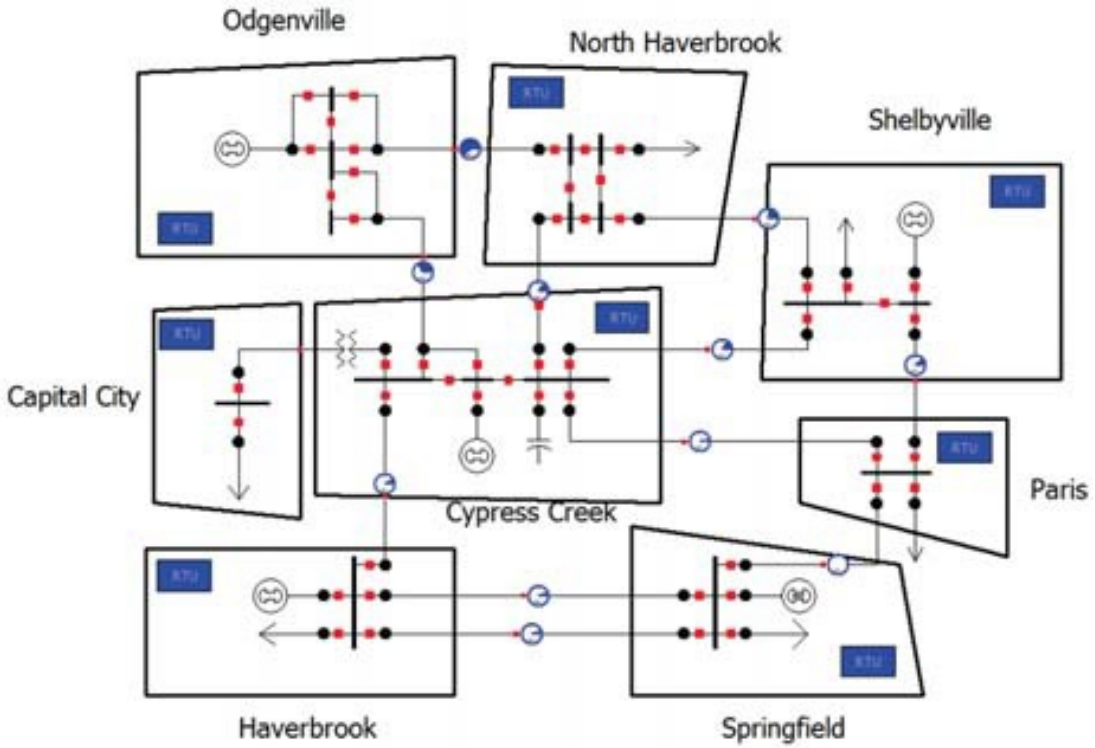

Figure 1: 8bus One-line diagram [8].

consumed to reconfigure buses for study.

The solution to overcome this is the node-breaker models. The simplified bus models in the bus branch configuration are replaced by fully built substations with elements including breakers, switches, branches, or shunts are modeled individually and connected via nodes. are few example of node breaker models.

Of all the available electrical bus system schemes, selection of a particular scheme depends on the following factors -

- Voltage of the power system

- Location of substation in power system
- Flexibility of the system
- Cost for installation

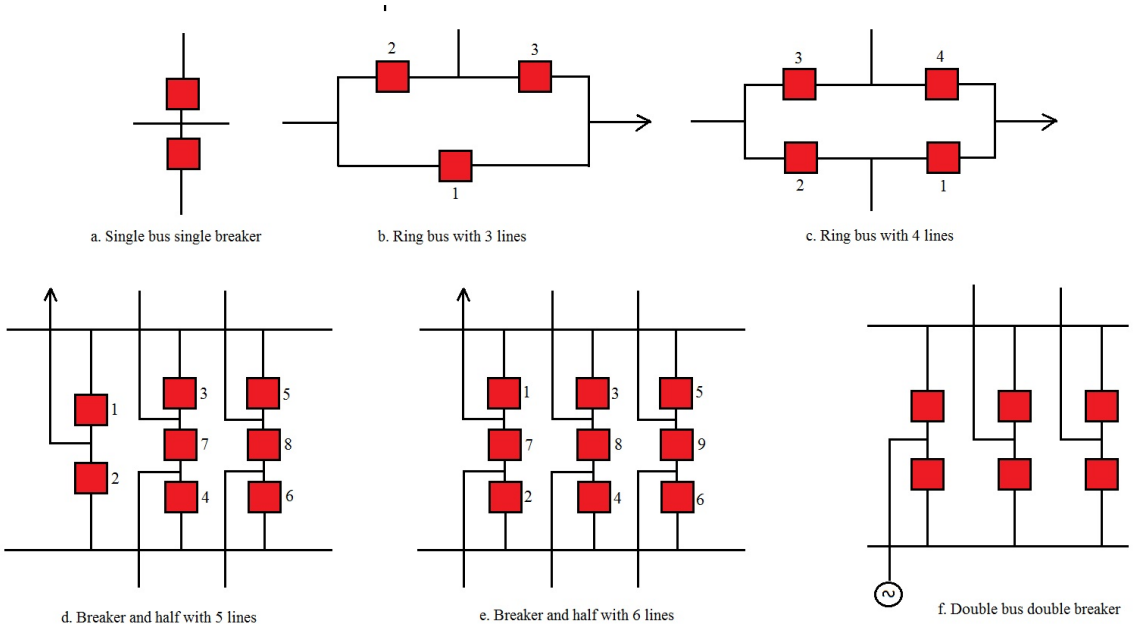

Figure 2: Different types of Node breaker models used in COSMIC.

Once a bus system scheme is selected, we need to arrange the elements in such a way that -

- The system is simple.
- Different equipments can be maintained easily
- Minimize power outage during maintenance.
- The system is scalable with growth of demand.

- Optimizing the selection of scheme so that maximum output is given from the system.

The most commonly used node breaker bus bar arrangements are discussed below-

- Single Bus System The cheapest and the simplest bus system is the Single Bus System. In this scheme, all the feeders and transformer bay are connected to only one single bus. The advantages of Single Bus System are -
  - Simple in design.
  - Cost effective scheme.
  - Convenient to operate.

  The only disadvantage of Single Bus System is that it is not easily maintainable without interrupting the feeder or transformer.

  The indoor 11 KV switchboards is one example that follows a single bus bar arrangement.

- Double Breaker Bus System

  Double Breaker Bus System has two bus bars that are identical to each other. The two bus bars should be connected with a breaker to every feeder in parallel. The incoming or outgoing feeders can be taken from any bus similar to double bus bar system. The breakers and its associated isolators are closed in order to put the feeder to respective bus. The total number of feeders are divided into two groups - one is fed from one bus and the other group is fed from the bus similar to the first one. At any point of time, a feeder can be transferred from

one bus to the other. As the feeders are placed because of operating breakers, it is not necessary to use a bus coupler.

- One and A Half Breaker Bus System

  An improvement over double breaker bus system is the One and A Half Breaker Bus System. It has a simple design with two feeders fed from two different buses through their associated breakers and a third breaker called the tie breaker is used to couple these two feeders. Generally, the buses are responsible to power up the two circuits by closing all the three breakers. The tie breaker is used as coupler. In this scheme, we use less number of circuit breakers than double breaker bus system i.e., only tie breaker is associated for every two circuits. However, the protection of the two circuits is complicated when their own breakers are taken out for maintenance since they are associated with the central breaker. In case of any feeder breaker failure, the second feeder breaker and the the tie breaker are used to feed the power. This scheme is not that popular because of the prohibitory costs of the equipment.

  The advantage of One and A Half Breaker Bus System is that it can be easily maintained without interrupting any feeders in the system since all the feeders can be fed from other healthy bus.

  The only disadvantage of One and A Half Breaker Bus System is that this scheme is expensive because of the installation of the tie breaker.

- Ring Bus System

  The design of the system is shown in the above figure. Each feeder circuit

is double fed by opening one breaker under maintenance and thus does not affect the supply to any of the feeder. This scheme has two disadvantages - The circuit being in a ring structure, it is not scalable. The reliability of the system is poor if any of the circuit breaker in the loop is a switch. The reason is that the closed loop becomes open and removal of any breaker in open loop interrupts all the feeders between removed breaker and open end of the loop.

In our model we are using the node breaker model based on number of lines connecting to the bus and the elements connected to it. In a general setup we are using a single bus single breaker, bus branch, for bus with two lines a Ring bus for 3 or 4 lines Breaker and half for more than four lines Double bus double breaker if a bus is associated with a generator. In this special case we ignore number of lines connected to the bus.

2.1.3 Protection System

In electrical engineering, whenever a fault is detected protection relays are used to trip a circuit breaker. Initially, faults like over-current, over-voltage, reverse power flow, over-frequency, and under-frequency are detected by protective relays which are electromagnetic devices that relies on coils operating on moving parts. Electromechanical relays are used only to indicate whether phase or zone targets are involved and failed to provide protection and supervision over the system failures. As a result Microprocessor-based digital protection relays came into picture. They can provide functions that can be carried out by two or more electromechanical devices. On

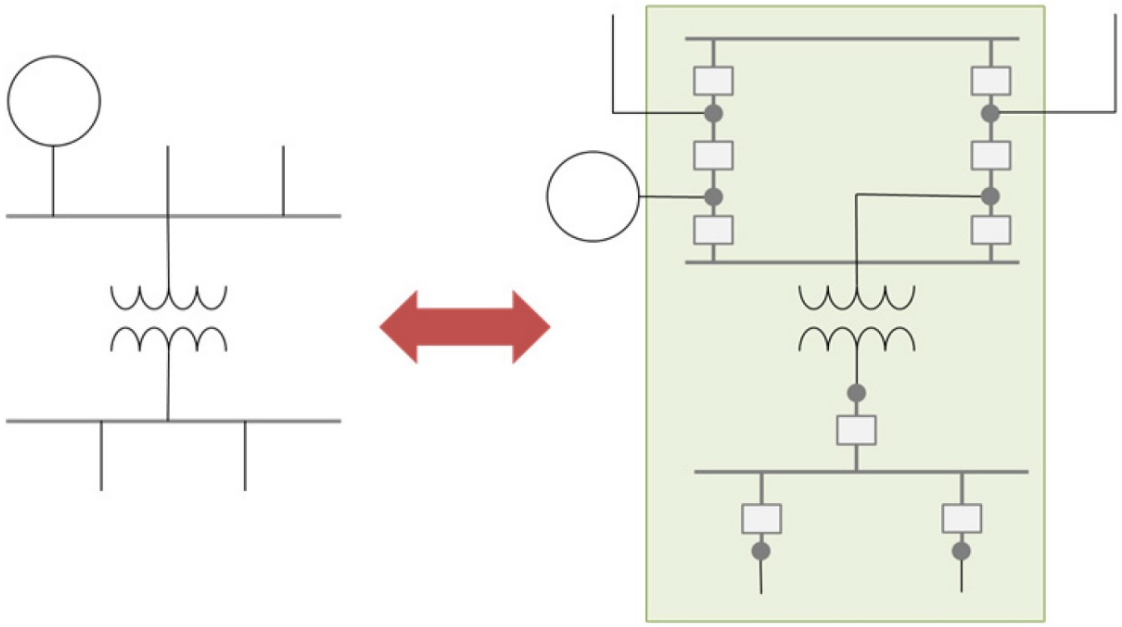

Figure 3: Traditional Bus-branch View vs. the Detailed Node-breaker View of a Substation [8].

the other hand, numerical relay are better than electromechanical relays in terms of capital and maintenance cost. Transmission lines and generators have a number of electromechanical devices, or few microprocessor relays dedicated for protection.

ANSI device numbers are used to denote various protective functions available on a given relay. For example, a timed overcurrent protective relay is represented by ANSI device number 51.

- Overcurrent Relay
- Distance relay
- Current differential protection scheme

- Directional relay
- many more..

The functionality of some of these relays are explained in detail in appendix.

2.1.4 Physical Impact

In an electric grid, when one infrastructure is disrupted, it can directly and indirectly affect other infrastructures. This impact could further effect large geographic regions by sending ripples throughout the power system and national economy. The 1998 power crisis in California for long time due to failure of the Galaxy 4 telecommunications satellite is one such example for ripple effect. So in order to find the cyber induced contingencies impact due to compromised target/s, we are considering two measurements provided by two different tools.

2.1.4.1 Performance Index

The severity of the potential malicious physical consequences (i.e. percentage of line overload) is measured through an index called performance index. Performance index characterizes the severity of line overloads cause by the contingency as shown in the following equation:

$$F(s) = \sum_{l \in L} \left[max\left\{ \frac{f_s(l)}{f^{MAX}(l)} - 1, 0 \right\} \right]^2 \tag{2.1}$$

Here, is the set of all lines, denotes flow on line in state , and denotes the maximum flow allowed on line . In the event that a power flow fails to converge, a severe physical impact can be assumed which justifies setting to a large number, the outage severity. The outage severity should be much larger than any of the line severity measures.

2.1.4.2 Load shed

Load shed is the amount of load lost are shed to reduce the system stress during a contingency. For example, if we consider a voltage magnitude or frequency signals at a load Bus i are lower than the specified thresholds, the UVLS relay or UFLS relay will shed a 25% (default setting of cosmic) of the initial Pd,i to avoid the onset of voltage instability and reduce system stress. Thus whenever an abnormality occurs there will be some load loss or load shed occurs as a consequence of the physical contingency. This consequence of loss of physical entity is considered as physical impact in dynamic setting used for cosmic analysis.

2.1.5 Tools

2.1.5.1 PowerWorld

To generate performance index of cyber induced physical contingencies we used PowerWorld. It simulates the underlying power system and solve the power flow equa-

tions to calculate the physical index, which in turn will be used to calculate the security index. In particular, we used the Simulator Automation Server(SimAuto) toolbox to set up a real-time connection to PowerWorld. SimAuto of PowerWorld allowed us to take advantage of the power of automation to extend the functionality of PowerWorld Simulator to customize for our application. The ability to launch and control PowerWorld Simulator from within our CyPSA application, enabled us to: access the data of a Simulator case, perform defined Simulator functions and other data manipulations, and send results back to our original application, to a Simulator auxiliary file, or to a spreadsheet. SimAuto acts as a COM(Component Object Model) Object, which can be accessed from various Windows-based programming languages that support COM compatibility. With COM technology incorporated into PowerWorld Simulator, we are able to obtain the following benefits -

- Ability to create custom applications to automate frequent tasks;
- Addition, modification, and retrieval of Simulator case data at runtime;
- Capability to carry out such development with the most simple and common tools; and
- Easy integration of results into Microsoft Excel.

2.1.5.2 Cascading Outage Simulator with Multiprocess Integration Capabilities - COSMIC

Cascading Outage Simulator with Multiprocess Integration Capabilities (COSMIC) [19] is a new non-linear dynamic model designed for cascading failures in power systems. In COSMIC, dynamic components are modeled using differential equations and their associated power flows are represented by using non-linear power flow equations, load voltage responses are represented explicitly, and discrete changes like components failures, load shedding are represented by a set of equations that indicate the proximity of thresholds that trigger these changes. Given the set of exogenous disturbances that may trigger a cascade and the dynamic data for a power system, COSMIC uses a recursive process to compute the impact of the events triggered. The differential-algebraic equations (DAEs) are used for computing besides monitoring the discrete events, including events that further divide the network into islands.

Song et.al., [19] proposed a model that replaces the commercial tools and provide a platform for research and development where one can explicitly test the impact of the assumptions made while modeling dynamic cascading failure. With the help of this tool, the users can modify the existing system components, add new ones, and integrate advanced remedial control actions. In addition to these, the dynamic / adaptive time step and recursive islanded time horizons that are implemented in this simulator allows faster computations during, or near, steady-state regimes, and fine resolution during transient phases. Moreover, we can be easily integrated the tool with High Performance Computing (HPC) clusters and is capable of running many

simulations simultaneously at a much lower cost when compared to commercial tools. The different types of protective relays modeled in COSMIC are - over-current (OC) relays, distance (DIST) relays, and temperature (TEMP) relays for transmission line protection as well as under-voltage load shedding (UVLS) and under-frequency load shedding (UFLS) relays for stress mitigation.

2.2 Power System Control and Communication

For the cyber communication in power grid a Wide Area Network is used. A computer network that occupies a relatively large geographical area is called a Wide Area Network (WAN). Generally, two or more local-area networks (LANs) combine to form a WAN. Public networks like the telephone system or leased lines or satellites can serve as a medium for the computers to be connected to WAN. Internet is one example of a WAN.

As we discussed, SCADA systems are used to control the power systems. Even for converting the entire grid to smart system we will be using SCADA as a center for controlling purposes. This brings a lot of changes to the existing system. As part of smart grid every physical components and consumers will be communicating to provide optimal usage of power increasing the reliability of grid. These communications include

- Monitoring lines using protection relays and RTU's
- Controlling operations open/close of Circuit breakers
- power consumption from consumer

- Power generation based on the usage
- Switching and many more...

Due to these there could be data integrity threat and flase data injections. Over past two decades research has been carried to detect and mitigate cyber attacks. But applying the existing cyber network solutions directly to the CPS networks will not be applicable mainly due to the dependencies due to the cyber-physical inter connections. On the other hand online framework has been proposed to detect malicious activities in a cyber-physical system [8, 27, 29, 31]. They uses the information from distributed power system meters and cyber side vulnerability information to detect the anomalies an attacks.

2.2.1 SCADA

The SCADA network plays an important role in modern day power system operation and control [21]. By enabling monitoring and controlling, a closed control system is created between control centers and field devices. The physical components of the power system like circuit breakers are directly connected Intelligent Electronics Devices (IED). Research has been carried out in risk modeling for such SCADA based networks [20]. Modern IEDs are programmable and can function as both sensors and actuators. Thus, they are capable of implementing automation and logic at device level by enabling system operators. With the help of their sensing functionality, the state of power system variables are notified by IEDs to Remote Terminal Units (RTU). Each substation has multiple RTUs that are responsible for collecting data from

multiple IEDs. The collected information includes the status of the circuit breakers and analog measurements like current and voltage of transformers. Modern IEDs and RTUs use Ethernet interface and are accessible through TCP/IP protocols. Some of the other protocols supported are IEC 61850, DNP3.0, ICCP, UCA2.0 and Modbus. With the support of many protocols, the communication infrastructure is readily available for Internet Service Providers. The SCADA servers control center receives the information gathered by RTUs. This real-time system information is accessed by the control applications running on the application servers. Depending on the type of control center, the applications ranges from state estimation at the ISO level to local voltage control at transmission substation-level. The post pre-processing information obtained from the application servers is accessed by the system operator to take an appropriate control action. This control message is then relayed to the IED actuators through the corresponding RTU. In practice, there are utilities that provide remote access capabilities to vendors for maintenance and upgrade purposes and to corporate offices for market operations. These access capabilities serve as a backdoor for attackers to gain to the SCADA infrastructure.

2.2.2 Smart Grid

A smart grid is a fully automated power distribution system. It monitors the usage and voltage levels by making adjustments constantly to make sure that everything runs at a optimal level. This gives us a vision of what a smart grid can deliver but there are other elements like load tap changers, capacitor banks and reclosers that

are not smart enough to make adjustment on their own. They have to be directed to when and how to respond.

SCADA, supervisory control and data acquisition, acts as a smart grid decision making system. Smart grid's line sensors and other connected equipment are responsible to send a stream of data to central control room. This information is analyzed and SCADA systems in the control room are responsible for taking automated decisions and executing them by regulating voltage levels, optimizing efficiency, routing and generation. In real-time, these decisions are taken by running algorithms on the data received and then direct the elements to make necessary adjustments to optimize voltages and self-heal any disruption issues during this process.

2.2.3 Software Vulnerability : NVD Database and CVSS Scoring

As we know with the introduction communication elements in the power system is advantageous in improving reliability and safety. But they also bring the adversary of malware or software vulnerability to the system. The major cause of cyber security problems are because of the software vulnerabilities. Thus we will look in to some vulnerability databases and scoring system available in rating the criticality of a vulnerability.

The National Vulnerability Database (NVD) is a public data source that maintains standardized information about reported software vulnerabilities [3]. Since its inception in 1997, NVD has published information about more than 43,000 software vulnerabilities affecting more than 25,000 software applications. This information is

potentially useful in understanding trends and patterns in software vulnerabilities. It helps us to better manage the security of computer systems that are pestered by the ubiquitous software security flaws.

In addition to this, effort has been made in rating the IT vulnerabilities. One such famous standard metric is called Common Vulnerability Scoring System (CVSS) (Mell, Scarfone, and Romanosky 2006; Mell, Kent, and Romanosky 2007) [1]. It is an industry standard vulnerability scoring system that provides an open and standardized method for rating IT vulnerabilities. CVSS is used by a number of organizations to provide their vulnerability assessment and the National Institute of Standards and Technology, published a publicly accessible National Vulnerability Database (NVD). CVSS can describe a vulnerability with over a dozen metrics, and they can be organized into three groups -

- The Base metric group The Base metric group quantifies aspects of the vulnerability that are intrinsic, fundamental, and are unaffected by time or location. This group provides descriptions on how one can access vulnerability, how complex is the vulnerability to exploit, and how many times one has to authenticate to exploit a vulnerability. All of these sub-metrics are necessary to reach our goal of scoring stepping-stone paths.

- The Temporal metric group The Temporal metric group represents the vulnerability attributes that may change with time. A relevant metric for us in this group gives us the information on the availability of code to exploit the vulnerability.

- The Environmental metric group The Environmental metric group contains no metrics that can be related to the difficulty of accessing a vulnerability. Like the base metric group, it has metrics that speak about the impact of an exploit. This would be interesting in an analysis, for example, in finding stepping-stone paths that can maximize the impact besides considering the difficulty in accessing it.

The NVD database we use provides only the Base metrics, which are described in Table 1. [16]

AccessVector	local access required	0.395
	accessible from adjacent network	0.64
	accessible from remote network	1.0
AccessComplexity	high	0.35
	medium	0.61
	low	0.71
Authentication	requires multiple authentications	0.45
	requires single authentication	0.56
	no authentication required	0.704

Table 2.1: Exploitability metrics - base group CVSS metrics [1].

Each group has a qualitative part, and their corresponding quantitative part that come from CVSS standard. The AccessVector (Av) describes how close the attack must be to the victim host in order to gain access to the exploit. The AccessComplexity (Ac) qualifies the difficulty in executing an exploit. The AccessComplexity is high when specialized conditions like the attacker must have administrative privileges, or the exploit requires some sort of spoofing, are required. In addition to the

specialized conditions, it may be given if the attack needs to get inside of a race condition when there is only a narrow window of opportunity. The AccessComplexity is medium when specialized conditions like a user requires some particular level of authorization or some information has to be gathered before launching an attack, or a small amount of social engineering is needed, are required. The AccessComplexity is low when specialized conditions dont exist. Based on the number of authentications required to exploit the vulnerability, the AccessAuthentication (Aa) differentiates. According to the CVSS standard, these three metrics are combined to create a composite Exploitability Score. CVSS exploitability score for the attack vulnerability is the metric we use to assess the exploitability of power network and is given below -

$$\varepsilon = 20 \times A_v \times A_c \times A_a$$

This implies, the larger the ε is, the easier it is to exploit the vulnerability. CVSS scores are also used to address the impact of the vulnerability on confidentiality, integrity, and availability. We use this as scale to measure the cyber impact of a particular vulnerability.

The cyber cost (C) incurred for an attacker to exploit a cyber component can be derived from exploitability score as follows :

$$C = 11 - \varepsilon$$

In order to measure the difficulty to penetrate into the power network we are using the vulnerability information that attacker need to exploit.

2.2.4 Attack Graphs

In particular, CyPSA generates an attack graph leveraging the cyber-physical model and available known-vulnerability information from public vulnerability databases like the National Vulnerability Database (NVD) [3]. An attack graph is a graph representation that captures potential attack paths leading to specific threats (*e.g.,* a line outage in this case) to a given system. In this case the attack graph captures potential attack paths that enable an adversary to impact the physical grid by gaining control over devices like relays that can open or close lines by signaling to breakers. Here each node in the attack graph represents a host or device and each directed edge represents a cyber vulnerability exploitation that allows an attacker to gain control of the destination node by leveraging the presence of a an exploitable vulnerability.

2.2.4.1 Attack Cost

In order to assess the risk to the system, it is necessary to understand the chance of a potential threat and its impact on the system. Given the critical nature of electrical grid it is reasonable and prudent to operate under the assumption that it is under constant threat of cyber-attacks. Further, what-if scenario analyses that considers certain elements of the network as being compromised and under adversary control are useful to identify weaknesses in the system's security controls. With this in mind, as was done in the CyPSA framework, we use the cost (C) of launching an attack instead of chance of a threat materializing to assess the risk.

An attack consists of a series of vulnerability exploitations that take an adversary

from a source node to a desired target node and is also referred to as an *attack path*. For every vulnerability reported, Common Vulnerability Scoring System (CVSS) [1] provides an exploitability score associated with it. It is expected that the higher the exploitability score the easier it is to exploit the vulnerability. Thus a complementary value of exploitability score normalized to range within the scale of 1 to 10 is used to represent the cost of exploiting the vulnerability. The cost of a an attack then is the summation of costs of exploiting each vulnerability along the path.

A list of known-vulnerabilities

2.2.4.2 Attack Impact

The physical impact (PI) of a cyber attack on the electrical network can be captured using a variety of measures. CyPSA focused on the threat of cyber-induced line outages and used *performance index*, which captures the flow overloads caused by a line outage, as the impact metric. In this work we also focus on cyber induced line outages but we use load shedding [19] as the impact metric in our illustrations. Load shedding captures the amount of load that needs to be shed to reduce the stress on the grid elements caused by the outage. But the proposed security metrics can be used with performance index or any other suitable physical impact metric.

For scalability of analysis one can classify the nodes in an attack graph into three types: *(i)* Target Nodes, *(ii)* Source Nodes, and *(iii)* Intermediate Nodes or Stepping Stones. Target nodes represent control devices like relays which when taken over by an adversary can impact the physical system directly and are of interest for risk

assessment. Source nodes represent nodes that could potentially originate attacks into the system like jump hosts or other externally connected devices. Intermediate nodes are nodes that are not the primary target of an adversary but are used as stepping stones to reach a target node. This classification allows one to identify a set of source and target nodes of interest and focus the analysis on attacks paths from sources to targets. Figure 1 shows a sample attack graph with two source and target nodes and one intermediate node connected by edges indicating the presence of an exploitable vulnerability and associated cost for exploiting the vulnerability. Note that while the figure only shows one edge between two nodes it is possible there might be multiple edges with different or similar costs. In this work we focus on graphs with one minimum cost edge between nodes and reserve analysis of multi-graphs for future work.

Security Index [7] defined as follows is used in CyPSA for risk assessment and identifying critical target, source and intermediate nodes:

$$S.I = \frac{P.I}{C} \tag{2.2}$$

Here $P.I$ represents the potential physical impact of compromising a node, and C represents cost of minimum-cost attack path. Note that physical impact metrics like performance index are routinely computed in power system operations and are available so in theory a power system operator already know what his critical nodes are from a purely physical impact perspective. However, what is not obvious with a cyber-physical analysis is how difficult or easy it is for an cyber-adversary to access such critical nodes. Thus, security index provide one way to identify critical nodes

taking into account both the physical impact and difficulty of imposing that impact from a cyber-attack perspective. For example, if compromise two nodes has the same physical impact then the node that is easy to exploit or gain control over should be prioritized for security efforts and controls. While this is a good first security metric, as we will show in the rest of the paper this metric alone does not provide the full picture. Thus in this work we define and illustrate novel security metrics inspired by network graph metrics.

If n such paths exist from different hosts. Then,

$$SecurityIndex = I_c * \Big(\frac{1}{c_1} + \frac{1}{c_2} + ... + \frac{1}{c_n}\Big),$$

where c_1, c_2,.., c_n are the cost associated with n attacks from different sources. As discussed attacks can be categorized in to two types. 1. Isolated Attacks objective to compromise a single target 2. Coordinated attacks objective to compromise more than one target

2.2.5 Cyber Tools

Cyber based tools used in our project are Nmap for scanning and NPview for firewall visualization and attack graph generation. We have embodied the analysis described in this paper within a software tool, NP-View, orginally developed under research contracts at the University of Illinois, now licensed by Network Perception. 2 NP-View is marketed for use in security audits performed in the power industry, but has more general application. From the configuration files of routers, switches, and

firewalls it infers the network topology, and augments this with evidence of additional hosts obtainable from the scanning tool nmap (Lyon 2009). It then computes all of the connectivity the configurations permit; for our purposes, in particular, it computes which pairs of hosts (hs;hd) exist such that hs can send a message that reaches hd, and all of the ports (and protocols) involved in those transfers. Figure 1 presents a screen shot of NP-View on a sample network, and then the results of a stepping-stone analysis based solely on hop-count distance between attacked host and networks from which attacks might be launched.

2.2.5.1 NP-View and Nmap

Nmap is an active scanning tool capable of discovering and reporting a significant amount of information about the state of a host. NP-View can import an Nmap report from which it extracts information about open services on the host, and the Common Vulnerabilities and Exposures (CVE) identity of their vulnerabilities. It then looks up the CVSS score for each CVE entry from the NIST NVD database, and uses it in the kind of analysis developed in this paper. The most easily accessible pathways to vulnerable hosts are reported and (ultimately displayed in ways similar to that in Figure 1).

2.3 Related Work

Many works have been proposed from a wide range of fields such as computer science,economics and reliability theory for a quantitative representation of security

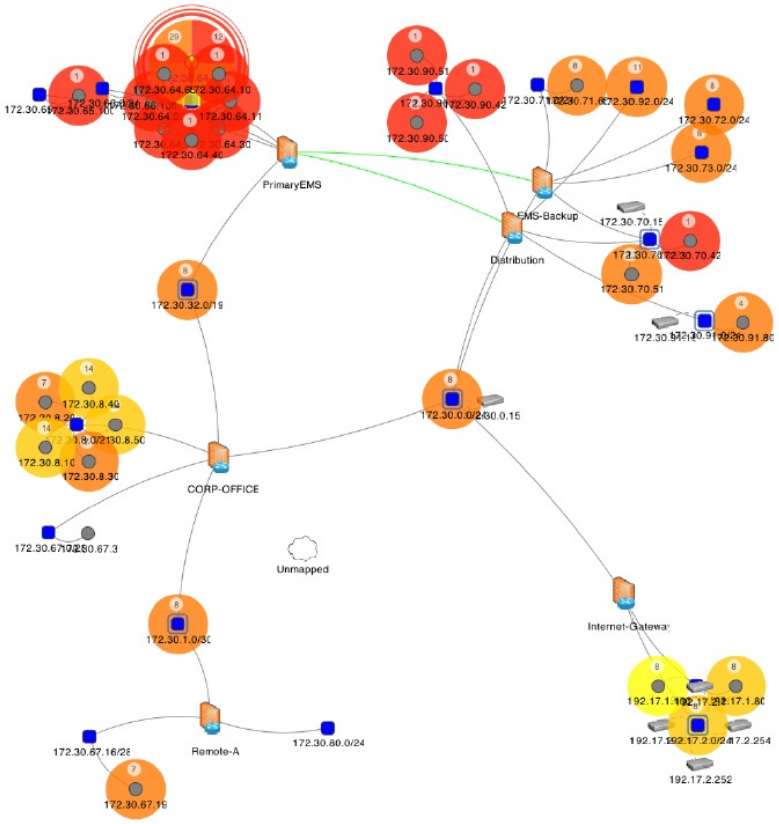

Figure 1: Screen-shot of NP-View analysis software showing stepping stone vulnerabilities.

Figure 4: NP View Screenshot [8].

known as security metrics [23]. Most of the proposed security metrics by these works used attack graph models generated by considering percentage of compromised hosts [13], the weakest adversary required to compromise a network [18], attack likelihood [4], and resilience to zero-day attacks [15, 26]. Due to the lack of validation and comparison between these methods, security metrics has been considered a weak hypothesis [23].

However, efforts have been made by CVSS [1] and NSIT [9] to standardize the security metrics. But, they considered the impact of individual vulnerabilities in isolation, and not the overall impact of combined vulnerabilities. This would imply that a security metric should be defined by predicting the next possible action that an attacker would choose to exploit the network. Static adversary-driven security assessment techniques [11,12,25] and defense-centric security assessment approaches are few of the research efforts in this direction of computer network contingency analysis, which could be used to identify the set of next possible adversarial actions. But, due to the lack of awareness for future adversarial actions, unpredictability of attackers behavior which is very hard or if not impossible in practice and failing to incorporate the effects of physical contingencies, these techniques have not been implemented.

Volkanovski et al. [24] introduce a power system reliability analysis algorithm using fault trees generated for each load point of the system. The proposed method focuses only on accidental failures due to natural causes, and hence does not consider maliciously induced power component failures.

Security metrics for Cyber Situational Awareness(CSA) have been proposed in a generalised way by Cheng et.al., [6]. In their work they proposed existing techniques in risk assessment and better ways to state of art security assessment for enterprise networks and also attack graph based vulnerability assessment. However, that work does not take into account the power network topology and case where the targets have different physical impacts and consequences when attacked in groups.

On the other hand, Chen et al., [5], proposed a workflow based security assess-

ment framework and demonstrated its use using the case of Advanced Metering Infrastructure. Noel et.al. [17] has defined attack graph analytics using CVSS score. They tried to differentiate the network score based on the criteria like size, victimization and topology of the attack graph. This work explains the importance of various metrics during risk analysis. However they are limited to the assessment of the cyber-infrastructure and does not take the electrical infrastructure into account.

Similarly, [30, 32] concentrated mostly on the computational assets and did not consider power system dynamics in details in their analyses. Thus, many of the past contingency analysis techniques are limited to the assessment of the cyber-infrastructure and either consider natural incidents to be root causes of the power system failures or do not take the electrical infrastructure into account. As correctly pointed in [29], many ignored cyber side events and, in particular, contingencies due to deficient or compromised cyber components. Due to the current advancements, good research is being done in proposing and analyzing cyber physical models.

Vellaithurai et al. [22] in his paper, proposed a security-oriented stochastic risk management index, CPIndex, to measure the security of the cyber-physical network. They build stochastic Bayesian network models using topology of power networks and used belief propagation algorithms on these models to compute the indices.

Chapter 3: Problem Statement and Threat Model

3.1 Problem Statement

Attacker sophistication is increasing over time irrespective of the effort put in network security hardening. Attacks like coordinated cyber physical attacks and adaptive, high impact, targeted attacks on critical infrastructures are reported in recent times. These attacks show that there is a real need for prioritizing the assets criticality and risk analysis. In coordinated attacks there is a need for special metrics that can help in identifying the critical nodes that involve in attack propagation. As smart attacker uses stepping stones like the intermediate nodes to mask his location and can be able to reach any hosts that can not be reached prior by increasing the attack surface. In a centralized network like power grid, there is always a possibility of having a shortest path from source to destination. But, it always ignores the chance of causing co-ordinated attacks like if an intermediate host is compromised it has more effect on the network as it gives a chance for more targets to be compromised. Thus, in order to identify and prioritize the assets based on these attacks metrics will play a crucial role.

3.2 Threat Model

Threat modeling plays often an important role in risk assessment. During an attack, the physical components are also being effected when the cyber components are compromised. In an isolated attack, this breach could be limited to a single or individual physical components whereas in co-ordinated many cyber and physical components of power system might get compromised. Thus leading to confidentiality and data integrity threats. Even though the firewall settings are strong enough to prevent the security threats, there will be some communication medium from which the attackers can cause threats by leveraging vulnerabilities in the system. We are considering an external attacker who initially tries to enter the network by compromising a jump host in a DMZ. Then, the attacker will try to reach the control network or physical components by exploiting the vulnerabilities in the host forming a stepping stone attack. In our model, we depict such security threats using attack graphs. The attack graph are pruned to get attack trees where in the leaf nodes represent the controllers, for example the relay controllers, that control and monitor the physical components. In case of co-ordinated attacks, a smart attacker will choose intermediate nodes as stepping stones to reach multiple targets, whose combined cost might be a way less than shortest paths towards the target from the root. Thus, we are computing a ideal attack tree for a co-ordinated attack using ADMST algorithm which is explained later. Line outages in a power grid could be caused by, but not limited to,

- a compromised relay sending unauthorized open commands or a relay acting on compromised settings, or

- false command injection (including changing relay settings) by a compromised operator HMI or on a compromised communication link between HMI and relay, or
- a line open command sent by an operator who was misled by false sensor data, or
- protection systems kicking in after other potentially maliciously induced line outages, or
- a compromised breaker.

There are several systems that provide the vulnerability information like Industrial control systems cyber emergency response team (ICS-CERT).

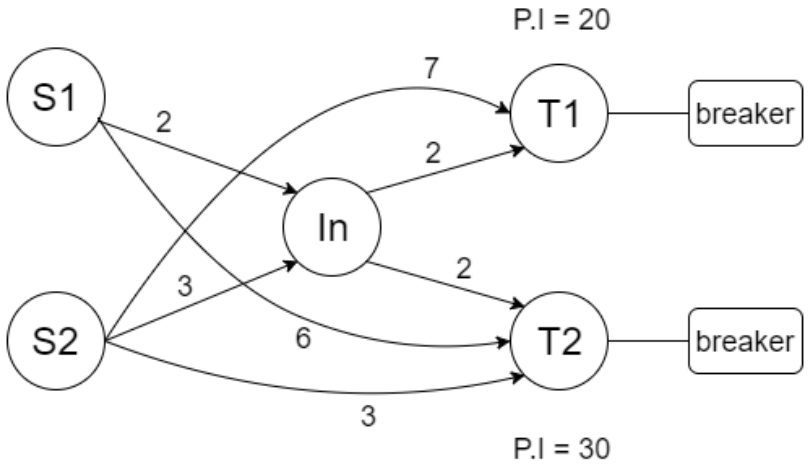

Figure 1: Sample Attack Graph

3.3 Cyber Physical Modeling

This work builds on the cyber-physical modeling and security assessment framework, CyPSA, developed in [7, 8, 29]. Here we provide some background on the framework to provide the necessary context for the security metrics proposed in this work.

In this section we will explain how to create a cyber physical model using CyPSA framework. CyPSA framework uses integrated cyber-physical models of the electric grid infrastructure for security assessment. At a high-level, a cyber-physical model captures the electrical network topology of the grid, the cyber-topology of the control network and their interconnections into an integrated model. Electrical network topology is at the node-breaker level rather than at the bus-branch level. This information in typically available from an Energy Management System (EMS). Cyber-topology includes both that of the control center and substations. Cyber-network topology information is not typically maintained as well as the electrical network topology but today with the advent of commercial tools like NP-View[1] that can infer a network topology using firewall rules it is possible to generate this information very easily.

The interconnections between cyber and electrical topologies are typically control devices likes relays that can open and close breakers or remotely controlled switches, and sensors. This information is typically harder to obtain in an easily ingestable format and in an automated way as there is no standard format and each utility stores and manages this information differently. In some cases this may not even be available in a digital format and is only accessible as CAD drawings.

[1] `http://www.network-perception.com`

More details on the components of a cyber-physical model of the kind used by CyPSA and their representation can be found in [27]. With devices like digital relays that can open or close power lines it is plausible for a cyber-attacker to impact the physical system through remote attacks especially when such devices are remotely accessible typically for remote configuration and maintenance. An integrated cyber-physical model allows one to study the risk of cyber-attack induced electrical outages and their impact on the system operation and energy delivery function.

3.3.1 Physical Modeling

The power system physical model explains the configuration and electrical characteristics of its components. The topology describes the way the components are connected. The state of the power system is said by the voltage and angle values of electric power at a given instance in time. This is used to estimate the future as well as the current conditions of the power system. For every 3-5 minutes, a state estimator gives measured data to power system model in order to estimate the current condition of the system. This state estimator model can then be used to predict the impact of outages based on the current conditions of the power system. This entire process of estimating the future from the current conditions of the system is called contingency analysis.

Figure 3 shows a full breaker-level topology diagram in a state estimator. Even in a simple model like Figure 3 multiple breakers may be involved in isolating a line from the rest of the system. For example, since breaker a1, a2, and b1 are open, Line

A is open.

In the full topology model, measurements from the SCADA system are used to map the devices. To work with full topology models, PowerWorld implements integrated topology processing (ITP) feature. ITP performs model consolidation only internally as needed in order to prevent numerical instability. To easily interpret full topology model data, most EMS systems have a capability to export to a text file format.

3.3.2 Cyber Modeling

The cyber system model represents the connectivity and interactions among cyber nodes and existing security mechanisms that restricts the communication between connected hosts. Routers and firewalls determine which hosts on a network are able to communicate, and the cyber system model must represent this logical level. Building and managing cyber network models is a challenging process for an organization. Automated tools can help; the CPMA framework makes use of Network Perceptions NP-View software [4], which builds a logical network model by parsing firewall rule-sets. The cyber topology shown captures the connections to the substation RTUs allowed by the firewall rules, but it does not capture details in the protection schemes at the substation level. There is currently no universal format to exchange cyber topologies, yet it is necessary for the future of cyber-physical modeling that we can easily store and accept information in a well-defined, easy to handle format. The CPTL language [27] being developed at the University of Illinois is our candi-

date for developing models for this framework. CPTL explicitly captures the cyber model information and its connections with the power model. These cyber-physical interconnections are critical to the analysis.

3.3.3 Cyber Physical Interconnection

The physical entities will be tied to the cyber elements. This helps in corelating which is controlling what and decides the impact of compromising a cyber element with respect to physical. Thus on creation of cyber physical model through CyPSA

Algorithm 1 Zabbix and Power World interactions [8, 29].

Program 2 Example of sending command to open line

```
objectID = "BRANCH 'Capital City$BRK$4647'";
FieldID  = "LineStatus";
Value    = "Open";
SendSetDataMessage(tsmSetData, connectedList
     [c]->socket(), ObjectID, FieldID, Value);
```

Program 3 Example of getting performance index

```
objIDs.add("PWCaseInformation");
fldIDs.add("OverloadRank");
SendGetData(tsmGetClientState, true,
     connectedList[c]->socket(), objIDs,
     fldIDs, 1 );
```

framework we will do the risk analysis by measuring the physical impact through

dynamic simulator COSMIC and rank the contingencies. A brief flow chart of the procedure can be found below :

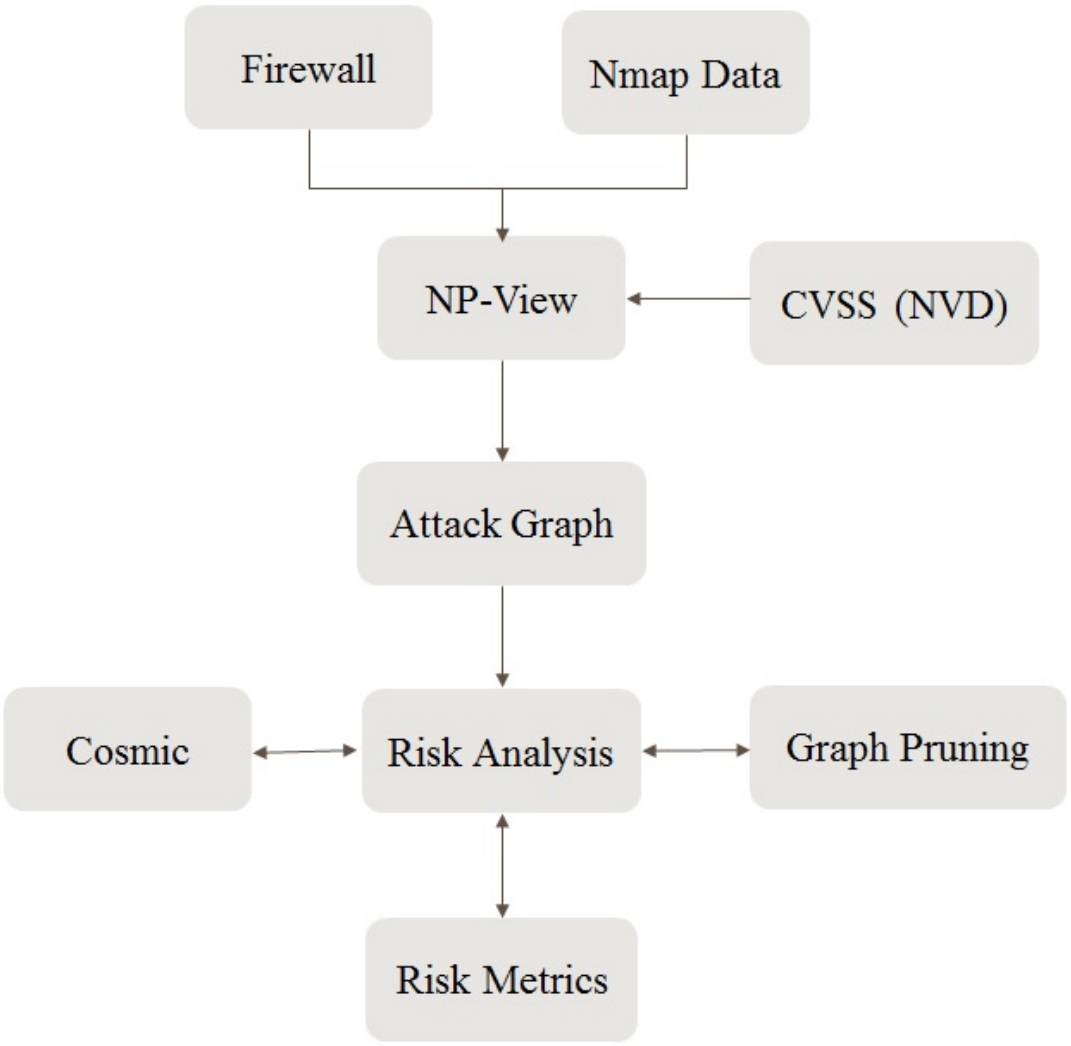

Figure 2: Flow chart explaining the framework and methodology.

Chapter 4: Risk Analysis

As discussed in Section 2.1, it necessary to have security metrics to make sure how secure a system is. But there is not much work done in the measuring a security metrics for power systems. Only a limited number of new papers on security metrics bring up a key issue in attempting to measure security. Generally there are 3 methods of assessing security metrics.

- Analytical approach
- Experimental approach
- Simulation

In my thesis work, I have used the simulation method to measure the security of the system. In this section, we propose security metrics for risk assessment of critical assets being compromised and their consequences. In a cyber physical model, each physical asset (for example, a relay that control a circuit breaker) will be monitored or controlled by a IP based cyber network. In such a model, the risk of losing an asset is equal to compromising the cyber element associated with it. Therefore, to assess the risk of assets being compromised, we need to consider two things Physical impact or effect of losing the target/s - The consequence of an attack in physical network perspective can be measured with performance index and load shed. Whenever a line goes out, the performance index is computed as the percentage of overloaded

$$S.I_i = I_c * \frac{1}{C_{min_i}}$$

Figure 1: Security Index for an attack

electricity over the other lines in the network and load shed is the loss of power due to line outage. Cost involved in causing the attack - It is the cost involved in exploiting a host from its neighbor host. It is calculated using the below formula ranging from 1.24425 to 9.9968 with lower bound signifying impossible or very hard to achieve and upper bound being easy. can be scaled from 1 to 10 using (11-Exp. Sub score) as the cost. Let Ic be the impact an attacker could achieve with a cost C on the system after a successful attack. Then, Figure 1 gives the security index of an attack to compromise a target [29].

The security metrics for the electric grid can be broadly categorized in to three:

- Single Target - Attacks that are concentrated on single asset or target
- Multiple Target - Coordinated attacks that try to compromise two or more targets
- Overall Security Metric - A total security metric that helps in limiting the overall security posture

In later sections we will see the metrics for respective criteria for different kinds of nodes(like source, intermediate and target) in attack graph.

4.1 Single Target

This metric include the metrics related to individual asset or target attacks. For all the attacks that include

In an n-node network, when each node can be assumed as destination, then it can have n-1 possible sources from where it can be attacked. In addition to that, there could be m different attacks that could be possible from any host u to host v in a network. If we consider all those possible attacks, then the attack graph will be huge to analyze. Let us consider a small example with 3 nodes in a network and each has 4 vulnerabilities that can be chosen for compromising.

From the above figure, we can see the complexity of the attack graph. If one host is compromised, then it can be used as a source to compromise other hosts in a network. Let us assume that we are interested to reach C from A. We have 6 ways to attack C from A based on the vulnerabilities that we have on targets or intermediate hosts that lead to targets. If we have a similar case for n nodes with k vulnerabilities in each host, the complexity of analyzing and identifying the critical path in the network is high. Thus, simplifying the attack graph is essential. Assuming the attacker has knowledge of vulnerability information and network topology, attacker uses All pairs shortest path to choose the minimum cost to reach host. Hence the previous attack graph can be simplified to the below assuming A as jump host. This is the case for reaching a single or isolated target.

In measuring the overall security of a network, a crucial issue is to correctly compose the measure of individual components. Incorrect compositions may lead to misleading results

$$S.I_i = P.I_i * \sum_{j=1}^{k} (\frac{1}{C_{min_{ij}}})$$

Figure 2: Security Index for a target from different sources

Table 4.1: Notations Used

Literal	Description
$P.I_i$	Physical impact of losing control over $asset_i$
$C_{min_{ji}}$	Minimum cost attack to compromise $asset_i$ starting at $source_j$
C_{ji}	Cost of attack to compromise $asset_i$ starting at $source_j$
$C_{DMST_{(s)}}$	Directed minimum spanning tree (DMST) based cyber cost to compromise set of assets s
S	Set of source nodes
T	Set of target nodes
In	Set of Intermediate nodes
$j \rightarrow i$	denotes an attack path from j to i
$j \rightarrow_{min} i$	denotes the minimum cost attack path from j to i

In case of attacking multiple assets, All pairs shortest path will not be the best possible way to compromise multiple hosts. For example if the attacker wants to reach 2 targets C and D, it takes the minimum cost path from A to C and the minimum cost path from A to D and the resulting attack graph would be as below

4.1.1 Metrics for Target Nodes/Assets

This set of metrics focuses on the *target nodes* in the attack graph. Target Nodes are those nodes which when compromised can be used to directly manipulate the physical infrastructure. Protection relays are a good example as they manipulate line connectivity in the grid and could have a significant impact when compromised.

Metric 1: Min-Cost Target Node Security Index

This metric considers the minimum cost attack path to compromise a target node and the impact of the compromise. It is the same as the *Security Index* metric proposed in [29]. Min-cost security index for a target node i is defined as follows:

$$M.T.S.I_t(i) = P.I_i * \frac{1}{\min_{j \in S}(C_{min_{ji}})} \tag{4.1}$$

Here, $P.I_i$ is the physical impact of compromising the target node i, and $C_{min_{ji}}$ is the minimum cost attack path between a source node j and the target node i. Thus, this metric picks up the minimum cost attack path to the target node i from among minimum attack cost paths corresponding to each source node in the graph. For example, in Figure 1 the Min-Cost Target Node Security Index for target node $T1$ picks from among the minimum cost attack paths to $T1$ from sources $S1$ and $S2$. It is the two hop path through In with a hop cost of 2 each and thus the index is given by,

$$M.T.S.I_t(T1) = 20 * \left(\frac{1}{2+2}\right) \tag{4.2}$$

Metric 2: Target Node Security Index

While min-cost target node security index helps identify critical nodes that have significant impact and low access costs for an attacker it doesn't provide the full picture. For example, consider two target nodes $T1, T2$ with the same physical impact score. Let us say that target node $T1$ has a lower minimum attack cost path

than target node $T2$ but that $T2$ has multiple attacks paths. Presence of multiple attack paths increases the chances that an adversary is able to find one of them. This security metric tries to capture this increased chance for an adversary to find one of the multiple attack paths by considering all attack paths to a target node and is given by

$$T.N.S.I_t(i) = P.I_i * \sum_{j \in S} \frac{1}{C_{min_{ji}}} \tag{4.3}$$

Here $P.I_i$, and $C_{min_{ji}}$ are defined similar to those in equation 4.1. Note that $\sum_{j \in S} \frac{1}{C_{min_{ji}}}$ is also referred to as *reachability index* of a node later in the paper. The T.S.I for target $T1$ from Figure 1 which can be reached from the sources $S1$ and $S2$ is given by,

$$T.N.S.I_t(T1) = 20 * \left(\frac{1}{2+2} + \frac{1}{3+2} \right) \tag{4.4}$$

4.1.2 Stepping Stone Node Metrics

This set of metrics focuses on the intermediate nodes in the attack graph. Intermediate nodes acts as stepping stones to compromise the target nodes.

Metric 3: Intermediate Node Min-Cost Betweenness Security Index

This metric inspired by the *betweenness centrality* [] captures the importance of intermediate nodes as enablers of minimum cost attack paths between source and target nodes. Min-cost betweenness security index for an intermediate node k is defined as follows:

$$M.B.S.I_{in}(k) = \sum_{\{i,j|i\in T, j\in S, k\in j\rightarrow_{min} i\}} P.I_i * \frac{1}{C_{min_{ji}}} \tag{4.5}$$

Here $j \rightarrow_{min} i$ denotes the minimum cost attack path from j to i. For example, betweenness security index for the intermediate node In in Figure 1 is calculated based on its presence on the minimum cost attack paths between source nodes $S1, S2$ and target nodes $T1, T2$. As shown in the figure, using the intermediate node In, an attacker has the shortest path from source $S1$ and $S2$ to compromise the target $T1$. Similarly, to compromise the target $T2$, an attacker has the shortest path from source $S1$ using the intermediate node In. But, the shortest path to compromise the target $T2$ from source $S2$ doesn't include the intermediate node. Hence, min-cost betweenness security index for In is given by,

$$M.B.S.I_{in}(In) = 20 * \left(\frac{1}{2+2} + \frac{1}{3+2}\right) + 30 * \left(\frac{1}{2+2}\right) \tag{4.6}$$

Metric 4: Intermediate Node Betweenness Security Index

This metric, similar to T.N.S.I in equation 4.3, captures the importance of intermediate nodes across all attack paths and is given by

$$B.S.I_{in}(In) = \sum_{\{i,j|i\in T, j\in S, k\in j\rightarrow i\}} P.I_i * \frac{1}{C_{ji}} \tag{4.7}$$

The total betweenness security index for intermediate node In now considers all the attack paths possible from all sources $S1$ and $S2$ to all targets assets $T1$ and $T2$ that go through In. It is given by,

$$B.S.I_{in}(In) = 20 * \left(\frac{1}{2+2} + \frac{1}{3+2}\right) + 30 * \left(\frac{1}{2+2} + \frac{1}{3+2}\right) \tag{4.8}$$

4.1.3 Source Node Metrics

Metric 5: Min-Cost Source Node Security Index

This metric captures the importance of sources nodes by considering the target nodes in the system for which they act as the source of a minimum cost attack and is given by

$$M.S.S.I_s(j) = \sum_{\{i,j|i\in T, j\in S, j\in \min_S(j\rightarrow_{min} i)\}} P.I_i * \frac{1}{\min_{j\in S}(C_{min_{ji}})} \tag{4.9}$$

For example, in Figure 1, source $S1$ can launch a minimum cost attack path to asset $T1$ but not for asset $T2$. Because, asset $T2$ has a minimum cost attack path from source $S2$. Hence the security index of source $S1$ is given by,

$$M.S.S.I_s(S1) = 20 * \left(\frac{1}{2+3}\right) \tag{4.10}$$

Metric 6: Source Node Security Index

This metric captures the importance of source nodes considering all minimum cost attack paths originating from this node and is given by

$$S.S.I_s(j) = \sum_{i\in T} P.I_i * \frac{1}{C_{min_{ji}}} \tag{4.11}$$

To see the difference between M.S.S.I and S.S.I, for the example in Figure 1, the source security index of source $S1$ is given by all the minimum cost attacks that it can launch in order to compromise the assets $T1$ and $T2$. That is,

$$S.S.I_s(S1) = 20 * \left(\frac{1}{2+3}\right) + 30 * \left(\frac{1}{2+2}\right) \tag{4.12}$$

Note that in the case of M.S.S.I we only consider an attack path from a source j to target i if that is the minimum cost attack path to i among all attack paths to it. In contrast, in S.S.I we consider the minimum attack paths originating from a given source to all targets in the graph.

4.2 Multiple Targets

Smart Attacker. Network Topology. Expert in power and cyber data attacks. For example: Consider an attack graph as shown in fig. Assume the attacker wants to co-ordinate his attack in such a way that he can compromise Asset C and Asset D with an attack originating from jump-host A.

This metric considers the importance of identifying the vulnerable sources that can be attacked by using jump host to launch minimum cost attack in the network and is given by

$$C.S.I_{(s)} = P.I_{(s)} * \frac{1}{C_{ADMST_{(s)}}} \tag{4.13}$$

The C_{ADMST} is the minimum cyber cost required to reach all hosts in the target set. We took the modified version of directed minimum spanning tree(ADMST) algorithm to compute the cyber cost. The ADMST used instead of minimum cost attacks as there could be intermediate nodes that could ease the attack paths cost by reaching more assets. Thus ADMST will always return cost that could be lesser or equal

to the minimum individual attacks to compromise the target. The proof of this is beyond the scope of this paper. We would recommend to refer these papers [2, 28].

In the above figure, let us assume there is a smart attacker at node D who is aware of network topology and vulnerabilities. If he wants to compromise targets C and E, he chooses to attack them using the intermediate node instead of attacking the targets with their individual minimum cost path. Because individual attacks paths (D-¿E,D-¿B-¿C) gives a total attack cost of 9 (3 + 6) but if the attacker uses the intermediate node B to compromise both E and C, the cost becomes 8. It is given by:

$$C.S.I_{(C,E)} = 50 * \left(\frac{1}{3+3+2}\right) \tag{4.14}$$

4.3 Overall Security Metric

Metric 7: Total Security Index

This metric aims to capture the overall security posture of the network. This can be helpful for tracking the progress of security efforts and also helping with prioritizing security controls. Total security index captures the overall risk of the system to cyber-induced outages and is defined as follows

$$T.S.I = \sum_{i \in T} M.T.S.I_t(i) = \sum_{j \in S} M.S.S.I_s(j) \tag{4.15}$$

An overall security metric that is expressed in terms of T.N.S.I or S.S.I may also be useful. Similarly, variations of B.S.I that take coordinated attacks into account can also be defined. Further we haven't explored metrics for coordinated attacks

in this work. These and other variations will be considered in future work. We now proceed to illustrating the proposed metrics using cyber-physical models of test systems.

Chapter 5: Evaluation

5.1 Testbed

For the physical models like 9-bus, 39-bus and RTS-96 bus cyber physical model is created manually. Thus after the setup risk of cyber induced contingency will be calculated. This entire evaluation can be categorized in to three phases :

5.1.1 Attack Graph Generation

- Input : firewalls, services
- Tools : nmap, NP-View
- Computation : NP-View builds graph with parsed vertices and edges from connectivity and vulnerability data provided through firewalls and services.

  Add hosts as vertices, keeping track of their services and known vulnerabilities. If nmap scans reported a running service at a device/vertex Associate service id and corresponding vulnerability to that vertex Else Associate to that vertex a high reachability cost of 1000 Add edges between hosts based on firewall analysis connectivity Add intranet edges (hosts in the same network) Compute & generate attack graph

- Get list of all shortest paths in graph from each attacker vertex (in attacker file) to limited target vertices (if a file of limited targets was provided)
- Get path sequence and path weight for each path (with option to keep only the easiest)

Save attack graph as XML formatted file

The administrator is provided with the opportunity of selecting assets that might have compromised and assets that are patched in the network to check how the actions might effect the network posture by running the application again. If either file is changed, the attack graph is updated accordingly and a new file is generated. If a node or asset is compromised, the IP addresses are read from the file and the new attack graph is generated accordingly. Generally, there should be at least one node compromised in the file in order to have a cyber attack graph. If no nodes are compromised, then the cyber attack graph will be empty. The graph is usually initially generated by compromising the specified entry/internet node called jump host. If a node or asset is patched, the IP addresses are read from the file and the associated assets are removed from the attack graph, reducing the size.

Thus generating an attack graph.

- Output : Attack Graph

5.1.2 Power Simulation

5.1.2.1 PowerWorld Contingency Analysis - Performance Index

- Input : Physical contingency (single or multiple)
- Tools : PowerWorld Trainer
- Computation : For each physical contingency set of targets the breakers that need to be open will be given such that base case file of the power system will be modified and simulation of the case is ran to see the performance index of the case.
- Output : Performance Index

5.1.2.2 Cosmic Contingency Analysis - Load shed

- Input : Physical contingency event(single or multiple)
- Tools : PowerWorld Trainer
- Computation : This is an offline process where for each contingency events will be generated with approximate time of occurrence and the consequence of the event could be load shed or islanding.
- Output : Performance Index

5.1.2.3 Outage cases that did not converge

If case fails to converge in any of the tools a high relative value will be set for performance index or sum of load lost will be considered as load shed.

5.1.3 Ranking Contingencies

- Input : Physical Impact and Cyber Cost associated
- Tools : python
- Computation : Using the metrics the assets will be ranked using metrics as dicussed in 4.1 and 4.2
- Output : Ranked assets

5.2 Results

5.2.1 WSCC 9-Bus

It is known as Western System Coordinating Council (WSCC) 9-bus testing system. There are three generation sets and three loads located on a loop structure. Based on the cyber attack graph generated we were able to identify 8 target nodes. Among those we have presented the indices for 6 target nodes[1] in Table 5.3. As seen, contingency of line (4-6) and line(7-8) lead to load shed the same amount 22.5MW but

[1]All indices will be presented in the full version of the paper.

they have different reachability numbers with the node controlling line (7-8) being slightly more reachable leading to a security index.

In addition the table also shows that node (10.37.1.250) that controls bus 7 is a crucial intermediate node as it can be leveraged to attack relays controlling three lines and can shutdown the whole bus leading to a large load shed as is reflected by both M.B.S.I. (86.2) and B.S.I. (98.63) for that node. Similarly we have identified two main attack source nodes, namely, FTP server and DMZ Jumphost. Among those DMZ Jumphost as expected has a higher security index as it is typically used to connect to many other nodes.

5.2.2 39-Bus

It is known as New-England test system with 10 generations, 19 loads, and 46 lines. Using a setup similar to the one used for 9-bus test system, we have identified 19 target nodes in the attack graph. Table 5.6 shows indices for 6 of them. It is interesting to note that when considering only the physical impact, attack leading to outage of line (10-32) has higher priority than the one for line (6-31), but when all attack paths are taken into account line (6-31) that causes a lower amount of load shed comes out at the top. For cases where the power simulation do not converge or creates island, generator or load isolation were given big numbers to showcase their importance on physical impact side. In this case the relative ordering of intermediate and source nodes happens to line up along the lines of their physical impact.

5.2.3 RTS-96 Bus

There are 73 buses and 120 branches in RTS-96. It consists of three identical, interconnected 24-bus islands. Bus numbers with 100 level are located in the first island, 200 level is second island, and 300 level is third island [10]. Overall, we simulate 8 line fault combinations and 4 bus fault combinations. The results are shown as Table 5.7, 5.8 and 5.9.

By comparing line combination 6 and 3, the later one has less fault locations but has more impact.

When tripping a branch, it will cause overloading on the other branches, which can trigger overcurrent relay (line combination 5).

The most significant fault combination is bus combination 4. When there is a fault occurs on bus 107, the voltage drop on bus 203 will trip under voltage load shedding relay, and cause an amount of 45MW load shedding. The total amount of load shedding for bus fault combination 4 is 321MW.

5.3 Limitation

The illustration of metrics shows that for a given configuration the proposed metrics are able to identify critical cyber assets under different conditions and consequently can help prioritize limited cyber security resources. However, it is important to keep in mind that the synthetic cyber-physical models are used for illustration purposes and that the ranking of assets could be very different with a different model. Further, the absolute values for the security indexes themselves do not have any inherent

Table 5.1: Prioritization of Contingencies by Security Metrics for 9-Bus

IP Address	Contingency	Type	Load Shed (MW)	Reach-ability Index	M.T.S.I.	Total Reach-ability Index	T.N.S.I.
10.37.1.101	Line (2-7)	Target	163(island, generator)	0.48828	79.5896	1.2501	203.7663
10.37.1.103	Line (5-7)	Target	31.5	0.4167	13.1261	0.4167	13.1261
10.37.1.102	Line (7-8)	Target	22.5	0.29411	6.6175	0.48828	10.9863
10.34.1.103	Line (4-6)	Target	22.5	0.2616	5.886	0.37037	8.333
10.36.1.102	Line (6-9)	Target	0	0.33298	0	0.33298	0
10.39.1.101	Line (8-9)	Target	0	0.4167	0	0.4167	0

Table 5.2: Prioritization of Contingencies by Security Metrics for 9-Bus

IP Address	Contingency	Type	Load Shed (MW)	Reach-ability Index	M.B.S.I.	Total Reach-ability Index	T.B.S.I.
10.37.1.250	Line (2-7),(5-7),(7-8)	Intermediate	217	n/a	86.2071	n/a	98.633
10.36.1.250	Line (6-9),(4-6)	Intermediate	22.5	n/a	0	n/a	5.698

Table 5.3: Prioritization of Contingencies by Security Metrics for 9-Bus

IP Address	Contingency	Type	Load Shed (MW)	Reach-ability Index	M.S.S.I.	Total Reach-ability Index	S.S.I.
10.40.1.22	Line (2-7),(4-6),(5-7),(6-9),(7-9),(8-9)	Source	239.5	n/a	105.2192	n/a	188.4623
72.36.82.194	Line (2-7)	Source	163	n/a	0	n/a	53.65

Table 5.4: Targets : Prioritization of Contingencies by Security Metrics for 39-Bus

IP Address	Contingency	Type	Load Shed (MW)	Reachability Index	M.T.S.I.	Total Reachability Index	T.N.S.I.
10.52.1.102	Line (21-22)	Target	1000*(does not converge)	0.4167	416.7	0.4167	416.7
10.61.1.102	Line (6-31)	Target	200*(2 islands, generator, load)	0.48828	97.656	1.2501	250.02
10.40.1.103	Line (10-32)	Target	316.1(2 islands, generator)	0.37037	117.063	0.37037	117.063
10.44.1.101	Line (13-14)	Target	82.12 (cascade)	0.708616	58.1915	0.8265	67.8722
10.45.1.103	Line (15-16)	Target	82.12 (cascade)	0.48828	40.0976	0.8265	67.8722
10.64.1.101	Line (20-34)	Target	0(2 islands, generator)	0.4167	0	0.4167	0

Table 5.5: Intermediate Nodes: Prioritization of Contingencies by Security Metrics for 39-Bus

IP Address	Contingency	Type	Load Shed (MW)	Reach-ability Index	M.B.S.I.	Total Reach-ability Index	B.S.I.
10.46.1.250	Line (16-21),(16-24),(15-16)	Intermediate	82.12	n/a	40.0976	n/a	40.0976
10.70.1.22	Line (21-22),(13-14)	Intermediate	1000*	n/a	58.1915	n/a	386.2

Table 5.6: Sources: Prioritization of Contingencies by Security Metrics for 39-Bus

IP Address	Contingency	Type	Load Shed (MW)	Reach-ability Index	M.S.S.I.	Total Reach-ability Index	S.S.I.
10.70.1.22	Line (21-22),(6-31),(10-32),(13-14),(15-16),(20-34)	Source	1000*	n/a	1128.42	n/a	1128.42
72.36.82.194	Line (21-22)	Source	1000*	n/a	416.7	n/a	580.34

Table 5.7: Line Faults(Target): Prioritization of Contingencies by Security Metrics for RTS-96

Description	Contingency	Load shed	Reach-ability Index	T.N.S.I
Line fault 1	line 103-124	47.25MW load shedding (LS)	0.8265	39.0521
Line fault 2	line 303-324	47.25MW LS	0.7624	36.0234
Line fault 3	line 207-208	45MW LS 1 generator and 1 load partitioned	0.8265	37.1925
Line fault 4	line 307-308	45MW LS 1 generator and 1 load partitioned	0.8265	37.1925

Table 5.8: Target Node Comb: Prioritization of Contingencies by Security Metrics for RTS-96

Description	Contingency	Load shed	Reach-ability Index	T.S.I
Line comb 1	line 119-120, 120-123, 118-121	0	1.5688	0
Line comb 2	line 103-124, 202-204, 302-304, 110-111, 209-211, 309-311, 101-103, 121-122, 220-223, 101-105, 123-217, 221-222	47.25MW LS; overcurrent (OC) relay trip line 106-110	6.3277	298.9838
Line comb 3	line 108-110, 207-208, 307-308, 115-121, 215-221, 315-321	90MW LS; 2 generators and 2 loads partitioned	4.2357	381.213
Line comb 4	line 115-121, 215-216, 315-316	0	2.6333	0
Line comb 5	line 109-111, 208-209, 308-309	OC trip line 106-110	2.6333	0
Line comb 6	line 112-123, 211-214, 311-314, 114-116, 118-121, 213-223, 218-221, 313-323, 318-321	47.25MW LS	4.86	229.635
Line comb 7	line 115-116, 214-216, 314-316, 103-124, 202-204, 302-304, 112-123, 211-214, 311-314	47.25MW LS; OC trip line 106-110; 2 generators and 2 loads partitioned	4.86	229.635
Line comb 8	line 209-211, 220-223, 221-222	0	1.2501	0

Table 5.9: Bus Comb: Prioritization of Contingencies by Security Metrics for RTS-96

Description	Contingency	Load shed	Reach-ability Index	T.S.I
Bus comb 1	bus 108, 111	1 load partitioned	7.866	0
Bus comb 2	bus 124, 224, 324	94.5MW LS; OC trip line 106-110; 3 loads partitioned	7.866	743.337
Bus comb 3	bus 318, 325	1 generator and 1 load partitioned; system into 2 islands	5.2333	0
Bus comb 4	bus 107, 123, 215, 318	321MW LS; OC trip line 206-210; 4 generators and 3 loads partitioned; system into 2 islands	5.6867	1825.527

meaning but can only provide relative ordering among assets. Further research is also needed to understand how to interpret the magnitude of differences between security indexes of different assets.

Chapter 6: Conclusion and Future Work

6.1 Conclusion

Good Security metrics can be a very useful tool to prioritize security efforts and to track progress. However, good security metrics are hard to design and validate given the uncertainty introduced by unknown and continuously evolving quantities such as unknown vulnerabilities, attacker capabilities etc. In this work we take a first step towards defining multiple cyber-physical security metrics for electrical grid infrastructures and illustrating their value in relatively ranking critical assets. However, further research is needed to validate these metrics in the real world and understanding how to interpret the differences in their absolute values.

6.2 Future Work

A lot of scope in attack graph pruning for cyber physical systems. Application of multi graph. Local community detection equivalent methods in finding strongly connected attacks and considering them as potential cascading outage scenario and simulation of it. Comparing the metrics to different scenarios.

Bibliography

[1] Common vulnerability scoring system. [online]. available: https://nvd.nist.gov/cvss.cfm.

[2] Directed minimum spanning trees. online link: https://www.cs.princeton.edu/courses/archive/spring13/cos528/directed-mst-1.pdf.

[3] National vulnerability database. [online]. available: http:// nvd.nist.gov/.

[4] Network perception, inc. (2015) np-view: Network security audit for critical infrastructures. [online]. available: http://www.network-perception.com.

[5] Binbin Chen, Zbigniew Kalbarczyk, David M Nicol, William H Sanders, Rui Tan, William G Temple, Nils Ole Tippenhauer, An Hoa Vu, and David KY Yau. Go with the flow: Toward workflow-oriented security assessment. In *Proceedings of the 2013 workshop on New security paradigms workshop*, pages 65–76. ACM, 2013.

[6] Yi Cheng, Julia Deng, Jason Li, Scott A DeLoach, Anoop Singhal, and Xinming Ou. Metrics of security. In *Cyber Defense and Situational Awareness*, pages 263–295. Springer, 2014.

[7] Kate Davis, Robin Berthier, Saman Zonouz, Gabriel A. Weaver, Rakesh B. Bobba, Edmond J. Rogers, Peter W. Sauer, and Nicol David M. CCyber-Physical Security Assessment (CyPSA) for Electric Power Systems, 2016.

[8] Katherine R Davis, Charles M Davis, Saman A Zonouz, Rakesh B Bobba, Robin Berthier, Luis Garcia, and Peter W Sauer. A cyber-physical modeling and assessment framework for power grid infrastructures. *Smart Grid, IEEE Transactions on*, 6(5):2464–2475, 2015.

[9] Timothy Grance, Joan Hash, Marc Stevens, Kristofor O'Neal, and Nadya Bartol. Sp 800-35. guide to information technology security services. 2003.

[10] Cliff Grigg, Peter Wong, Paul Albrecht, Ron Allan, Murty Bhavaraju, Roy Billinton, Quan Chen, Clement Fong, Suheil Haddad, Sastry Kuruganty, et al.

The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee. *IEEE Transactions on power systems*, 14(3):1010–1020, 1999.

[11] Elizabeth LeMay, Michael D Ford, Ken Keefe, William H Sanders, and Carol Muehrcke. Model-based security metrics using adversary view security evaluation (advise). In *Quantitative Evaluation of Systems (QEST), 2011 Eighth International Conference on*, pages 191–200. IEEE, 2011.

[12] Elizabeth LeMay, Willard Unkenholz, Donald Parks, Carol Muehrcke, Ken Keefe, and William H Sanders. Adversary-driven state-based system security evaluation. In *Proceedings of the 6th International Workshop on Security Measurements and Metrics*, page 5. ACM, 2010.

[13] Richard Lippmann, Kyle Ingols, Chris Scott, Keith Piwowarski, Kendra Kratkiewicz, Mike Artz, and Robert Cunningham. Validating and restoring defense in depth using attack graphs. In *MILCOM 2006-2006 IEEE Military Communications conference*, pages 1–10. IEEE, 2006.

[14] T. McAvinew and R. Mulley. *Control System Documentation: Applying Symbols and Identification*. ISA-The Instrumentation, Systems, and Automation Society, 2004.

[15] Miles A McQueen, Trevor A McQueen, Wayne F Boyer, and May R Chaffin. Empirical estimates and observations of 0day vulnerabilities. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–12. IEEE, 2009.

[16] David M Nicol and Vikas Mallapura. Modeling and analysis of stepping stone attacks. In *Proceedings of the 2014 Winter Simulation Conference*, pages 3036–3047. IEEE Press, 2014.

[17] Steven Noel and Sushil Jajodia. Metrics suite for network attack graph analytics. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, pages 5–8. ACM, 2014.

[18] Joseph Pamula, Sushil Jajodia, Paul Ammann, and Vipin Swarup. A weakest-adversary security metric for network configuration security analysis. In *Proceedings of the 2nd ACM workshop on Quality of protection*, pages 31–38. ACM, 2006.

[19] Jiajia Song, Eduardo Cotilla-Sanchez, Goodarz Ghanavati, and Paul DH Hines. Dynamic modeling of cascading failure in power systems. *IEEE Transactions on Power Systems*, 31(3):2085–2095, 2016.

[20] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2012.

[21] Keith Stouffer. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16.

[22] Ceeman Vellaithurai, Anurag Srivastava, Saman Zonouz, and Robin Berthier. Cpindex: cyber-physical vulnerability assessment for power-grid infrastructures. *IEEE Transactions on Smart Grid*, 6(2):566–575, 2015.

[23] Vilhelm Verendel. Quantified security is a weak hypothesis: A critical survey of results and assumptions. pages 37–50, 2009.

[24] Andrija Volkanovski, Marko Čepin, and Borut Mavko. Application of the fault tree analysis for assessment of power system reliability. *Reliability Engineering & System Safety*, 94(6):1116–1127, 2009.

[25] Lingyu Wang, Tania Islam, Tao Long, Anoop Singhal, and Sushil Jajodia. An attack graph-based probabilistic security metric. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 283–296. Springer, 2008.

[26] Lingyu Wang, Sushil Jajodia, Anoop Singhal, Pengsu Cheng, and Steven Noel. k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, 11(1):30–44, 2014.

[27] Gabriel A. Weaver, Kate Davis, Matt Davis, Edmond J. Rogers, Rakesh B. Bobba, Saman Zonouz, Robin Berthier, Peter W. Sauer, and Nicol David M. Cyber-Physical Models for Power Grid Security Analysis: 8-Substation Case. In *International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016.

[28] Liang Zhao, Hiroshi Nagamochi, and Toshihide Ibaraki. A linear time 5/3-approximation for the minimum strongly-connected spanning subgraph problem. *Inf. Process. Lett.*, 86(2):63–70, April 2003.

[29] Saman Zonouz, Charles M Davis, Katherine R Davis, Robin Berthier, Rakesh B Bobba, and William H Sanders. SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures. *IEEE Transactions on Smart Grid*, 5(1):3–13, 2014.

[30] Saman Zonouz, Amir Houmansadr, and Parisa Haghani. Elimet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)*, pages 1–12. IEEE, 2012.

[31] Saman Zonouz, Katherine M Rogers, Robin Berthier, Rakesh B Bobba, William H Sanders, and Thomas J Overbye. SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures. *IEEE Transactions on Smart Grid*, 3(4):1790–1799, 2012.

[32] Saman A Zonouz, Himanshu Khurana, William H Sanders, and Timothy M Yardley. Rre: A game-theoretic intrusion response and recovery engine. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):395–406, 2014.

APPENDICES

Appendix A: Power System Protection Devices

A.1 Protection System

Different Types of Protection Schemes are :

A.1.1 Overcurrent relay

One kind of protection relay is the overcurrent relay. It operates when the load current is higher than the pickup value. An instantaneous over current (IOC) or a Definite Time Overcurrent (DTOC)is denoted by the ANSI device number 50. In a general setup, the overcurrent relay will be associated to a current transformer and calibrated such that it operates at or above a specified current level. When the relay is allowed to function, a (open) circuit breaker is tripped with the operation of one or more contacts. The Definite Time Overcurrent Relay (DTOC) is extensively used in United Kingdom but has a disadvantage of being slow for finding faults closer to the source. As a result, IDMT relay has been developed. For (TOC) or (IDMT) protection, the ANSI device number is 51. the IDMT relay curves are specified by IEC standard 60255-151.

A.1.2 Distance relay

Distance relays are different from other forms of protection in a way that the performance is governed by the ratio of current or voltage magnitude and not by their magnitudes. Distance relays are actually two coil relay where in the two coils are energized by voltage and current respectively. A positive or pick up torque is produced by the current element and a negative or reset torque is produced by the voltage element. The relay operates when the ration of voltage to current falls below a specified value. Whenever a fault on a transmission line is detected, at that point there is an increase in fault current and decrease in voltage. The location of CTs and PTs are used to measure the ratio of voltage to current. The voltage at the PT location depends on the distance between the PT and the fault.If the measured voltage is less, the fault is nearer and vice-versa. Hence the protection called Distance relay.

A.1.3 Current differential protection scheme

The differential protection scheme detects faults identified within its protected area and therefore it is 100% selective. The location of current transformers decide the boundary of the protected area. It allows tripping without additional delay and thus time grading with other systems is not necessary. Hence it is well-known for its fastness and used to protect lines, generators, motors, transformers and other electric power plants with multiple terminals.

In commonly available standard modules, overcurrent protection and differential protection (non-adjustable) schemes are combined with GFCI (ground fault circuit

interrupter) circuit breakers.

A.1.4 Directional relay

In directional relay, the direction of the fault is determined by an aditional polarizing source of voltage or current. Directional elements are responded to the phase shift between a polarizing quantity and an operate quantity. The relay's upstream or downstream location can be used to locate the fault by allowing the protective devices to operate in or outside the protection zone.

We have used all types of relays on physical network for monitoring based on standard usage for our test models.

APPENDICES

Appendix A: Power System Networks

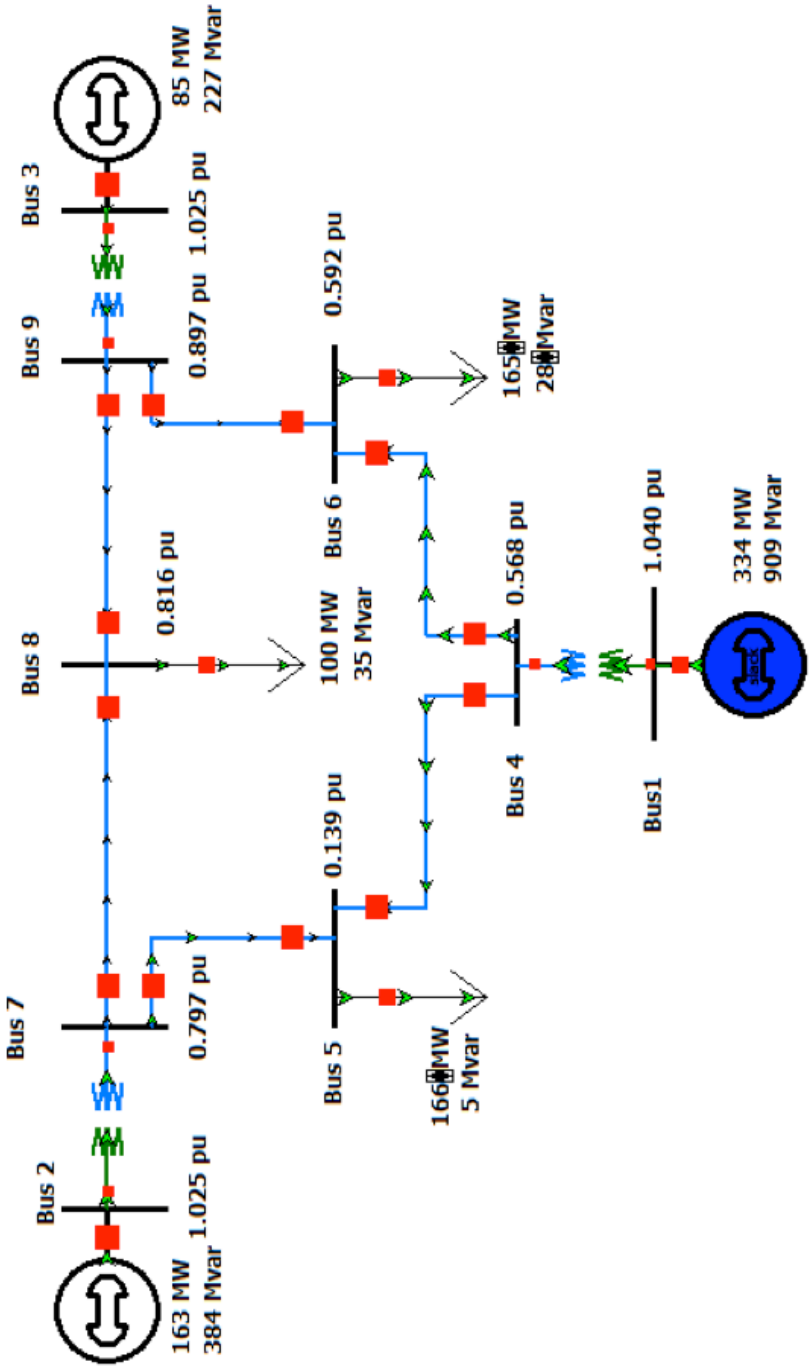

Figure 1: 9 bus One-line diagram [8].

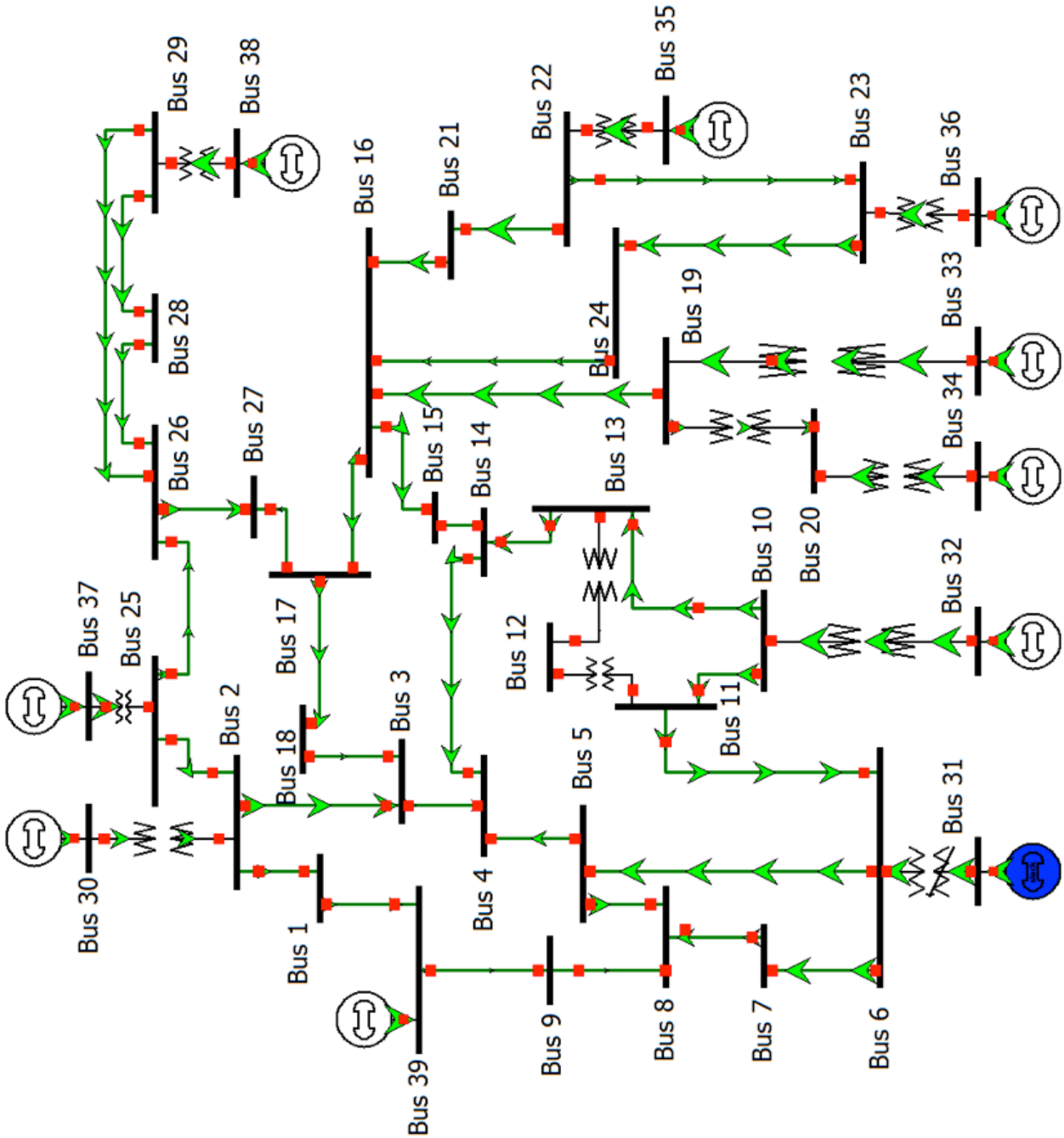

Figure 2: 39 bus One-line diagram [8].

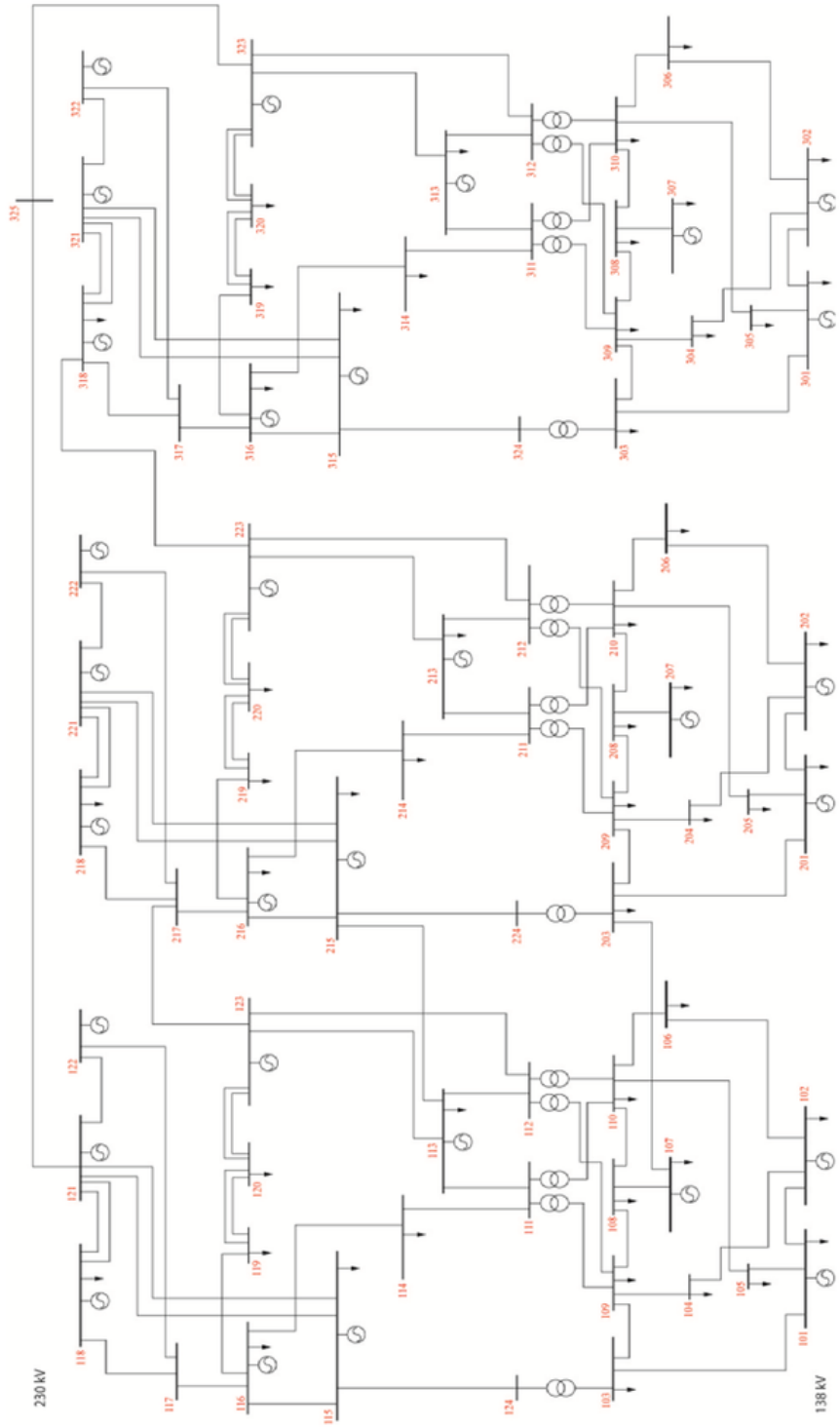

Figure 3: RTS 96 bus One-line diagram [8].