Cyber-Physical Resilience Enhancement Strategies for Modern Power Grids

by

Nancy Mohamed

A thesis

presented to the University of Waterloo

in fulfillment of the

thesis requirement for the degree of

Doctor of Philosophy

in

Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2021

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner	Medhat Morcos Professor
Supervisor(s)	Magdy Salama Professor
Internal Member	Sheshakamal Jayaram Professor
Internal-external Member	Jatin Nathwani Professor
Other Member(s)	Mostafa Shaaban Associate Professor

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Continuous research efforts are dedicated to developing methods to improve existing security tools to better fit the nature of smart grids. However, there is no perfect security scheme for every potential attack threat. Instead, the new concept of resilience has emerged as a strategic objective in power system planning. Grid resilience is related to the power system's ability to continue operating and delivering power even in the event of low probability, high-consequence disruptions such as cyber-physical attacks. Grid resilience objectives focus on managing and, ideally, minimizing potential consequences resulting from these disruptions. This thesis focuses on enhancing the cyber resilience of the grid through boosting the system preparedness and recovery potentials through three resilience-enhancing strategies.

For boosting the preparedness potential, this thesis focuses on identifying and assessing the system cyber vulnerabilities (threats) so that protective measures can be planned for and proactive plans can be prepared, as recommended by the American National Infrastructure Protection Plans (NIPPS). With this intention, the first strategy is to develop a cyber-based risk assessment framework. The substation vulnerability has been studied under different attack scenarios that are classified based on different attacker models. The outcomes of this analysis are both the risk indices and the asset ranking according to their cyber resilience to help the operator set up informed preventive and corrective plans. The IEEE 30-bus test system has been used to test the algorithms of risk quantification.

The second strategy aims to enhance the attack detection capabilities of protective relays to tackle the problem of online settings which are susceptible to modification and fabrication attacks. This thesis develops a tool for detecting compromised settings sent to adaptive protective relays based on physical properties only. Implementing the tool first involves an offline phase in which Monte-Carlo simulation is used to generate a training dataset. Using Rough set classification, a set of IF-Then rules are obtained for each relay and loaded to the relays at the initialization stage. The second phase occurs during online operation, with each updated setting being checked by the corresponding relay's built-in tool to determine whether the setting is genuine or compromised. A test dataset has been generated to assess the tool performance using the IEEE 34-bus test feeder with DGs included.

The third strategy proposed is for the recovery phase. One of the requirements for a resilient distribution system is the ability to supply power to critical loads during disruptive events. It is important when restoring the critical loads to put into consideration the network resilience against post-restoration attacks. This thesis formulates an optimization problem for reconfiguring the network to maximize the restoration of priority loads upon attacks through resilient paths utilizing the cyber-based risk analysis outcome obtained during the pre-disturbance phase. The formulated problem considers both operation and network configuration constraints. The IEEE 37-bus test system has been used to validate the usefulness of the technique. The algorithm has been tested using single and multiple contingencies scenarios, and the results were compared to the algorithms proposed in the literature.

Acknowledgments

First of all, praise be to Allah, the Cherisher and Sustainer of the worlds, who gave me the courage and patience to carry out this work.

I then acknowledge my sincere gratitude to my supervisor, Prof. Magdy Salama, for his professional guidance, valuable advice, and continual support during my struggles. He has always been very patient and had a profound belief in my abilities. Without his insightful feedback, the completion of this work would not have been possible.

I would also like to express my deepest appreciation to my committee members for their time and constructive advice.

Last but certainly not least, I must express my very profound gratitude to my parents, who taught me the value of education and hard work. I would like to extend my sincere thanks to my sisters for their love and encouragement throughout my whole life. I am also very grateful to my husband and children for their love and understanding.

Dedication

In the memory of my father,

To my Mother who has devoted her life to me and who always rains me with love and kindness,

To my son and daughter who fill my life with joy and hope,

To my dear sisters who never let me down,

To my beloved husband who believed in me even at times when I did not believe in myself

…

Table of Contents

LIST OF FIGURES

LIST OF TABLES

NOMENCLATURE

Abbreviation	Definition
AI	Artificial Intelligence
CC	Cyber Criminal
IBDG	Inverter-based Distributed Generator
NVD	National Vulnerability Database
CNT	Complex Network Theory
CT	Current Transformer
CPRA	Cyber-physical Risk Assessment
DOS	Denial Of Service
DOE	Department Of Energy
DFS	Depth-First Search
DER	Distributed Energy Resource
DG	Distributed Generator
DNR	Distribution Network Reconfiguration
OpenDSS	Electric Power Distribution System Simulator
EPRI	Electric Power Research Institute
ETT	Elementary Tree Transformation
ERR	Error Rate
FDI	False Data Injection
FN	False Negative
FP	False Positive
FERC	Federal Energy Regulatory Commission
GOOSE	Generic Object Oriented Substation Event
HSA	Harmony Search Algorithm
HMI	Human Machine Interface
ICS-CERT	Industrial Control Systems-Cyber Emergency Response Team
ICT	Information And Communication Technology
IT	Information Technology
I/O	Input/Output
IEDs	Intelligent Electronic Devices
IEC	International Electro-technical Commission
IDS	Intrusion detection systems
MITM	Man-In-The-Middle
MMS	Manufacturing Message Specification
MOM	Method, Opportunity, and Motive
MPC	Model Predictive Control
MST	Minimum Spanning Tree
NS	Nation State

NIPPS	National Infrastructure Protection Plans
NIST	National Institute of Standards and Technology
NIDS	Network Intrusion Detection System
NLW	Normalized Load Weight
NSW	Normalized Substation Weight
NERC	North American Electric Reliability Corporation
PRN	Post-Restoration Network
PES	Power and Energy Society
PAO	Probability of Attack Occurrence
PAC	Programmable Automation Controller
PLC	Programmable Logic Controller
RCS	Remote Controlled Switches
RTU	Remote Terminal Unit
RED	Required Redundancy
RTD	Resistance Thermal Detector
RPM	Reverse Pyramid Model
RIF	Risk IF Failure
SMV	Sampled Measured Values
SK	Script Kiddie
SME	Subject Matter Expert
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition
TDS	Time Dial Setting
TGR	Tree-Growth Regulator
TN	True Negative
TP	True Positive
VT	Voltage Transformer

Chapter 1: Introduction

1.1 General Overview

The need for communication technologies to help monitor and collect data from all over the power grid puts the grid at risk of cyber and cyber-physical attacks in addition to the existing physical vulnerabilities. According to the Department of Homeland Security[1]–[3], cyber incidents in the energy sector reported to and handled by the Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) surpass the events reported in all other industries over the period 2013-2016, as shown in Figure 1.1. In Canada, over one-fifth of businesses, including businesses in the electric power sector, reported that cybersecurity incidents affected their operations in 2017 [4]. As the number of cyberattacks increases, the cost of cybercrime continues to rise. In 2017, the average annual cost of cybercrime in the energy sector was $13.2 million and rapidly increased to $13.77 million in 2018 [5].

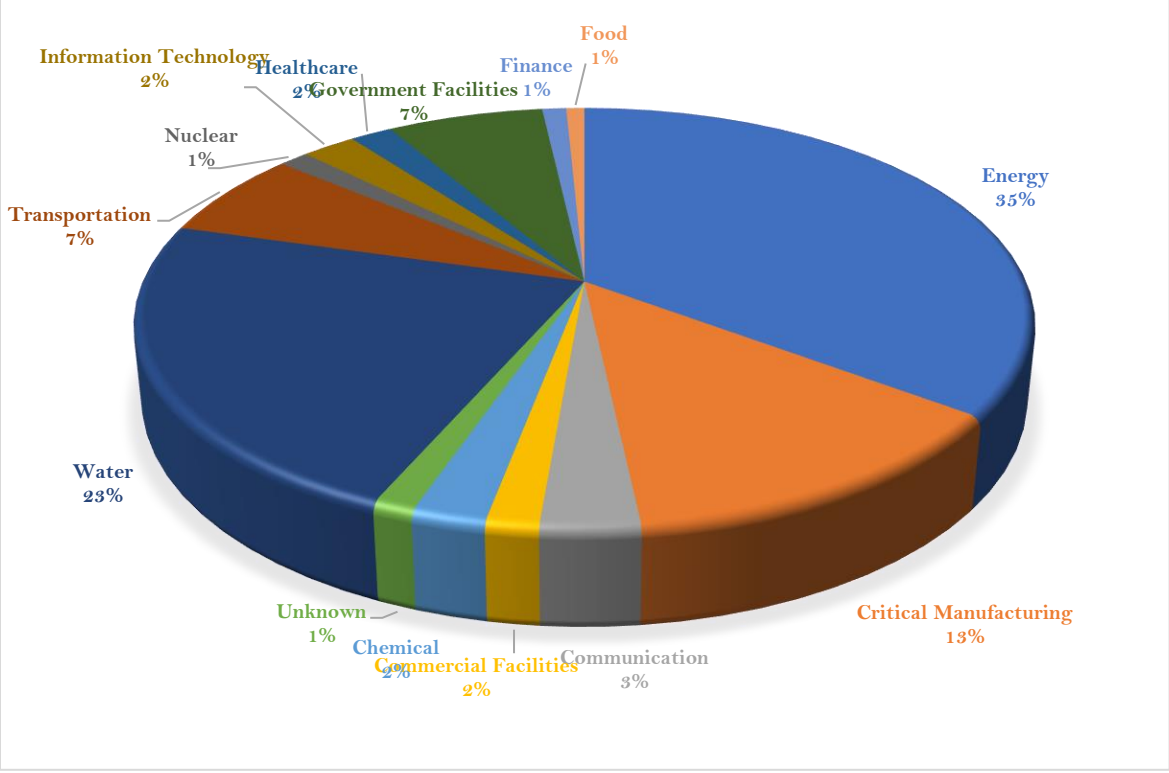


Figure 1.1 Total Cyber incidents reported by sectors during the period 2013-2016

A reliable electricity supply is vital in ensuring safety, productivity, health, and comfort for people. In addition, other crucial urban infrastructures such as drinking water systems, transportation networks, and telecommunication networks are also becoming highly dependent on electric grids. However, the ongoing development and modernization of power grids increase the integration of Information and Communication Technologies (ICT) and the vulnerabilities they introduce to the grid.

There are three prerequisites for any type of threat agent conducting a successful cyber attack: Method, Opportunity, and Motive, known as MOM. First, the method indicates that the attacker must have sufficient skills, tools, knowledge, and other resources that help exploit the defender's system vulnerabilities. Each attacker type has different levels of attacker resources. On the other hand, Opportunity implies that defenders have weaknesses (vulnerabilities) in their systems, which would allow attackers to access the network and attempt to exploit these vulnerabilities. Lastly, the motive denotes the purpose for conducting an attack. There must be anticipated benefits that would drive the attacker's motivation to conduct a certain attack. Since defenders have some control over the vulnerabilities of their systems' assets, the intuitive question that arises is: Why are existing security technologies not directly deployed to modern power grids?

While there are numerous cybersecurity methods that have been well-protecting the Information Technology (IT) networks, they are not very effective when directly deployed to power networks. The reason is that power networks and IT networks are different in nature in several ways including, security objectives, network architecture, technologies used, and quality of service requirements [6]. Despite all the best efforts of ongoing research dedicated to developing cybersecurity tools for power grid applications, there is still no perfect cybersecurity scheme feasible for preventing every potential grid attack [7],[8], especially with the growing concern about insider threats [9] and the inevitable zero-day attacks [10]. Nevertheless, extensive research has already anticipated some catastrophic consequences that utilities, industries, or governments are unprepared for.

1.2 Growing Cyber-Physical Grid Vulnerability

The cyber attack against the substations of the Ukrainian power grid in December 2015, which interrupted approximately 225,000 customers by several circuit breakers' tripping, has directed researchers' attention to substations' cyber-physical vulnerabilities. Primarily, this thesis focuses on cyber-physical attacks, which are the kinds of cyber attacks that have impacts on the physical system (power system) operation. Such attacks are gaining more attention since they are replacing physical attacks. Cyber-physical attacks can cause similar damage resulted from physical attacks without the same political, social, or moral risks that would usually follow an explicit physical attack [11].

1.2.1 Substation Cyber Vulnerability

According to IEEE Std1402™-2000 (IEEE Guide for Electric Power Substation Physical and Electronic Security), a substation intrusion is defined as unauthorized access to the substation property through physical presence or external influence. As stated by this definition, substations are vulnerable to two kinds of intrusions: physical and electronic. The standard then referred to the electronic intrusion as "an entry into the substation via

telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices. These devices include digital relays, automation equipment, computers, Programmable Logic Controllers (PLCs), and communication interfaces.".

It is very important to identify and assess substation vulnerabilities for several reasons. First, a study conducted by the Federal Energy Regulatory Commission (FERC) in 2013 concluded that the U.S. could suffer a coast-to-coast blackout with coordinated attacks on only nine key substations out of the existing 55,000 substations [7]. Substations are usually more vulnerable to cyber attacks than other more-secured high-priority assets such as SCADA and control centers.

In addition, since the SCADA system gathers meters measurements and control field devices through substations, both cyber and physical domains are interlinked within substations. The interlinking devices typically are PLCs, Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). PLCs are legacy devices that are programmed to perform protection and control functions. However, they have limited communication and processing capabilities. RTUs are electronic devices used to support the interface between field devices and controllers. IEDS are microprocessor-based controllers which are also used for protection functions. Due to their interoperability and advanced communication capabilities, they have been heavily deployed in modern substations. IEDS are complex and can have various settings, do several functions, and receive control commands from remote users to control power-system devices. Consequently, they help improve the network operating efficiency while minimizing human intervention. An example of IEDs is the communication-assisted digital relay, whose vulnerabilities are fully discussed in Chapter 4.

In fact, Substation Automation Systems (SASs) are currently experiencing many upgrades as part of the smart grid initiative. While Some SAS functions need operator intervention, others are closed-loop functions. For example, operators need to control CBs and change tap positions on transformers. However, protection schemes are real-time operations, and therefore do not mainly depend on operators. This work will specifically look at applications that affect the operation of relays, circuit breakers, and switches.

1.2.2 The IEC 61850 Vulnerability

Another aspect of the substation's vulnerability is the communication protocols used. Essentially, the IEC 61850 international standard has been created to tackle the problem of the growing complexity of SASs [12]. In other words, the simple, straightforward protocols of the older SASs no longer satisfy the requirements of modern intelligent system devices. Therefore, there is a need for a unified protocol such that different devices from different manufacturers can talk to each other with no trouble. The IEC 61850 standard defines abstract data models which can be mapped into three communication protocols: GOOSE, SMV, and MMS. Both GOOSE and SMV are time-critical and devoted to high-speed information exchange, thus are used for protection operations in power grids [13]. On the other hand, their time-constraint requirements make it very hard to implement any security means for integrity and confidentiality such as encryption or digital signatures, which increases latency [14], [15]. Even MMS is designed with little attention to security [16]. Due to the reasons above, substation functions, especially protection functions, are vulnerable to security attacks because of protocols' vulnerabilities, resulting in undesired tripping commands.

1.2.3 Interactions Between Cyber and Physical Layers of Substations

Different cyber-physical attacks would have varying severity of impacts on substation level and/or grid level, based on the attacker attributes (i.e., motivation, determination, and capabilities), as discussed in Chapter 3. The cyber-physical interactions in a targeted substation can be summarized in Figure 1.2.

.

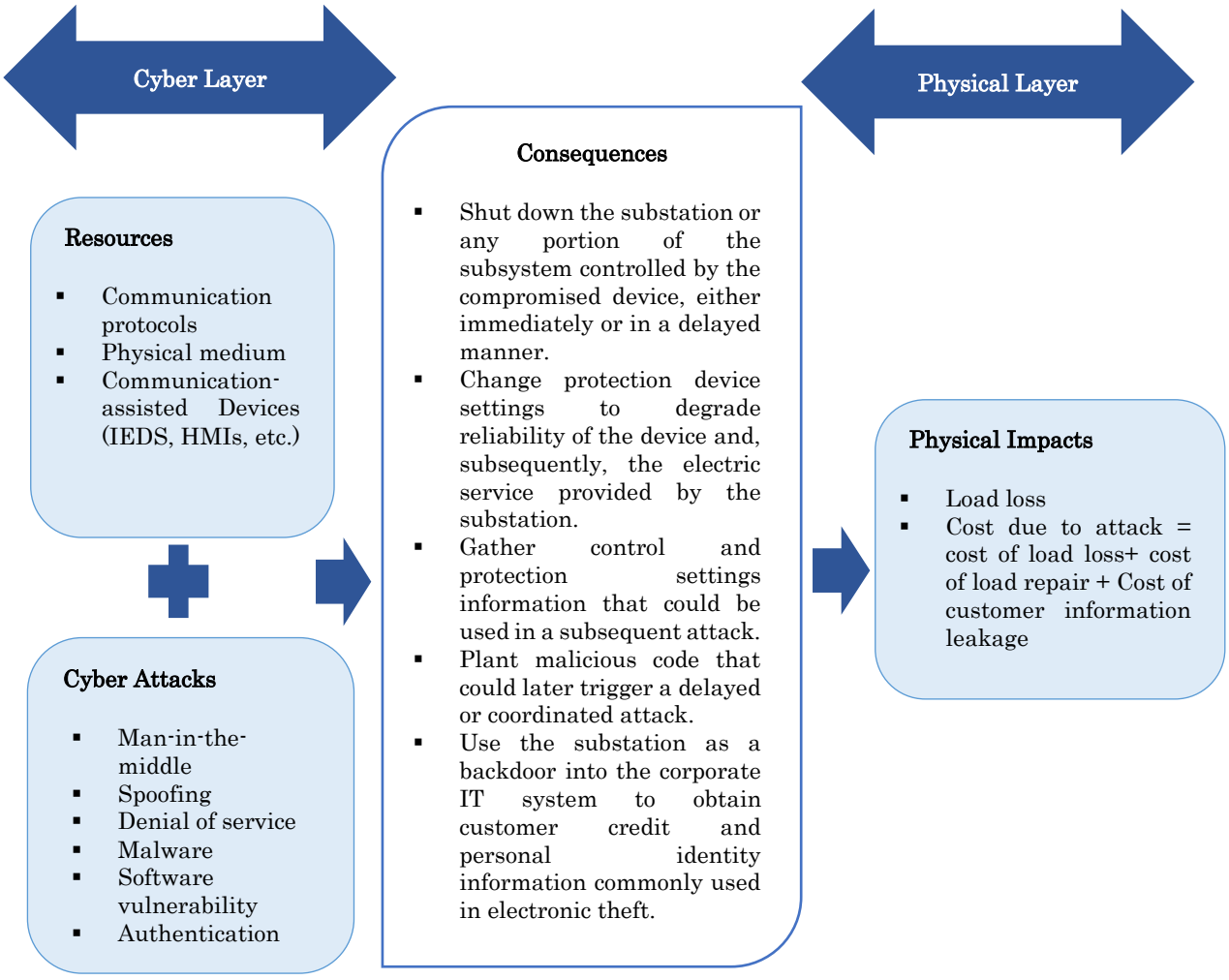


Figure 1.2 The Cyber-physical Interactions in a Targeted Substation

1.3 The Need for Resilient Power Grids

Due to the aforementioned cyber vulnerabilities along with the lack of a perfect cyber defense scheme, the concept of resilience begins to attract research attention and is steadily emerging as a strategic objective in power system planning. The Department of Energy (DOE) has considered the 'Resiliency Model' a part of its grid modernization initiative. Grid resilience refers to the power system's ability to continue operating and delivering power even during

disruptive events. Thus, the grid resilience objective is ideally minimizing potential consequences resulting from these disruptions. Minimizing the consequences can be done before, during, and/or after the event occurrence, as explained in the resilience states in Chapter 2. Adopting the "resilience mindset" would help lessen the economic, technical, social, and political impacts of disruptive events. Disruptive events are those having low probability but high impacts. These events can be classified into natural and man-induced disasters. Although these events are not common, they can cause devastating damage to grids when they occur. (Please refer to Appendix-A for a full discussion of the types of events falling within the scope of the resilience analysis).

To enhance grid resilience, there are two main categories of strategies proposed in the literature realized through: grid hardening and smart/operational measures. Grid hardening is the physical reinforcement of the system infrastructure to improve its ability to sustain the impacts of disruptive events, enhancing the infrastructural resilience. These measures include vegetation management near power lines, undergrounding power lines, upgrading utility poles and adding guy wires, relocating network key assets, adding redundant transmission routes, installing additional lines, breakers, and transformers, and installing black-start capabilities. Thus, hardening measures primarily aim to reduce the physical impact of disruptive events. Although those measures are more resilience-effective when compared to the operational measures, they must be planned wisely. The measures effective to a specific threat may have a negative effect on a different occasion. For instance, as aforementioned, undergrounding is an effective solution in the face of storm events. However, underground cables are then vulnerable to flooding and storm surges.

Smart/operational measures, on the other hand, include the non-physical strategies that help boost system performance in the face of disruptive events. Smart/operational measures are more affordable than hardening measures [17]. Examples of operational-oriented measures are advanced energy management system, allocation and dispatch of emergency response resources, microgrid networking, leveraging distributed energy resources, risk analysis for disruptive events, adaptive protection and control schemes, and optimal reconfiguration and DG Islanding.

Although considerable research has been devoted to enhancing the grid resilience against natural disasters, less attention has been paid to cyber-physical-attack-based strategies. In essence, natural disasters and targeted attacks differ in several ways [18]. For example, while different natural disasters cause the arbitrary failure of network elements, the malicious attackers intentionally prefer the most critical network components. Also, the damage resulted from a natural disaster event is mostly physical damage to the system's infrastructure. In contrast, malicious attacks usually result in undesired switching actions (which eventually can lead to cascading outages) or in disclosing customers' confidential data.

1.4 Research Motivation and Literature Gaps

This thesis focuses on three strategies for enhancing power grid resilience: cyber-physical risk assessment, detection of cyber-physical attacks on adaptive protective relays, and critical-load restoration problem. The rest of this section discusses the importance of this research, including the research gaps that will be tackled in this work.

1.4.1 Cyber-Physical Risk Assessment

When the researchers realized that cyber-physical attacks become inevitable in modern power systems, they began to investigate the cyber-physical risk of power systems following the same example of the conventional risk analysis process in terms of selecting targets and event probabilities, as will be seen in Chapter 2. However, the nature of cyber-physical attacks is different from reliability-based events. The attacker's resources, experience, and motivation affect both the likelihood of attack and the target selection, hence the negative consequences. Thus, the cyber-based risk analysis process should be attacker-specific. The level of attacker knowledge —of the cyber system and technology techniques used and their knowledge of the power system structure and operation— should affect the risk analysis.

On the other hand, the power network data available publicly for different systems vary. Principally, because of the open data policies [19], lots of energy data, models, and topologies are now publicly available. In addition, there are numerous projects and research dedicated to collecting power system data from formal and semi-formal agencies, cleaning and republishing the data, and predicting the data missing [20], [21], [22]. Still, some regions do not release information about their networks online. For example, Ref. [23] gives an idea about the percentage of African countries that disclose their energy data, shown in Table 1.1. Moreover, the reference states that two-thirds of the assessed data is not even provided/updated in a timely manner.

Table 1.1 Percentage of African Countries Disclosing the Respective Energy Data

Data Category	Percentage of Countries Providing Datapoints
Electricity consumption	73%
Prices	60%
Power stations and electric capacity	60%
Electricity transmission networks (geographic position)	37%
Power outages	20%
No data online	10%

Hence the availability of public data should be a factor to consider in the analysis. Different attacker levels of knowledge of the power system are modeled in this work to build a more comprehensive cyber risk analysis framework. Although the model covers different kinds of attack strategies, determining which to consider in the analysis is up to system operators based on their estimation of the amount of the publicly-released network data.

That being said, we know that the system is designed to satisfy the N-1 criterion, which depends on finding the worst-case scenarios when identifying critical targets. Now, the first question arises: can the N-1 criterion handle the emerging cyber-physical risks as well? The answer is no. The N-1 criterion is effective when handling reliability-related events such as a faulted line or aging equipment failure. However, cyber-physical attacks can target more than one device nearly simultaneously in one power grid, like the case of the Ukraine attack. Such an attack is classified as a coordinated attack, i.e., attacks in which various commands

are employed, and various components are targeted. Therefore, the N-1 criterion can no longer satisfy the new requirements of modern power grids. Hence, for risk and contingency analyses, there is a need for a more comprehensive framework that takes into account cyber contingencies along with the physical ones [24]. Accordingly, the next logical question is: will worst-case scenarios (if N-k applied) be the most efficient solution that gives the most inclusive results against all disturbing events, including cyber-physical attacks? Our answer is no since designing mitigation plans based on risks of worst-case scenarios (i.e., assuming the attackers have full knowledge of power and cyber systems and have unlimited resources and capabilities) may be leading to planning too conservatively, which may be not reasonable for the low probabilities of such events. Consider the example of a 118-bus system, and for just identifying all N-4 combinations, we need more than 8 million simulations. Much criticism has been raised concerning the use of worst-case scenarios [25]. Arguably, they are often not worth the effort to develop or investigate, and relying on such scenarios in planning may waste resources preparing for very rare contingencies. Thus, it is recommendable to evaluate whether the development of these cases is reasonable and feasible [26].

1.4.2 Detection of Cyber-Physical Attacks on Protective Relays

Continuous research efforts are dedicated to developing methods to improve existing security tools to better fit the nature of modern power grids. According to [26], this improvement can be achieved in two ways. The first depends on handling any problem at the system's borders using firewalls, encryption, and IDSs. First, the IDSs are usually unable to detect unknown attacks. Besides, most of these techniques might not be adequate for protection relaying applications, as explained in Section 1.2.2 [14]. However, in the second approach, normal system behavior and control operations are modeled to detect anomalies arising from attempts to disrupt system performance. In other words, the approach depends on using available physical system information to fill this cybersecurity gap. This approach mathematically models and analyzes the dynamic behavior of the power system in order to distinguish between normal and abnormal operations. However, it is not practical to implement this technique directly in a relay because, as an embedded system, it has limited computational overhead. This thesis proposes a new solution to this problem by splitting it into two steps: offline and online, which are thoroughly explained in Chapters 2 and 4.

1.4.3 Critical-Load Restoration Problem

Network reconfiguration within power systems is used to improve system performance by reducing power losses and improving power quality. However, during faults, reconfiguration can also be used to supply power to affected customers by sectionalizing the network and using tie switches. Besides, distributed generation can play a fast start-up backup role during these periods. Such a real-life example is what happened during Hurricane Sandy when people with solar panels shared emergency power with their neighbors [27]. With growing penetration levels of DGs in distribution networks, intentional islanding can play a vital role in enhancing power system resilience by energizing critical loads after disruptive events.

Several studies in the literature have employed DGs to build microgrids for the distribution service restoration after disruptive events. However, the existing DGs' capacity is insufficient to supply all out-of-service loads after these events until all the repair work is done. In this case, loads should be restored based on their priorities. Therefore, critical-load restoration is one of the main objectives of power system resilience. This problem should be formulated to

maximize out-of-service loads to be restored and to maximize the resilience of the post-restoration network while satisfying the operational and topological constraints of the network. The whole analysis should be done in a timely manner. These limitations in the literature will be tackled in the proposed algorithm.

1.5 Research Aims and Objectives

Based on the aforementioned motivations, this thesis mainly focuses on developing smart/operational strategies that enhance the cyber-physical resilience of power grids through boosting the preparedness potential and the fast recovery potential of the grid.

- **System Preparedness**

System preparedness is the assessment conducted to identify and evaluate the system vulnerabilities and prioritize the most vulnerable assets. Such assessment is to be used in preparing preventive and corrective plans. The preparedness potential for a resilient power system also complies with the requirements of the NIPPS, plans which intend to enhance the protection and resiliency of the critical infrastructure, including the energy sector [28]. By conducting risk-informed assessments, the effects of serious risks can be reduced. In the plans, the risk management activities also embrace monitoring cyber systems continuously, using security protection systems to detect attacks, and implementing intrusion detection and protection systems for critical networks.

- **System Fast Recovery**

Traditionally reliability metrics are designed to measure a system's performance with the aim of providing power to all the connected loads. During extreme conditions, the system priority would be restoring as much power as possible to critical loads, and this is one of the main requirements of resilient distribution systems [29],[30].

In the light of enhancing preparedness and fast recovery potentials, the main objective of this thesis is threefold, outlined in Figure 1.3:

1- Proposing a comprehensive cyber-physical risk assessment for substations based on a threat-oriented approach to identify threats and vulnerabilities and quantify consequences. Based on the risk assessment, the substations can be ranked according to their importance to help the operator be aware of the critical assets in the network and take protective actions accordingly.
2- Applying this knowledge obtained in reinforcing the most vulnerable substations with a reliable attack-detection capability for the protection relays using only physical properties.
3- The knowledge obtained will also help realize fast restoration of the priority loads in the network following attacks using a resilient network reconfiguration strategy as a vital step in the whole recovery process.

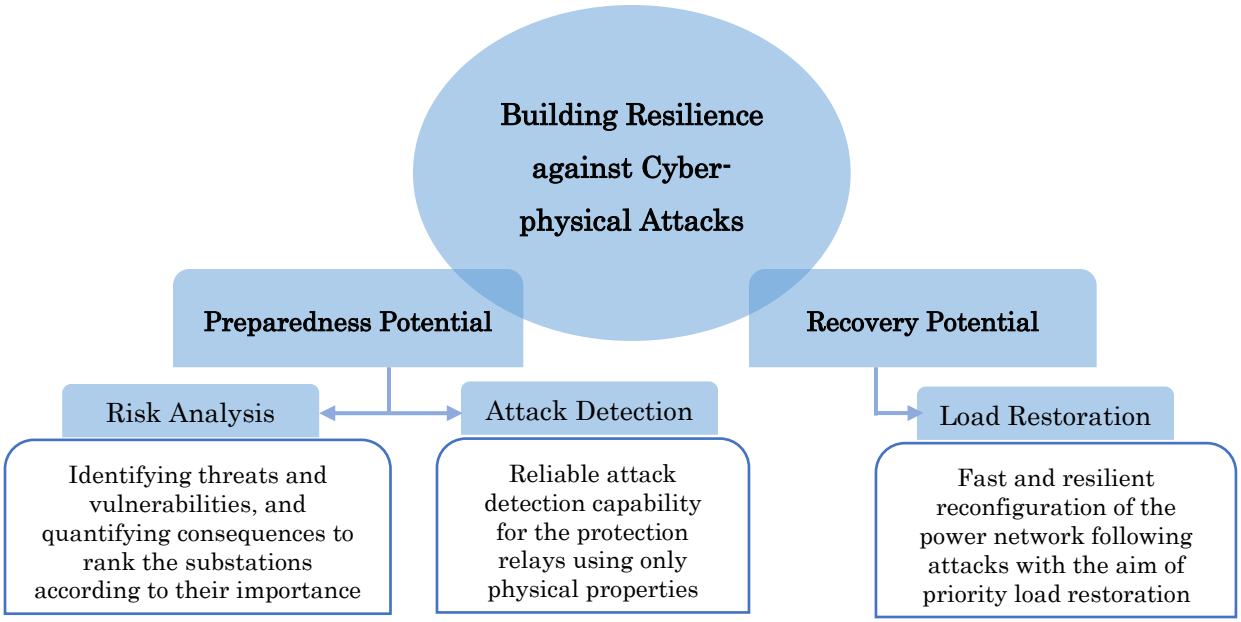


Figure 1.3 Research Main Objectives

For realizing these objectives, the research sub-objectives can be listed as follows:

1- For risk quantification, this thesis aims to estimate the likelihood of successful attack occurrence. An adversary-capability approach will be used to find the attack probability based on different attackers' attributes. In this regard, the identification of the substation's threats and vulnerabilities will be performed so that attack trees can be constructed and different attack scenarios generated. These scenarios will be required to employ the threat-oriented risk analysis approach.
2- Also, for risk assessment, the thesis aims to develop an impact analysis algorithm for quantifying the physical impacts of attacks on the customers served. The algorithm will include a method for detecting islands formation and a load/generation dispatching technique. Furthermore, the impact calculation should consider the consequences resulting from the operational network constraints for a more realistic analysis.
3- The thesis aims to develop a probabilistic cyber-risk assessment algorithm that considers mediocre attacks, i.e., where attackers have limited resources and zero (or very low) power system knowledge. Attack assumptions should be established to fit the attributes of this type of attacker. The model will simulate the randomly-selected attack targets and will be required to quantify their impacts.
4- The thesis also intends to study the structural vulnerability of the power network based on the complex-network theory to identify the candidate critical targets from the attacker's perspective. To achieve that, different centrality metrics will be studied, and two different attack formulation strategies will be proposed to formulate six different topological-based attacks. The candidate targets should be selected to cause the maximum system performance degradation based on the giant component size measure.

5- Based on the structural vulnerability study, the thesis also aims to develop a cyber-risk-based assessment algorithm to consider the intermediate attacks, i.e., where attackers have average resources and purely-topological power network information. From the perspectives of system planners and operators, the attack impact will be evaluated for the identified candidate critical substations. The likelihood of attacks will be calculated based on the number of nodes removed. Risk indices for the substations and the whole system will be defined.
6- The thesis aims at evaluating the cyber-based risk for sophisticated attacks, ones with full power system knowledge and abundant resources, by enumerating the substation combinations, measuring the attack impact for each combination, estimating the attack likelihood. Finally, substations' criticality can be screened and ranked.
7- The thesis aims at enabling adaptive communication-assisted protection schemes with flexible settings by developing a detection tool for identifying compromised settings sent to protective relays. Implementing the tool will first involve an offline phase in which the Monte-Carlo simulation will generate a training dataset. Using Rough set classification, a set of IF-Then rules will be obtained for each relay and loaded to the relays at the initialization stage. The second phase should occur during online operation, with each updated setting being checked by the corresponding relay's built-in tool to establish the setting legitimacy.
8- The thesis finally aims to propose a resilience-based reconfiguration technique formulated to maximize the priority load restoration while maximizing the paths' resilience subject to operation and network topology constraints. For different attack scenarios, available Reconfiguration Paths will be identified using the depth-first search algorithm. Then, an optimization problem will be formulated to maximize the objectives subject to the operational and network constraints.

1.6 Thesis Outline

The remainder of this thesis is structured as follows:

Chapter 2 presents a brief background on power system resilience as a relatively new concept emerging in power grids. Then, it gives a detailed literature review on specific resilience enhancement strategies: cyber-based risk assessment, cyber-attack detection for protective relays, critical load restoration methods. It also discusses the limitations of the existing research.

Chapter 3 presents the comprehensive cyber-based risk assessment framework. Substations' Cyber threats and vulnerabilities are identified. Access points and attack pathways are discussed. An adversary-capability model is used to estimate the likelihood of the attack occurrence. An impact analysis algorithm is proposed. Structural vulnerability for the power network and the associated attack formulations are investigated. Three different approaches for risk assessment based on the attacker attributes are proposed, and numerical examples are then investigated.

Chapter 4 introduces a novel cyber-physical attack detection tool for adaptive protective relays. The tool can detect compromised settings sent to adaptive protective relays based on electrical properties only, making it more reliable. The data-mining-based algorithm is proposed and studied on the IEEE 34 bus system to validate the tool efficiency.

Chapter 5 proposes a resilience-based approach for distribution system reconfiguration based on the vulnerabilities of the lines to pick up priority loads after attacks. The reconfiguration is done to restore the maximum amount of priority load while selecting the more cyber-resilient paths in fear of a coordinated attack to follow. The proposed algorithm is validated by applying it to the IEEE-37 node test system. The results obtained are compared with other algorithms in the literature.

Chapter 6 provides a summary and conclusions of the thesis. Future research directions are also discussed.

Appendix A presents a detailed background on power system resilience, the type of events associated with this concept, followed by a clarification of some common misconceptions that the resilience and reliability concepts are similar. It then reviews hardening strategies and additional smart/operational measures proposed in the literature for enhancing power system resilience.

Chapter 2: Background and Literature Review

2.1 Introduction

Physical security and cybersecurity are often handled as two completely separate areas when planning for defense and protection schemes. The concept of prevention has always been the best way of defense. The growing risks of cyber and cyber-physical attacks are becoming more challenging, especially because those threats now have different sources of disruptions, thus are hard to expect and enumerate. In addition, the attack may lie dormant for months gathering information about the system, such as the case of the Ukraine attack. Thus, instead of prevention, grid planners and operators need to figure out how to make the system withstand those shocks as they unfold and keep working instead of trying to prevent every single disruption.

2.2 Grid Resilience Definition

As reviewed in Appendix-A, resilience has several definitions in different contexts, excluding power grids. It was not until April 2018 that the IEEE Power and Energy Society (PES) published a technical report to define electric grid resilience. The task force has adopted the following definition and considered it a somewhat general description. As stated, electric grid resilience is "The ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event."[31]. This definition is adequate and hence will be adopted in this thesis as well.

2.3 Resilience States

Based on the resilience definition, the system performance against a disruptive event can be represented in Figure 2.1 [31]–[34]. Note that this graph is guidance for general states of a power system response in the face of disrupting events. For each real-life event, the representation of system response in each state and the transitions between the states could differ depending on several factors discussed in the rest of this section.

2.3.1 Pre-disturbance Resilient State ($t_0 \leq t < t_{es}$)

Before the occurrence of a disruptive event, the system operates in a normal state as expected. During this state, system operators should define hazards and system vulnerabilities. They should identify critical assets and perform risk assessments. Such preparedness would help in handling any upcoming events.

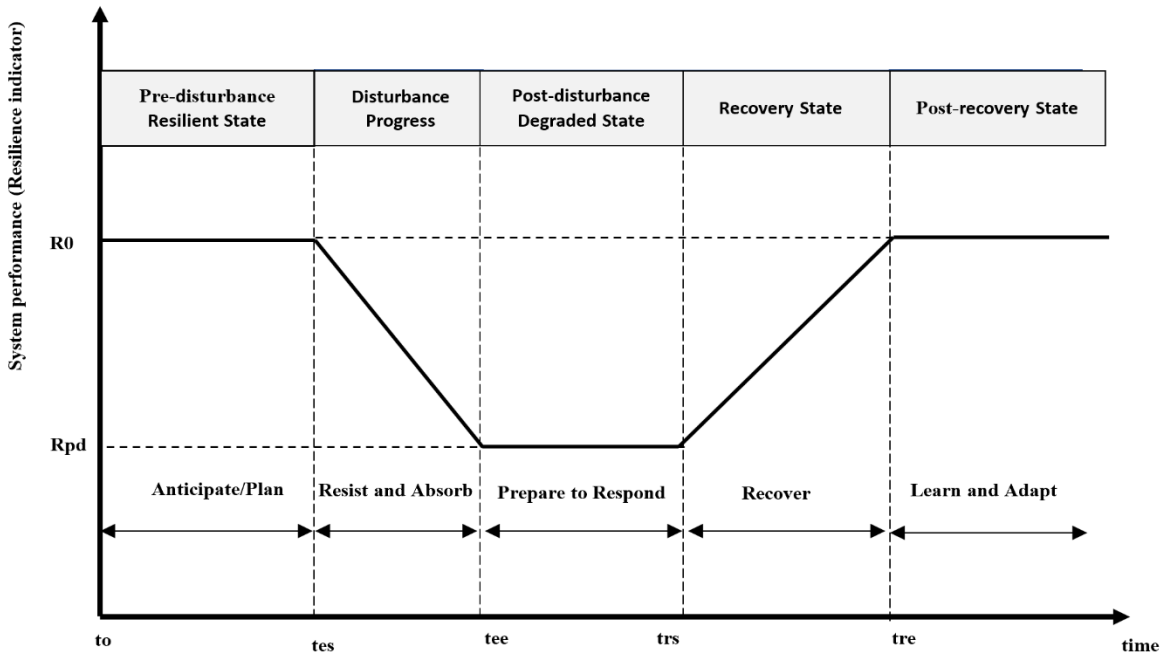


Figure 2.1 Resilience States

2.3.2 Disturbance Progress State ($t_{es} \leq t < t_{ee}$)

At an instance t_{es}, a disruptive event hits the system and degrades its performance from R_0 to R_{pd} due to the failure of one or multiple system components. Advanced situational awareness would help allow system operators to remain informed on the evolving conditions. The final value of the resilience indicator, R_{pd}, would depend on several aspects such as disruptive event type, impact severity, and network topology.

2.3.3 Post-disturbance Degraded State ($t_{ee} \leq t < t_{rs}$)

Following the event, the system enters the degraded state and stays there until the recovery process starts. Thanks to the integration of cyber systems in modern power grids, the updated status of system components can be collected. Hereafter, priority setting and damage assessment can be conducted to take appropriate corrective actions. The length of this state depends on several aspects including, resources and analysis tools in hand, operational flexibility, operator's training, etc.

2.3.4 Recovery State ($t_{rs} \leq t < t_{re}$)

This state is concerned with recovering the system as fast as possible. The recovery duration is affected by several aspects, including the damage caused, the amount of resources (material and human) available, the amount of high priority load connected, and the accessibility to the affected zones.

Once the restoration is completed, the post-restoration resilience indicator may or may not be as high as the initial level R_0. That is because, even though the system has been recovered from an operational point of view, the infrastructure may take longer to fully recover, depending on the type and severity of the event. This fact will be discussed in Section 2.4.

2.3.5 Post-recovery State (Adaptation) ($t \geq t_{re}$)

It is a learning state where what happened during previous states should be analyzed and then assessed. Thanks to such analyses, the development process of the existing plans and standards can be carried out to enhance the system in order to sustain future similar events. One revision example is revising the federal emergency management plan after Hurricane Katrina [35]. Another example is when industry standards were revised after the 2003 blackout [36].

2.4 Infrastructural and Operational Resiliencebgg

We all recognize that reliability can be featured by adequacy and security. Likewise, power system resilience intrinsically comprises two classes [37], [38], [39]: infrastructural resilience and operational resilience, as depicted in Figure 2.2. Power system infrastructure resilience can be defined as the physical strength of a power system for minimizing the portion of the system that becomes non-functional. In contrast, power system operational resilience denotes the characteristics that would maintain operational strength for a power system, i.e., ensuring that all the customers are served while encountering an extreme event. According to these definitions, the infrastructural resilience indicator can be the number of online transmission lines, whereas the amount of generation capacity and/or load supplied would be indicators for operational resilience.

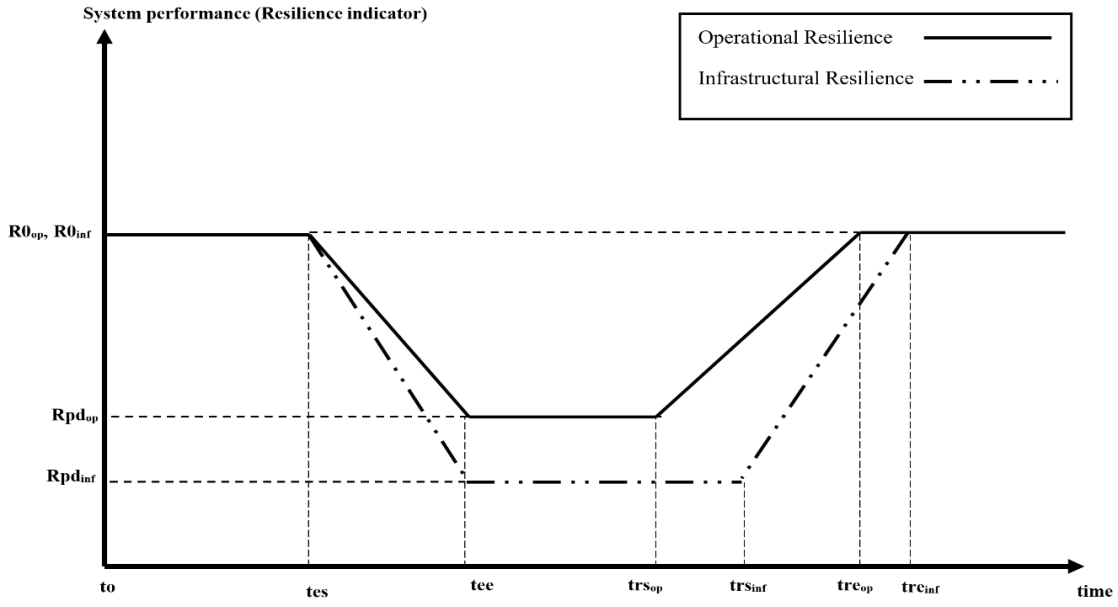


Figure 2.2 Infrastructural Resilience and Operational Resilience

From the graph, we notice that sometimes system recovery could be achieved through two phases, first, by performing network reconfiguration to secure power supply to the out-of-service loads, which would turn the resilience index to its pre-disturbance value. The second phase would be working on the repair process of system lines and components which is usually a long process. The infrastructural resilience index should be back to its pre-disturbance value by the end of the second phase. Chapter 5 aims to improve the process of reconnecting customers to the power supply as fast as possible to enhance the grid resilience operationally.

2.5 SAS Architecture under IEC61850

The IEC61850 is a unified protocol popular all around the world. It facilitates the substation's communication and interoperability, which will be critical in developing smart grids. It divides data communication in SAS into three principal levels: Process, Bay, And Station [40], [41]. The hierarchy and architecture of the IEC61850 SAS are shown in Figure 2.3.

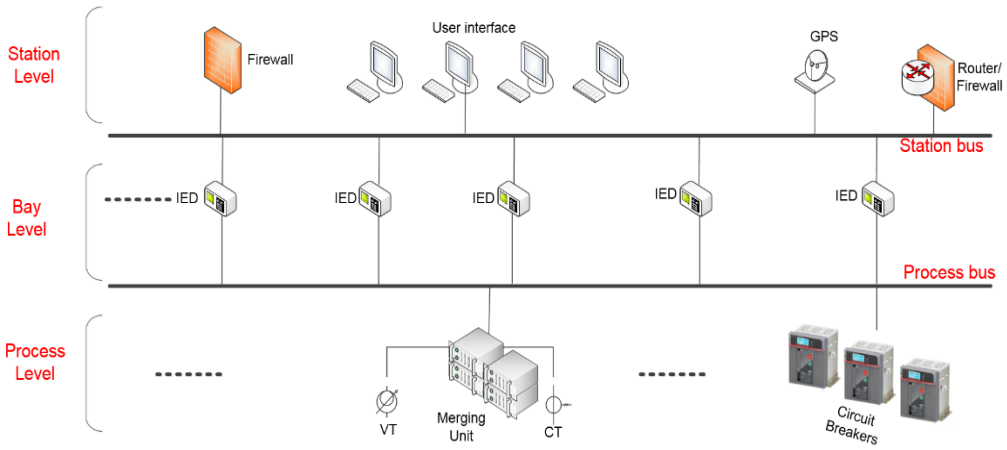


Figure 2.3 IEC61850 SAS Architecture

2.5.1 Process Level

This level contains the switchgear devices which are connected to the substation bay-level devices. These switchgear devices comprise actuators (breaker and remotely-operated switches), intelligent sensors, Current Transformers (CTs), and Voltage Transformers (VTs), Resistance Thermal Detectors (RTDs), and all other Input/Output (I/O) devices. This level has two functions. First, it collects system data from sensors and sends them off to bay-level devices. Second, it executes the control commands received from the bay-level devices.

2.5.2 Bay Level

This level connects the station-level devices to the process ones. It contains the control and protection IEDs. Thus, this is where the relays are placed. Digital relays are replacing the existing electromechanical ones due to their cost, flexibility, and functionality. Depending on the communication commands received from the station level, these IEDs are capable of performing the bay control and protection functions. The bay level automation system is placed in stand-alone kiosks, away from switchgear devices.

2.5.3 Station Level

This level is connected to the bay level IEDs devices through the station bus. It analyzes the data coming from the whole bay level. Station level uses dedicated software devices for archiving, automation, data storage, and management of several bay level devices. It also has a Human Machine Interface (HMI) and gateways to communicate with the control center. It also communicates with other remote entities for monitoring, maintenance, etc. Station-level devices are housed in a separate room away from all switchgear equipment.

2.6 Cyber-Physical Risk Assessment

Although there are many studies on different strategies used to enhance the power system resilience in general, as reviewed in Appendix-A, the research devoted to tackling the problem of cyber-physical resilience remains limited. This strategy would belong to the pre-disturbance (preparedness) state wherein system operators need to evaluate the critical elements in the network to prepare for preventive or corrective plans. Risk analysis is used to evaluate the risk of cyber attacks on the physical layer of the power system. This thesis considers different types of attacks with different levels of knowledge of attackers of the physical (power) system, which can be briefly described as follows:

i. No or very low knowledge of power systems; hence, the attack targets are selected randomly.
ii. Purely-topological information of power system; hence, the targets are selected based on topological criteria.
iii. Full power system knowledge where the targets are selected such that maximum damage happens with the least number of targets disconnected.

Therefore, this chapter will review the work done according to this classification as randomly-selected targets' attacks (will be referred to as random attacks), topological-based attacks, full power system information attacks. In addition, some work has considered quantitative risk analysis, while others have performed qualitative analysis. Both types will be considered in this review as well.

2.6.1 Preliminaries

Risk is defined as the probability of a loss. Accordingly, the risk is modeled as a function of the probability of a threat event and its potential adverse impact.

- *Risk Probability*

Risk probability, sometimes referred to as likelihood, is the chance/possibility that a risk event will occur. The risk probability can be represented in a qualitative or a quantitative manner. For qualitative, it can be denoted as rare, possible, frequent, etc. For quantitative, it is described numerically, i.e., using scores, frequencies, percentages, etc.

- *Impacts of risk*

Impacts can be defined as the event's consequences on the project objectives, e.g., cost, schedule, quality, scope, health, safety. The consequences can be either beneficial or harmful to the project objectives. These impacts can be represented qualitatively or quantitatively. Typically, it can be measured by a five-point scale: very low, low, moderate, high, and very high, and it can also be defined using numerical scales. Different objectives affected must be considered.

To ensure the quality and credibility of the analysis, general definitions of impact and probability levels must be fitted to the substation's security context.

2.6.2 Quantitative Analysis

Fundamentally, quantitative risk methods enable us to assign numeric values for the probability and impact of each event so that we can quantify the overall risk exposure of the system [42]. The main output is a prioritized list of quantified risks.

A. Random Attacks

In random attacks, the attackers select the targets to be attacked in a random way. These targets can be the whole substation or specific components inside substations (or even their parameters/settings). Ref. [43], [44] have developed a risk assessment framework to evaluate the cyber-physical vulnerability of power systems. They focus on studying the cyber attacks that target the relay devices only. Each substation contains a number of relays, each of which has many parameters that can be manipulated. The capability of an attacker is assumed as a variable p, which denotes the percentage of the parameters the attacker will alter. Each parameter, i, has its minimum and maximum limits, $A_{i,min}$ and $A_{i,max}$, respectively. The altered value, z_i, can be formed as

$$z_i = A_{i,min} + \alpha \left(A_{i,max} - A_{i,min}\right) \tag{2.1}$$

where α is a uniformly-distributed random variable between 0 and 1. The framework is then divided into two parts. The first analyzes the protection schemes and bus configuration and generates a list of settings and parameters. The second is a Monte-Carlo-simulation-based analysis. It randomly selects the parameters to be compromised and the values for α for each of those parameters. When parameters change, some CBs may change their statuses, and consequently, a new system topology G will be generated. After that, power flow analysis is done, and the physical impact, represented by the Expected Load Curtailment (ELC) in this study, is then calculated. The probability of attacker illegal access and cyber vulnerabilities were ignored, and the focus has been directed only towards the physical impacts. Thus, the

impact (ELC) is used to evaluate the cyber-attack risks. The ELC is given by Equation (2.2) which can be simplified to Equation (2.3).

$$ELC = \sum_{\forall G} P(G).LS(G) \tag{2.2}$$

$$ELC = \frac{1}{NJ}\sum_{j=1}^{NJ} LS(G_j) \tag{2.3}$$

For a system topology G, the LS is the load curtailment, and P is the probability of this topology. N is the total number of parameters inside a substation, and j refers to the iterations.

Ref. [45] proposes a stochastic counterfactual risk analysis framework. This method is established in the context of the direct and indirect impacts of the cyber-physical attack on Ukraine. The physical impact which decision-makers consider in this study is the total number of population disruptions. The Sets of scenarios, which targeted different numbers of substations (4, 7, and 14), were selected randomly. This study also considers the indirect impacts due to the interdependence between the power system and both the railway network and water distribution system. Therefore, certain substations have been found more critical due to their functionality to those interdependent key assets.

B. Purely-Topological Attacks

The pure topological attacks are those in which the attackers choose the node(s) to be attacked based on the pure Complex Network Theory (CNT) metrics. In pure CNT, substations are represented as nodes and transmission lines as edges, as explained in Chapter 3. However, it does not take into account either line weight or direction data [46].

Ref. [47] developed a cascading failure analysis model based on complex network theory. The model can recognize the critical and high probability events employing the edge betweenness centrality. The event impact is estimated using the expected percentage of the load loss and the expected percentage of the line cut to calculate the risk. Ref. [48] studies the vulnerabilities of power grids due to node failures. To calculate the critical level for a node, the authors have defined three metrics. The first metric is the percentage-of-failure, λ, defined as

$$\lambda = 1 - \frac{N'}{N} \tag{2.4}$$

where N' is the number of nodes that survived the attack, and N is the total number of nodes. The second metric is Required Redundancy (RED) for a node which denotes the minimal required system tolerance, which does not result in cascading failure when this node is removed. Lastly, the Risk if Failure (RIF) metric, which is defined as

$$RIF_i = \frac{L_i}{\sum_m L_m} \quad (2.5)$$

where L_i is the betweenness (load) of the node i and L_m is the load of the m's neighbors of the node i. The higher the RIF value is, the more probable the cascading failure takes place with the removal of node i. Therefore, RIF was considered as a risk index representative in this paper. Using these three topological metrics, the authors could find the optimal victim nodes that the attackers should select to attack to cause the failure. Based on the simulation results, the RIF metric effectively finds the critical nodes that result in greater damage. However, the attack strategies presented in this paper is designed for single-node attack and need to be extended to consider multi-node attack cases.

Ref. [49] presents a framework for quantitative vulnerability assessment of critical infrastructure systems which is applied to electric power delivery. Vulnerability is described as sensitivity to threats and hazards that substantially will reduce the system's ability to maintain its intended function. This kind of study, power system structural vulnerability, is inspired by the conventional risk assessment with more attention has been directed towards them, especially after the Northeast Blackout of 2003. Since then, CNT has been increasingly used to model and analyze power system networks. Ref. [50] studies the structural vulnerability of the North American power grid. The study determines the network's ability to transfer power between generators and consumers when specific nodes are disrupted in a different order. Different removal orders were used to examine the vulnerability: random order, node degree order, and node betweenness (load) order. Node removals are done one by one, first randomly, then in descending order of their centrality: degree or load. The study concludes that the grid can withstand only a few node removals if the attack is formulated using those centrality metrics before an outage of considerable parts of the network occurs. For example, only 4% of the high load nodes can cause up to 60% loss of connectivity. Similarly, a study was done on the topological vulnerability of the European network against attacks in [51]. Ref. [19] assesses the vulnerability of power grids to targeted attacks using two graph models for power grids based on lines and load data available. It first calculates different centrality metrics of each node. Then, it forms multiple attack strategies using those metrics. Nodes can thus be ranked based on their importance. Applying this methodology to real and hypothesized systems, the power grids are found to be highly vulnerable to targeted attacks. The study also concludes that using the betweenness and closeness centrality metrics for attack formulation results in the most destroying impacts on power networks. Using such information enables grid operators to make better decisions for protecting the most vulnerable nodes.

Note that the primary goal of the structural vulnerability study is finding and evaluating the network's critical nodes in addition to analyzing their removal impact on the system performance. These studies do not typically provide an attacker model. They generally assume that attackers (physically or cyber-physically) are capable of taking down the whole substation without further details[52]. Simply, when a node is removed, the associated substation is assumed to be out of service.

C. Full Power System Information Attacks

The full power system information attacks are those in which the attackers select the nodes to be attacked based on full knowledge of the power system under attack along with power system analysis techniques. By exploiting the full system information, smart attackers can maximize the attack consequences on the system with a smaller number of attacked targets. Ref. [53] evaluates the risk of hypothesized substation outages due to intrusion attack and identifies critical substations and hypothesized critical combinations for security protection planning. Due to the large number of substation combinations that exist in a power system, it is not practical to exhaustively enumerate the whole set of critical combinations. Therefore, this paper uses the reverse pyramid model (RPM), a procedure of segmentation that divides the total substations into smaller substation lists. The elimination of the combination subset is done based on the validation of power flow modules. The sorted list of substation combinations is denoted as the "bottleneck list". The substation's risk, $R(s)$, would determine the rank of each substation based on the following definition:

$$R(s)=\begin{cases}1 & ,if\ k=1\\ \frac{N_s}{N_b} & ,if\ k>1\end{cases} \tag{2.6}$$

where k denotes the number of substations in a combination. The substation risk index is one (the highest value) if there is only one substation in a combination of the bottleneck list. If there is more than one substation in a combination ($k>1$), the risk index of the substation would be the ratio of the number of combinations in the bottleneck list that contain this specific substation, N_s, to the total number of combinations in the bottleneck list, N_b . Similarly, Ref. [54] employs the RPM algorithm to find the systems' critical busbars (inside the substations). It specifically studies the risk of potential coordinated cyberattacks on substations' busbars.

Ref.[55] used a new measure called Risk-if-failure (RIF) to estimate the critical level for each node which is defined as follows,

$$RIF=\frac{P_i}{\sum_{m\in\Gamma_i}P_m} \tag{2.7}$$

where P_i is the node i′s load and P_m is the load of the nodes that are neighbors to node i. Γ_i is the set of nodes neighbors to node i. Based on this metric, the optimal victim nodes that attackers should choose to cause cascading failure can be identified. The reference compared this method with targeting nodes randomly and with targeting nodes in order of their load, and it found that RIF is more effective for identifying vulnerable nodes. However, the analysis in this work is only limited to single-node attacks.

In [56], a vulnerability assessment framework has been proposed for quantifying the risk due to two attack classifications: brute force attacks and intelligent coordinated attacks, where risk is defined as the product of successful cyber intrusion probability and its associated consequence on the power system. This consequence is measured by the amount of load being unserved following the attack. Different combinations of power system components are used to form coordinated attack pairs. The impact on the power system is estimated by load unserved after a successful attack. No methodology for identifying critical components was suggested.

2.6.3 Qualitative analysis

In qualitative risk analysis, the risk probability and impact are estimated against predefined scales. Qualitative methods are used when the level of risk is not high enough to warrant the time and efforts necessary for making a full investigation or when the existing numerical data are not sufficient for a proper quantitative analysis. They can also be used as the basis for a more detailed subsequent analysis. Examples of qualitative methods are questionnaires, structured interviews, etc.

References [57], [58] have employed both Analytical Hierarchy Process (AHP) and (N-1) contingency analysis to perform the cyber-risk assessment, including both qualitative and quantitative data. The methodology is based on a two-pass engine model. The first pass engine is responsible for finding the criticality factor for substations in a power network using a business model and a network model. The AHP was used to construct the models and link them together. No case studies are presented in those references. To find the risk index of a substation, the following steps were used:

- Load weights are calculated as

$$LW_i = \sum_i OW_i * ILL_{ij} \tag{2.8}$$

where OW is the objective weight of the business mission components and is estimated using questionnaires. And $ILL_{ij}$is the impact of the loss of the load j on the business objective i, and can be obtained from the contingency analysis. The Normalized Load Weights (NLW) are then used for ranking loads.

- Then, the substation weights can be obtained from

$$SW_j = \sum_i NLW_i * SILL_{ij} \tag{2.9}$$

where $SILL_{ij}$ is the impact of the loss of substation j on the availability of load i. The proposed substation risk index depends on the Normalized Substation Weight (NSW) and the substation vulnerability index, which considers aspects of the remote access to substation and substation components, and they evaluated it through questionnaires.

- Finally, the substation risk index can be *qualitatively* through the generating rules, such as,

  If {substation vulnerability index is Low} & {NSW is Medium} Then (substation risk index is Low}

The substations are then ranked according to these rules.

The second pass engine is responsible for computing the risk index for each asset in a substation due to cyber-physical vulnerabilities through the following modules.

- Criticality Rating

Given substation layout and physical connectivity, all the possible paths between loads and sources can be identified. The criticality of a physical component i, CR_i, is obtained from

$$CR_i = \frac{n_i}{m} \tag{2.10}$$

where n_i is the number of presences of component i in all the paths m.

- Cost

Using questionnaires on cost elements, the total cost, i.e., cost due to load loss and repair, is calculated.

- Vulnerability index

Given the automation system configuration data and its assets, an attack graph can be constructed to list the possible attack scenarios. With the help of user's answers to questionnaires on security vulnerability along with the analysis of the attack graph, vulnerability indices for all the assets and the links inside the SAS can be calculated.

- Risk computation

Using the criticality, cost, and vulnerability indices modules, substation risk can then be obtained. Risk is the product of the probability of an event and its impact.

2.6.4 Limitations of the Previous Research

It is clear from this literature review that to perform a cyber risk assessment, attacker models should be developed to select the targets of the attacks. These attack targets can be selected either in a random, topological-based, or full-information-based manner. Due to the nature of the cyber-physical attacks, the study of the cyber-based risk analysis should consider the different motivations and capabilities of attackers which directly characterize attack attributes. These attributes affect the risk probability as well as the selection criterion of the attack targets. Consequently, it is not practical to study risk analysis considering that the attack targets for different networks would only be selected randomly. Risk analysis should neither be designed based on structural vulnerabilities only. In the same way, designing mitigation plans based on risks of the full-information attacks (i.e., worst-case scenarios) may not be reasonable for the low probabilities of the organization-level or state-level attacks, as discussed in Chapter 1. Considering such nature of the cyber-physical attacks, those previous studies, taken individually, tell different parts of a larger story. To fill this literature gap, this thesis proposes a comprehensive cyber-physical risk analysis framework that considers different attacker models and investigates their associated probabilities and impacts.

2.7 Cyber Attack Detection for Digital Relays

As mentioned in Section 1.3, adaptive protection and control schemes are among the operational strategies used to enhance grid resilience. In fact, protective relays are critical

components in substation operation. With the modernization of power grids, adaptive schemes which use digital relays are becoming vital, especially for the applications of microgrids with high penetration of renewable-type DERs. Due to the growing need for deploying attack-resilient designs, there has been increasing demand for developing cyber attack detection systems for those digital adaptive relays. In [59], a comprehensive study on the cybersecurity concerns for digital relays is presented, including settings considerations. Although the existing research addressing the attack detection problem for protection systems is still limited, solutions proposed can be classified into either developing Intrusion Detection Systems (IDS) that monitor the network for malicious patterns or using Artificial Intelligence (AI) based methods employing physical properties of the power system.

2.7.1 Intrusion Detection Systems

Reference [60] proposes a rule-based IDS for cyber threats of the IEC61850-based substations. It was developed based on the collected data generated from simulated attacks on the IEDs. The detection capability is tested through genuine user activity along with simulated attacks. In [61], a probabilistic decision-tree-based IDS for the IEDs in IEC61850-based substations has been developed. Simulated attacks on IEDs have been used to obtained two types of genuine user activity (casual browsing of data and downloading IED data) and two types of common malicious IED attacks (DOS and password crack attacks). Ref. [62] performed a systematic extraction of intrusion events within a substation for its proposed detection method. Different scenarios —including single and multiple attacks on more than one substation— are simulated in this work.

The methods above can effectively identify some cyber attacks against IEC 61850 and IEDs by investigating the footprints of the attacker's logs. However, they are not able to detect new or previously unknown cyberattacks. Therefore, after installation, they will require additional maintenance effort to keep their signature database updated.

2.7.2 Artificial-Intelligence-Based Methods Using Physical Properties

In addition to previously unknown attacks, False data injection (FDI) and Man-in-the-middle (MITM) attacks can target the payload of communication packets. Hence, sensor readings or relay settings, or CB statuses can be modified to cause undesired actions without being noticed. The detection of such complex attacks is better recognized using advanced data analytics with the help of power system properties.

In [63], a deep-learning-based detection system has been proposed, which was trained using voltage and current measurements resulting from the simulation of different types of faults. In this way, the proposed detection system is able to detect the maliciously injected voltage and current measurements. Reference [64] proposes a new model for cyber attack detection on SAS by utilizing criteria from both cyber and physical domains. The method uses protection coordination principles to help check the changes in protection settings. It also runs real-time power system analysis to assess the consequences of the control commands. This method can protect against sensor data injection and direct circuit breaker control attacks. In [65], an artificially Intelligent-expert-system-based model has been used for characterizing the power system in a multi-agent microgrid security framework. The model can detect malicious and erroneous CB switching commands. Reference [66] used physical limitations to help the Network Intrusion Detection System (NIDS). The proposed IDS keeps

monitoring and analyzing the network traffic exchanged within the physical system. It identifies traffic that deviates from the expected communication pattern or physical limitations. Its physical limitation is basically done by setting a predefined range for the pickup current of the instantaneous overcurrent; hence, anything outside this range will be considered malicious.

2.7.3 Adaptive Schemes for Digital Protective Relays

Designing a reliable protection scheme for modern grids is challenging because short-circuit current levels keep changing with DG units being connected/disconnected at any given time [67]. Each DG's contribution is based on its location, size, and generator type. The fault current contribution from synchronous-based DGs is much higher than the fault current contribution of inverter-based DGS (IBDGs). As a result, a high-penetration levels of DGs will affect the settings and coordination of protective devices, especially for the islanded microgrid cases [68].

Such consequences add to the complexity of the relays' detection and selectivity capabilities. They can result in the loss of some generators and loads when there is an unnecessary operation of some relays. These consequences, in turn, impair the protection system's basic requirements, thus degrading the power system performance as a whole [69].

To overcome those protection problems, several solutions have been proposed. A review of these solutions was carried out in [5], with a discussion of the practical limitations of each. That discussion concluded that adaptive protective relays are a promising solution [70]–[76] due to their flexibility in modifying both relay settings and characteristics online using external signals [77]. In the literature, the techniques used in adaptive relays differ. First, some schemes suggest sending the network status (DGs connected/disconnected, network configuration, etc.) to the relay through communication. Then the relay itself calculates the appropriate settings for each case [70]–[72]. The drawback of this technique is the time delay arises while the relay calculates the settings because grid protection applications are time-sensitive. Second, other schemes propose calculating different settings offline and pre-storing them in relays. The relay should match the real-time scenario, based on the network status received through communication, with the pre-stored data to get the appropriate settings, as used in [73]. However, it is not realistic to get and establish a manageable number of relay setting groups that could cover all possible scenarios in the network [74]. Third, to overcome the drawbacks of the previous approaches, an alternative approach is adopted [74]–[76], whereby an updated setting that fits the exact existing situation is sent directly to the adaptive relay. However, the problem of compromising these settings due to the cyber vulnerabilities of the smart grids is still a matter of concern.

While the use of physical properties helps detect unknown kinds of attacks, they are usually used to help the IDS. However, to the best of our knowledge, none of the existing methods address the problem of detecting the compromised settings for the adaptive relays with online updated settings. This work tries to fill this security gap by developing a detection tool that can be built into microprocessor-based relays to check the incoming settings against data integrity attacks, as explained in Chapter 4.

2.8 Critical Load Restoration Problem Formulation

Optimal reconfiguration and DG Islanding are among the grid-enhancing strategies, as mentioned in Section 1.3, especially for the fast restoration of critical loads. Critical-load restoration is one of the main objectives of power system resilience [29],[30], as discussed in Section 1.4.3. Although the existing research employing DGs for critical-load restoration after disruptive events is still limited, this section attempts to discuss and classify the existing literature. Different problem formulations have been adopted in the literature to the model reconfiguration problem. By controlling the tie switches, multiple microgrids, each with one DG, can be formed by solving an MILP problem. The ultimate goal is to maximize the number of loads to be restored, weighted by their priority levels, while guaranteeing that each microgrid is a self-adequate system. Several objective functions have been proposed in the literature subject to different network constraints for realizing this goal.

2.8.1 Objective Function

In [29], [78]–[83], the objective function used is to maximize the total weighted sum of loads picked up after disruptive events.

$$\max \sum_{i \in v} \omega_i P_{L,i} \tag{2.11}$$

where ω_i denotes the priority weight associated with the load at bus i.

In [84] and [85], The restoration objective is to maximize the cumulative service time of microgrids to loads weighted by their priority,

$$\max \sum_{i \in Z_{uni}} t_i c_i \tag{2.12}$$

where c_i is a weighting factor assigned to each load such that the amount of critical load to be picked up is maximized and the amount of non-critical load to be energized is minimized.

In [86], using a multi-criteria decision-making method, called PROMETHEE-II (introduced in [87]), each restoration path is assessed based on the values of three objective functions. First, the restoration paths between each DG and critical loads are found such that each path starts from one DG and ends with one or more critical loads. Then, the value of the three objective functions —the amount of restored energy of critical loads with priority, the time of the path preparation, and the number of switching operations— is calculated.

$$f_1(x) = f_{energy,x} = \sum_{i \in \Omega_x} c_i P_i^N \, T_i^r \tag{2.13}$$

$$f_2(x) = T_x^{res} = max\left\{ceil\left(\frac{S_x^M}{N_{fc}}\right) t_{sw}^m, S_x^R t_{sw}^r\right\}, \quad x \in path \tag{2.14}$$

$$f_3(x) = n_{ops}, x \in path \quad (2.15)$$

Finally, the best paths can be selected based on the values of the objective functions using the PROMOTHEE-II method.

In [29], the restoration model during a disruptive event aims to optimize the restoration reliability and restoration duration of the system's critical loads while aiming to restore a maximum number of critical loads for a given event condition. In [88], in addition to the primary objective of maximizing the total energy supplied to the critical loads weighted by their priority, another objective has been considered that minimizes the expectation of average voltage variation of critical loads during restoration. The two objectives can be expressed as,

$$Max \sum_{c \in C} W_c P_c^N T_i^R \quad (2.16)$$

$$Min \;\; E[\frac{1}{|C|} \sum_{c \in C} (\overline{V_c} - V_c^N)^2] \quad (2.17)$$

In [83], two objectives functions have been utilized. The first one is maximizing the number of critical loads, while the second is minimizing the restoration time.

$$\min \sum_{\forall k} \sum_{\forall t} t(S_{k,t} - S_{k,t-1}) w_k \quad (2.18)$$

In [89], in addition to maximizing critical loads restored, the minimum number of switches' operations was also considered.

$$Min\, n_{ops} \quad (2.19)$$

2.8.2 Constraints

Different types of constraints are proposed in the restoration problem's literature. They can be classified into operational and network constraints. Operational constraints include:

- **Bus Voltage Limitation Constraint** [49]–[54], [56], [58], [59]

  Steady-state bus voltages should be maintained within acceptable operating limits.

$$V_{min} \leq V_u \leq V_{max}, u \in \Omega \quad (2.20)$$

- **Branch Current Limitation Constraint** [80], [81], [84], [86]

  Branch currents should not exceed their limits.

$$I_l \leq I_{max,l} \ , l \in L \tag{2.21}$$

- **DGs Capacity Constraints** [29], [78]–[82], [84], [86], [88], [90]

The total power consumption of loads to be restored should not exceed the limit of DG power capacity, represented by:

$$\sum_{d=1}^{Nl} P_d \leq \sum_{j=1}^{NG} P_{Gj} \tag{2.22}$$

$$\sum_{d=1}^{Nl} Q_d \leq \sum_{j=1}^{NG} Q_{Gj} \tag{2.23}$$

- **Feeder Capacity Constraints** [29], [79]–[81], [86], [90]

A total load of each feeder should not exceed its capacity

$$P_k^2 + Q_k^2 \leq (S_k^{Max\,T})^2, k \in F \tag{2.24}$$

Also, it is required that a total load of each feeder not exceed the maximum capacity of the supplier transformer.

- **Power Flow Constraints** [29], [78], [79], [81], [82], [86], [88], [90]

In this review, unbalanced three-phase power flow equations or the Distflow model are usually used to satisfy the power flow constraints for distribution systems.

The Network constraints are responsible for ensuring the connectivity and the radiality of the distribution network. Almost all the references stressed the importance of the radiality constraints [29], [78]–[82], [84], [86], [88], [90], but the mathematical representation is rarely reported. Some articles use the graph theory properties to ensure the radiality condition, such as in [79], [80], as well as the work in this thesis. A summary of the literature review on the reconfiguration problem formulation is presented in Table 2.1.

Table 2.1 Summary for the Study of Distribution System Reconfiguration after disruptive events

Ref.	Problem Type	Objective Function(s)	Voltage Limit	Current Limit	Feeder Capacity	Power Flow	DG Capacity	radiality	Model and/or Method
[84]	Single-objective	Maximizes the cumulative service time of microgrids	✓	✓	-	✓	✓	✓	Maximum coverage problem
[86]	Multi-objective	• Maximize the amount of priority restored energy • Minimize preparing time of the path • Minimize the number of switching operations.	✓	✓	✓	✓	✓	✓	PROMETHEE-II
[79]	Single-objective	Maximize the total critical loads to be restored	✓	-	✓	✓	✓	✓	Spanning Tree Search
[29]	Multi-objective	• Maximize the number of restored critical loads • Minimize the effective restoration path unavailability	✓	-	✓	✓	✓	✓	• MILP and Distflow model • Simulation and solver software
[80]	Single-objective	Maximize the total critical loads to be restored	✓	✓	✓	-	✓	✓	Spanning Tree Search
[81]	Single-objective	Maximize the service restoration to loads on distribution feeders	✓	✓	✓	✓	✓	✓	• Spanning Tree Search, Distflow model, and Software solvers
[88]	Multi-objective	Minimizing the expectation of average voltage variation of critical load during restoration	✓	-	-	✓	✓	✓	LIP, Simulation and solver software
[78]	Single-objective	Maximize the total critical loads to be restored	✓	-	-	✓	✓	✓	MILP, software solvers
[90]	Multi-objective	• Maximize the total critical loads restored • Minimize restoration time	-	-	✓	✓	✓	✓	MILP
[82]	Multi-objective	• Maximize the total critical loads restored, • Minimize the number of switching operations	✓	-	-	✓	✓	✓	Harmony Search Algorithm (HSA)

2.9 Summary and Conclusions

This chapter intends to give a background on the concept of resilience in the context of power grids, on its states, and on its types. This chapter also sheds light on the architecture of the SAS under the unified IEC61850 protocol, which will help identify the cyber threat in substations later in this thesis. After, the chapter presents a literature review of the existing research for the strategies that help enhance the grid cyber-physical resilience. The limitations of the previous strategies were also discussed throughout this chapter. The following conclusions have to be highlighted.

For the cyber-physical risk analysis studies, qualitative analyses are not accurate enough in prioritizing critical assets of the network. Critical asset rankings are crucial for subsequent planning studies, e.g., to determine which assets should be prioritized for reinforcement using the cost/benefit analysis. In addition, in these previous studies, the probability of attack occurrence has not been sufficiently explored. It was recommended to be obtained through surveys and questionnaires [57], [58], or by calculating how many times the IDSs have detected these certain kinds of intrusions previously [56], not taking into account zero-day attacks. The probability is sometimes completely ignored in the analysis, and the risk index is thus defined as the expected value of the impact with respect to the number of simulation iterations [43], [44]. Also, for the impact quantification, only the direct impact of the event is considered ignoring operational constraints, which, in some cases, result in equal or higher impacts; hence it is not a valid assumption to overlook their contribution. Such limitation in the literature should be handled in the analysis along with the selection strategy of the targeted assets discussed in Section 2.6.4.

From the literature review, we also conclude that adaptive protection schemes are vulnerable to cyber attacks due to the limited overhead of the protocols used for these applications that hinders the application of proper cyber defense techniques. Those kinds of schemes are becoming vital for smart grids, especially for the applications of microgrids with high penetration of renewable-type DERs. This work tries to fill this security gap by developing a detection tool that can be built into microprocessor-based relays for checking the incoming settings against data integrity attacks with high detection capabilities and low execution time, as will be explained in Chapter 4.

For the load restoration in post-attack networks, we have concluded from the literature review that some existing studies attempted to restore the out-of-service loads by clustering the network and supplying the maximum number of loads only using available DGs, while others argue that the DGs can only supply loads for a certain period of time depending on the required demand. These researchers cluster the network and restore only critical loads. This thesis attempts to reconnect the largest portion of the out-of-service network back to the main grid. In this way, the maximum number of loads can be supplied from a reliable source. Because, in some cases, we cannot restore the whole (or some parts of the) disconnected portion back to the main grid, the algorithm would form a minimum number of clusters out of this unrestored part of the network for supplying critical loads for such cases. The algorithm will be developed and investigated in Chapter 5.

Chapter 3: Cyber-Physical Risk Assessment Framework for Modern Power Grids

3.1 Introduction

This chapter presents a comprehensive framework of the cyber-physical risk analysis as an important grid resilience-enhancement strategy for boosting the system preparedness, refer to Figure 1.3. Substation threats and vulnerabilities are investigated. The probability of attack occurrence is analyzed. Then, different attacker models are proposed for each attack type. The physical impacts of each kind of attack are measured to get risk indices used for identifying the critical assets in the network.

3.2 Risk Assessment Methodology

This section discusses the approaches proposed for the risk assessment study in this research. Basically, four elements are used to outline the risk assessment methodology [91]:

i. Risk assessment approach
ii. Analysis approach
iii. Explicit risk model
iv. Risk assessment process

3.2.1 Risk Assessment Approach

Risk assessments can be conducted either qualitatively or quantitatively, as discussed in Chapter 2. In our model, we employ a quantitative approach since numerical values are needed to rank the critical elements in the network, and thus more suitable for the objective of our system risk assessment study.

3.2.2 Analysis Approach

Three approaches are used for the analysis: threat/attacker-oriented, asset/impact-oriented, or vulnerability-oriented approach. All of them consider the same risk factors yet their orders within the analysis process are different. The order of analysis affects the level of details given to each risk factor. Our work adopts a threat/attacker-oriented model since it

emphasizes attack sources, distinguishes between attacker types, and identifies attacker motivations and capabilities to assess the risk.

3.2.3 Risk Model

It defines the risk factors to be analyzed and the relationships among them. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk factors typically comprise threat, vulnerability, likelihood, and impact. Risk factors will be decomposed into detailed attributes, as shown in the rest of this chapter. Figure 3.1 illustrates the attack graph-based risk assessment model used in this work.

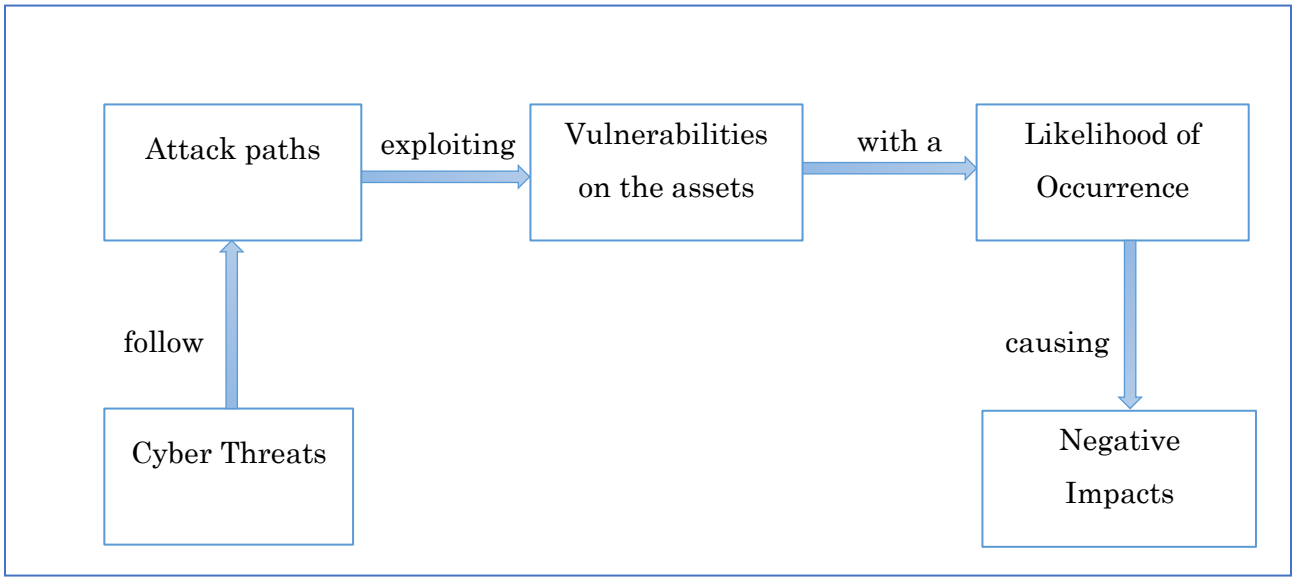


Figure 3.1 Proposed Risk Assessment Model

3.2.4 Proposed Risk Assessment Process (CPRA Framework)

The National Institute of Standards and Technology (NIST) has published a standard guide for conducting a cybersecurity risk assessment that can be found in [91]. Based on these guidelines, in this thesis, a framework is specifically tailored to fit the needs of the Cyber-physical Risk Assessment (CPRA) for modern substations with the scope aligned to the enhancement of the cyber resilience of power grids. The proposed framework principally comprises three stages of the assessment process: system characterization, risk factor identification and analysis, and risk evaluation, as depicted in Figure 3.2.

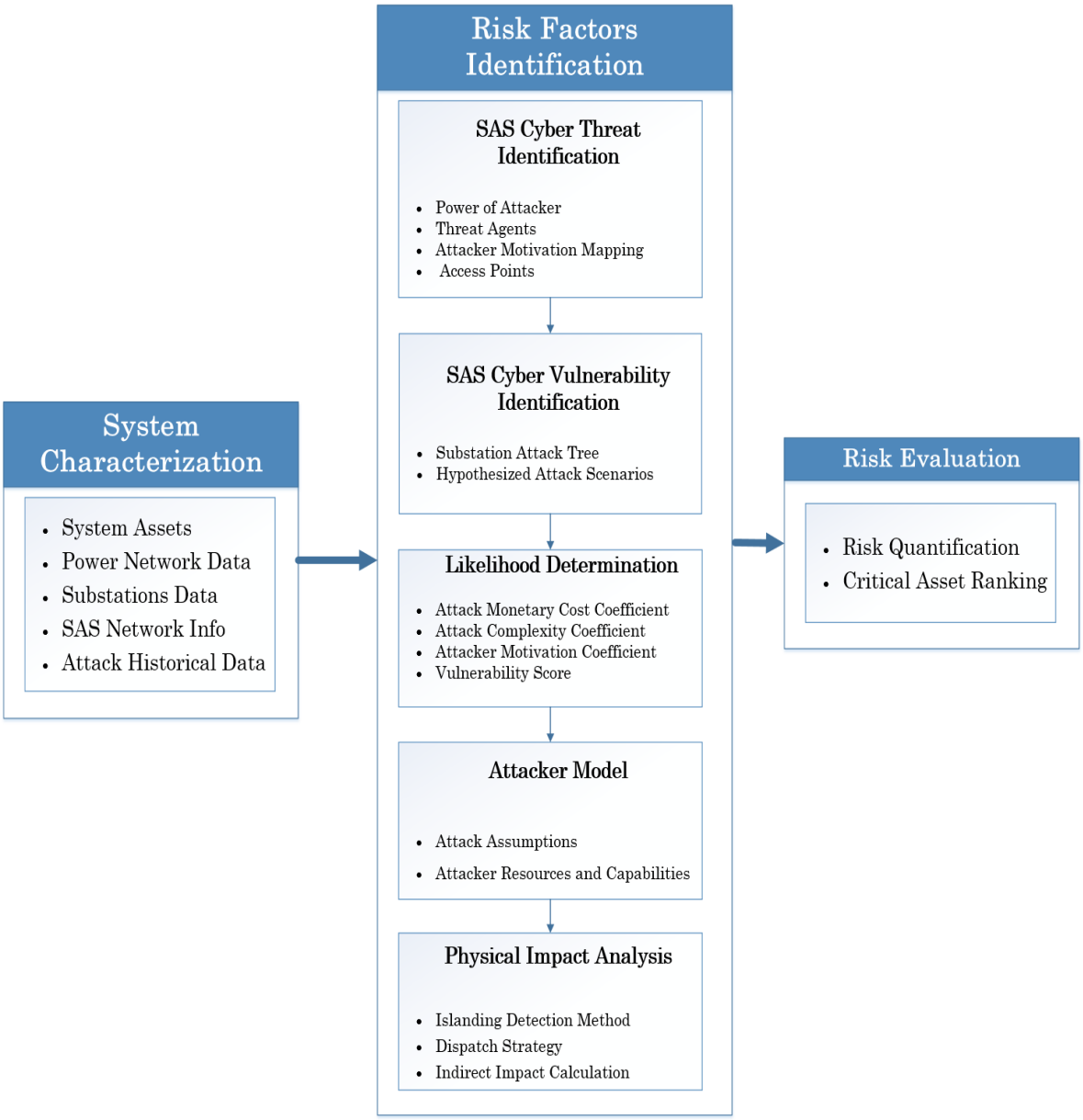


Figure 3.2 The Proposed CPRA Framework

3.3 Stage 1 – System Characterization

System Characterization is the process of identifying and gathering the information of system assets and objectives to gain a reasonable understanding of how the system operates and how it can be degraded. This information represents the inputs of the risk activities that will be analyzed in the next stage. They can be listed as follows:

i. System assets (for both cyber and physical systems).
ii. Power network data: network topology, element data, load types, etc.
iii. Substations' data: substation type, protection schemes, relay settings, number of circuit breakers, etc.
iv. SAS Network info, including the data that help construct the attack trees and look up the vulnerability scores of the devices.
v. Historical data of system attack incidents, which are needed by security experts and Subject Matter Experts (SMEs) to estimate some attacker attributes.

3.4 Stage 2 – Risk Factors Identification and Analysis

Threats, vulnerabilities, likelihood, attacker models, and physical impacts are the factors that will be used for risk assessment. Each of them decomposes into more detailed characteristics to effectively determine the risk.

3.4.1 SAS Cyber Threats Identification

The cyber threats that could target the physical system's elements (the disconnection of lines or substations as assumed in this work) through the cyber network are enumerated through two main tasks. The first task is related to the attacker itself and encompasses attacker profiles and motivations. The second is responsible for identifying all the access points to the SAS to capture all internal and external threat sources. These tasks are investigated in the rest of this section.

D. Power of Attacker

Essentially, in cyber-based risk assessments, the "power of attacker cannot be overlooked. According to the ANSSI classification (French Network and Information Security Agency, "Agence nationale de la sécurité des systèmes d'information"), power of attacker is designated as shown in Table 3.1.

Table 3.1 Power of Attacker

Level	Designation	Description/Example
1	Not-targeted	The victim is not determined, but the target is to infect as many devices as possible. (e.g., Viruses, worms)
2	Hobbyist	Individuals with very limited means, not necessarily intending to cause harm
3	Isolated Attacker	Individual or organizations with limited means, but with a certain determination
4	Private Organization	Organizations with substantial means (e.g., unfair business practices)
5	State Organization	Organizations with unlimited means and very strong determination

Based on the understanding of the levels of the power of different attackers, the attacker profiles can be specified.

E. Attacker Profiles

Profiles define templates or classes of attackers. The following six attacker profiles are selected from the collections of attacker profiles in the literature based on their relevance to the nature of cyber threats of power grid applications.

- ***Basic users/script kiddies***
  Threat agents*: unstructured hacker, hobbyist*

They are unskilled individuals who typically use tools (programs, scripts, etc.) that other people have developed for launching attacks.

- ***Insider attackers***
  Threat agents: *Disgruntled employees/contractors, Dishonest employees, Social engineering victims, Poorly-trained or careless employees.*

These are attackers who have authorized system access. Different employment positions provide different system access privileges (e.g., guest user, standard user, supervisor, administrator). Privilege allows users to access certain applications, override specific security restraints and may offer more elevated capabilities such as shutting down systems, configuring networks or devices, configuring users' accounts, etc. Thus, each user privilege is

directly related to the level of damage the attack can cause. Insider attacks are particularly more severe than external attacks because

- attackers already have authorized access,
- they can be aware of network topology and policies/procedures used, and
- establishments usually invest more in protection against external attacks.

- *Hacktivist*

  Threat agents: *activist hackers such as anonymous (hacker group)*

This class of attackers uses their hacking abilities to promote an ideological or political agenda. Often related to freedom of information.

- *Cybercriminals*

  Threat agents: *structured hacker/ black hat hacker*

These are attackers with wide security knowledge and skills. They also have planning and support functions that enable them to affect a large number of victims. Nevertheless, they have moderate sophistication when compared to nation-states. This category of attackers can exploit both known and zero-day vulnerabilities.

- Cyber-terrorist

  Threat agents: *individuals or groups with (sponsored by) political, religious groups.*

Cyber terrorists are politically or religiously motivated attackers who use information technology with average resources to cause disruptions to intimidate a government or cause widespread fear. Therefore, these kinds of attacks primarily target the physical availability of the system, not taking into account the attack's stealthiness.

- *Nation-State*

  Threat agent: *attackers sponsored by a nation or state.*

This profile comprises the most sophisticated threat actors with dedicated support (resources, personnel, and extensive planning and coordination). They can be employees (or ex-employees) to a government or state organization who performs destructive cyber operations to networks of other governments or industry groups. They basically target public infrastructure systems, e.g., power grids.

F. Attacker Motivation

After identifying the potential attacker profiles, we map those attackers and their motivations in Table 3.2, wherein the attacker's motivation is classified into the following categories: monetary, curiosity, ego, revenge/anger, unintentional error, ideological /political, notoriety, and knowledge.

Table 3.2 Attacker Motivations' Mapping for Attacker Profiles

Attacker Profiles		Attacker Motivations							
		Monetary	Curiosity	Ego	Revenge/ Anger	Unintentional error	Ideological/ Political	Notoriety	knowledge
Skiddie		N	Y	Y	N	N	Y	N	N
Insider	Disgruntled or dishonest employees	Y	N	N	Y	N	N	N	N
	Poorly-trained or careless employees	N	Y	N	N	Y	N	N	N
Cyber terrorist		Y	N	N	Y	N	Y	N	Y
Professional criminals		Y	N	N	N	N	N	N	N
Hacktivist		N	N	N	Y	N	Y	Y	Y
Nation-state		Y	N	N	Y	N	Y	N	Y

G. Substation Potential Access Points

As a final step in the threat identification process, all possible threats to the targeted elements must be determined. Enumerating these threats is vital for capturing all the external and internal sources that can cause harm to the targeted assets of the SAS. Figure 3.3 depicts the substation ICT network and its cybersecurity threats sources [64], [92], [93].

According to Figure 3.3, a cyber attack can be either initiated from inside the substation network or from the outside, i.e., control center, remote access, corporate office, or another substation. The entry points can then be listed as follows,

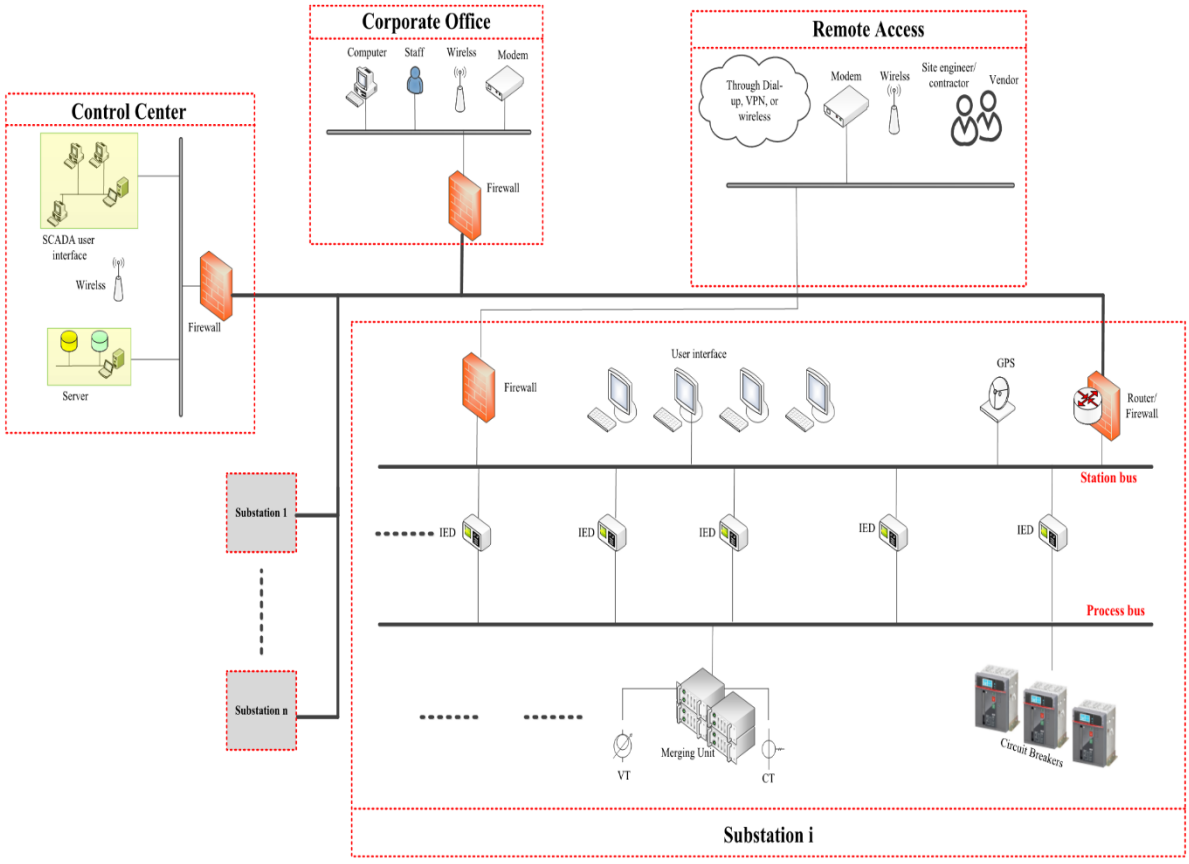


Figure 3.3 Threat Sources (Access Points) of the SAS Network

i. Attacks from Inside the Substation Network (IN)

- IN-CN: Gain access to substation cyber network (CN)
- IN-F1, IN-F2: Compromise firewalls (F)
- IN-HMI: Gain access to user interface (HMI)
- IN-B1, IN-B2, IN-B3: access bay level devices (B) #1, 2, and 3, respectively.

ii. Attacks from Outside the Substation Network

- **Via Remote Access Points (RM)**
  RM-1: remote access points through dial-up, VPN, or wireless.

- **via corporation office network (CO)**
  CO-1: Gain access to the corporate network

  CO-2: Compromise firewall

- **Via Control Center Network (CC)**
  CC-1: Compromise firewall

  CC-2: Gain access to control center network

  CC-3: Compromise the server in a control center

  CC-4: Compromise the user interface in a control center

- **Via Neighbor Substation Network (NS)**
  NS-1: Gain access to neighbor substation network

- **Via Wide Area Network (WAN)**
  WAN-1: Access wide area network

3.4.2 SAS Cyber Vulnerability Identification

Vulnerability is a weakness that attackers can exploit to gain unauthorized access (or perform an unauthorized action) to an asset. Substations have several types of cyber vulnerabilities, as discussed in Chapter 1. After identifying threat sources (access points), attack vectors and hypothesized scenarios could be established with the aid of attack trees.

A. Substation Attack Tree

An attack tree is a multi-level conceptual diagram that visualizes how an asset can be attacked. It is used to understand and analyze threats and potential attack scenarios of a targeted asset. It has one root node that corresponds to the ultimate goal (change Circuit

Breaker (CB) status in this work). Different ways (pathways) to achieve this goal are through leaf nodes, each of which is a step that contributes towards achieving the ultimate goal. Figure 3.4 is a simple example of substation attack tree with an ultimate goal of disconnecting a CB [64], [92], [94], [95].

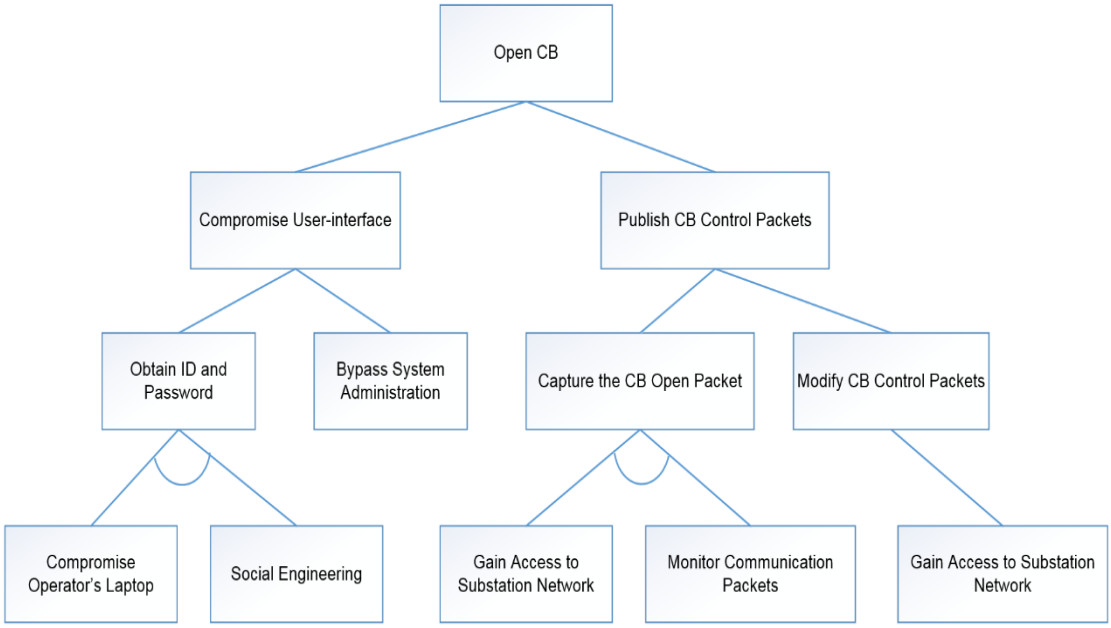


Figure 3.4 Substation Attack Tree

B. Hypothesized Attack Scenarios

Based on threat sources obtained in Section 333.4.1-*D*, along with the substation attack tree, hypothesized attack pathways can be identified. For example,

- The path (CO-1 > CO-2 > WAN-1 > IN-F2 > IN-CN > IN-HMI) corresponds to an attack which can be initiated by social engineering as a suspicious email that resulted in the infection of an employee's computer by compromising the computer (e.g., gaining access ID and password) software applications on the user interface inside the substation are compromised. Eventually, the breaker's status can be changed. This pathway is shown in Figure 3.5.

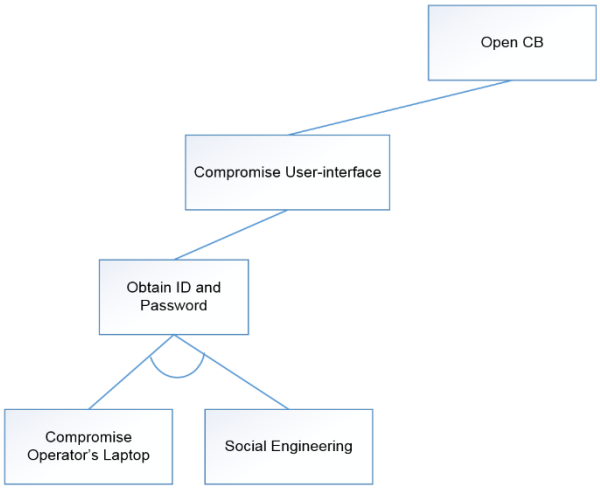


Figure 3.5 A Subtree for a Substation Attack Scenario

3.4.3 Likelihood Determination

The likelihood of cyber attack occurrence is based on " an analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities" [91]. The adversary needs to spend a set of resources for each attack. To determine these resources, risk assessors typically rely on available evidence, experiment, and the judgment of Subject Matter Experts (SMEs). Then, a simple technique to determine the likelihood of a specific attack scenario for a given adversary is to weigh the resources available to the attacker against the attack scenario's requirements.

As aforementioned, a threat-oriented approach has been employed for the analysis with the help of the attack tree for a given attacker. Also, the Probability of Attack Occurrence (*PAO*) is attacker-type-specific. For example, the value *PAO* of an attack action can be different for different attackers. Consequently, we adopt an adversary capability-based modeling approach [96]–[98] to determine the *PAO*. This approach assumes a relationship between the *PAO* of a successful attack and the attacker's resources, namely, attacker budget, attacker skills (technical abilities), and attacker motivations (including the level of determination), along with the vulnerability score of the targeted asset. Hence, a combination of these factors will be employed to assess the overall likelihood score. For the purpose of illustration, in this section, we will focus on three attacker profiles: Script kiddie (SK), Cybercriminal (CC), and Nation-state (NS).

$$PAO = C_{cost} \times C_{Complexity} \times C_{Motivation} \times C_{Vulnerability} \quad (3.1)$$

where C_{cost}, $C_{Complexity}$, $C_{Motivation}$ are attack cost coefficient, attack complexity (sophistication) coefficient, and attacker motivation coefficient, respectively. And $C_{Vulnerability}$ is the standardized asset's vulnerability score.

A. Attack Monetary Cost Coefficient

The total monetary costs required for each attack action in the attack tree is first assessed. For example, if a leaf node action needs the attacker to obtain a specific device, the device cost can then be determined by its market price [96]. Another example, for the action of developing a malicious code, the total cost can be estimated as 16276$ calculated as follows: buying a platform to develop a malware costs $700, developing the malware costs $15576 (3 months x 22 working days/month x 4 hours/day x $59 developer salary/hour) [97].

The larger the attacker's budget (with respect to the attack cost) is, the more possible (desirable) the attack is (to the threat agent). Based on the publicly available information, reference [97] assigned the following attacker budgets to different attackers: 1,500$ for SK, 30,000$ for CC, and 100,000$ for NS. Based on Equation (3.2), we can map the attack cost to the cost coefficient using Figure 3.6. For the example of developing the malicious code, the cost coefficients would be 0.092, 1.0, 1.0 for a Skiddie, CC, and NS, respectively.

$$C_{cost} = \begin{cases} \dfrac{Attacker\ Budget}{Attack\ Cost}, & Attacker\ Budget < Attack\ Cost \\ 1, & Otherwise \end{cases} \tag{3.2}$$

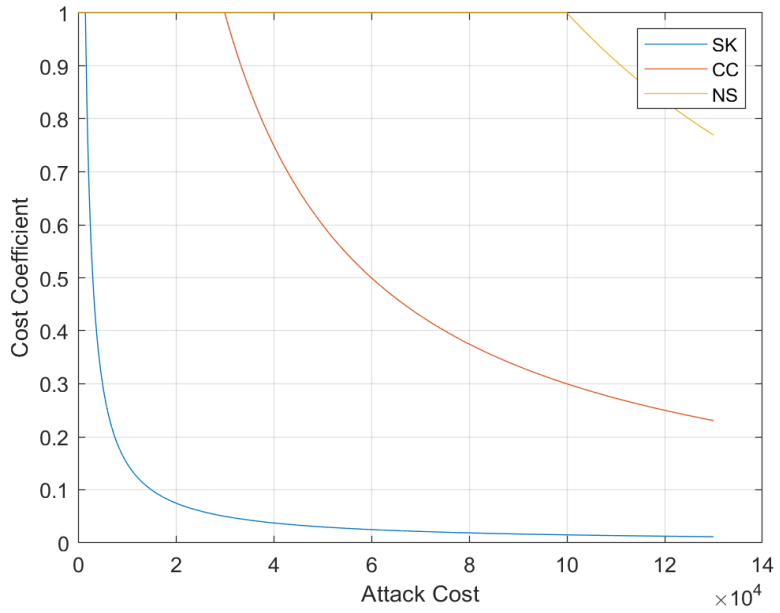


Figure 3.6 Attack Cost Coefficients for Different Attackers

B. Attack Complexity Coefficient

The technical ability ratings of the leaf nodes in the attack tree are determined. For each attack scenario, the technical ability of different nodes would be the one with the higher rating. Experts and analysts submit a technical ability scale related to IT exploits, as shown in Table 3.3.

Table 3.3 Attacker's Technical Ability Scale [96]

Range	Description
1-10	No technical skills
10-20	Average computer user (e.g., office employee)
20-30	Script kiddie
30-40	A user professionally trained in IT
40-50	Senior IT user (e.g., Programmer, senior network administrator)
50-60	Senior IT User with research facilities
60-70	World-class expert
70--80	Practically impossible, theoretically possible
80-90	Believed to be impossible
90-100	Provably impossible

Based on the technical ability scale, the following attacker capabilities are assumed: 20, 40, and 80 for SK, CC, and NS, respectively. The complexity coefficient denotes the probability that an attacker can launch an attack of specified complexity. For coefficient determination, similar mapping curves are obtained in

Figure 3.7 for each attacker type using Equation (3.3) to find the attack complexity coefficients.

$$C_{complexity} = \begin{cases} \dfrac{Attacker\ Capability}{Attack\ Complexity}, & Attacker\ Capability < Attack\ Complexity \\ 1, & Otherwise \end{cases} \quad (3.3)$$

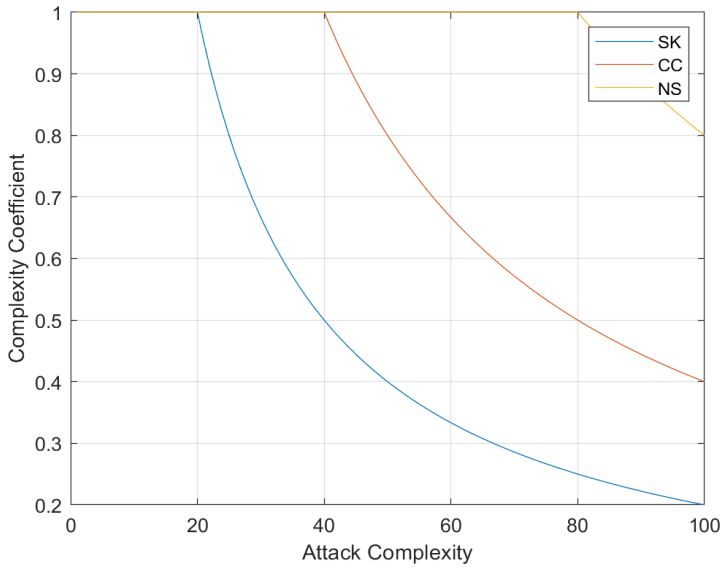


Figure 3.7 Attack Complexity Coefficients for Different Attackers

C. *Attacker Motivation Coefficient*

Attacker motivation is principally associated with attacker type. With the help of the data in Table 3.1 and Table 3.2, the attacker motivation coefficient will be classified into five bands given in Table 3.4.

Table 3.4 Suggested Scores for Attacker Motivation

Rating	Description
0.1-0.2	Very Low
0.2-0.35	Low
0.35-0.5	Medium
0.5-0.7	High
0.7-1.0	Very high

D. *Vulnerability Score*

Vulnerability assessment of a targeted asset is essential to analyze attacks that directly target that asset. The Common Vulnerability Scoring System (CVSS) provides standardized vulnerability Scores needed for evaluating the severity of security vulnerabilities. All the analysis and vulnerability information are recorded in the NIST National Vulnerability Database (NVD), which provides the CVSS scores for all known vulnerabilities. The CVSS calculator V3.1 is available online [99].

3.4.4 Physical Impact Analysis

The physical impact analysis investigates the consequences that can be caused by a successful cyber attack from the power system perspective. In this work, we assume two possible attacker actions:

i) Targeting a substation: all lines, generators, loads, capacitors, and/or transformers connected to this substation are disconnected.
ii) Targeting a line: the attacked line is not in service and will be disconnected from the network.

Following an attack, the network topology needs to be updated. The new topology is then used to measure the level of harm resulted from the attack occurrence. In this thesis, the Overall Interrupted Load ratio, *OLI*, is used to measure the physical impacts and can be defined as the amount of total power of the loads that will be interrupted (unserved) due to the consequences of the failure of the attacked target(s). It can be defined as

$$OLI = 1 - \frac{\sum_{i=1}^{N} P_{L,i}^{LC}}{\sum_{i=1}^{N} P_{L,i}^{BC}} \tag{3.4}$$

where P_i^{LC} is the active power of the load that remains connected after disruption of node i. $P_{L,i}^{BC}$ is the active power of the load connected before disruption, i.e., in the base case. The ratio OLI can be decomposed into two components: direct interrupted load, LI_{Direct}And indirect interrupted load, $LI_{Indirect}$. The direct interrupted load, as the name suggests, is the amount of load that will be interrupted since it is directly connected to the node(s) being attacked, whereas the $LI_{Indirect}$ is the amount of load that will be interrupted due to the operational constraints of the post-attack network. First, after removing the failed attacked elements, the network may be split into several subnetworks. The generation capacity in each subnetwork should be higher than the load supplied. That might result in some loads to be shed, thus indirectly interrupted. Also, the new topology might cause the limits of the flows in the lines to be exceeded, which will also result in some load shedding, adding up to the indirect interrupted load component. Thus, the OLI can also be expressed as,

$$OLI = LI_{Direct} + LI_{Indirect} = \frac{\sum_{i=1}^{N} P_i^{LD}}{\sum_{i=1}^{N} P_{L,i}^{BC}} + \left(\frac{\sum_{i=1}^{N} P_i^{LE} + \sum_{i=1}^{N} P_i^{LS}}{\sum_{i=1}^{N} P_{L,i}^{BC}} \right) \tag{3.5}$$

where P_i^{LD} is the active power of the load directly disconnected, P_i^{LE} is active load shed due to insufficient generation in each subnetwork, and P_i^{LS} is the load shed to satisfy the line flow constraints. The following subsections discuss the islanding detection algorithm and the power dispatch method used.

A. Islanding Detection Technique

The system's topology can be affected if the network is disconnected and separated to m sub-network due to the attack. The effect is modeled according to the following rules:

Let G be the graph for the post-attack network where $G = (N, E)$, N is the set of nodes (substations), and E is the set of edges (lines). Then, to find the number of subnetworks, S, evolved after removing the victim elements, we use the algorithms shown in Figure 3.8 based on the Depth-First Search (DFS) algorithm.

```
Initialize all nodes as not visited
For every node 'N', Do
       If 'N' is not visited, Do
              Call DFS(N)


DFS(N)
       Mark 'N' as visited
       For every adjacent node 'M' of 'N', Do
       If 'M' is not visited, Do
       Recursively call DFS(M)
```

Figure 3.8 Pseudocode of Islanding Detection Algorithm

B. Power Dispatch Strategy

After the failure of the attacked substation(s), some generators or loads may be disconnected from the network, causing an energy imbalance between the generation and consumption. Therefore, there is a need for re-dispatching the generation or the demand in each subnetwork to satisfy the operational and power flow constraints. In case the generation is higher than the demand, the decrease of the i^{th} generator's output, $\Delta P_{G,i}$, can be expressed as,

$$\Delta P_{G,i} = \frac{P_{G,i}^{0} \times \left(\sum_{i \in N_G} P_{G,i} - \sum_{j \in N_L} P_{L,j}\right)}{\sum_{i \in N_G^0} P_{G,i}^{0}} \tag{3.6}$$

where N_G *and* N_L are the set of generator nodes and load nodes of the subnetwork following the attack, respectively. N_G^0 is the set of generator nodes of the subnetwork before the attack event. $P_{G,i}$*and* $P_{L,j}$ are the output energy of i^{th} generator and consumption energy of the j^{th} load following the attack, respectively. And $P_{G,i}^{0}$ is the output energy of i^{th} generator before the attack event.

Likewise, the reduction in the energy of the j^{th} load, $\Delta P_{L,j}$, can be calculated as,

$$\Delta P_{L,j} = \frac{P_{L,j}^{0} \times \left(\sum_{j \in N_L} P_{L,j} - \sum_{i \in N_G} P_{G,i}\right)}{\sum_{i \in N_L^0} P_{L,j}^{0}} \tag{3.7}$$

C. Overall Impact Analysis Algorithm

Based on the aforementioned methods, the following steps should be performed to quantify the attack's physical impacts.

a. Run power flow for the base case.
b. Remove the targeted element(s) and update the network.
c. Calculate the direct load interrupted component.
d. Detect if any subnetworks are formed.
e. For each subnetwork:
    i. If the subnetwork does not contain any generator, then all the load within this subnetwork will not be served,
    ii. If the subnetwork's total generation capacity is larger than the total demand, run power flow analysis, check the line flow constraints. In case there are any violations, curtail the generation using Equation (3.6) until the violations are cleared;
    iii. If the subnetwork's total generation capacity is less than the total demand, reduce the load first to balance the supply and demand using Equation (3.7), then repeat step (*ii*).

f. Calculate the indirect interrupted load component and the overall load interrupted ratio.

D. Simulation Results and Discussion

Throughout this chapter, the IEEE 30-bus test system [100] will be used to demonstrate the application of the algorithms developed within the CPRA framework. The single line diagram of this system is given in Figure 3.9. It is a 6-generator system with generator data given in Table 3.5. the total load demand is 283.4MW, and the difference between the total power generated and demand is equal to 17.5MW (transmission losses).

In this section, the impact of one substation failure at a time is analyzed. Using the algorithm in Subsection 3.4.4, the fractions of load interrupted related to different impact's components are shown in Figure 3.10 to Figure 3.13. From these results, it is clear that the indirect load interrupted due to practical operation constraints, which is typically neglected during the analysis in previous research, is significant compared to the portion of the direct load interrupted.

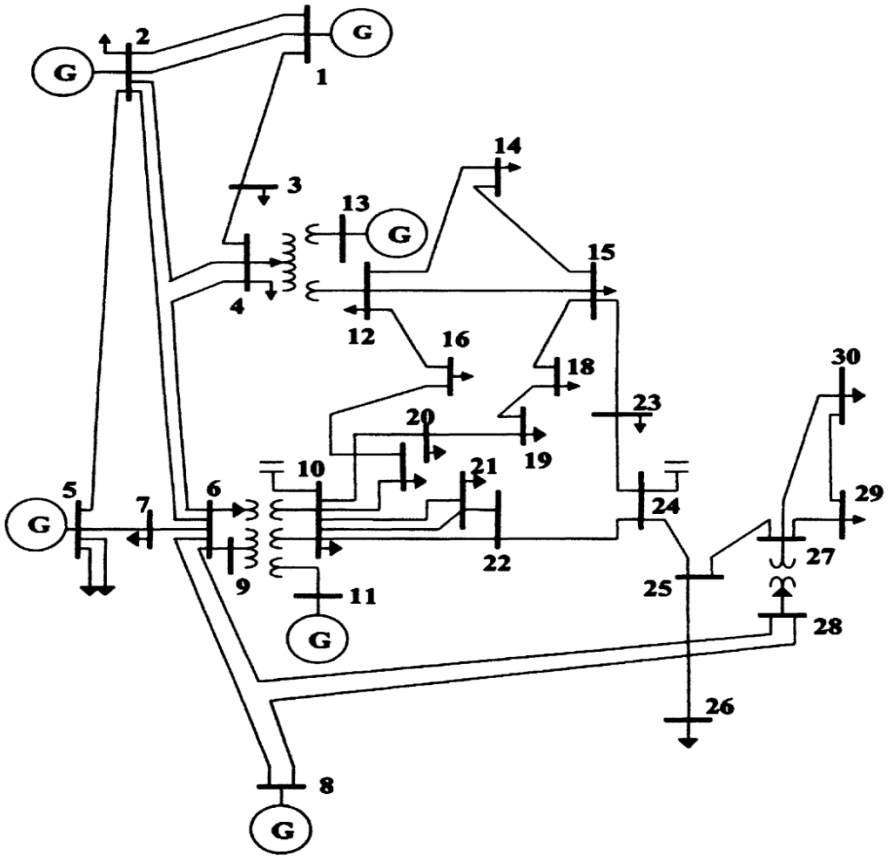


Figure 3.9 Single Line Diagram of The IEEE 30-Bus System

Table 3.5 Generator Data

Gen. ID	Bus no.	P_{Gen} (MW)	P_{Limit}(MW)
G1	1	260.9	270
G2	2	40	80
G3	5	0	50
G4	8	0	35
G5	11	0	30
G6	13	0	40

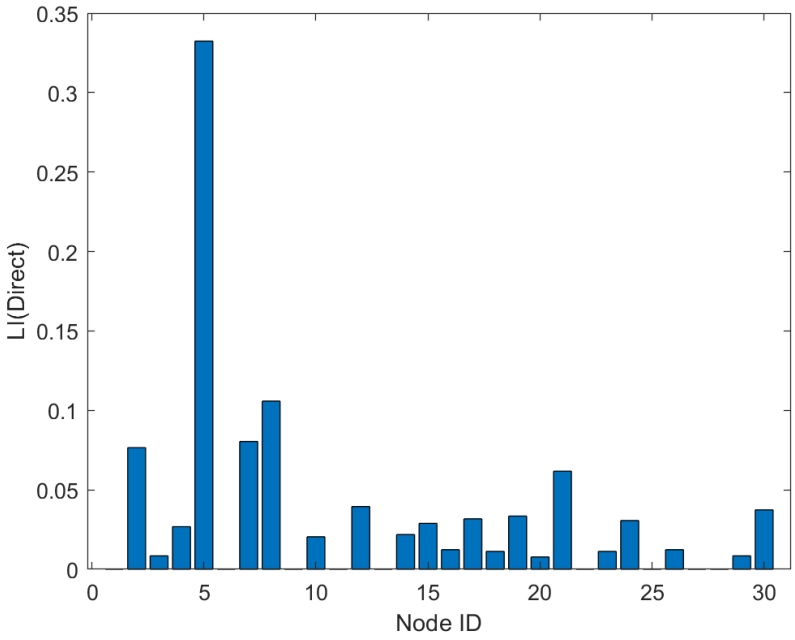


Figure 3.10 Fraction of Direct Load Interrupted

-

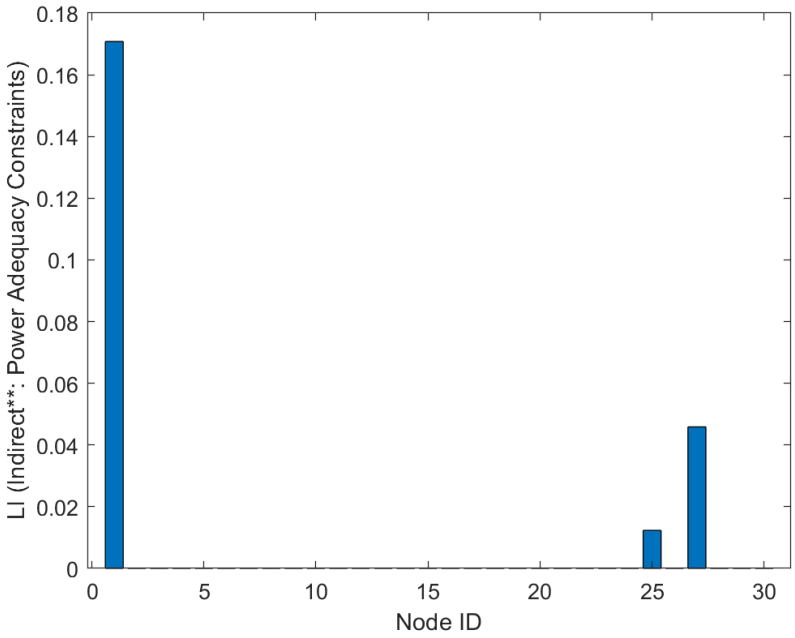


Figure 3.11 Fraction of Indirect Load Interrupted Due to Power Adequacy Constraints

-

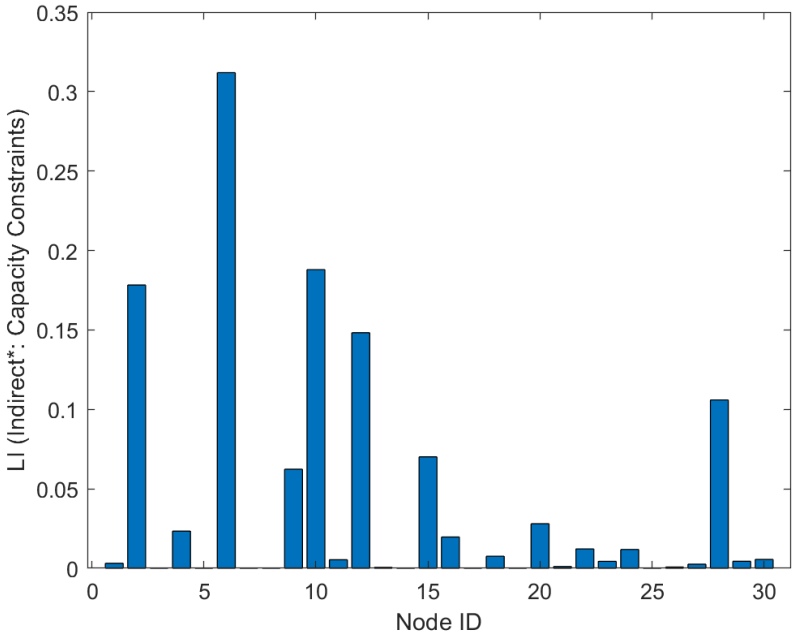


Figure 3.12 Fraction of Indirect Load Interrupted Due to Line Capacity Constraints

-

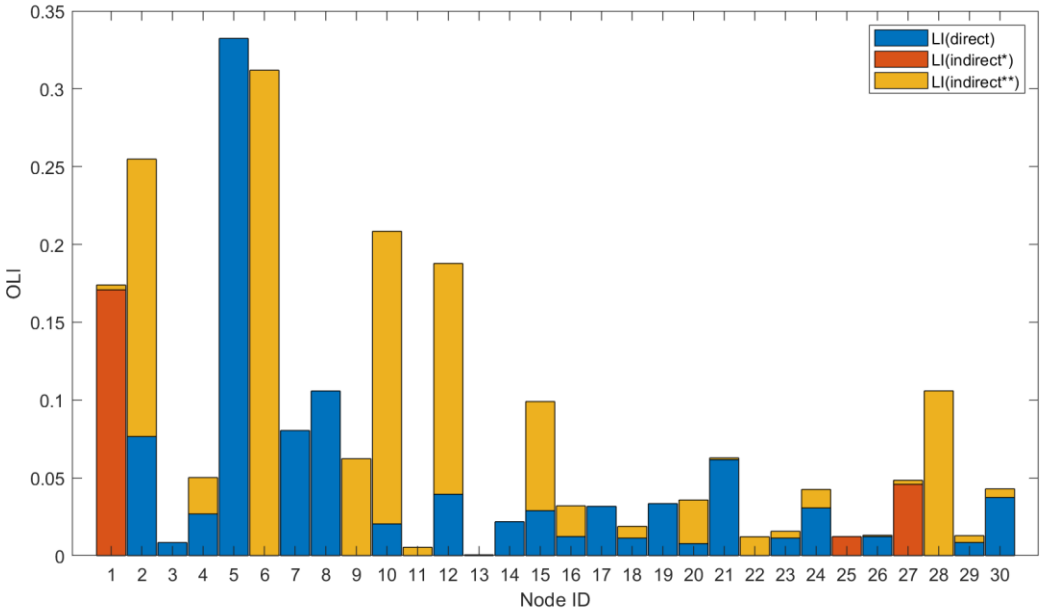


Figure 3.13 Total Load Interrupted for Individual Node Failure

When node 1 fails, generator G1 is disconnected. The total capacity of the generators in service is 235MW which is less than the needed generation by 66MW. Therefore, this portion is cut off the existing loads using Equation (3.7). Now, checking the line capacities, in this case, we found that the flows in 'Line.21-22 and Line.22-24 exceed their capacities by 92.6kW and 799.14kW, respectively. Thus, an amount of 891.74kW of power will also be cut off from the amount of load served.

On the other hand, for the case of failure of Node 25, the node itself has no direct load connected; however, Node 26 forms an island with no generators available, which results in the interruption of the load connected to this node. In this case, there are no violated line flow constraints. Finally, in case of failure of Node 27, an island will be formed containing Node 29 and Node 20, which have no generators; thus, their loads will be disconnected. An additional 735.87kW will be cut off due to exceeding the capacity limit of Line 22-24. To sum up, the results give us an idea of the impact of each individual node failure on the amount of load supplied in the network. These impacts will be used directly in this work whenever the attack formulated targets just one substation; this will be further explained throughout attacker models in Section 3.4.5.

Applying the same procedures for line removals, the *OLI* is now composed of the indirect load interruption components, as shown in Figure 3.14. While the network is interconnected, the major contribution of the interruption is due to the violation of line flows.

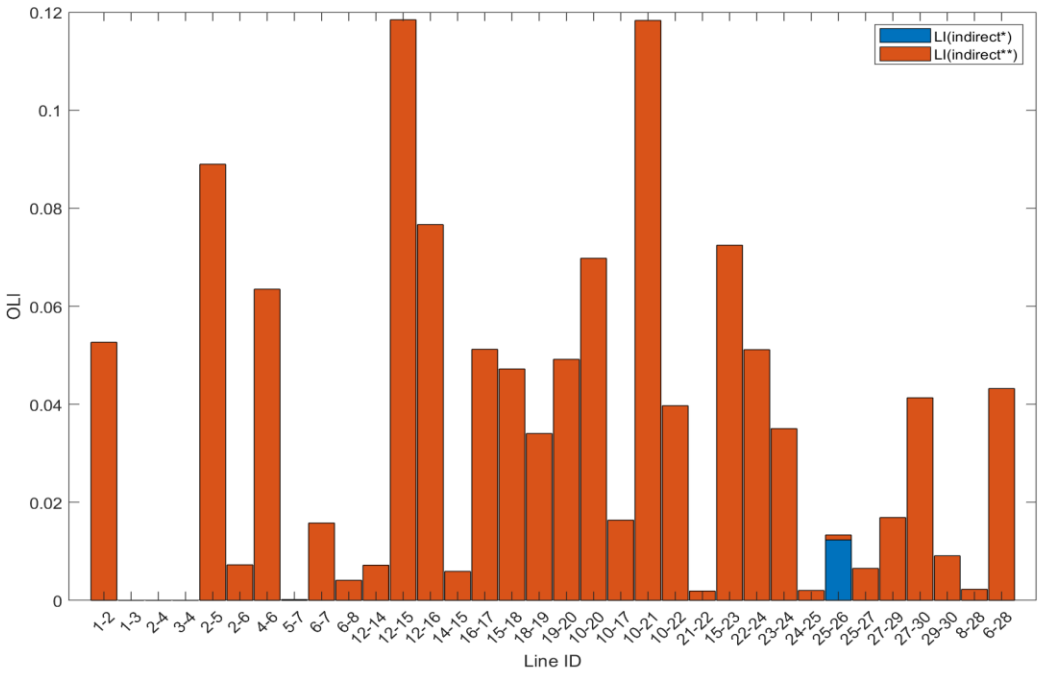


Figure 3.14 Total Load Interrupted for Individual Line Failure

3.4.5 Attacker Models

As we have seen, there are different potential attacker profiles threatening substations. However, the boundaries between these profiles are not well-defined, and sometimes it becomes challenging to assign a certain real-life attacker to just one explicit profile. Therefore, when employing attacker models in a specific study, attackers are often classified into broader groups according to the requirements of that study. Often attackers are classified into wider groups for risk analysis studies according to their attributes (resources, level of knowledge, etc.) [101]–[104]. To mimic broader types of attackers in this work, we are defining three classes of attackers: mediocre, intermediate, and sophisticated.

i) Mediocre attackers: attackers who have limited attack skills and few resources. They also have no or low knowledge about power systems. This kind might include not-targeted attacks, script kiddies, and unintentional failures. Based on these characteristics, we assume the attacker disturbs just one target. The attacker is probably irrational.

ii) Intermediate attackers: this type of attacker might mimic cyber criminals and hacktivists. They are the ones with higher intent of destruction and a moderate amount of resources. Consequently, they aim to target the relatively critical components (topologically critical) to maximize the negative consequences of the attack within their available capabilities. Given these attacker attributes, we assume that these attackers can target one or multiple substations, i.e., single or coordinated attacks. Also, we assume that they plan for their attack utilizing the topological information of the power system.

iii) Sophisticated attackers: these attackers obviously have the highest motivation and resources. They are capable both cyber-wise and engineering-wise, i.e., the attacker can gain complete access to the network traffic and use sophisticated tools. In addition, they are also capable of acquiring detailed information about the power system operation. The nation-state attackers are the best example of this group.

3.4.6 Topological-Based Attacks

Topological measures enable attackers to figure out the relatively critical components of the electrical network whenever reliable data of the network (e.g., the admittance of the transmission lines, power injection, and loads) are not available. Given the purely-topological information (generator and load nodes are unknown), a power system can be represented by a graph G, denoted as $G = (V, E)$, where V is the set of vertices (nodes), with $|V| = n$, connected by a set of edges (links), $E = \{\{i, j\}: i, j \in V, i \neq j\}$, with $|E| = m$. The adjacency matrix of the graph G is the $n \times n$ matrix $A = (a_{ij})$such that

$$a_{ij} = \begin{cases} 1, & \text{if there is an edge between vertex } i \text{ and vertex } j \\ 0, & \text{otherwise} \end{cases} \quad (3.8)$$

A. Centrality Metrics

Centrality measures are used to rank the relative importance of nodes of a graph by capturing the intrinsic topological characteristics of the network. There are several types of graph metrics the attacker can use to select the victim nodes/edges. This thesis studies three widely-used centrality metrics (in the literature) and formulates two attack strategies for each. Those metrics are degree centrality, betweenness centrality, and closeness centrality. Based on the attacks formulated, attackers can check the attack impact topologically as well. Thus, the following methodology will be used to simulate the topological-based attack.

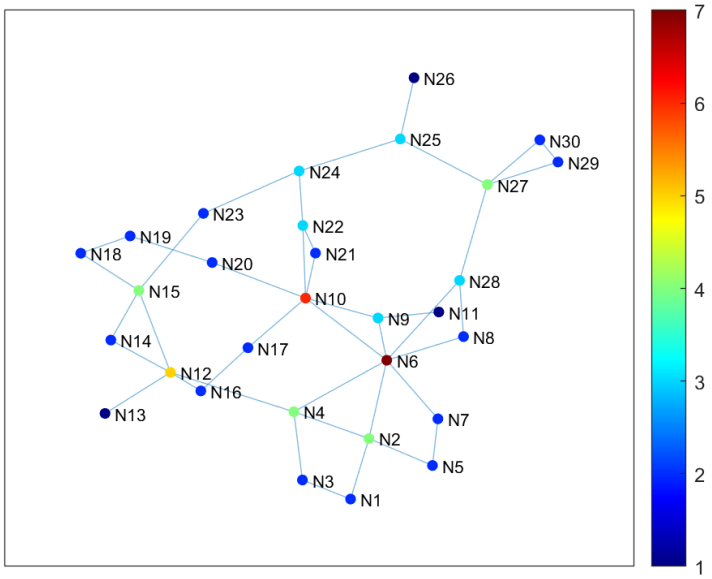
i) Calculate different centrality metrics of each node and edge in the power system under study.
ii) Formulate different node-attack and edge-attack strategies based on those centrality metrics,
iii) Analyze the impact of those attacks on the system's performance from the attacker's perspective.

- *Degree Centrality (C_D)*

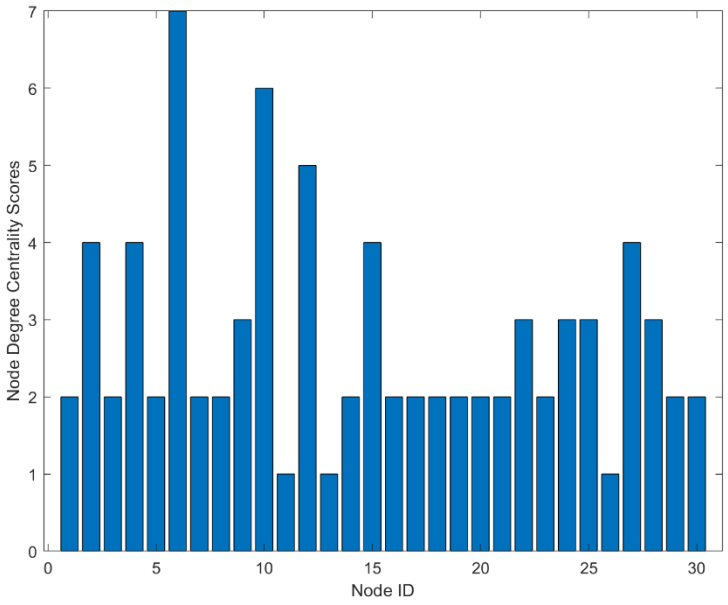
The node degree centrality (vertex degree) of a vertex v —for a given graph $G(V, E)$ with $|V|$ vertices and $|E|$ edges— quantifies the total number of edges incident to the vertex v. It can be expressed as [19],

$$C_D(v) = deg(v) = \sum_j a_{ij} \tag{3.9}$$

where the sum is over all vertices in the network. Degree centrality is perhaps the simplest centrality measure to compute yet effective. The higher the score, the more central the node is. It refers to how strategically important a node is in terms of the number of edges that will be affected by the failure of this given. Figure 3.15 gives the simulation results of the node degree centrality scores for the IEEE 30-bus system.



(a)



(b)

Figure 3.15 Nodal Degree Centrality Scores

The importance of an edge can be calculated based on the degree centrality of the two nodes it links. The edge degree centrality is defined as in [105],

$$C_D(e_{ij}) = \sqrt{C_D(i) \times C_D(j)} \qquad , i \neq j \in V, e_{ij} \in E \tag{3.10}$$

where $C_D(i)$ and $C_D(j)$ are the degree centrality scores of nodes i and j, respectively. Likewise, the edge degree centrality scores for the IEEE 30-Bus system have been calculated and presented in Figure 3.16.

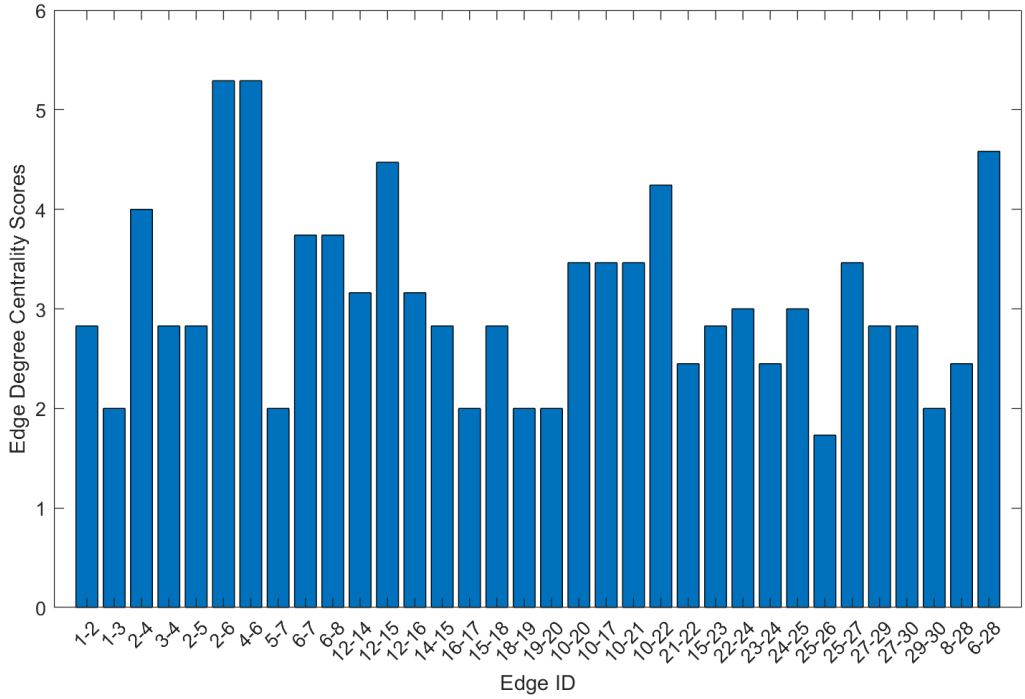


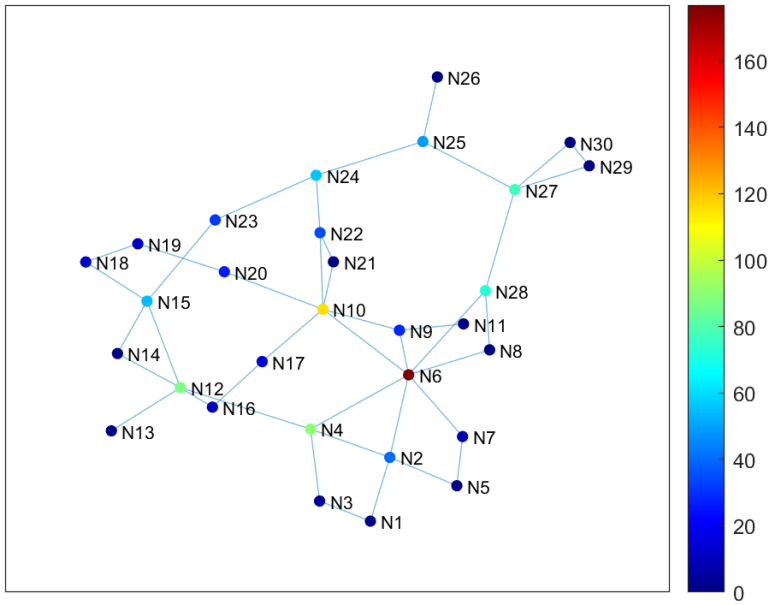
Figure 3.16 Edge Degree Centrality Scores

- ***Betweenness Centrality (C_B)***

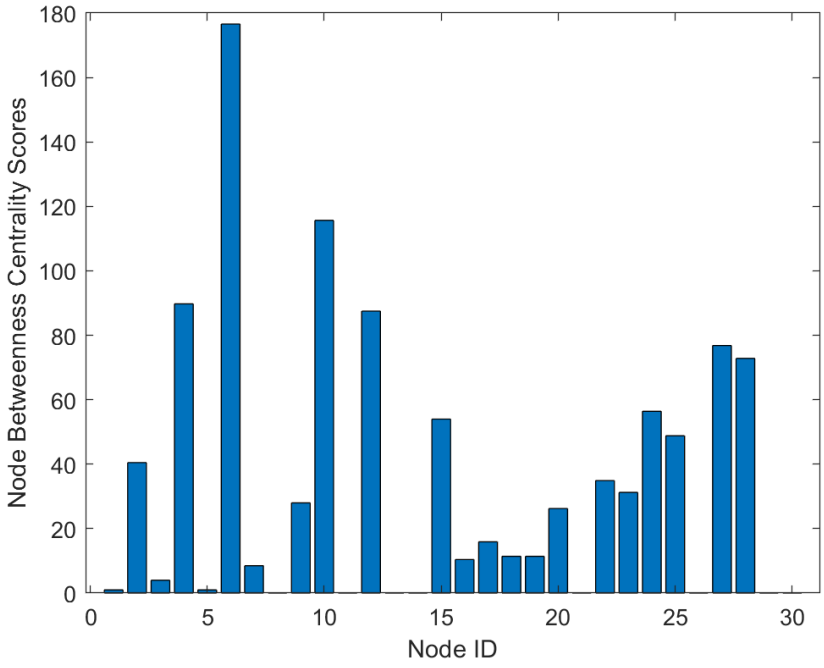
The node betweenness centrality quantifies how often each node v appears between the paths linking other pairs of nodes. Hence, it can be defined as the fraction of shortest paths passing through a node v [19].

$$C_B(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{3.11}$$

where σ_{st} denotes the total number of shortest paths from node s to node t, where $s, t \in V$. $\sigma_{st}(v)$ is the number of those paths that $v \in V$ lies on them. The node betweenness centralities of the system under study have been calculated with the help of Dijkstra's algorithm, which searches for the shortest paths between nodes in the graph. The corresponding scores obtained are given in Figure 3.17.



(a)



(b)

Figure 3.17 Nodal Betweenness Centrality Scores

The betweenness centrality measure relates the importance of a node in relation to the shortest path. Since the role of the power grid is to link generators and customers, power is assumed to be routed through the most direct path. A node with a higher betweenness value means that for certain paths, this node is critical to support the power transfer in the network. The attack or failure of this node would lead to a number of nodes being disconnected or connected via longer paths. Henceforth, the betweenness score of a substation is an indication of how much power it is conveying. Therefore, betweenness centrality is an effective measure and is often referred to as load. All in all, the betweenness centrality reflects how frequently each substation is involved in the transmission of active power.

Analogous to $C_B(v)$, the edge betweenness $C_B(e_{ij})$ of an edge $e_{ij} \in E$ is defined as the sum of the fraction of all shortest paths that pass through e_{ij} [106].

$$C_B(e_{ij}) = \sum_{s \neq t \in V} \frac{\sigma_{st}(e_{ij})}{\sigma_{st}} \quad , e_{ij} \in E \tag{3.12}$$

$\sigma_{st}(e_{ij})$ is the fraction of times edge e_{ij} lies on the shortest paths between any pair of nodes s and t and σ_{st} is the number of shortest paths from s to t that pass through the edge e_{ij}. Likewise, edge betweenness scores have been calculated for the system under study and shown in Figure 3.18.

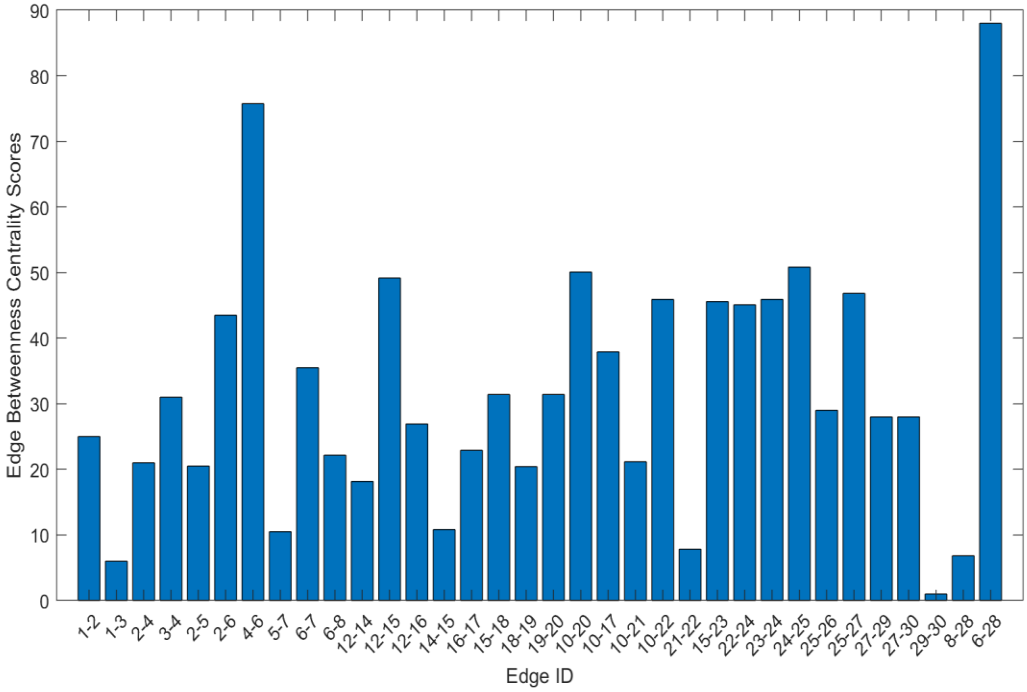


Figure 3.18 Edge Betweenness Centrality Scores

- *Closeness Centrality (C_C)*

Closeness centrality is another measure that quantifies the node importance based on the average farness from all the other nodes. It is often used in power networks to indicate how a given node removal can propagate/affect the other nodes in the system. It can be defined as the inverse of the sum of all shortest paths from a vertex v to all other vertices. It is generally given by [105]:

$$C_C(v) = \frac{1}{\sum_{i \neq v \in V} d(i,v)} \tag{3.13}$$

where $d(i,v)$ is the distance between node v and node i . It is usually referred to its normalized form which characterizes the average length of the shortest paths rather than their sum.

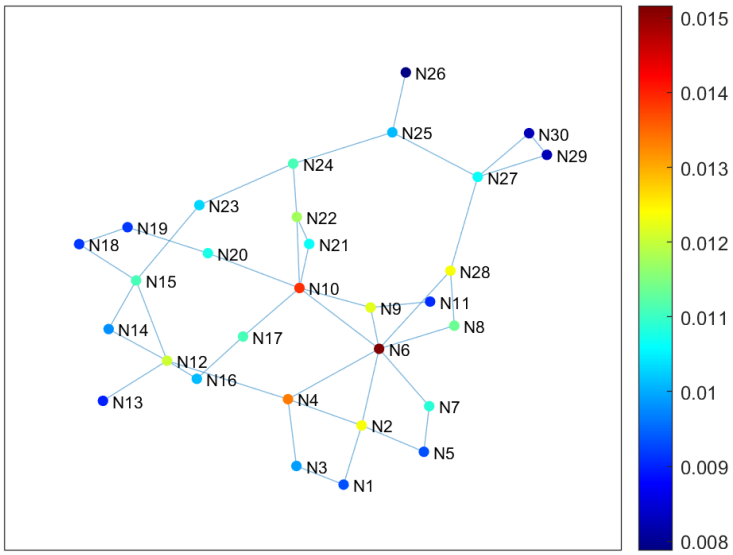
$$C'_C(v) = \frac{(n-1)}{\sum_{i \neq v \in V} d(i,v)} \tag{3.14}$$

Nodes with a high closeness score have the shortest distances to all other nodes. Node closeness scores have been obtained, and the results are given in Figure 3.19.

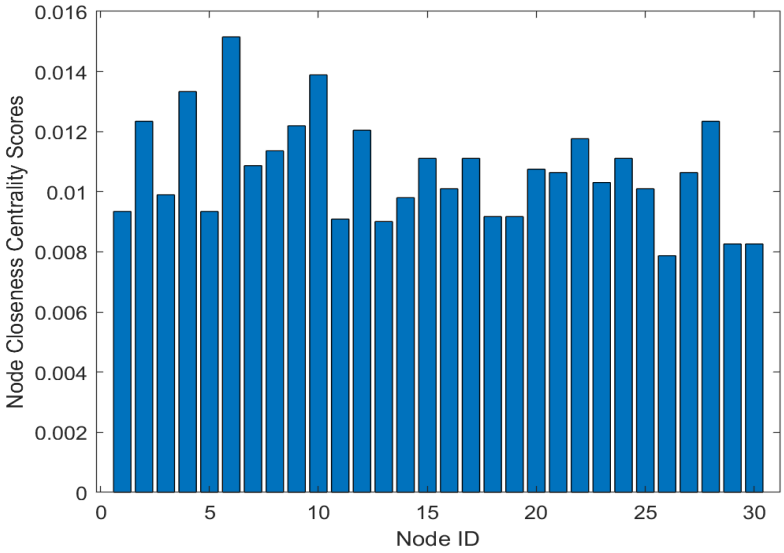
Similarly, edge closeness centrality can be expressed as in [105].

$$C_C(e_{ij}) = \sqrt{C_C(i) \times C_C(j)} \qquad , i \neq j \in V, e_{ij} \in E \tag{3.15}$$

The scores are shown in *Figure 3.20*.



(a)



(b)

Figure 3.19 Nodal Closeness Centrality Scores

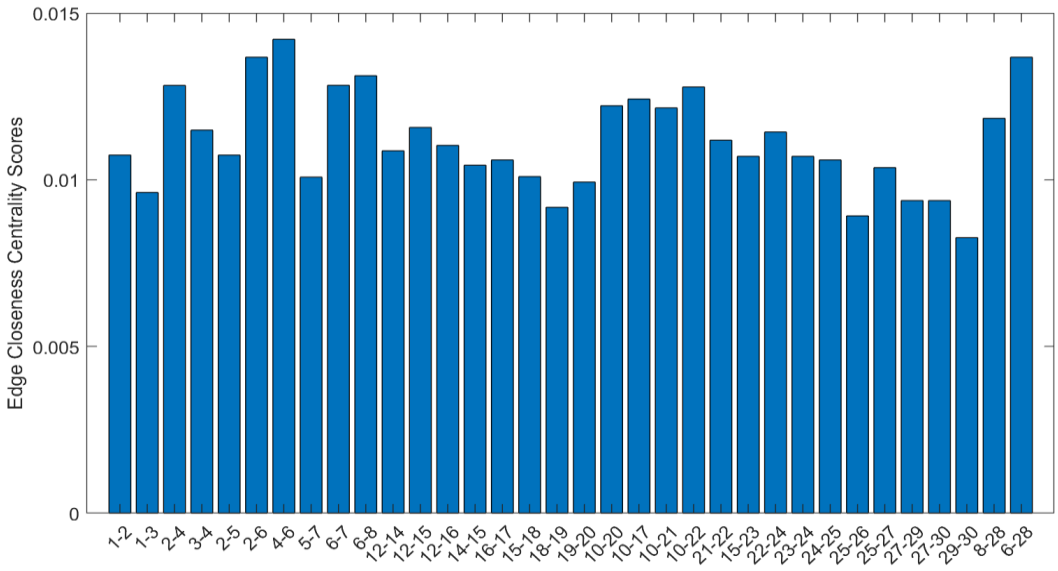


Figure 3.20 Edge Closeness Centrality Scores

B. Substation Attack Formulation

Based on the results obtained from each of the abovementioned metrics, two kinds of attacks can be formulated: static or dynamic. In the static formulation, if the attacker, for example, is conducting a node degree static attack, the target node will be the one with the highest degree score. Then the rest of the nodes will be attacked according to the ordering of their node degrees in decreasing order. In contrast, for a dynamic attack formulation, the attacker starts with the node with the highest score, but then the network is updated, and the centrality scores are recalculated. The node that will be attacked next will be the node with the highest score and so on. The algorithms for these two types of attack formulation strategies are shown in Figure 3.21 and Figure 3.22. Applying these two kinds of strategies to the IEEE 30-Bus system, the order of nodes removed in each attack formulation is given in Table 3.6 (up to 30% node removal).

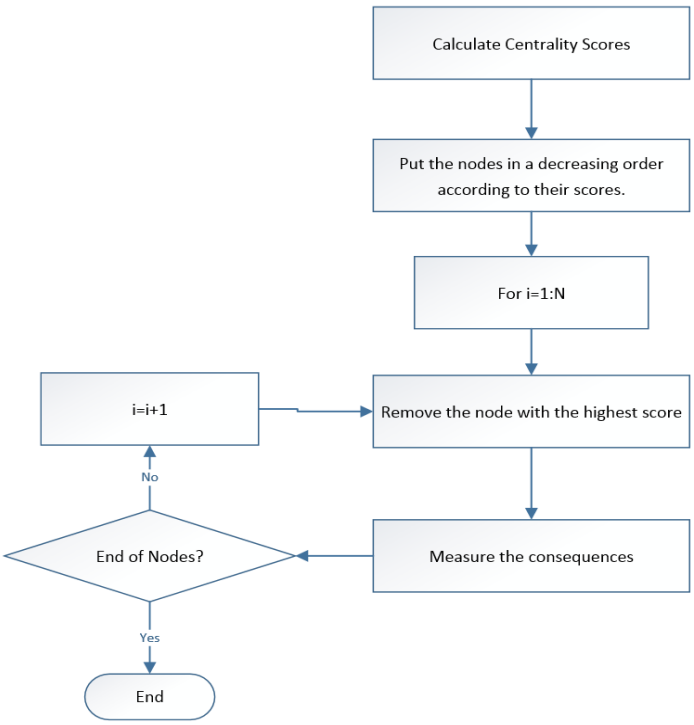


Figure 3.21 Static Attack Formulation Strategy

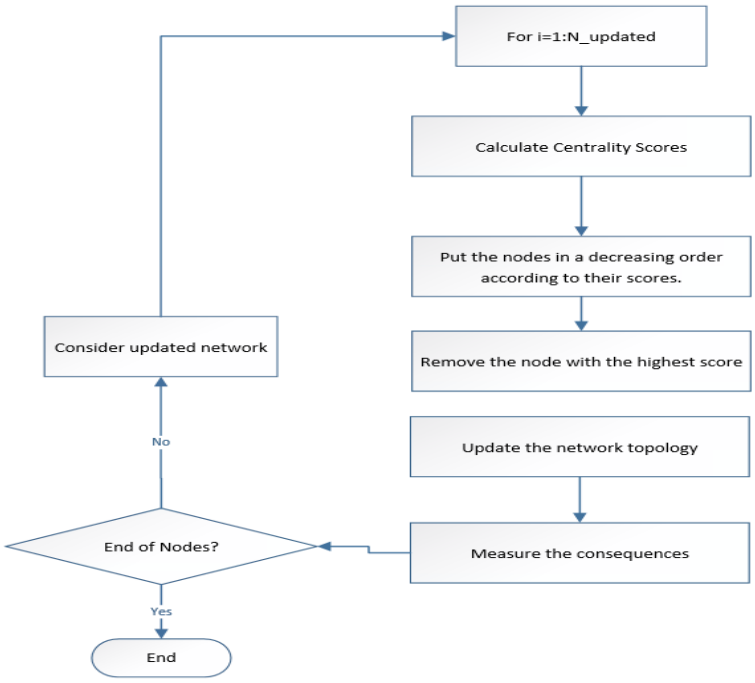


Figure 3.22 Dynamic Attack Formulation Strategy

Table 3.6 Order of Targeted Nodes for The IEEE 30-Bus System

Descending Order	Static Formulation			Dynamic Formulation		
	Degree	Betweenness	Closeness	Degree	Betweenness	Closeness
1	**6**	**6**	**6**	**6**	**6**	**6**
2	**10**	**10**	**10**	**10**	**12**	15
3	**12**	4	4	**12**	24	**10**
4	27	**12**	28	27	**10**	4
5	15	27	2	2	27	25
6	4	28	9	15	15	**12**
7	2	24	**12**	24	2	27
8	28	15	22	3	3	2
9	25	25	8	19	19	22
10	24	2	24	5	--	19

C. Topological-Based System Performance

After developing different attack formulations, the attacker would check which formulation would result in the highest consequence on the network.

In the context of graph theory, the giant component is the connected component that has the largest fraction of the entire graph's vertices.

$$GCS = \frac{\max\{N_m\}}{N}, \qquad m = 1,2,\dots,M \tag{3.16}$$

where N is the number of the graph nodes, and N_m is the number of nodes in the m^{th} subnetwork has given that the post-attack network has been partitioned into m components. As stated in the literature [107], the size of the giant component has a high correlation coefficient with the amount of load interrupted. Therefore, it is widely used when only pure topological information is available.

From Table 3.6, we notice that 'N6' is the most central node in the network, which means substation #6 is the most critical one when only purely topological information is reliable. Figure 3.23 shows the post-attack network when 'N6' is removed. We also notice that 'N10' and N12' corresponds to the next critical substations from the centrality perspective.

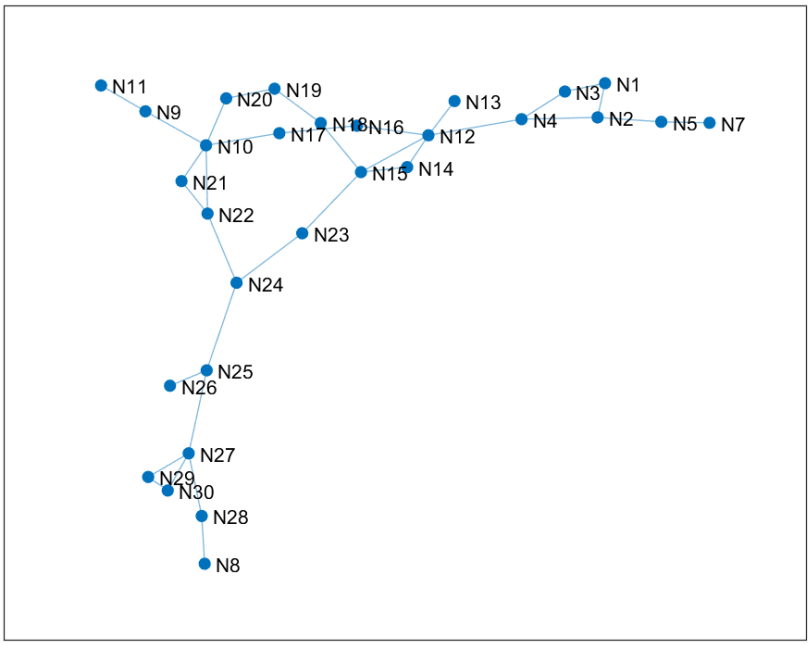


Figure 3.23 Post-Attack Network (Targeting 'N6')

The quantity $(1 - GCS)$ has been calculated considering different numbers of nodes attacked and given in Figure 3.24 and Figure 3.25 for static and dynamic attack formulations, respectively. The results show that, for the system under study, if the attacker would conduct a single attack, 'N6' would be the target node, but the system will remain intact. However, if the number of nodes attacked is greater than 1, i.e., p>1. The attacker will choose the formulations that give the higher negative consequences. Using Figure 3.24 and Figure 3.25, along with Table 3.6, The attacker can get the critical node combinations depending on the number of nodes they intend to target. For example, for p=2, the combination {N6, N10} would be the most critical for all static formulations, whereas the combination of the betweenness formulation {N6, N12} is the most critical for the dynamic kind of attacks. For p=3, combinations {N6, N10, N12} and {N6, N15, N10} are critical for static and dynamic attack formulations, respectively, and so forth. We can also conclude that the IEEE 30-bus system is topologically vulnerable to centrality-based attacks since removing only three nodes can result in disconnecting more than 60% of the nodes in the network.

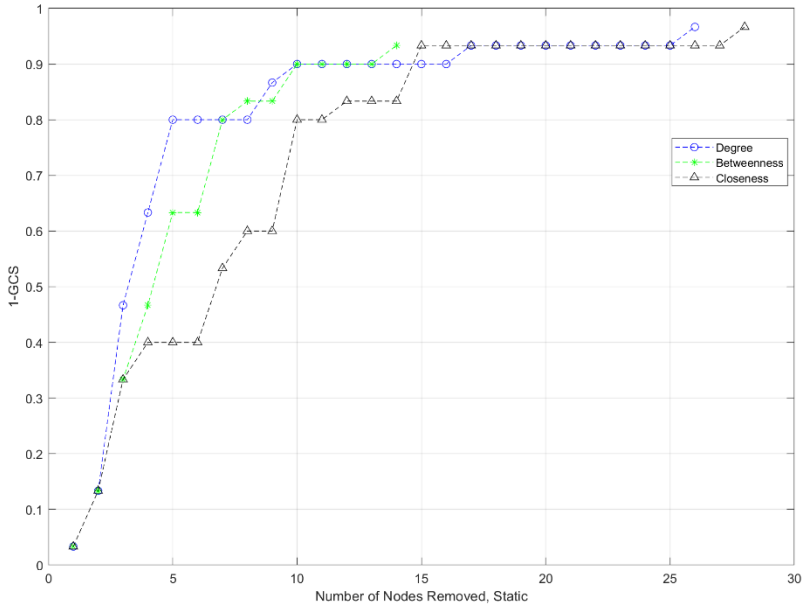


Figure 3.24 System Performance Using Topological Measures for Static Attacks on Nodes

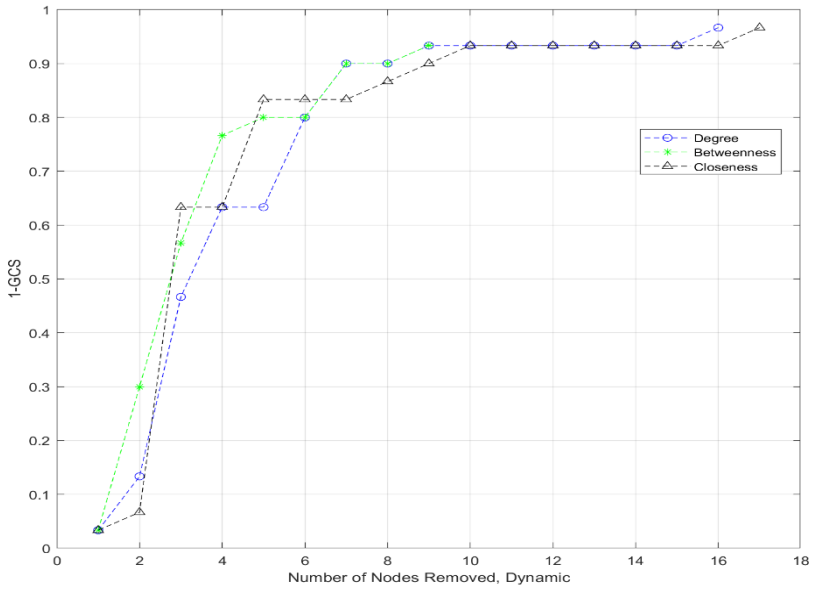


Figure 3.25 System Performance Using Topological Measures for Dynamic Attacks on Nodes

The same procedures have been applied for the line failure case. The quantity $(1 - GCS)$ has been evaluated for static and dynamic attack formulations; the results are presented in Figure 3.26 and Figure 3.27, respectively.

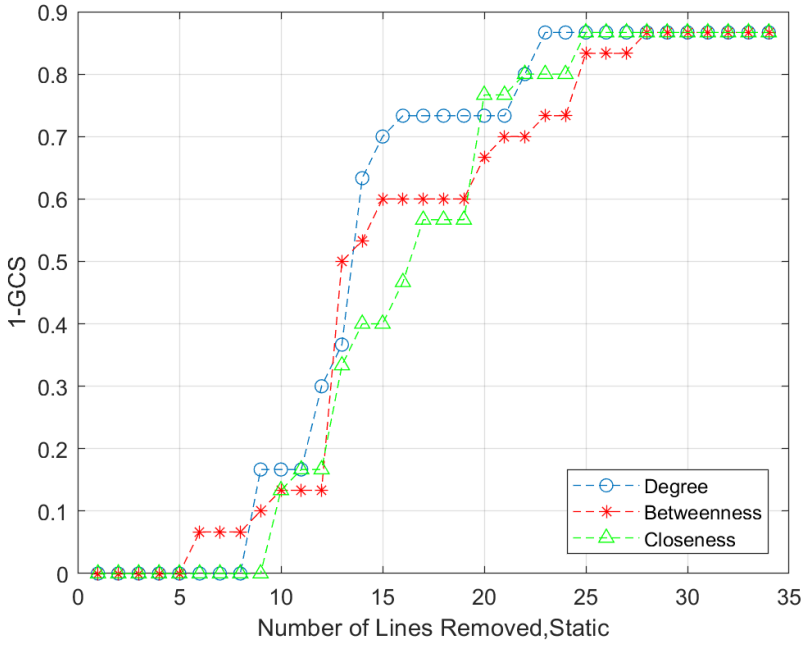


Figure 3.26 System Performance Using Topological Measures for Static Attacks on Lines

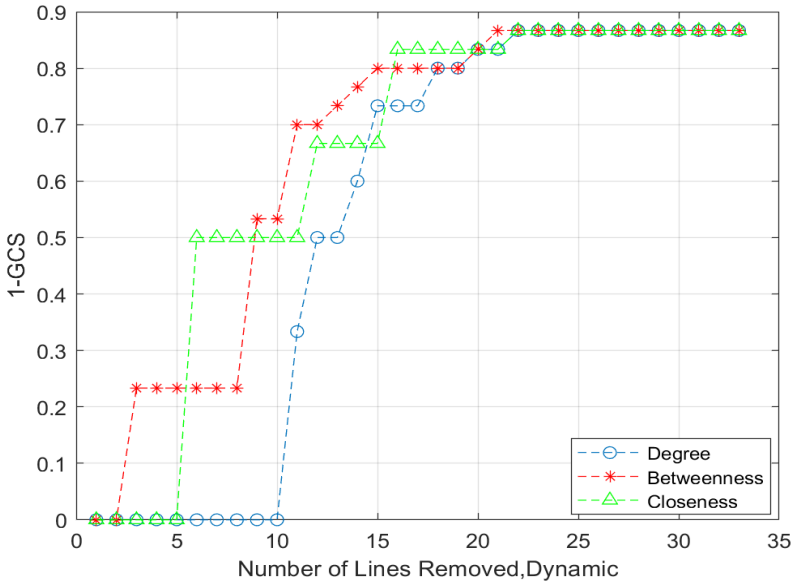


Figure 3.27 System Performance Using Topological Measures for Dynamic Attacks on Lines

3.5 Stage 3 –Risk Evaluation

Risk is quantified for the whole system against the potential attack scenarios obtained from the attack tree. For demonstration purposes, data for practical attack tree scenarios for attacking a power system are adopted from [97] and listed in Table 3.7. To account for the uncertainty in modeling attackers, attacker's attributes are defined as random variables with probability distributions whose parameters are given in Table 3.8. The Monte Carlo simulation is then used to estimate the likelihood of the attack occurrence for each proposed attacker model.

Table 3.7 Attack requirement Data for Different Scenarios

Scenario	Overall Attack Cost	Attack Complexity required	Vulnerability Score
1	236$	7.5	0.4558
2	20,000$	12.5	0.4558
3	17,211$	27	0.4558
4	20,000$	11.66	0.4558
5	17,211$	30	0.4558
6	20,000$	15	0.4558
7	17,211$	29	0.4558
8	20,000$	15	0.4558
9	17,211$	32.5	0.4558
10	15,576$	55	0.9
11	20,768$	55	0.8

Table 3.8 Probability Distribution Parameters of Attackers' Attributes

Attacker	Budget $X \sim N(\mu, \sigma^2)$		Technical Ability $X \sim N(\mu, \sigma^2)$		Motivation $X \sim U(a, b)$	
	μ	σ	μ	σ	a	b
Mediocre	1,500$	200$	25	4	0.1	0.35
Intermediate	30,000$	3,000$	45	4	0.35	0.7
Sophisticated	100,000$	10,000$	80	5	0.7	1

3.5.1 Mediocre Attacks

The proposed algorithm for mediocre attacks' analysis is presented in Figure 3.28. For the IEEE 30-bus system, the simulation results for each scenario's likelihood of attack occurrence are given in Figure 3.29. The risk index for the substation i, RI_{S/S_i}, is calculated as the sum of substation risks for all possible scenarios, where the risk of a given scenario is the product of the probability of attack and its impact, as discussed in Chapter 2. RI_{S/S_i} can be expressed as,

$$RI_{S/S_i} = \sum_{k=1}^{N_{scenarios}} \overline{PAO}_k \times OLI_i \tag{3.17}$$

The results are presented in Table 3.9. Also, the system risk index under each attack scenario of mediocre attacks is shown in Figure 3.30. Finally, the total system risk from mediocre attacks, $R_{S,M}$, is the sum of the risk index (due to mediocre attacks) of all substations within the system, which can be written as,

$$R_{S,M} = \sum_{i=1}^{N} RI_{S/S_i} \tag{3.18}$$

And $R_{S,M}$ is found to be 0.4266 in this case.

Table 3.9 Estimated Risk Indices for Substations

Substation no.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Risk Index	0.0306	0.0448	0.00149	0.0088	0.0585	0.0549	0.0142	0.0186	0.0109	0.0367
Substation no.	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Risk Index	0.0009	0.0330	0.00011	0.0038	0.0174	0.0056	0.0056	0.0033	0.0059	0.0063
Substation no.	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
Risk Index	0.0111	0.0021	0.0028	0.0075	0.0022	0.0023	0.0085	0.0186	0.0023	0.0076

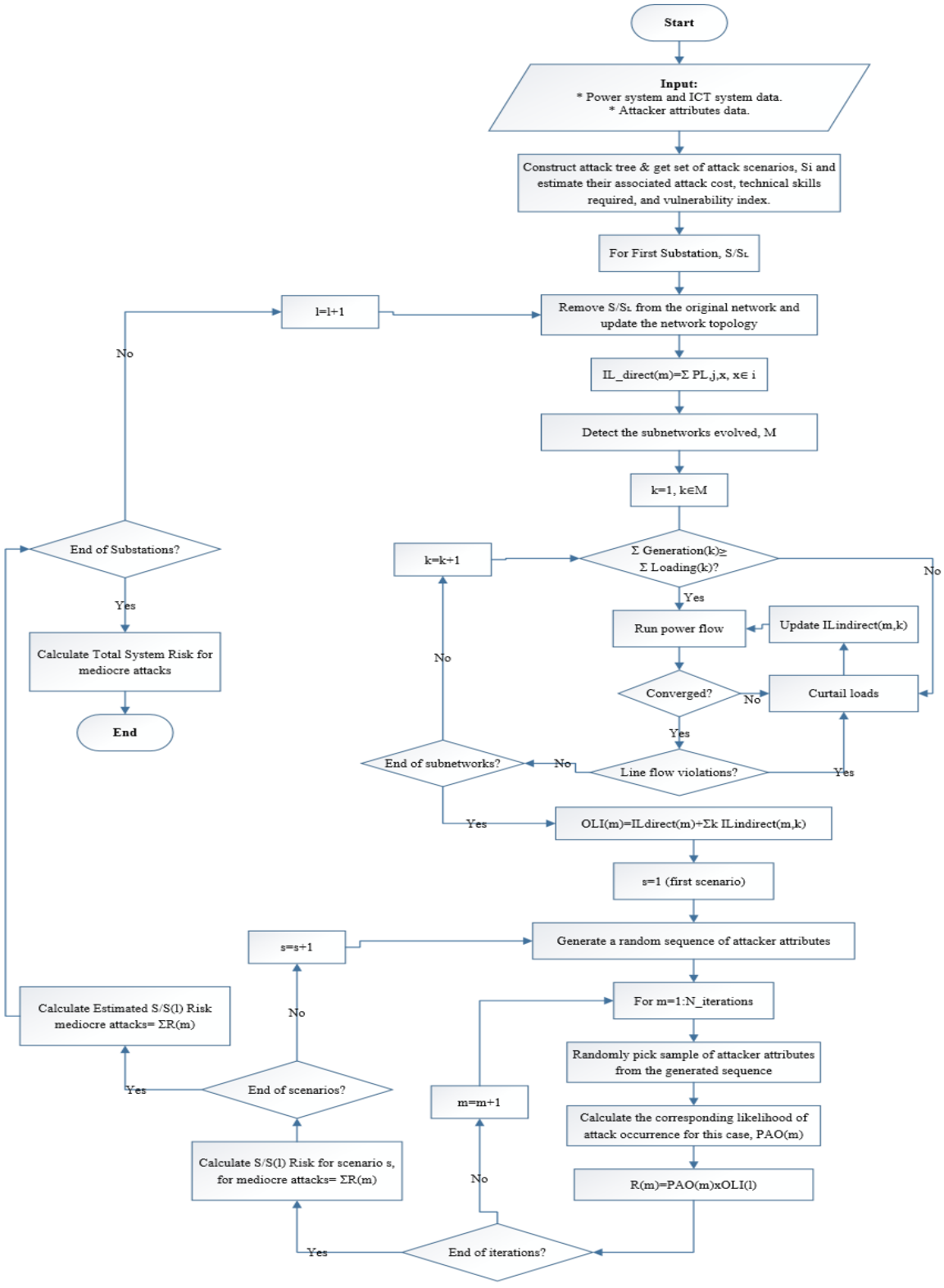


Figure 3.28 Proposed Algorithm for Mediocre Attack Analysis

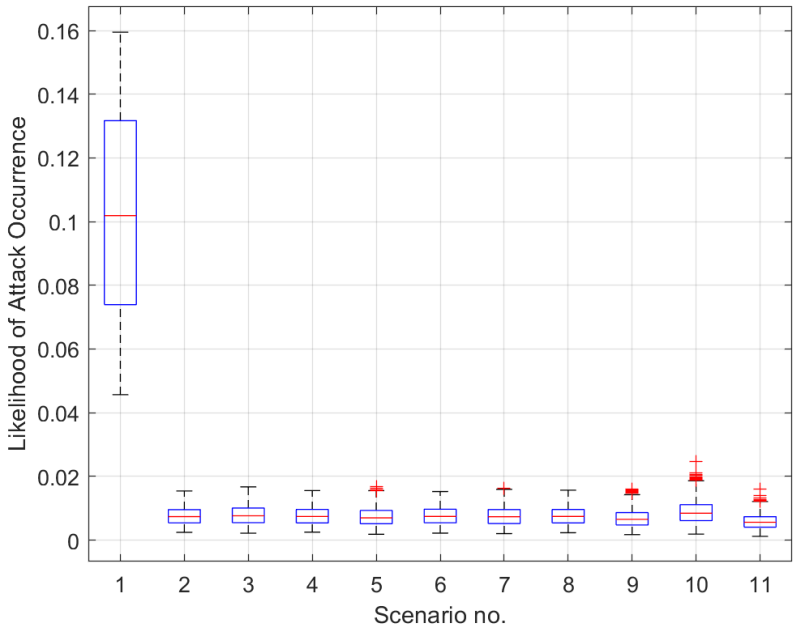


Figure 3.29 Likelihood of Attack Occurrence for Mediocre Attacks

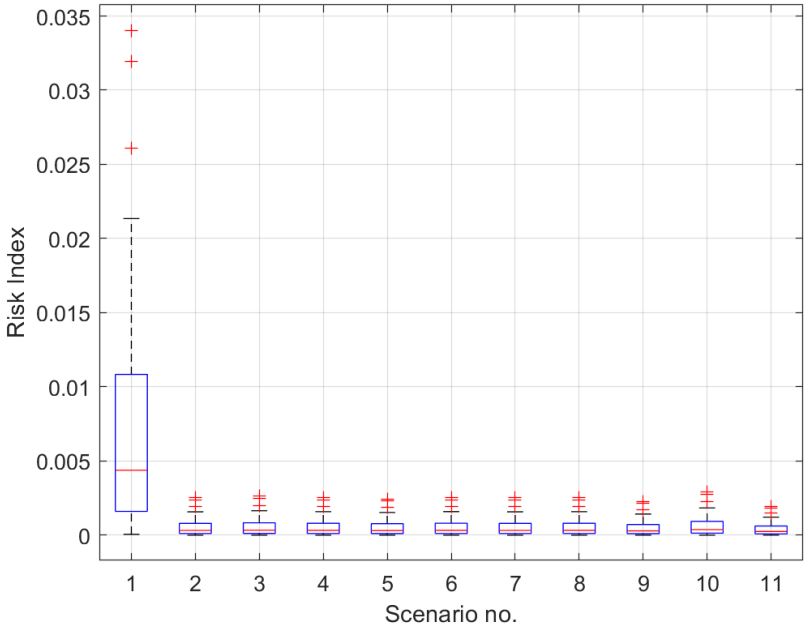


Figure 3.30 System Risk Indices for Mediocre Attacks

3.5.2 Intermediate Attacks

For the IEEE 30-bus system, intermediate attackers' likelihood of attack occurrence is calculated for different scenarios based on the algorithm proposed in Figure 3.31. The results are given in Figure 3.32. Assuming the attacker's budget is divided equally between targets when $p > 1$, the likelihood of attack occurrence for $p > 1$ is given in Figure 3.33. The ratio OLI is calculated for the six attack formulations developed in Section 3.4.6, for different numbers of nodes removed, using the algorithm given in Section 3.4.4. Simulation results are given in Figure 3.34.

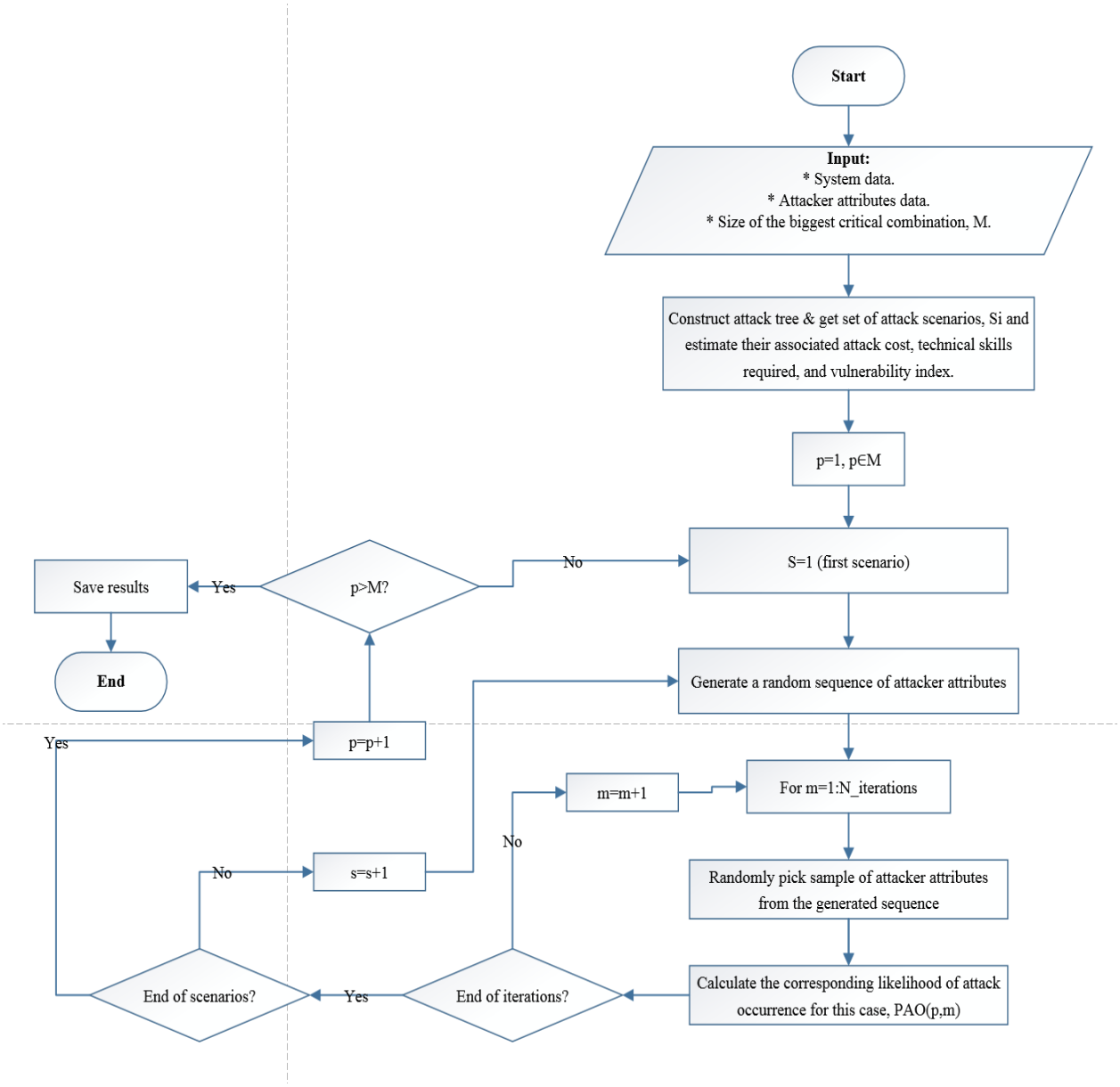


Figure 3.31 Evaluation of Likelihood of Intermediate Attack Occurrence for p≥1

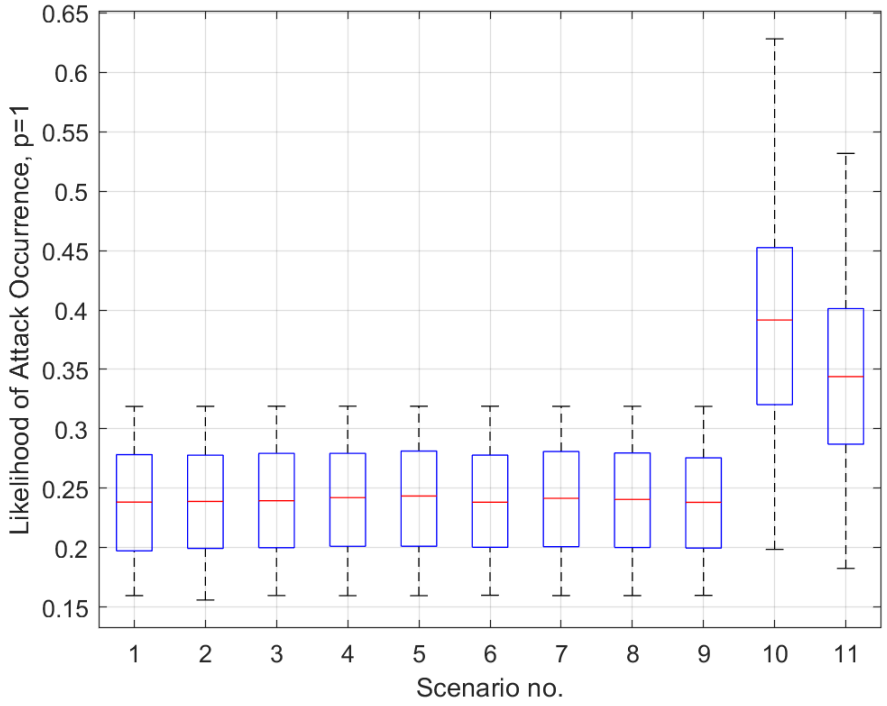


Figure 3.32 Likelihood of Attack Occurrence for Intermediate Attacks, p=1

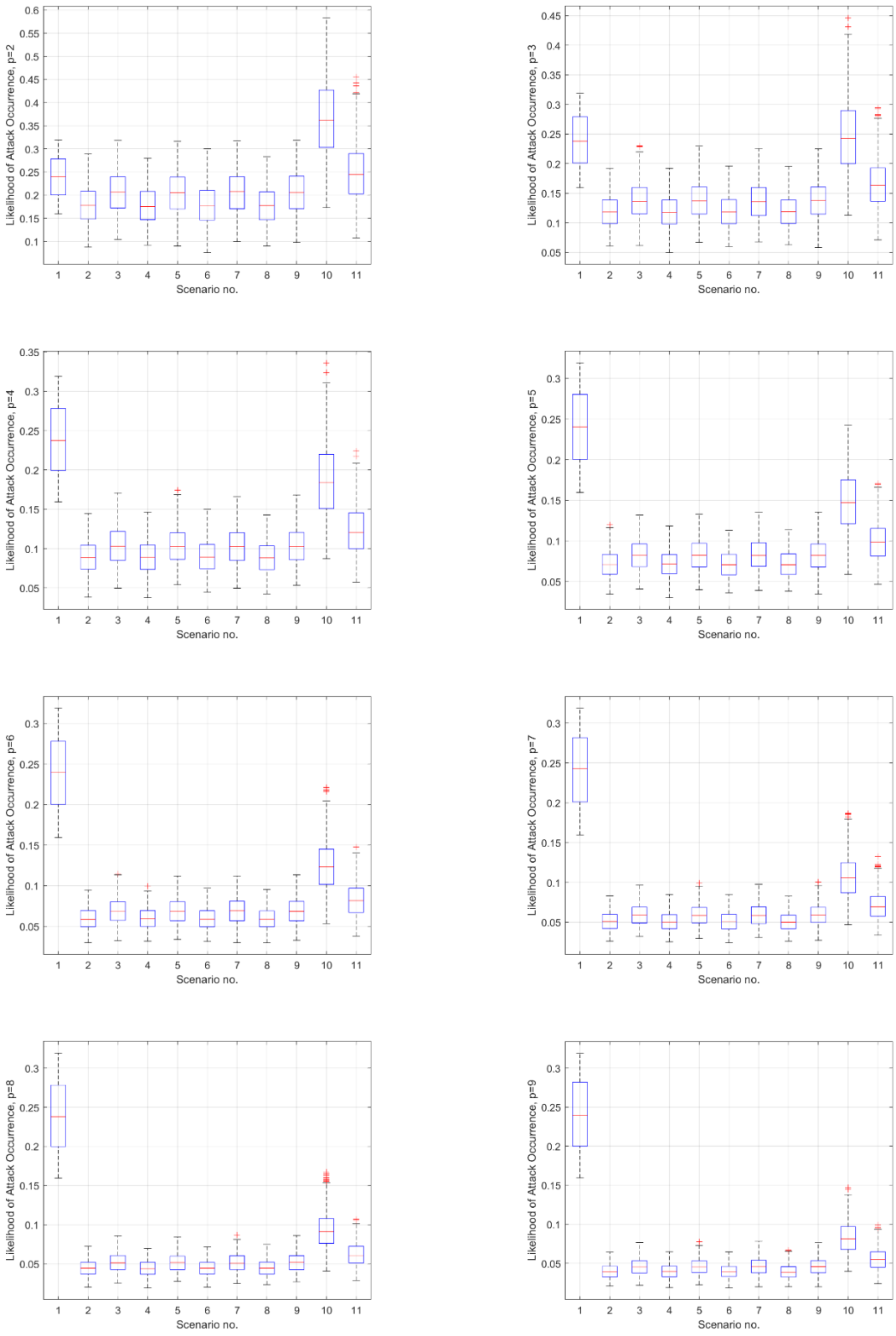


Figure 3.33 Likelihood of Attack Occurrence for Intermediate Attacks (p=2:9)

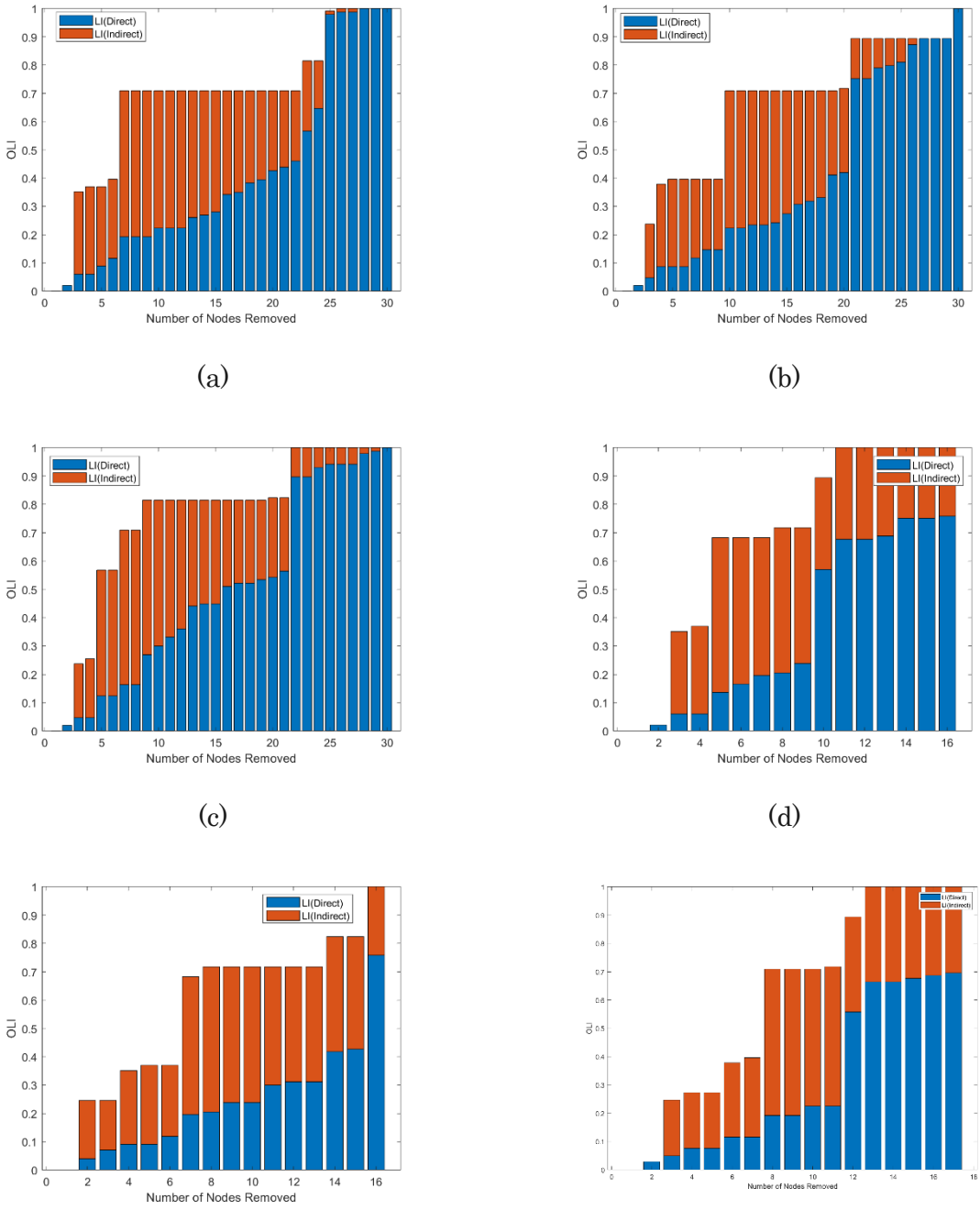


Figure 3.34 OLI for Different Number of Nodes Removed Based on: (a) Static Node Degree Attack, (b) Static Node Betweenness Attack, (c) Static Node Closeness Attack, (d) Dynamic Node Degree Attack, (e) Dynamic Node Betweenness Attack, and (f) Dynamic Node Closeness Attack.

The total system total risk from intermediate attacks, $R_{S,E}$, is calculated as,

$$R_{S,E} = \sum_{m=1}^{N_{scenarios}} \sum_{k=1}^{N_{combinations}} \overline{PAO}_{m,k} \times OLI_k \tag{3.19}$$

The system risk index for each scenario is given in Figure 3.35, and $R_{S,E}$ is found to be 0.5171.

In this case, the risk index for a substation i, RI_{S/S_i}, can be calculated considering all the critical combinations that contain the substation i, where the impact is shared among all the substations in each combination. The likelihood is also based on p from Figure 3.32 and Figure 3.33. Hereafter, RI_{S/S_i}, for critical substations is given in Figure 3.36 and Figure 3.37.

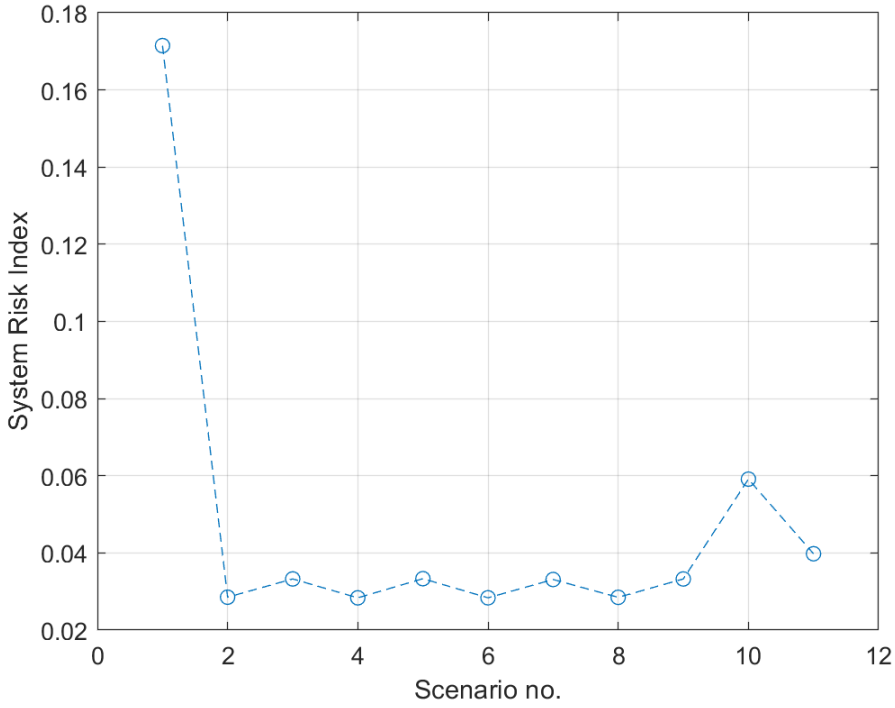


Figure 3.35 System Risk Indices for Intermediate Attacks

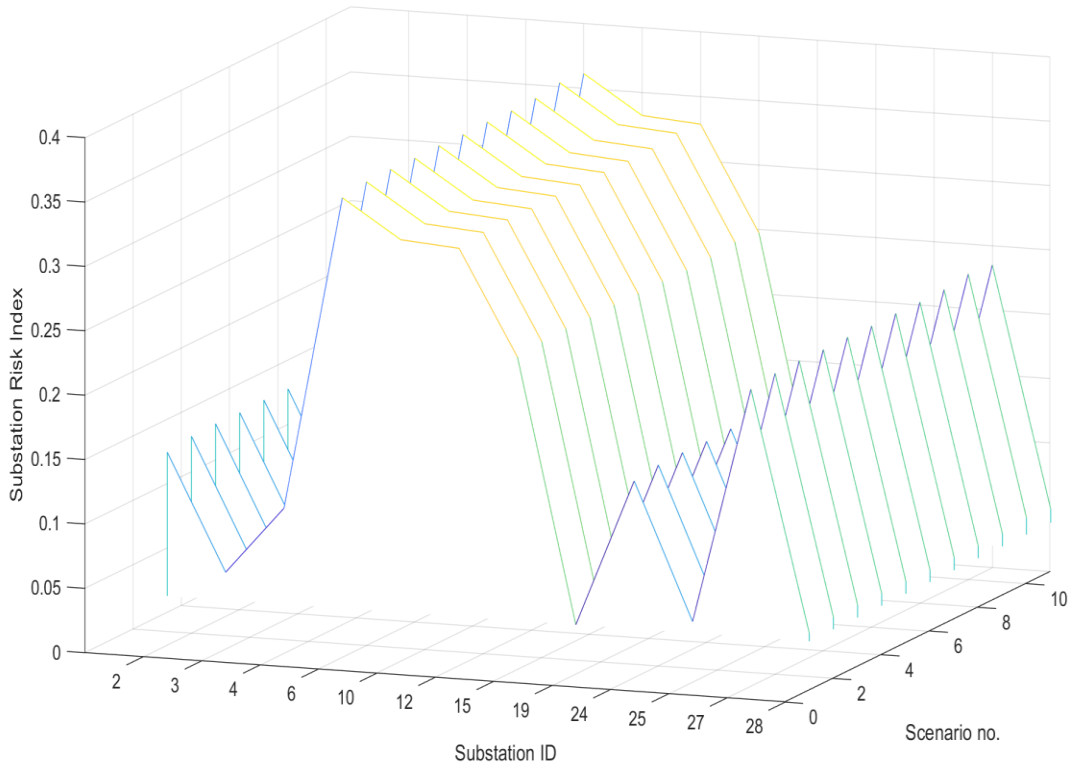


Figure 3.36 Substation Risk Indices for Intermediate Attacks

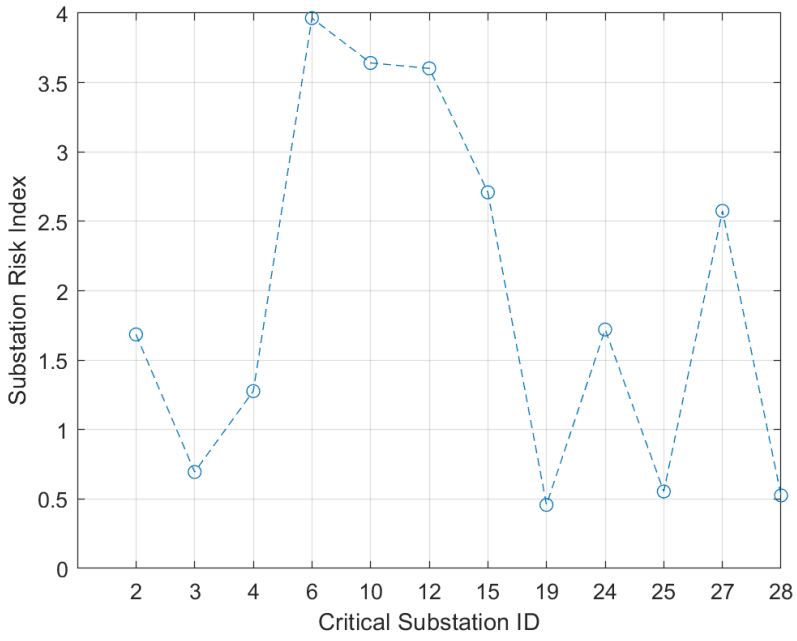


Figure 3.37 Risk Indices of Critical Substation for Intermediate Attacks

3.5.3 Sophisticated Attacks

For assessing the risks in case of sophisticated attacks with the highest attacker's resources and knowledge about power systems. First, we will find all possible combinations of the victim elements, C. The total combination enumeration (the sum of n-select-k) is:

$$\mathbb{C} = \sum_{k=1}^{n} C_k^n \, , k = 1, \dots , n \tag{3.20}$$

In this thesis, for the sake of illustration, k will be set to {1, 2}.

$$C_k^n = \binom{n}{k} = \frac{n!}{k!\,(n-k)!} \tag{3.21}$$

$$= \begin{cases} n & , k = 1 \\ \dfrac{n(n-1)}{2} & , k = 2 \end{cases}$$

Therefore,

$$\mathbb{C} = n + \frac{n(n-1)}{2} \tag{3.22}$$

where n is the total number of substations in the given network. For the IEEE 30-bus system, $\mathbb{C} = 465$ combinations. The next step is picking the i^{th} combination, where $i \in C$. Remove the substations included in that combination from the original network. The next step is to calculate the physical impact using the algorithm in Section3.4.4. The ratio OLI is calculated for the all the combinations, C, and simulation results are given in Figure 3.38 and Figure 3.39. The likelihood of attack occurrence for $p = 1$ and $p = 2$ is calculated and the results are given in Figure 3.40 and Figure 3.41, respectively.

Assume that the threshold of the load unserved is set to 20%, i.e., the contingency is critical if more than 20% of the system loads are interrupted. Based on this assumption, critical contingencies are identified. Risk indices for the system are calculated and shown in Figure 3.42. The total system risk in this case $R_{S,S}$ *is equal to* 75.26. Finally, Figure 3.43 and Figure 3.44provides the risk indices for substations.

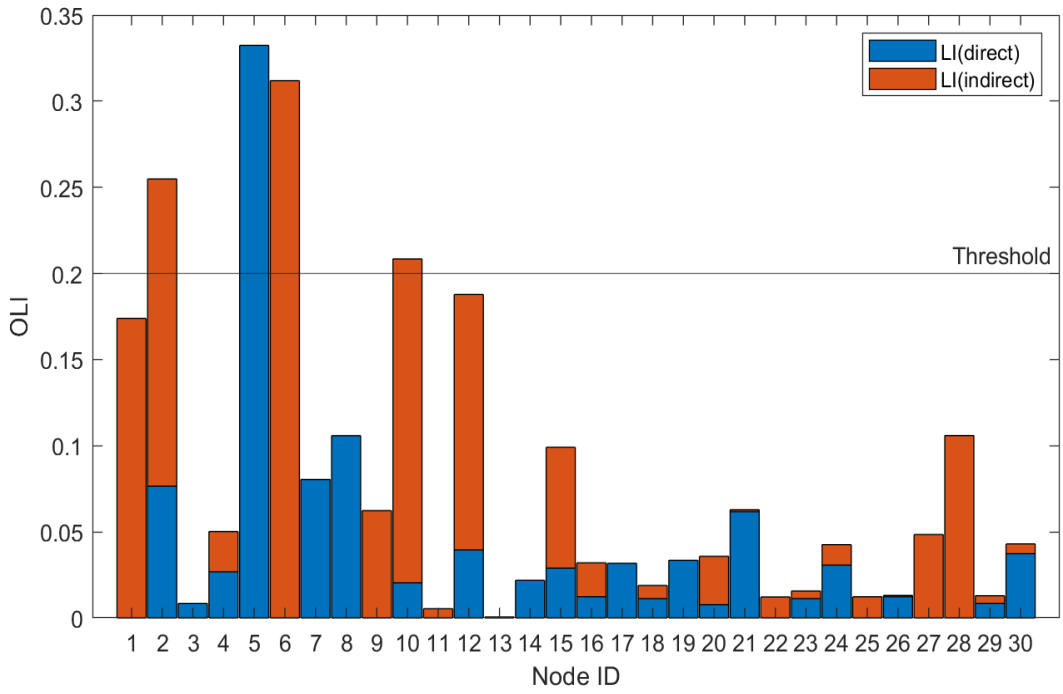


Figure 3.38 OLI for all N-1 Contingencies

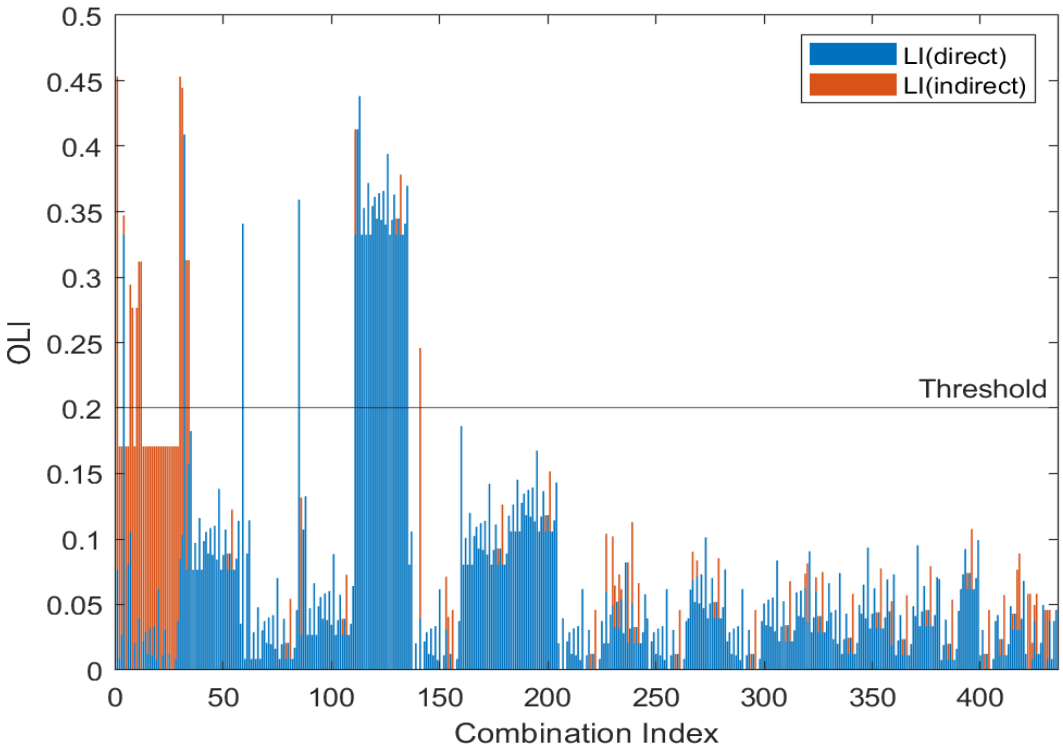


Figure 3.39 OLI for all N-2 Contingencies

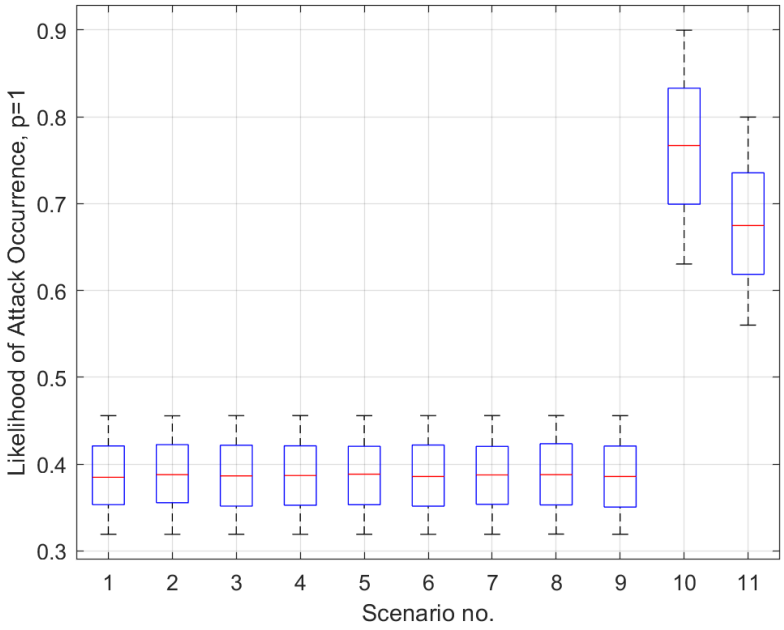


Figure 3.40 Likelihood of Attack occurrence for Sophisticated Attacks, p=1

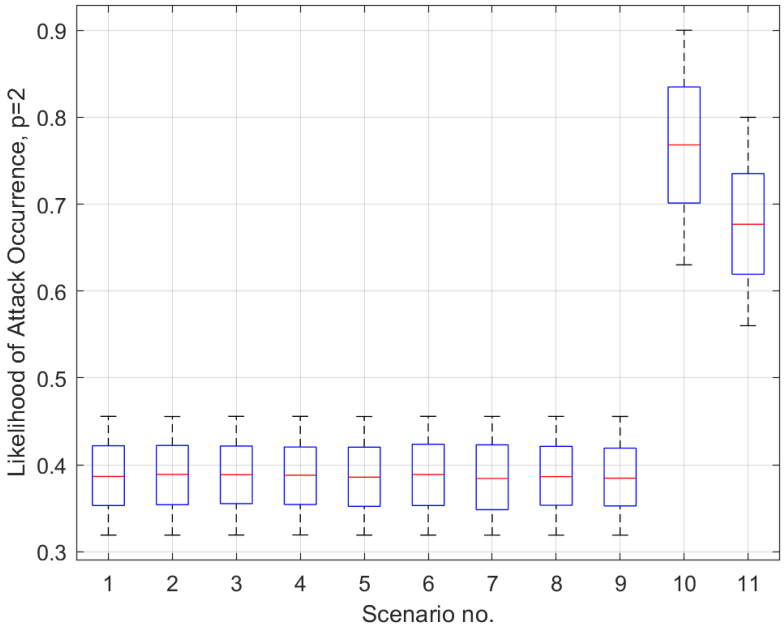


Figure 3.41 Likelihood of Attack occurrence for Sophisticated Attacks, p=2

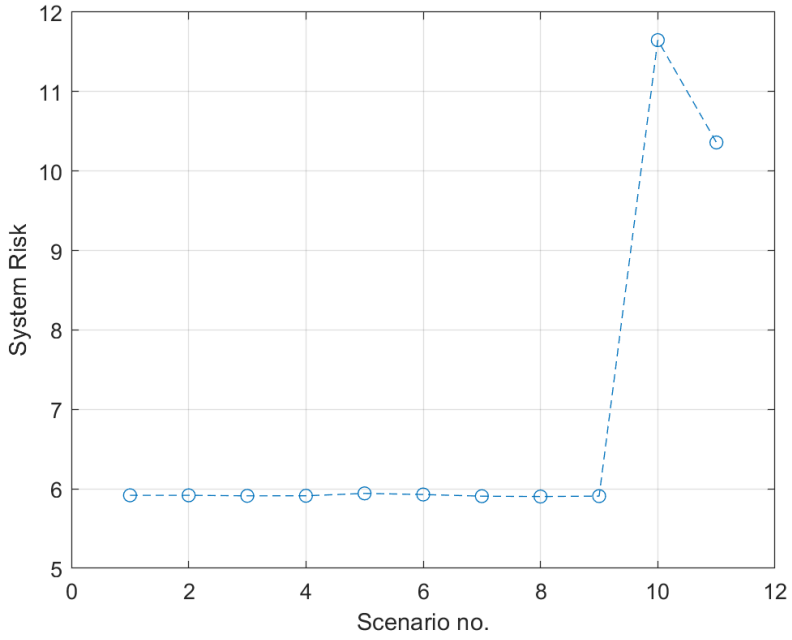


Figure 3.42 System Risk Indices for Sophisticated Attacks

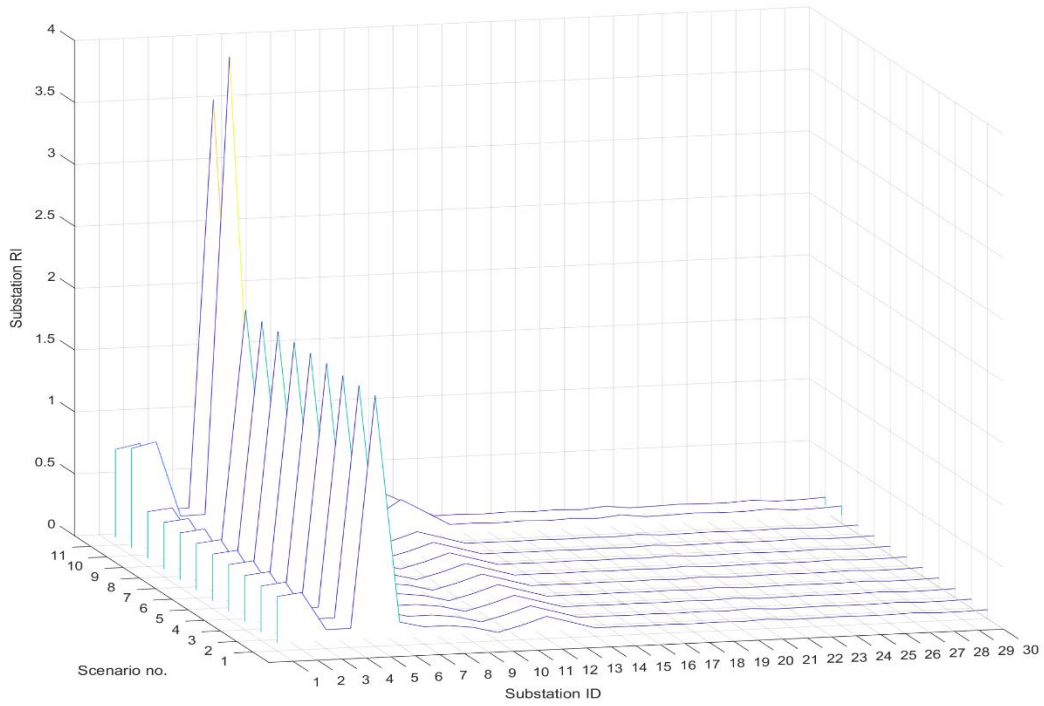


Figure 3.43 Substation Risk Indices for Different Scenarios of Sophisticated Attacks

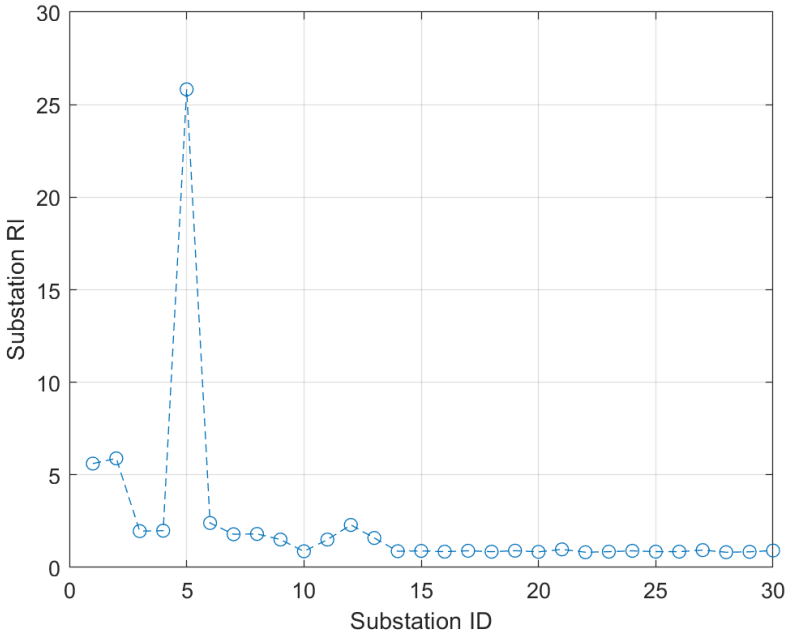


Figure 3.44 Substation Risk Indices for Sophisticated Attacks

3.5.4 Substation Ranking

From the results obtained, critical substations' rankings are listed in Table 3.10. Comparing the mediocre- and the sophisticated-attack-based substation ranking, we notice that a substation criticality is not only determined by the impact it causes when failed but also depends on the impact it causes when being combined with other substations' failure in the network. When comparing the intermediate attacks to the others, we notice that N6 is the most critical node from the attackers' point of view with purely topological info because of its high centrality. However, surprisingly, N6 causes no impact on the system loads when disconnecting. That is because the network is interconnected, and the existing generation capacity is still sufficient to supply the loads when the configuration changes.

Table 3.10 Critical Substation Ranking for Different Attack Types

Substation Ranking	Mediocre Attacks	Intermediate Attacks	Sophisticated Attacks
1	N5	N6	N5
2	N6	N10	N2
3	N2	N12	N1
4	N10	N15	N6
5	N12	N27	N12
6	N1	N24	N4
7	N28	N2	N3
8	N8	N4	N8
9	N15	N3	N7
10	N7	N25	N13

3.5.5 Risk Quantification for Lines

It is crucial for the operator to identify critical lines in the network. Such information is useful for making proper decisions. In this thesis, lines' criticality is used in Chapter 5 for obtaining a resilient reconfiguration strategy. The risk indices for lines can be evaluated in the same way as substations' indices. This section gives the results obtained for lines when different attacker models are used. For mediocre attacks, estimated risk indices for lines are given in Table 3.11, while the system risk for different attack scenarios is presented in Figure 3.45.

Table 3.11 Estimated Risk Indices for Lines

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
0.0093	0	0	0	0.016	0.001	0.011	3.48E-05	0.0028	0.0007	0.0013	0.0209
13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
0.014	0.001	0.009	0.008	0.006	0.009	0.012	0.003	0.021	0.007	0.0003	0.0128
25	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**		
0.0091	0.0062	0.0004	0.0024	0.0012	0.003	0.007	0.0016	0.0004	0.008		

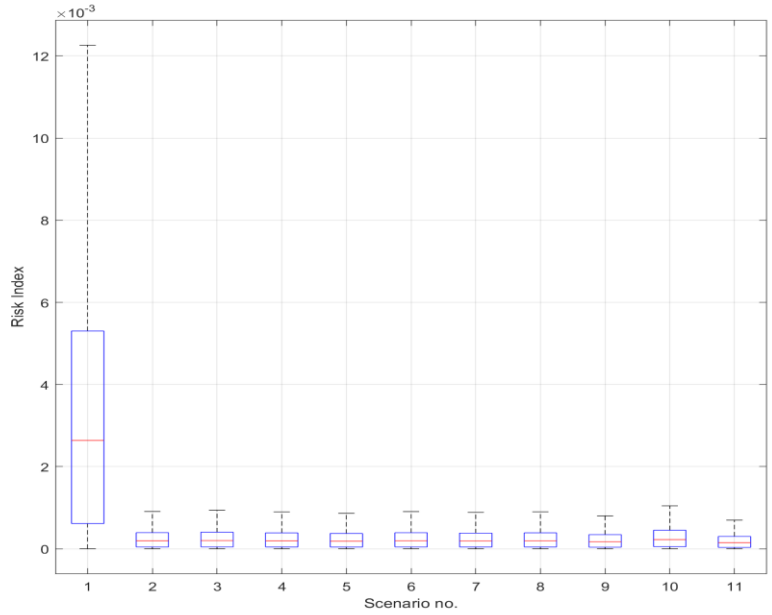


Figure 3.45 System Risk Indices for Mediocre Attacks--Lines

For intermediate attacks, critical lines' and system's risk indices are given in Figure 3.46 and Figure 3.47, respectively.

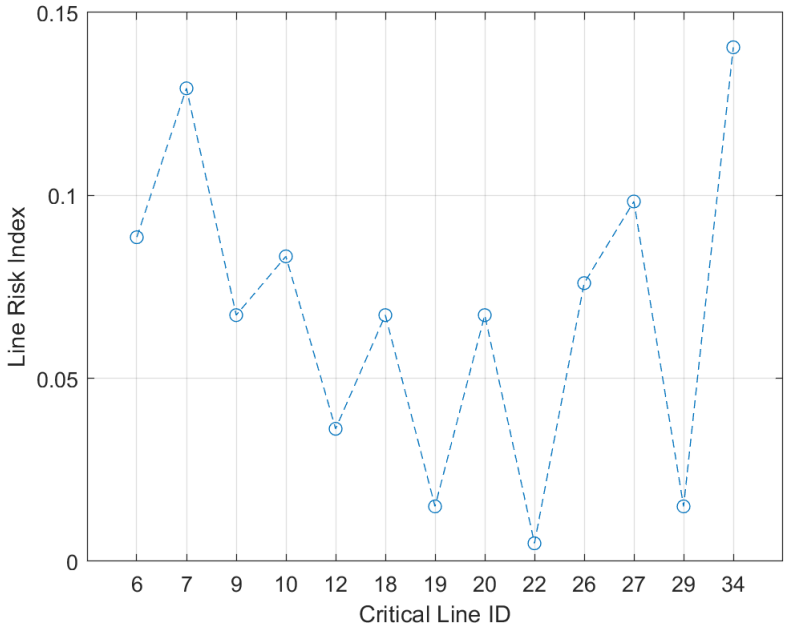


Figure 3.46 Risk Indices of Critical Lines for Intermediate Attacks

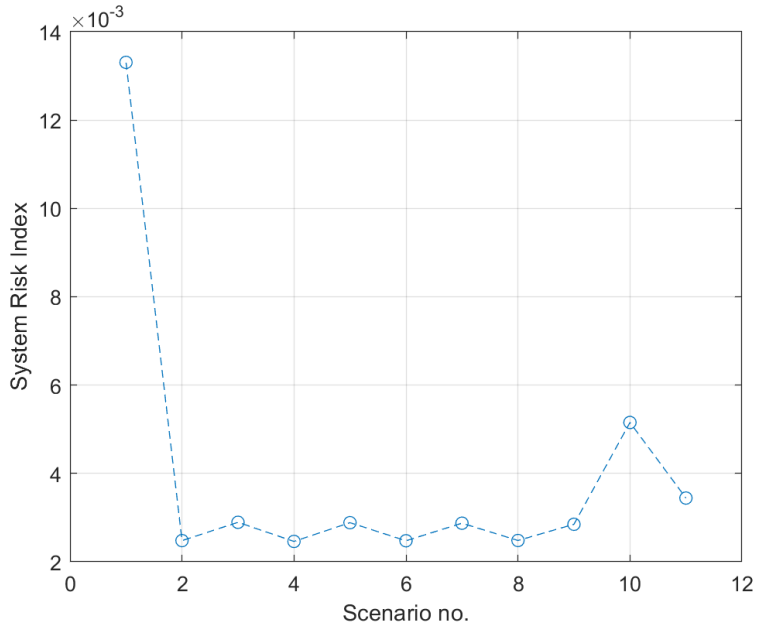


Figure 3.47 System Risk Indices for Intermediate Attacks—Lines

Finally, for sophisticated attacks, the OLI for single and double contingencies are presented in Figure 3.48 and Figure 3.49, respectively. The risk indices have been calculated for the critical lines and are given in Figure 3.50 and Figure 3.51. Finally, the system risk due to sophisticated attacks is provided in Figure 3.52.

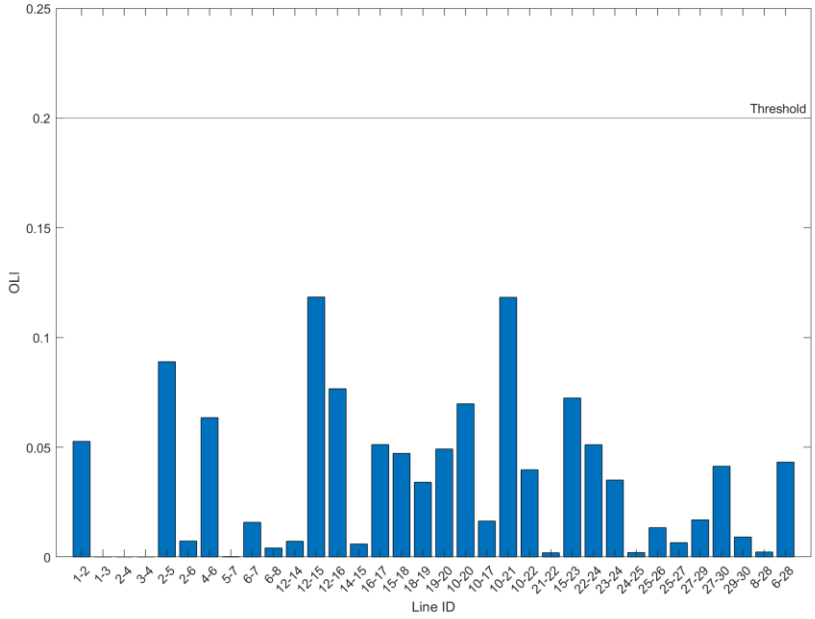


Figure 3.48 OLI for all N-1 Contingencies--Lines

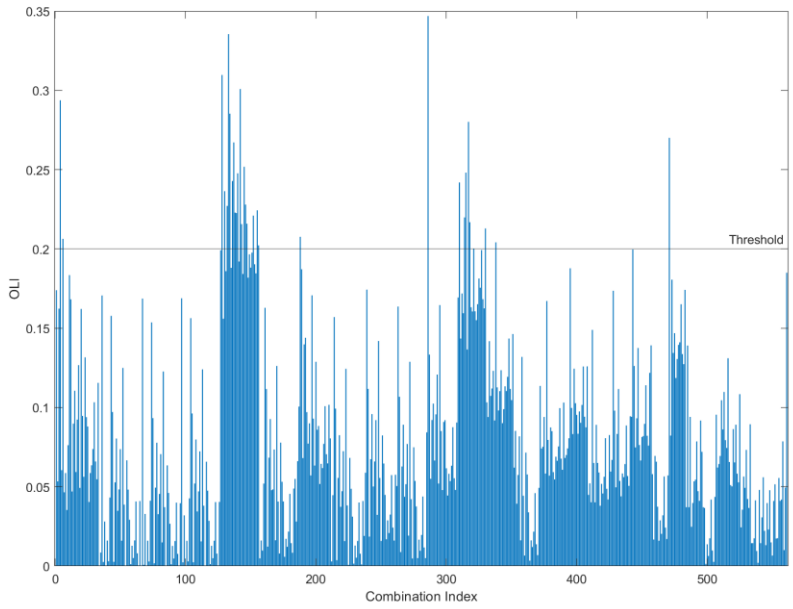


Figure 3.49 OLI for all N-2 Contingencies--Lines

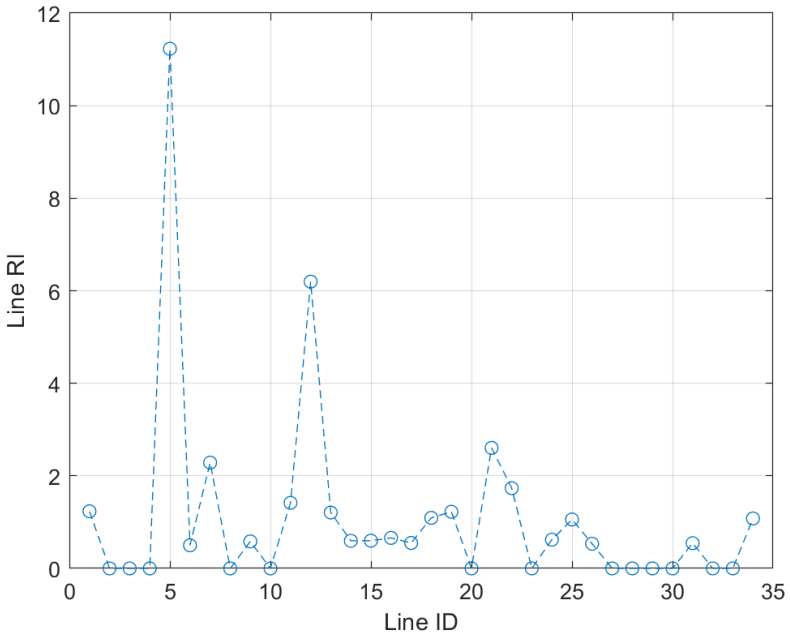


Figure 3.50 Line Risk Indices for Sophisticated Attacks

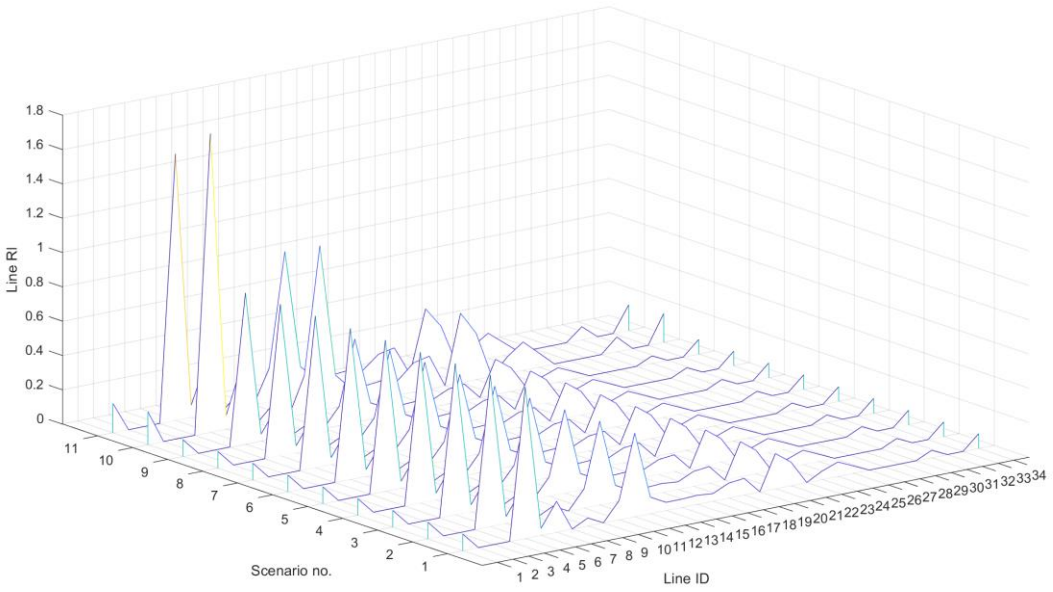


Figure 3.51 Line Risk Indices for Different Scenarios of Sophisticated Attacks

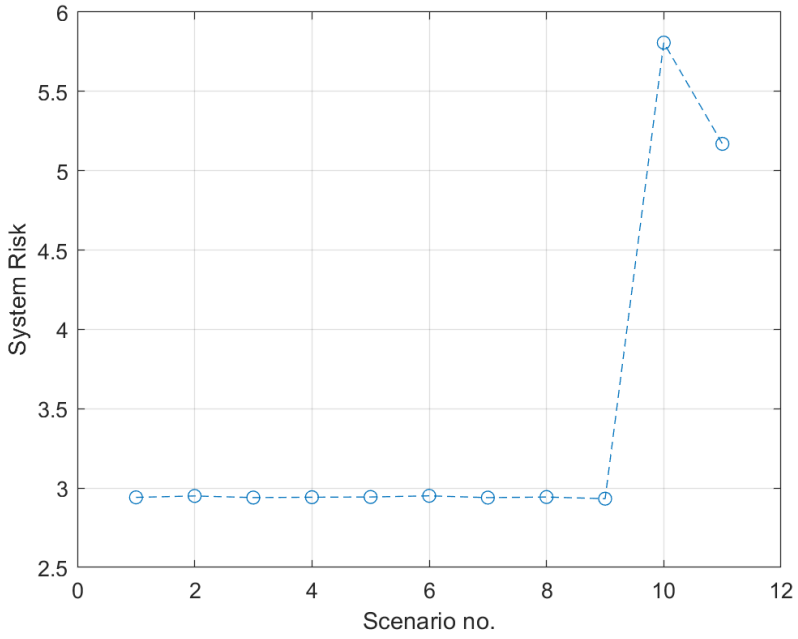


Figure 3.52 System Risk Indices for Sophisticated Attacks--Lines

3.6 Summary and Conclusions

In this chapter, we presented a systematic approach for analyzing the cyber-physical risk for power grids. This work sheds light on the importance of attacker attributes in cyber-physical risk analysis. These attacker models not only affect the attack probability but also affect the selection of targets, and hence the consequences it brings to the system. An adversary capability-based model has been used to determine the probability of attack occurrence. Identifying substations' potential threats and vulnerabilities helped construct a substation attack tree. Such trees are very useful in determining and enumerating attack scenarios. Proper attacker models tailored for power grids have been determined and used to determine the attacker's strategy for selecting the target assets to maximize the attack impact of the network. The attack impact is measured in this work using the ratio of loads interrupted both directly and due to operational constraints. The simulation results show that the loads interrupted due to operational constraints are mostly comparable to (and even sometimes higher than) the directly interrupted ones; hence they must be included in the analysis for accurate determination of the impacts. Also, a vulnerability analysis has been done that first evaluated three commonly-used centrality measures for network nodes. Based on these measures, static and dynamic strategies have been used to formulate attacks. The giant size component measure has been used to determine the critical sets of substations that the topological-information-based attack can use to cause maximum damage (according to the attacker's limited resources). Finally, the risk is quantified for both substations and lines for the three attacker models presented. Total system risk for different attack scenarios is calculated for each attacker type as well. The Substations finally were ranked for each attacker type. The results showed that different attacker resources result in a completely different set of critical assets. Thus, the operator must determine which model of the three attacker models is suitable for a given network based on its importance and the amount of accessible public data, as discussed in Chapter 1.

The analysis also concludes that even though the N-k is a tedious and resource-requiring approach, it fails to identify the whole critical targets of the system when the full system data are not accessible. The analysis also shows that there are factors affecting the risk of the substations, such as the system topology, the criticality of the substation in combination with other substations in the system. This analysis provides important data for the next risk management step, i.e., determining the resources to be protected when doing risk/benefit analysis and selecting mitigation methods. From the results obtained for the system risk, it is profound that there are certain scenarios where the system is more vulnerable. Using these data, the cyber protection mitigation schemes can be prioritized for those vulnerable paths and devices to boost the system's resilience against cyber-physical kinds of attacks.

Chapter 4: Data Mining Based Cyber-Physical Attack Detection Tool for Attack-Resilient Adaptive Protective Relays

4.1 Introduction

This chapter presents the proposed detection tool for the overcurrent adaptive protective relays, as the second grid resilience enhancement strategy, refer to Figure 1.3. As discussed in Chapter 1, maintaining a proper operation of the adaptive protection schemes is truly an important strategy in enhancing grid resilience. Designing cyber detection and protection systems for these schemes boosts the preparedness potential of the network as recommended by the NIPPS. This chapter proposes a detection tool —based on Rough set analysis— responsible for identifying compromised settings sent to overcurrent relays.

4.2 The Need for Adaptive Protection Schemes In Modern Grids

In fact, the trend of upgrading existing power grids is resulting in dependency on communication technologies to guarantee reliable, efficient, and secure power transfer and delivery [108]. Accordingly, the existing physical infrastructure has to be tightly coupled to cyber infrastructure. In addition, new elements are being introduced to the power grid, such as distributed generators (DGs), storage systems, and smart meters, which impose adopting digital two-way communication technology. Thus, the power grid is becoming vulnerable not only to physical threats but also to cyber attacks. These further arrangements increase the complexity and the requirements of power grids.

Designing a reliable protection scheme for modern grids is complicated because short-circuit current levels keep varying in the network, as discussed in Chapter 2, which add to the complexity of the relays' detection and selectivity capabilities. It can also result in the loss of some generators and loads when there is an unnecessary operation of some relays. These consequences would degrade the power system performance in turn [109]. To overcome those protection problems, several solutions have been proposed. A review of these solutions was carried out in [110], with a discussion of the practical limitations of each. It concludes that adaptive protection schemes are the best to handle these challenges with the help of communication-assissted relays. However, the problem of lacking cybersecurity means for these relays is still unsolved. This thesis tries to fill this security gap by developing a detection tool that can be built into microprocessor-based relays for checking the incoming settings against data integrity attacks. Relays will be trained to differentiate between genius and compromised settings (or erroneous settings) without the need for any cyber properties.

4.3 Cyber Challenges of Communication-assisted Protection Systems

4.3.1 Cyber Vulnerabilities of Protection System

Remote access to protection devices is always needed to assess power networks, identify fault locations to help repair crews, analyze protection devices' operation, and attain information for planning studies. Protection engineers typically need to read the data stored in relays, fault recorders, etc., to analyze system disturbances, coordinate protection schemes, and ensure compliance with the related standards. They should also have access to change settings and check breaker status and intrusion alarms as required [59]. The cyber-physical attack on substation networks can be launched from different points such as remote access points, control centers, or substation user interface, as explained in Chapter 3.

4.3.2 Consequences of Cyber Attacks on Relays

Cyber-attacks can result in critical disruptions and other consequences for different targets in the power grid. From a cybersecurity perspective, the attack on the relay can result in either a relay sending a tripping signal when it should not or failing to send that signal when it should. From a power system viewpoint, incorrect settings have a considerable effect on grid operation. In other words, false tripping interrupts network customers unnecessarily, degrading network reliability. Besides service continuity problems, it causes component outages that can sometimes initiate cascading failure, disturbing grid stability [111]. Undesirably, the risk to stability is reflected as a risk to power system safety. On the other hand, failure to send tripping signals when required results in network-asset damage and potential harm to bystanders.

4.4 The Rough Set-based Rule Learning

This section will give an overview of the main steps of implementing Rough set classification, which will be used in the offline phase of our algorithm (developed in Figure 4.9). The Rough set theory was first proposed by the Polish computer scientist Zdzisław Pawlak in 1982 [114] and is concerned with classifying and analyzing imprecise knowledge [112]. The concept behind this classification is employing indiscernibility relations to evaluate to what extent two objects are similar.

4.4.1 Information Tables

A dataset is modeled in the form of an information table, wherein each row represents an object (a case or an event), and each column represents an attribute (a variable) that can be measured/supplied for each object [112]. Attributes are divided into two types: conditional and decisional.

Let $I = (U, A)$ be an information system, where U(the universe) is a finite set of objects, and A is a finite set of attributes such that $\forall\, a \in A\ \ a: U \rightarrow Va, Va$ is called the value set of attributes.

4.4.2 Indiscernibility Relation and Set Approximation

The theory sees the data as equivalence classes, in other words, sets of objects indiscernible with regard to the attributes. A Rough set is a set of objects that the equivalence classes cannot exactly represent because the set may include and exclude objects which are indiscernible with regard to the attributes P [113].

For any $P \subseteq A$,

$$IND(P) = \{(x, y) \in U^2 \mid \forall\, a \in P, a(x) = a(y)\} \tag{4.1}$$

where $IND(P)$ is called the P-indiscernibility relation; that is, if $(x, y) \in IND(P)$, then objects x and y are indiscernible from each other by P attributes. In that way, any target set, X, can be approximated using 1) the equivalence classes that are completely contained in the set (the lower approximation of X or the positive region) and 2) the equivalence classes with at least one object in the set (the upper approximation of X or the negative region):

Lower approximation:

$$\underline{P}X = \{x \mid [x]_P \subseteq X\} \tag{4.2}$$

Upper approximation:

$$\overline{P}X = \{x \mid [x]_P \cap X \neq \emptyset\} \tag{4.3}$$

where $[x]_P$ is the equivalence classes of the P-indiscernibility relation. And the difference between the upper and the lower approximation creates the boundary region,$BR(X)$, which consists of the objects that cannot be ruled in or out of the target set, X. The representation of these approximations can be depicted in Figure 4.1.

$$BR_P(X) = \overline{P}X - \underline{P}X \tag{4.4}$$

4.4.3 Reducts

After getting the equivalence classes, a reduction is required to attain the set approximation by keeping only attributes that preserve the indiscernibility relation while rejecting any redundant attributes. Hence, a reduct can be defined as a minimal subset of attributes that enables the same discernibility as the whole set of attributes. In other words, it distinguishes one object from all objects with a different decision [114]. Unfortunately, finding the set of all reducts is an NP-complete problem [115]. However, finding reducts can be achieved by several approximation algorithms, e.g., greedy algorithms, genetic algorithms, etc. [115], which are all based on constructing a discernibility matrix and the corresponding discernibility functions.

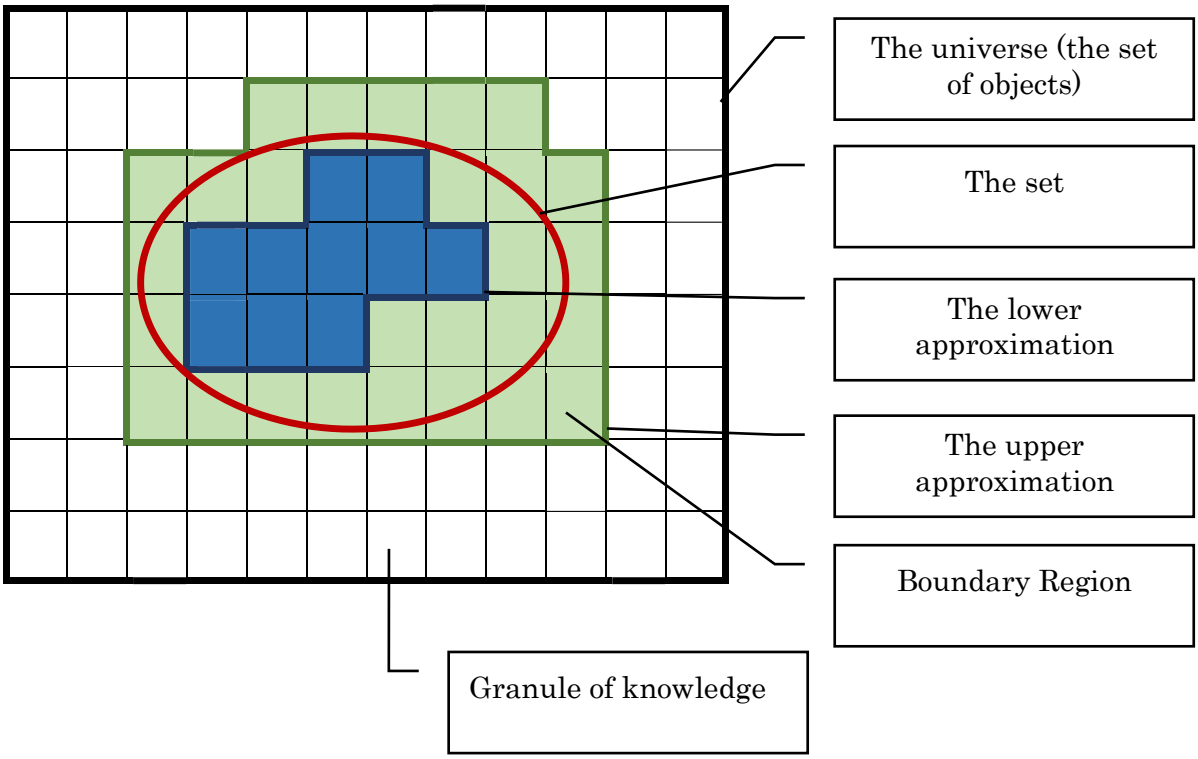


Figure 4.1 Representation of Approximation Sets

4.4.4 Decision Rules

Based on the values for each attribute in the reduct, If-Then rules can then be generated. The Then-part can include more than one decision class, depending on whether the decision class is rough with respect to the attributes in the reduct.

4.5 Proposed Detection Tool for Digital Relays

The arrangement of the targeted adaptive overcurrent protection scheme employs digital relays that isolate faults by taking appropriate tripping decisions based on settings obtained from a central processing unit. This unit calculates the settings required for each relay based on the current status of the network, e.g., the network topology, connected DGs/loads.

To solve the problem of a relay's limited computational capabilities, Rough set classification can be implemented in two phases. First, the knowledge extractor generates a set of rules that will determine the normal and abnormal behavior of the system. This phase can be carried out offline during the initialization process, and its output (the set of rules) can be loaded into the relay during this process. Then, the second phase is implemented online during operation, wherein the incoming settings will be checked using the preloaded set of rules. This second phase is simple and could easily be implemented in the digital relay. The

verification of the settings received can be determined by three attributes: the bus voltage of the associated relay, its line current, and the relay setting (TDS).

4.5.1 Probabilistic Analysis

For planning purposes, the probabilistic approaches can reflect the uncertainties in variables such as the load demand and the generated power of DGs. These variables are affected by certain external factors that are hard to predict accurately, such as weather conditions. To consider these uncertainty's impacts, a probabilistic model is then needed. Probabilistic short circuit analysis aims at calculating a probability distribution of short circuit current magnitudes at various locations in the system. This approach can provide information on the likelihood that short circuit currents exceed/fall below certain values.
In this research, the probabilistic analysis is used to get a database of:

1- the bus voltages, which are considered the pre-fault voltages,
2- the load currents seen by each relay before the fault occurrence, and
3- the fault currents seen by each relay in the network.

In order to build this database, an algorithm based on Monte Carlo simulation will be developed.

4.5.2 System Uncertainties Associated with Fault Calculation

Probabilistic analysis of short circuit currents for relay coordination is primarily affected by the following statistical variables, which are associated with the power system operating conditions at the time of fault occurrence, namely

1- DG availability
2- Renewable DG levels
3- Loading levels

Besides, these variables affect the pre-fault conditions, i.e., the pre-fault voltages and the loading current. In this work, to be more generic (considering microgrid applications), the pre-fault conditions cannot be neglected when performing short circuit analysis because the microgrid fault currents, especially during the islanded mode of operation with IBDGs, equal just a few multiples of normal currents before faults. In conclusion, there are three input variables as listed above, and three output variables represent sets of pre-fault voltages, loading currents, and fault currents. Now, details of the input variables are found in Table 4.1.

Table 4.1 Input Random Variables

Random Variable	Its Type	Its Value & Probability
X_1: DG availability	Discrete	▪ {0,1}, '0' represents not connected, '1' connected. ▪ {10%, 90%}, for example.
X_2: Renewable DG level	Continuous	Explained in Section 4.5.4.
X_3: Loading level	Continuous	Explained in Sections 4.5.3 and 4.5.4.

4.5.3 Modeling of Load Demand and DG Injected Power

For load demand modeling, the load data given in the IEEE RTS [116] is used. Then, the whole year is divided into four seasons, and each season is represented by two clusters: a weekday and a weekend cluster. Consequently, the whole load curves should be classified into eight clusters (4 seasons × 2 clusters/season). Note that the IEEE RTS assigns the same data for spring and fall, which reduces the number of clusters to six, as listed in Table 4.2.

Table 4.2 Different Load Models

Season's Cluster	Model
Summer Weekday	L_1
Summer Weekend	L_2
Winter Weekday	L_3
Winter Weekend	L_4
Fall/Spring Weekday	L_5
Fall/Spring Weekend	L_6

Each model is intended to be denoted by a representative load curve (centroid) along with a PDF for the error around this centroid. For obtaining the centroids, the K-means clustering is applied by minimizing the squared error function between a data point x_i^j that belongs to a cluster and the cluster centroid c_j, represented by the following optimization problem,

$$Min. \quad \sum_{j=1}^{k}\sum_{i=1}^{n} || x_i^j - c_j ||^2 \tag{4.5}$$

The reason behind clustering the load demand into eight models per year instead of only one is that demand is seasonal and has a recognizable variation between weekend and weekday levels.

4.5.4 Simulation Results

A MATLAB m-file has been developed for clustering the data; the obtained centroid values for the 24 hours are listed in Table 4.3. Each centroid is plotted with associated curves of the same cluster, and the results are presented in Figure 4.2 to Figure 4.7.

Table 4.3 Clusters' Representative Centroids

	L_1	L_2	L_3	L_4	L_5	L_6
1	0.523	0.478	0.576	0.530	0.449	0.423
2	0.491	0.452	0.542	0.489	0.442	0.411
3	0.474	0.426	0.516	0.462	0.428	0.389
4	0.458	0.420	0.508	0.449	0.414	0.372
5	0.458	0.413	0.508	0.435	0.421	0.366
6	0.474	0.401	0.516	0.442	0.464	0.366
7	0.523	0.401	0.637	0.449	0.514	0.383
8	0.621	0.426	0.740	0.476	0.606	0.417
9	0.711	0.523	0.817	0.544	0.678	0.468
10	0.777	0.556	0.826	0.598	0.706	0.502
11	0.810	0.588	0.826	0.612	0.713	0.519
12	0.818	0.601	0.817	0.618	0.706	0.530
13	0.810	0.601	0.817	0.612	0.664	0.513
14	0.818	0.594	0.817	0.598	0.656	0.507
15	0.818	0.588	0.800	0.591	0.642	0.507
16	0.793	0.588	0.809	0.591	0.628	0.485
17	0.785	0.594	0.852	0.618	0.642	0.479
18	0.785	0.607	0.860	0.680	0.656	0.496
19	0.760	0.614	0.860	0.673	0.685	0.519
20	0.752	0.614	0.826	0.659	0.699	0.564
21	0.752	0.646	0.783	0.639	0.685	0.547
22	0.760	0.601	0.714	0.625	0.642	0.535
23	0.711	0.568	0.628	0.591	0.571	0.507
24	0.589	0.517	0.542	0.550	0.499	0.479

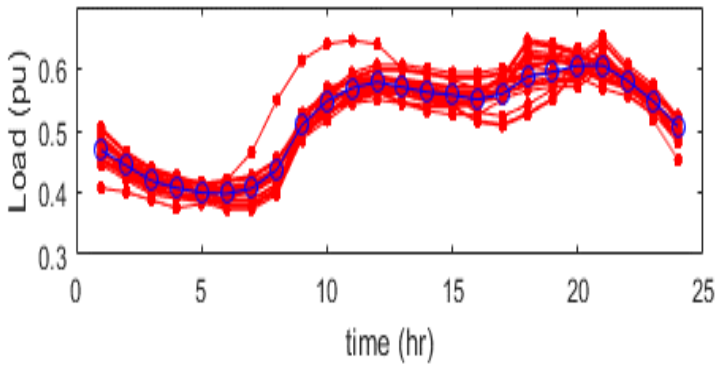


Figure 4.2 Cluster of Load Demand Curves for Summer Weekdays and Its Representative Centroid, L1

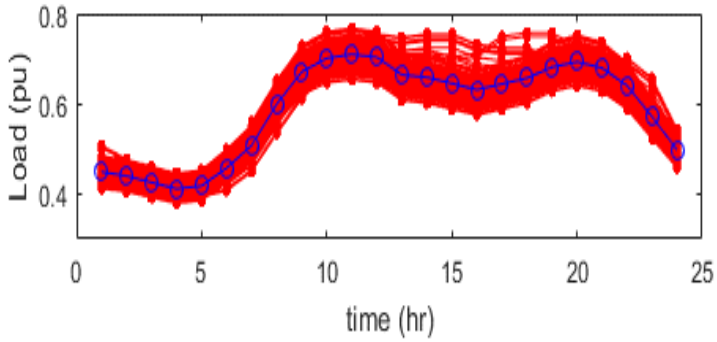


Figure 4.3 Cluster of Load Demand Curves for Summer Weekends and Its Representative Centroid, L2

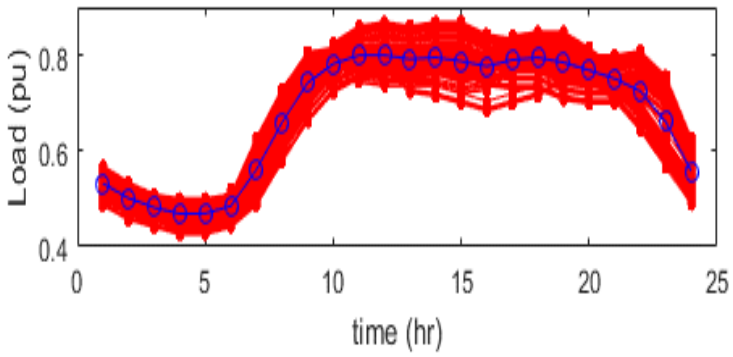


Figure 4.4 Cluster of Load Demand Curves for Winter Weekdays and Its Representative Centroid, L3

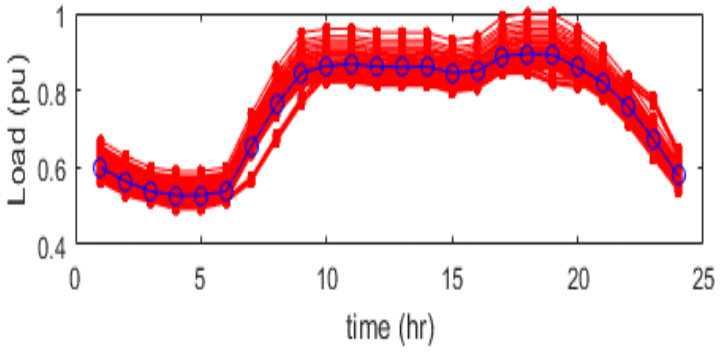


Figure 4.5 Cluster of Load Demand Curves for Winter Weekends and Its Representative Centroid, L4

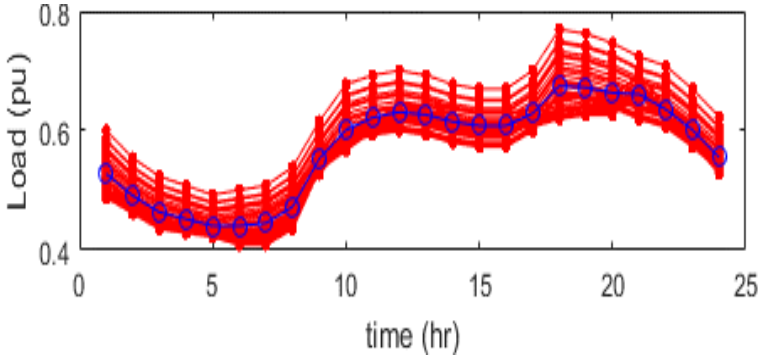


Figure 4.6 Cluster of Load Demand Curves for Spring/Fall Weekdays and Its Representative Centroid, L5

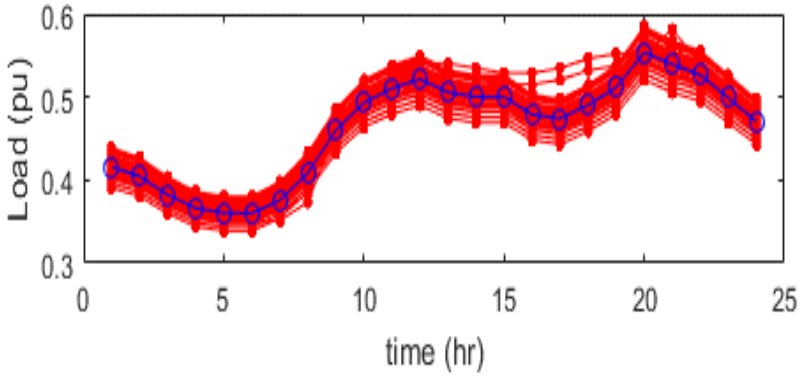


Figure 4.7 Cluster of Load Demand Curves for Spring/Fall Weekends and Its Representative Centroid, L6

As mentioned, each model will be represented by a centroid and a PDF of the error to further improve the modeling. The differences between all load curves belonging to a certain cluster and their representative load curve are calculated to select a proper PDF. The PDF for the error is best fitted to Weibull distribution as stated in [117]. The Weibull parameters are given in Table 4.4, where α_w, β_w, and Γ_w are the Weibull shape, scale, and location parameters, respectively.

Table 4.4 Weibull PDF Parameters for Different Load Models [117]

Model	α_w	β_w	Γ_w
L_1	2.4226	0.09934	-0.08812
L_2	1.7979	0.05353	-0.04758
L_3	5.247	0.22676	-0.20872
L_4	5.1698	0.16188	-0.14876
L_5	8.2088	0.21547	-0.20307
L_6	17.046	0.29313	-0.28402

In a similar way, DGs injected output power can be clustered. The data used is taken from Ref. [118]. The best PDF to fit the wind output power data, according to that reference, is the Johnson SB distribution during all the seasons. The Johnson SB PDF fit parameters obtained is shown in Table 4.5, where γ and δ are shape parameters, λ is a scale parameter, and ζ is a location parameter.

Table 4.5 Johnson SB PDF Parameters for Different Wind DG Models [118]

Model	Season	γ	δ	λ	ζ
WD_1	Spring	0.40832	0.46673	0.97881	-0.0765
WD_2	Fall	0.1866	0.49059	0.98015	-0.00616
WD3	Summer	0.48423	0.55561	0.97956	-0.00874
WD4	Winter	-0.0199	0.48906	0.95746	0.005568

The DG availability is used for dispatchable DGs. However, because the DGs were assumed to be renewable in this simulation, the DG availability random variable here will be considered to reflect only the maintenance periods, with a PMF= {0.05 0.95}.

4.5.5 Proposed Algorithm for Initialization Phase

Monte Carlo Simulation-based algorithm that models the required network is developed as shown in Figure 4.8. It consists of running the load flow analysis to get the pre-fault voltages and currents and then performing short circuit calculations to get short circuit currents. For simulation purposes, an OpenDss script was created for the analysis, driven by a MATLAB m-file through the COM interface to provide the values of the random variable for each iteration. The outputs of this simulation are used for the second step, wherein the relay settings are calculated.

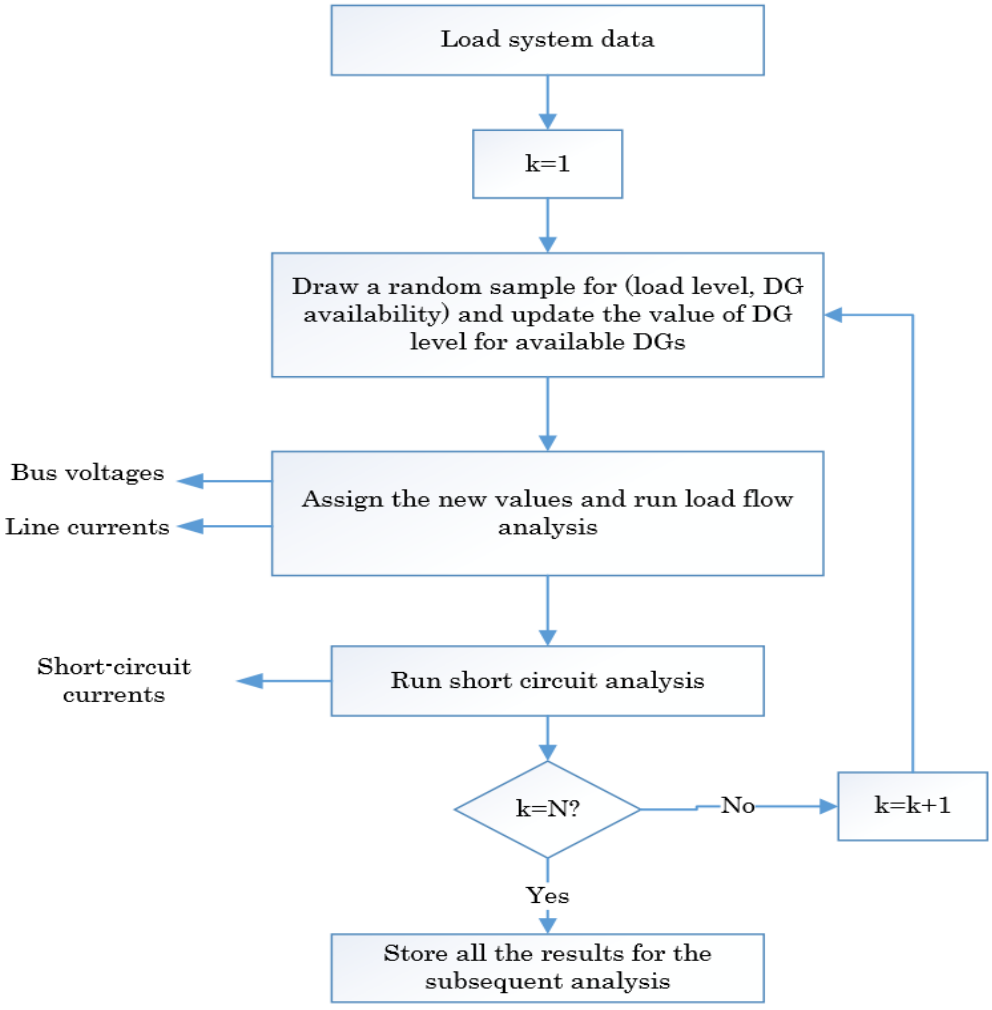


Figure 4.8 Probabilistic Analysis Algorithm

For realizing the offline procedures, the flowchart shown in Figure 4.9 is proposed. Its steps can be explained as follows,

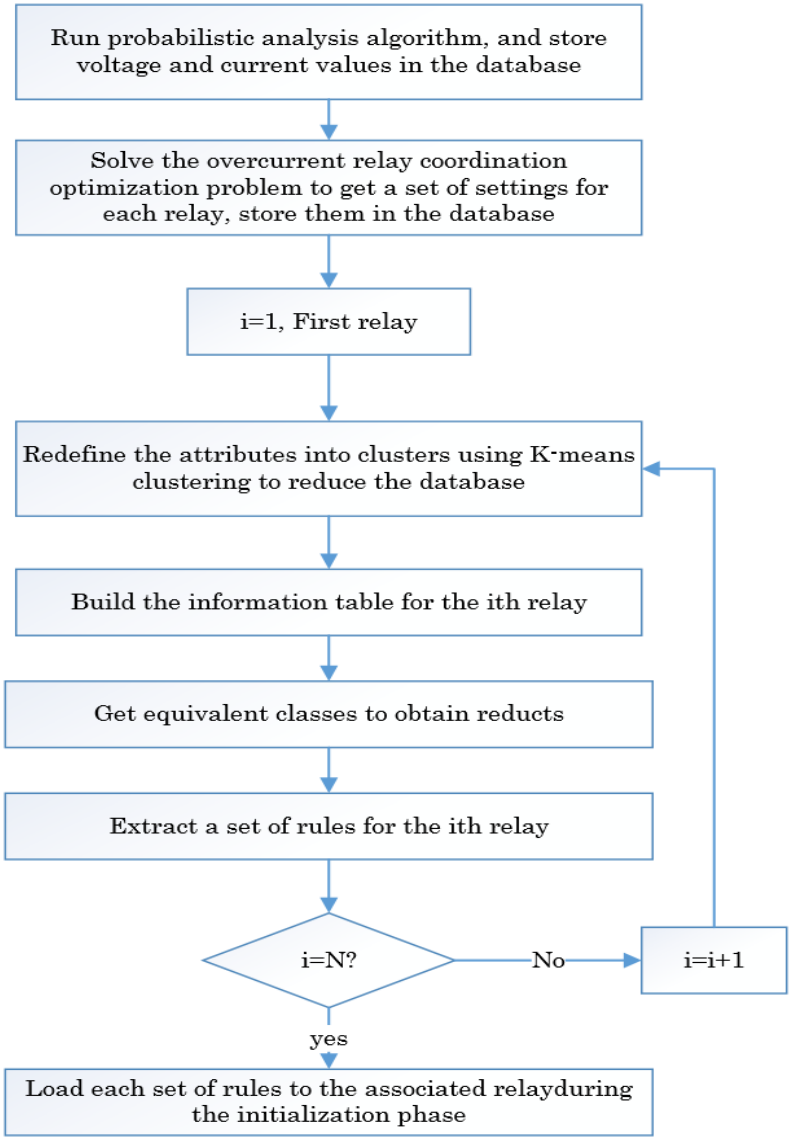


Figure 4.9 Cyber attack Detection--Offline Phase

The relay time-current characteristic can be given as in [119],

$$t = \frac{\beta}{\left(\frac{I_{SC}}{I_P}\right)^{\alpha} - 1} . TDS \tag{4.6}$$

where t is the relay operating time. The parameters α, β are standard values determining the degree of the inverse of the relay characteristics. TDS is the time dial setting (relay setting). I_P is the relay pickup current and I_{SC} is the short circuit current passing through the relay. An optimization problem is formulated where the objective function, denoted by 'T', is the summation of the operating times of all relays. Those times are to be minimized while maintaining the conditions of protection coordination.

$$Min. \quad T = \sum_{i=1}^{n} W_i t_i \tag{4.7}$$

where n is the total number of relays, and t_i is the operating time of the i^{th} relay. The weighted coefficient, W_i is a value that depends on the probability of a short circuit fault occurring in the i^{th} zone, which is assumed to be one here. This problem is subject to the following constraints,

- ***Limits of the relay settings:***

$$TDS_{min} \leq TDS \leq TDS_{max} \tag{4.8}$$

where TDS_{min}, TDS_{max} are the minimum and maximum TDSs for each relay, respectively.

- ***Coordination criteria:***

$$t_j - t_i \geq CTI \quad \forall (i,j) \in \Omega \tag{4.9}$$

The time t_j is the operating time of the backup relay, and Ω is the set of the main/backup relay pairs. The values of each attribute can be redefined into levels/clusters in order to classify them based on their values. Using k-means clustering, each attribute is classified into 10 clusters. Performing this step for all the attributes can reduce the set of relations but conserves the same classification of the original set of examples.

A knowledge database (information table) must then be built. The rows will contain the events which are the study cases in this application; the columns hold the attributes. The conditional attributes in this application are the bus voltage of the associated relay and its line current, whereas the decisional attribute is the relay setting (TDS). Next, the reducts are found, and the set of rules —in the form of IF-Then rules— will be generated.

4.6 Simulation Setup and Results

4.6.1 System Description

The IEEE 34-bus distribution test system [120] has been adopted for this case study with some modifications. Two identical distributed generators are connected to buses 854 and 840, with an installed capacity of 336 KW each. The relays are then located as well. All relays are communicating with the central processing unit to get the updated settings. The single-line diagram is shown in Figure 4.10.

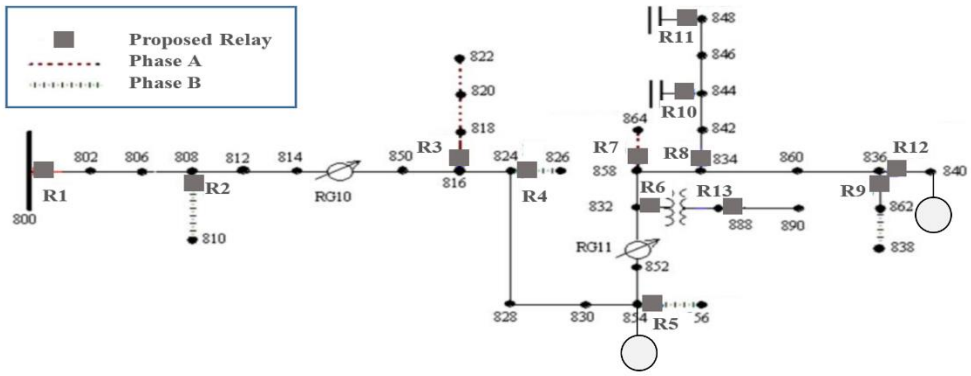


Figure 4.10 IEEE 34-bus Test System with DGs and Proposed Relays

4.6.2 System Modeling

This system was modeled in the Electric Power Distribution System Simulator (OpenDSS) [121]. An OpenDSS script file has been created to perform load flow and short circuit analysis in the presence of the DGs. This script is driven by a MATLAB m-file developed to perform the Monte-Carlo simulation. The DG availability's random variable here is represented by a binomial distribution, with a probability p that the DG is connected to the network. For the DG connected to Bus 854, p=0.9, and p=0.5 for the one connected to bus 840. DGs are assumed to supply 50% of the load demand, shared equally between them. The simulation runs 2000 iterations, giving a maximum percentage error of the voltage mean of 0.2811% and the current mean of 3.2%, for all the relays, for a 95% confidence interval (assuming normal distribution). Using the outputs of this step, the coordinated relays TDSs are then calculated for the 2000 cases.

4.6.3 Rough Set and Rule Generation

Relay#1 is located at the point of common coupling with the grid, Relay#8 protects a feeder with spot and distributed loads, and Relay#12 is located on a line that has a DG connected. Due to their importance and diversity, those relays are selected for testing. For these relays, each voltage and current attribute is clustered into 10 clusters using K-means. However,

when clustering the attributes of the relays, a fewer number of distinct centroids have been obtained. The results are given in Table 4.6. An information table has been constructed using the clustered attributes. Using Rosetta software [122], the information table was first reduced using Genetic Algorithms. The set of rules were generated: 44 rules for Relay#1's case, 42 rules for Relay#8's case, and 38 rules for Relay#12's case. If the incoming setting satisfies any of these rules, it is marked as genuine and will be used by the relay.

Table 4.6 Centroids for Investigated Relays

No.	Relay#1			Relay#8			Relay#12		
	V	I	TDS	V	I	TDS	V	I	TDS
C1	1.014	27.33	0.206	0.851	17.78	0.102	0.949	8.20	0.001
C2	0.993	45.44	0.001	1.0173	14.19	17.857	1.008	1.23	20
C3	1.047	33.37	0.105	0.939	21.35	0.095	0.968	7.98	
C4	1.031	50.77	0.208	0.996	14.53	0.001	0.898	0.82	
C5	1.008	19.64	0.202	1.061	18.76	0.098	1.055	2.09	
C6	1.019	23.29		0.959	15.29		1.029	8.39	
C7	1.026	36.19		0.976	16.88		0.846	1.60	
C8	0.985	40.06		1.039	14.87		0.988	1.39	
C9	1.000	56.61		0.912	19.84		0.874	1.86	
C10	1.039	30.55		0.883	15.95		0.925	1.03	

As an illustration,Table 4.7 to Table 4.9 show samples of the generated rules for Relay#1, Relay#8, and Relay#12, respectively. Support refers to the number of objects in the training set matching the corresponding rule, and the rule coverage is its support divided by the number of objects in the training set.

Table 4.7 Sample of Results of Relay#1's Rules

No.	Rule	Support	Coverage
R1	IF Voltage=4 AND Current=1 Then TDS=1	103	0.0515
R2	IF Voltage=1 AND Current=3 Then TDS=4	151	0.0755
R3	IF Voltage=10 AND Current=6 Then TDS=1	91	0.0455
R4	IF Voltage=2 AND Current=4 Then TDS=1 OR 4	74	0.037
R5	IF Voltage=6 AND Current=10 Then TDS=4	107	0.0535
R6	IF Voltage=4 AND Current=3 Then TDS=5	18	0.009
R7	IF Voltage=10 AND Current=10 Then TDS=5	26	0.013

Table 4.8 Sample of Results of Relay#8's Rules

No.	Rule	Support	Coverage
R1	IF Voltage=8 AND Current=4 Then TDS=1 OR 5	85	0.0425
R2	IF Voltage=4 AND Current=4 Then TDS=5	183	0.0915
R3	IF Voltage=4 AND Current=2 Then TDS=1	89	0.0445
R4	IF Voltage=2 AND Current=4 Then TDS=1 OR 5	129	0.0645
R5	IF Voltage=10 AND Current=1 Then TDS=1 OR 3	51	0.0255
R6	IF Voltage=10 AND Current=9 Then TDS=3	25	0.0125

Table 4.9 Sample of Results of Relay#12's Rules

No.	Rule	Support	Coverage
R1	IF Voltage=6 AND Current=4 Then TDS=1	16	0.008
R2	IF Voltage=8 AND Current=2 Then TDS=1	90	0.045
R3	IF Voltage=9 AND Current=9 Then TDS=1 OR 2	13	0.0065
R4	IF Voltage=1 AND Current=1 Then TDS=1	93	0.0465
R5	IF Voltage=3 AND Current=1 Then TDS=1	82	0.041
R6	IF Voltage=5 AND Current=4 Then TDS=1	59	0.0295

4.7 Performance Evaluation

For the purpose of validating the tool, a test dataset (set of attributes) of 200 cases has been generated for each relay under investigation. For relay settings: 100 left genuine, and 100 have been compromised using the following attack template. The classification results are then presented. Finally, the performance measures and execution times have been calculated.

4.7.1 Attack Template and model

To modify the relay setting, a scaling attack is used, which involves modifying true values to higher or lower ones depending on the scaling attack parameter λs [123].

$$f^*(t) = \begin{cases} f(t), & t \notin \tau \\ (1 + \lambda s) * f(t), & t \in \tau \end{cases} \quad (4.10)$$

where t and τ represent time and attack period, respectively. The choice of λs depends on the degree of an attacker's knowledge of the system and their desired impacts. The scaling parameter is selected to cover a wide range of values, extending from $[-0.1: 10]$. The values in the range $(-0.1 \leq \lambda s < 0)$ simulate attacks done by an adversary who wants the breaker to trip faster for normal currents or currents below the short circuit values. This case results in interrupting customers unnecessarily, and in some cases, can cause overloading over other lines, which can end up with cascading failure. The rest of the range (i.e., $0 \leq \lambda s \leq 10$), however, simulate the intention of delaying the breaker operation when it should act faster. That case can result in miscoordination between devices or even fires, safety hazards, and asset damage when main and backup protection devices are all targeted.

The following realistic limitations and assumptions are considered to model the cyber attack.

1- It is assumed that an attacker can gain access to the information of the protection systems and their communication protocols to manipulate the digital relay setting signal coming from a remote control center.
2- The measured voltages and currents are local and secured.
3- Attackers can target one or more relays at the same time.
4- Attackers know the line protected by the smart relays.
5- Attackers cannot trip circuit breakers directly.
6- Attacker capabilities are limited.

4.7.2 Classification Results

Using the mentioned attack template, all the test cases have been checked using the rules obtained in Section 4.6.3. The results are presented in the confusion matrices given in Table 4.10 to Table 4.12, where TP, TN, FP, and FN refer to true positive, true negative, false positive, and false negative, respectively.

Table 4.10 Results for Relay#1

Total=200		**Predicted**	
		Yes	No
Actual	Yes	True Positive (TP)=97	False Negative (FN)=3
	No	False Positive (FP)=0	True Negative (TN)=100

Table 4.11 Results for Relay#8

Total=200		**Predicted**	
		Yes	No
Actual	Yes	True Positive (TP)=97	False Negative (FN)=3
	No	False Positive (FP)=1	True Negative (TN)=99

Table 4.12 Results for Relay#12

Total=200		**Predicted**	
		Yes	No
Actual	Yes	True Positive (TP)=99	False Negative (FN)=1
	No	False Positive (FP)=0	True Negative (TN)=100

4.7.3 Performance Measures

The following outcome measures have been calculated, and the results are presented in Table 4.13:

- **Accuracy (classification rate)** is calculated as the number of all correct predictions divided by the total number of cases in the dataset.

$$Accuracy = \frac{TP + TN}{Total} \tag{4.11}$$

- **Error Rate (ERR)** is calculated as the number of all incorrect predictions divided by the total number of cases in the dataset.

$$ERR = \frac{FN + FP}{Total} \tag{4.12}$$

- **Sensitivity (probability of detection)** measures the proportion of actual positives being correctly identified. This measure is crucial for attack detection tools since false positives are better tolerated by the system than false negatives.

$$Sensitivity = \frac{TP}{TP + FN} \tag{4.13}$$

Table 4.13 Results of Evaluation Measures

MEASURES	Relay#1	Relay#8	Relay#12
ACCURACY	98.5%	98%	99.5%
ERR	1.5%	2%	0.5%
SENSITIVITY	97%	97%	99%

4.7.4 Execution Time

As mentioned, carrying out the proposed detection method is done in two stages: offline and online. The complex part is done offline and only once- during the system initialization phase, whereas simple calculations are done by the relay online. Needless to say, protection system applications are time-sensitive. Therefore, the time-latency of real-time communication used is always restricted to 4ms [124], [125]. In this section, the execution times of classifying the incoming settings have been monitored for all the relays under investigation using the test dataset used earlier. These times have been measured and are plotted in Figure 4.11. The simulation has been done in MATLAB, which can easily convert this code into other forms suitable for any smart relay hardware platform used, e.g., C, C++, or Structured Text and Ladder Diagrams (for PLC and Programmable Automation Controller (PAC) devices). Based on the simulation results, the average execution times measured for Relay#1, Relay#8, and Relay#12 are 0.45269ms, 0.43166ms, and 0.44203ms, respectively. With an eye toward considering the time requirements, the very rapid execution times here confirm the tool's practicality for protection system applications.

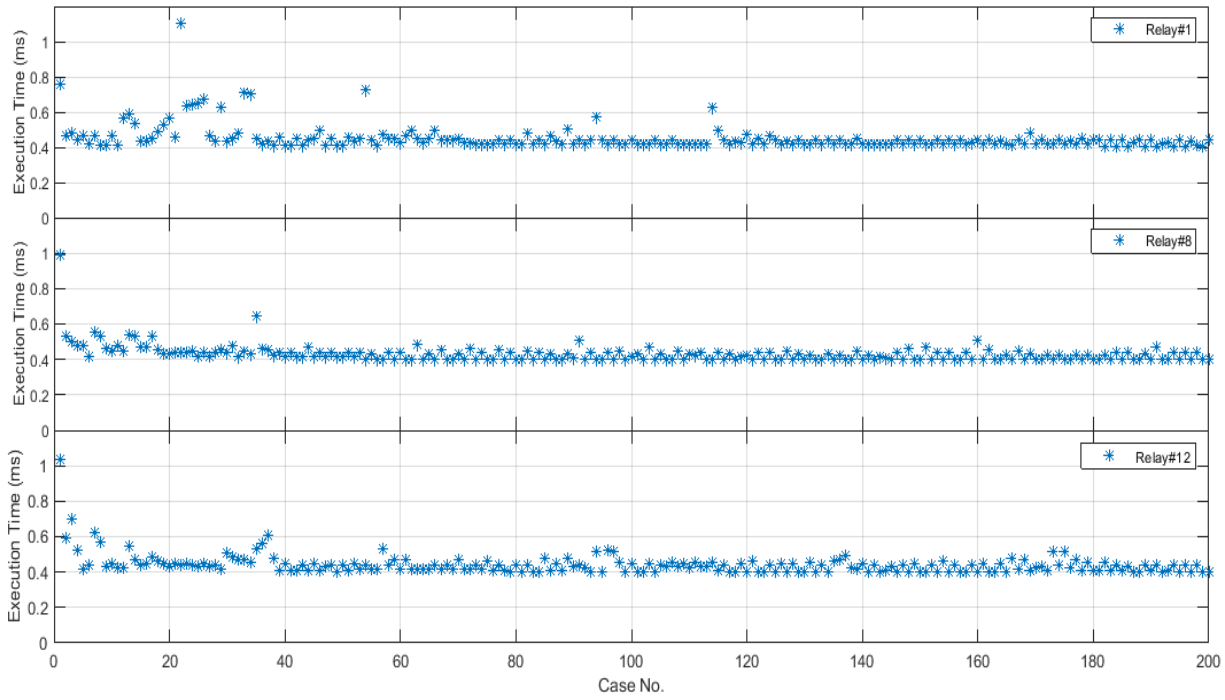


Figure 4.11: Execution Times for Relay#1, Relay#8, and Relay#12

4.8 Summary and Conclusions

The work in this chapter proposes a Rough-set based detection tool that can identify incorrect settings for overcurrent relays in active distribution networks. This work aims to enhance the security of communication-based overcurrent relays used in adaptive protection schemes. Using the tool proposed, protective relays are able to assess the accuracy and consistency of

the settings they receive, maintaining the data integrity requirements. The tool is reliable since it uses only local measurements and pre-stored physical properties to judge the settings. A probabilistic short-circuit analysis has been done using Monte-Carlo simulation to obtain the physical attributes needed in the Rough set analysis. This probabilistic analysis considers the DG availability, renewable DG levels, different loading levels throughout the week and season. The k-means clustering technique has been used to efficiently classify the physical attributes into clusters in order to have an adequate number of decision rules. These attributes have been used to construct the information table of the rough set for the training stage. Repeating these procedures for each relay, a number of If-then rules have been generated and assigned to the corresponding relay. In that way, the relay's online mission is to only compare incoming settings using the pre-stored rules, which is very convenient when considering staying within the confines of digital relays' limited computational capabilities and the time sensitivity of protection applications.

The detection tool has been tested on the IEEE 34-bus benchmark systems with DGs added. The evaluation assessment of the tool's performance has been conducted using various measures: accuracy, error rate, sensitivity, and execution time. The results demonstrate the tool's superior ability to classify settings rapidly and efficiently. These results make the tool trustworthy to be used whenever there is a lack of security measures due to the narrowband communication channels used in a power system or the time-critical communication protocols. In addition, it can be used as an extra line of defense when applying the defense-in-depth strategy.

Since detection takes place within the relay itself, the tool proposed in this thesis can judge incoming settings regardless of the type of attack resulting in those incorrect settings. As discussed in Chapter 3, compromising a substation can happen in many ways due to either insider or external attacks. The settings of the IEDs can be modified through the user interface system or network-based intrusions. Network intrusions can be initiated as packet monitoring which prepares for modification attacks or conducted through replay attacks. Incorrect settings have a wide range of undesirable effects ranging from unnecessarily customer interruption and equipment damage to a cascading failure and grid stability problems, as discussed in Chapter 1. Also, the test dataset used has covered a broad range of settings to simulate different potential attacker profiles, e.g., script kiddies and cyber criminals.

The results of the modified IEEE 34-bus test system model in this study show high accuracy (up to 99.537%) and a high probability of detection (sensitivity) ranges from 97% to 99%. Also, the investigations showed that the detection process required a very short time frame. The obtained results prove that this technique is suitable for real-time applications to protect the power network from moving into insecure states and ensure that the power system remains prepared in the face of cyber-physical attacks conducted through adaptive relays. In conclusion, securing adaptive protection schemes help enable the broad deployment of these schemes. In turn, several problems in modern power grids —such as all microgrid protection challenges, including changing network topology, intermittent natures of renewable DGs, varying short circuit currents, selectivity problems, and islanding— can be overcome. Therefore, securing adaptive schemes is considered crucial for modern power grids and grid cyber-physical resilience enhancement.

Chapter 5: Graph-theoretic Priority Load Restoration Strategy for Resilient Distribution Networks

5.1 Introduction

The Distribution Network Reconfiguration (DNR) is a combinatorial optimization problem that searches the available network configurations for an optimal solution that satisfies all the restoration constraints [126]. Thanks to the modern power grids, the reconfiguration process can be done remotely using remote-controlled switches [127]. In this chapter, a resilient priority load restoration strategy is proposed with the objective of enhancing the resilience of the power grid; refer to the main objectives in Figure 1.3. This restoration strategy aims to reconfigure the network to restore the maximum out-of-service load through resilient paths.

5.2 Load Prioritization

Critical loads/customers are those who provide daily services essential for preserving life, safety, and health of the communities, such as fire stations, hospitals and health facilities, police stations, water treatment/pumping stations, etc. These services are vital during major power outages. Utilities always work hard to prevent planned outages and load shedding to those customers. However, during disruptive events, critical customers can be affected too. Each Utility has its own load priority lists, which have the loads sorted according to their criticality. These lists are needed for several processes, such as load management systems and post-fault service restoration. In this chapter, we consider load priority for more realistic analysis.

5.3 Problem Description

Originally, reliability metrics were designed to measure the system's performance to provide power to all connected loads. However, as discussed in Chapter 2, during extreme conditions, the system priority would be restoring power to critical loads, and this is one of the main requirements of resilient distribution systems [29],[30], which cannot be captured by reliability metrics [128].

As illustrated in Figure 2.1, when a disruptive event hits the system, the system moves to a degraded state followed by a recovery state. The recovery state includes both the operational recovery and the infrastructure recovery, refer to Figure 2.2. Thus, the restoration process should be performed as fast as possible to restore the loads interrupted, i.e., using network reconfiguration, until the infrastructure repair is completed (which often takes a very long

time, as shown in Appendix A). During the restoration stage, either all the out-of service load will be picked up by re-routing power through tie switches or some parts of the network will have no way to reconnect back to the main grid. In the latter case, the out-of-service critical loads can be supplied from accessible DGs. In that case, the non-critical loads will be disconnected such that critical loads can be supplied for a longer period.

Also, since the event can be of a coordinated cyber-physical attack type, it is important to guarantee that the reconfiguration path is resilient to subsequent attacks. In this way, the restored loads have a better chance of survival in case there is a subsequent event. This problem will be taken care of in the proposed strategy.

5.4 Restoration Problem Formulation

In this chapter, a resilient restoration strategy is proposed that aims to maximize the restored loads based on their priority and maximize the resilience of the Post-Restoration Network (PRN), besides satisfying both operational and topological constraints.

5.4.1 Restoration Objectives

The proposed restoration objectives focus on the total restored demand and the resilience of the PRN for a given disruptive event. Post-restoration resilience is characterized by the risk factor of the tie switches that will be closed during the restoration process. In other words, the selection criterion of the restoration switches among all the candidate switches is to pick the switches with the least risk indices in fear of subsequent attacks. In this way, the restored priority loads will have a better chance of survival after restoration.

Accordingly, the objective functions maximize the total weighted sum of loads picked up after cyber-physical attacks and minimizes the total risk indices of the switches to be restored.

$$\text{Max} \sum_{i \in \Gamma} \gamma_i \, \omega_i \, P_{L,i} \tag{5.1}$$

$$\text{Min} \sum_{i,j \in A} \alpha_{ij} R_{ij} \tag{5.2}$$

where ω_i denotes the priority weight associated with the load i whose power is $P_{L,i}$ and belongs to the load set Γ. γ_i is a binary assignment coefficient where $\gamma_i = 1$ indicates that the load at node i is picked up, and $\gamma_i = 0$, otherwise. A is the set of tie switches available in the network, R_{ij} is the risk factor of the switch (i, j), and α_{ij} is the binary decision variable indicating if a given normally-open tie switch will be selected to be closed for the restoration solution, i.e., $\alpha_{ij} = 1$ means the switch (i, j) is closed, and $\alpha_{ij} = 0$ occurs when the switch is not selected for a given restoration plan. We define a coefficient β such that the second objective function is ignored if there is no more than one layout for the network to be restored using the available switches. The overall objective function can then be written as,

$$\text{Max}\ \frac{\sum_{\text{i}\in\Gamma}\gamma_i\ \omega_i\ P_{L,i}}{\sum_{\text{i}\in\Gamma}\ \omega_i\ P_{L,i}} - \beta \sum_{\text{i,j}\in\text{A}} \alpha_{ij} R_{ij} \qquad (5.3)$$

If the whole interrupted area cannot be restored to the main grid (intentional islanding), the following objective function will be applied for this specific area considering the set of critical loads only Γ_{CR}.

$$\text{Max}\ \frac{\sum_{\text{m}\in\Gamma_{CR}}\gamma_i\ \omega_m\ P_{L,\text{m}}}{\sum_{\text{m}\in\Gamma_{CR}}\ \omega_m\ P_{L,\text{m}}} - \beta_m \sum_{\text{i,j}\in A'} \alpha_{ij} R_{ij} \qquad (5.4)$$

Therefore, the load weights will be given as ω_m, which denotes the weight of the critical load m that belong to the microgrid, whereas all the non-critical loads within this microgrid will have weights set to 0. The second part of the equation will be considered for the general case of more than one unrestored clusters with multiple candidate switches. If there is only one restoration layout, then β_m will be set to 0.

5.4.2 Restoration Constraints

A. Operational Constraints

The reconfigured distribution system should maintain safe operating conditions. The following constraints denote the set of these anticipated operational conditions.

- **Bus Voltage Limits Constraints**

For reliable system operation, bus voltages are expected to fall within the acceptable range of normal voltage limits. The bus voltage can change for several reasons, such as the loading on the lines and the reactive power demand of the loads. The ANSI C84.1 standard recommends voltage variation limits of ±5% of the nominal voltage for 60Hz electric power systems above 100 volts.

$$|\ V_B^{min}\ | \ \leq |V_b| \leq |\ V_B^{max}\ | \qquad \forall b \in \mathcal{B}_{is} \qquad (5.5)$$

where V_b is the voltage at bus b, V_B^{min} and V_B^{max} are the lower and upper limit of the bus voltage, respectively, and B_{is} is the set of buses in service.

- **Line Current Limits Constraints**

Line currents should not be greater than the permissible values.

$$|I_l| \leq |\ I_l^{max}\ | \qquad \forall l \in E_{is} \qquad (5.6)$$

where I_l is the current flowing through a distribution line l, I_l^{max} is the upper limit of the line current of line l, and E_{is} is the set of the distribution lines in service.

- **Feeder and Transformer Capacity Constraints**

The apparent power of each feeder, S_j, should not exceed its maximum capacity.

$$|S_j| \leq |S_j^{max}| \qquad \forall j \in \mathcal{F}_{is} \qquad (5.7)$$

where S_l^{max} is the maximum value for the complex power injection in a feeder j which belongs to the set of feeders F_{is}. Similarly, the total load of each feeder should not exceed the maximum capacity of the supplier transformer.

$$P_k^2 + Q_k^2 \leq (S_k^{max})^2 \qquad \forall k \in K \qquad (5.8)$$

where P_k and Q_k are the active and reactive power injected into feeder k, respectively, S_k^{max} is the maximum capacity of the transformer at feeder k, and K is the number of feeders on which a transformer is connected.

- **DGs Capacity Constraints** (only for the case of intentional islanding)

The sum of critical load restored in each microgrid should not exceed the total generator(s) capacity.

Note that: In the post-restoration state, any critical load can only be energized by one isolated microgrid $m \in M$. Thus, we define a_i^m as a critical load-microgrid assignment variable. It is a binary variable assigned for each critical load $i \in \Gamma_{CR}$ in the network where a_i^m=1 indicates that the critical load i is restored by the microgrid m, whereas a_i^m=0 if the load i does not belong to m. Similarly, we define another binary variable b_i^m as the DG-microgrid assignment variable to indicate whether the DG j$\in \Lambda$ belongs to microgrid m or not.

$$\sum_{i \in \Gamma_{CR}} a_i^m P_{L,i}^{max} \leq \sum_{j \in \Lambda} b_j^m P_{G,j}^{max} \qquad \forall\, m \in M \qquad (5.9)$$

$$\sum_{i \in \Gamma_{CR}} a_i^m Q_{L,i}^{max} \leq \sum_{j \in \Lambda} b_j^m Q_{G,j}^{max} \qquad \forall\, m \in M \qquad (5.10)$$

- **Unbalanced Three-phase Power Flow Constraints**

An unbalanced three-phase power flow is performed to evaluate the feasibility of the candidate solutions using OpenDSS. More details about the power flow and simulation environment are provided in Section 5.5.

B. Network Topology Constraints

The connectivity and the radial structure of the network should be maintained during the restoration process. The elementary tree transformation and minimum spanning trees search are employed to realize the topology constraints using the available tie switches, as explained in Section 5.6.

5.5 Unbalanced Three-phase Power Flow Simulation Environment

The OpenDSS [121] is a distribution-system script-driven simulation tool released by the Electric Power Research Institute (EPRI). In this chapter, the OpenDSS has been integrated with a MATLAB code to implement the algorithm. The OpenDSS simulation engine has a component object model (COM), which allows MATLAB command to access OpenDSS features. A MATLAB script has been developed to generate graphs, check network connectivity, search for the minimum spanning trees, etc. MATLAB calls the OpenDSS engine to perform the unbalanced three-phase power flow for the subgraphs sent by the MATLAB script. OpenDSS returns all monitored information back to MATLAB to determine whether a proposed solution satisfies the electrical and operating constraints for different faults and network configurations. The nominal OpenDSS structure is depicted in Figure 5.1.

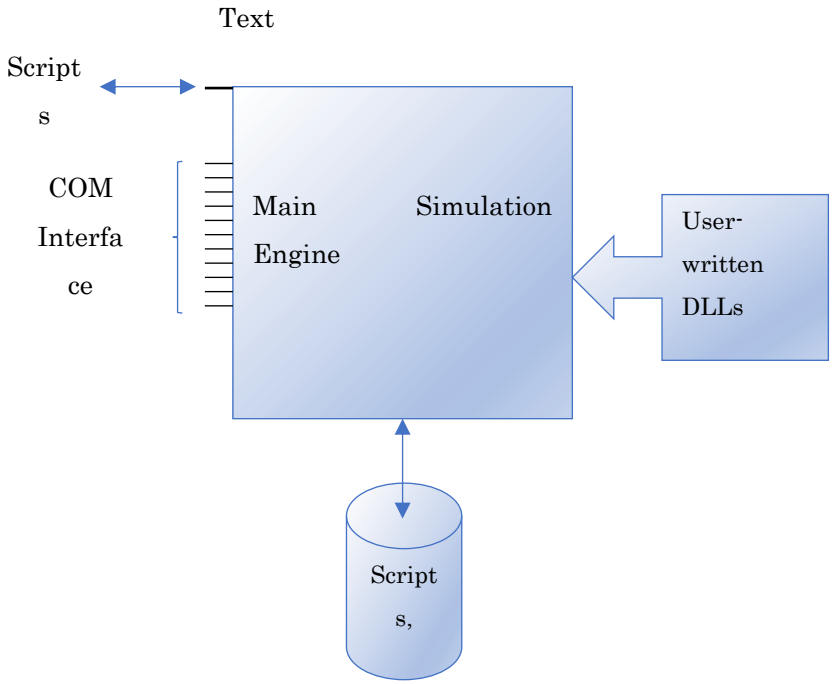


Figure 5.1 Nominal OpenDSS Structure

5.6 Graph Theory and Radial Distribution System Reconfiguration

5.6.1 Graphical Representation: Network and Fault Modelling

Let $G(V,E)$ be a graph, $V(G)=\{v_1, v_2,\ldots,v_N\}$ is the set of vertices of the graph G where N is the graph order, and the set $E(G)=\{(v_i,v_j)\}\subseteq V\times V$ is the edge set of the graph G. The graph, G, is a weighted graph when its edges have associated weights. The weight of each edge here represents its risk index, studied in Chapter 3.

A graph G is a tree, T, if it is connected and acyclic. Also, a tree, T, of a graph G is a spanning tree if it has all the nodes of G, i.e., $V(T) = V(G)$, but only $N - 1$ of the edges. During normal operation, the system topology is always kept radial. Subsequently, after the fault, the subnetworks formed will remain radial. To simulate a fault, remove some edges e. The $T - e$ gives N_c sub-trees where $N_c = |e| + 1$ components $(T_1, T_2, T_3, \ldots, T_{Nc})$, with orders $k_1, k_2, k_3, \ldots k_{Nc}$, respectively, where

$$k_1 + k_2 + k_3 + \cdots + k_{Nc} = N \tag{5.11}$$

And $E(T)$ is the disjoint union of $E(T_1)$, $E(T_2)$, $E(T_3)$, …, $E(T_{Nc})$, and $\{e\}$. However, when tie switches are turned on during the restoration process, cycles can be formed in the graph. To maintain the radiality condition during restoration, we will use the elementary tree transformation.

5.6.2 Elementary Tree Transformation for Maintaining Radiality

Due to a fault, switching operations happen in the system by opening a normally-closed sectionalizing switch(es). However, for the restoration process, other switching operations are needed by closing the normally-open tie switch(es). The latter should be done in a way that guarantees the network radiality is preserved.

A cut in the graph G is a partition of its nodes into two non-empty disjoint subsets (T_1, T_2) where $T_2 = V - T_1$. Also, the cut-set of a cut can be defined as the set of edges that cross the cut (have one end node in each subset of the partition). Thus, an edge e = (u, v) that crosses the cut (T_1, T_2) is a cut-set if $u \in T_1$ and $v \in T_2$.

Now, let T' be a spanning tree of a graph G and, let e"= (u", v") be an edge in G but not included in T', refer to Figure 5.2. Since T' is a spanning tree, there must be a path between nodes u" and v". Because the path must start in T_1, and end outside T_1 (ends in T_2 in this case), there must be an edge $e' = (u', v')$ on this path where $u' \in T_1$ and $v' \notin T_1$. Connecting both e' and e" together yields a cycle.

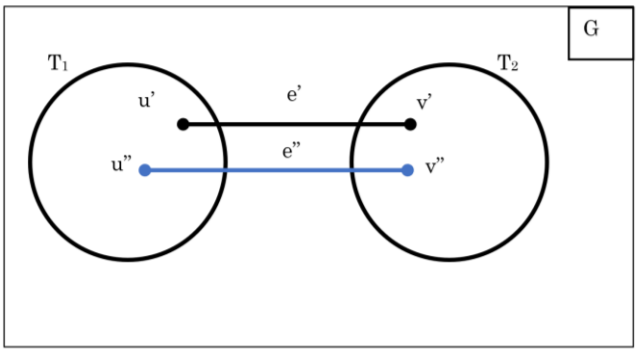


Figure 5.2 A cut in a given graph G

Hence, $T' - e' + e$" yields another spanning tree of the graph G, say T", where edges $e' \in T'$ and e" $\in T$". The transformation $T' \leftrightarrow$ T" is a cyclic interchange operation known as

Elementary Tree Transformation (ETT). It simply adds an edge to a spanning tree to create a cycle and then deletes another edge within this cycle.

Accordingly, each edge e' and e'' must have one end node belongs to one subset and the other end node belongs to the other subset in the graph. Based on this conclusion, when a fault occurs and the network is cut, the set of tie switches should be updated such that switches with both end nodes belong to the same subset (Intra-cluster switches) will be discarded from the algorithm because it will not keep the radiality conditions in the network. Hence, the candidate switches set is the one only including switches connecting different clusters. For example, let graph G in Figure 5.3 (a) is assumed a part of a distribution network with the available tie switches (edges e_{23}, e_{34}, and e_{45}--the blue lines). Let the spanning tree in Figure 5.3(b) represent the part of the distribution system G during normal operation. Assume node 1 is connected to the main substations, whereas nodes 2, 3, 4, and 5 are load nodes. If a fault occurs on line e_{35} (highlighted in red in Figure 5.3(c)), the sectionalizing switch disconnects this line, and the load at node 3 will be disconnected. The tree is now cut into two subsets, $T_1$and T_2, where$T_1(V) = \{1,2,4,5\}$ and $T_2(V) = \{3\}$. Applying EET, the switch e_{34} is selected to perform the cyclic interchange operation with e_{35} since its first end node $3 \in T_2$ and the second one, node $4 \in T_1$. The connection of edge e_{34} will results in the pickup of the load at node 3 and will generate a new spanning tree with the radiality being preserved. This new spanning tree is shown in Figure 5.3(d). Similarly, if another fault happens on line e_{14}, the switch e_{45} can be connected generating a newer spanning tree, as shown in Figure 5.3(e) and (f), and so on.

5.6.3 Minimum Spanning Tree Search

The minimum-cost spanning tree, known as the Minimum Spanning Tree (MST), is a spanning tree that has the minimum sum of edges' weights among all other spanning trees that can be formed out of the same graph. To leverage the resilience of PRN, the edges will be given weights based on their cyber risk indices. Prim's and Kruskal's algorithms are popular greedy algorithms used for finding the MST in weighted, undirected graphs. It starts at a root node then keeps building the tree by adding one new node at a time, depending on the cheapest possible connection between the tree and another node. The pseudocode of this algorithm is provided in Figure 5.4. On the other hand, Kruskal's algorithm can be explained in the following steps

1- Initialize a forest consisting of trees of nodes of the graph (each node represents a separate tree).
2- Sort all the edges in a queue in non-decreasing order based on their weights.
3- Pick the edge with the minimum weight.
4- Add this edge to the tree. If adding the edge forms a cycle, then discard this edge.
5- Repeat steps 3) and 4) until the edge queue is empty.

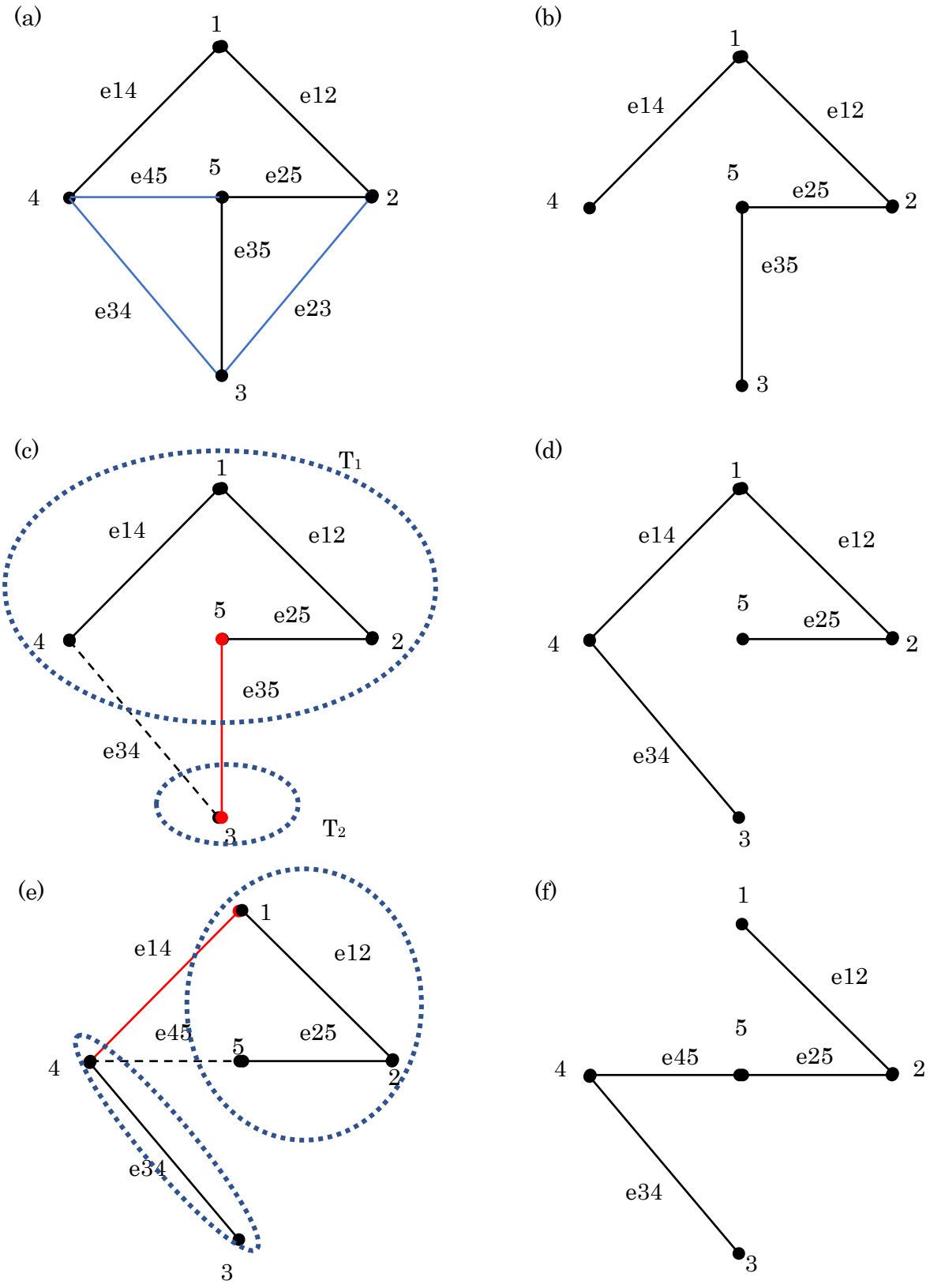


Figure 5.3 Example of Elementary Tree Transformation

Kruskal's algorithm is significantly faster than Prim's when applied to sparse graphs. In addition, Kruskal's algorithm can work on disconnected components and yield the minimum spanning forest, which Prim's cannot do. For all these reasons, Kruskal's algorithm is used in this work. Kruskal's pseudocode can be found in Figure 5.5.

```
MSTPrim(G)
V_Set={V0} // visited nodes = the source node
UV_Set = V [G]
MST_Edges={}  // edges form the MST
while UV_Set≠ ∅
        U → node from V_Set
        V→node not in unvisited nodes such that the edge (U,V) has the minimum cost
        // if two nodes have same weight, pick any of them.
        Add V to V_Set
        Add edge (U,V) to MST_Edges
End while
Return V_Set, MST_Edges
```

Figure 5.4 Prim-Dijkstra Algorithm Pseudocode

```
Kruskal(G)
F= ∅
For each v ∈ V(G) do
        MAKE-SET(v)   // every v in the graph is put in a separate set
Sort the edges of E(G) int nondecreasing order by weight.
For each edge (u, v) ∈E(G), taken by order  do
        If  FIND-SET(u) ≠ FIND-SET(v)
       then
            F= F ∪ {(u, v)}
            Union (FIND-SET(u), FIND-SET(v))  //combine the sets that u and v are in
Return F
```

Figure 5.5 Kruskal's Algorithm Pseudocode

5.6.4 Proposed Graph Simplification Approach

Basically, distribution networks encompass a large number of buses and lines. Thus, the application of the spanning trees would require very high computational capabilities and requirements. Instead, a new graph simplification method is performed in this thesis, which significantly reduces the algorithm's computational complexity. The graph is converted to multiple clusters after the fault occurrence that is represented by the cut-set as aforementioned. The simplified graph would be $H(V, E)$, where

$V(H) = \{xi | xi\ is\ a\ formed\ cluster \subset V(G), i \in \{1,2,..,Nc\}\}$, and

$E(H) = \{yj | yj \in Candidate\_Switches\_Set, j \in \{1,2,..,Ncan\}\}$.

In other words, the system can be simply viewed as a graph with clusters as vertices and inter-cluster tie switches as edges. Now, the adjacency matrix for this graph will be referred to here as a cluster adjacency matrix, A_c, can be represented on the form shown in Figure 5.6.

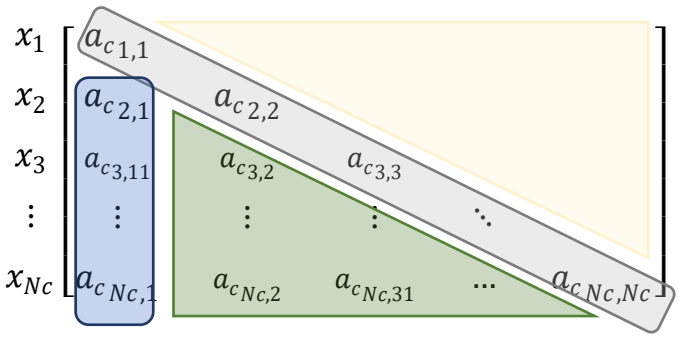


Figure 5.6 Cluster Adjacency Matrix Representation

Since the graph is undirected, the adjacency matrix is square ($N_c \times N_c$) and symmetric. Thus, we only need to find the lower triangular matrix, i.e., $A_{c_{ij}}\ for\ j \geq i$. Given that the diagonal elements here (shaded in grey) represent the intra-clusters switches that violate the radiality property, there is no need to find the diagonal elements as well. The blue-shaded elements in the first column correspond to the switches connecting the clusters to the Root Cluster. In contrast, the green-shaded elements relate to the switches connecting two different clusters. The union of the switches of the green and blue areas constitutes the *Candidate_Switches_Set* (the inter-cluster switches).

5.7 Assumptions

For implementing the proposed DNR strategy, the following assumptions are made.

1- Typical distribution systems are radially operated. Nevertheless, they are equipped with tie-switches and planned to work in an open-loop configuration. Such configuration is necessary to prevent complexity during fault allocation and protection coordination. Therefore, the radial constraint of each restoration path must be satisfied.
2- The distribution system has the Remote-Controlled type of Switches (RCS) since this is included within the initiative of the smart grid program for enhancing the advanced automation capabilities [129]. Also, each line has a sectionalizing switch that can be remotely controlled [82], [130], [131].
3- With the recent widespread deployment of smart meters in the network, remote disconnection of customer loads by the operators becomes feasible. Thus, we assume

that all the loads in the network can be disconnected/reconnected during the restoration process.

4- Because customer demands vary from time to time, when designing the isolated microgrids, loads are assumed to be fixed with their maximum demand just to guarantee supply adequacy during the operation.

5- The microgrid is capable of maintaining the voltage profile and stabilizing the frequency in the islanded mode of operation.

5.8 Graph-Theory-Based Resilient Distribution Network Reconfiguration Algorithm

Intending to tackle the resilient DNR problem, the proposed algorithm first tries to reconfigure the network using available tie switches to reconnect the isolated cluster(s) back to the Root Cluster and, in turn, to the main grid. If some (or all) of these clusters could not be restored to the main grid, the minimum number of microgrids would be formed for supplying the priority loads. This multi-stage restoration process, represented by the flowcharts in Figure 5.7 and Figure 5.8, can be decomposed into five sequential subroutines as follows,

A. Subroutine #1: Preprocessing

The first subroutine is where the system data are processed, a fault is simulated, and clusters are defined. The outcome of this stage is the set of clusters formed after a fault, leaving the graph ready for the restoration procedures. This subroutine includes the following,

Step 1) Input system data including lines' capacity, DG's capacity, Tie switches info (numbers, locations, and status), load buses, load priority list, resilience info (lines weights).

Step 2) Convert the distribution network to a graph, as discussed in Section 5.6.1.

Step 3) Fault is simulated. The faulted line is isolated, and the graph is updated.

Step 4) The algorithm searches for the set of clusters formed (connected components). Each cluster will be stored as a subgraph with its associated set of vertices and edges. The stump cluster that contains the substation will be referred to as the "Root Cluster", which all the other clusters will try to reconnect to.

A. Subroutine #2: Candidate Switches Search

This subroutine searches for the set of candidate tie switches by identifying the inter-clusters switches. All intra-clusters switches will be discarded.

Step 5) For each tie switch in each cluster, check if both end vertices belong to the same clusters. If yes, discard this switch and go to the next switch. If no, save it to the Candidate_Switches_Set.

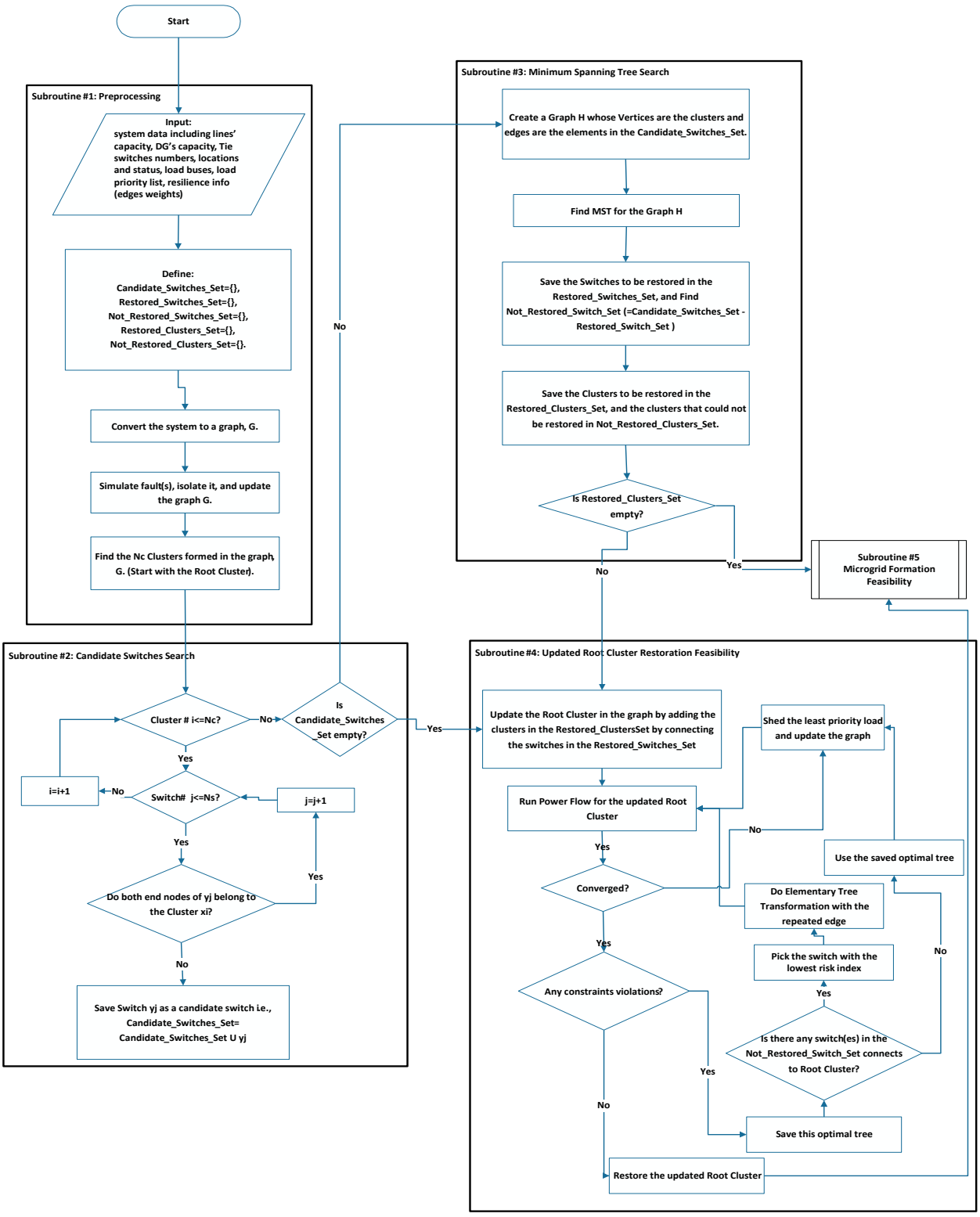


Figure 5.7 Flowchart of the DNR Algorithm

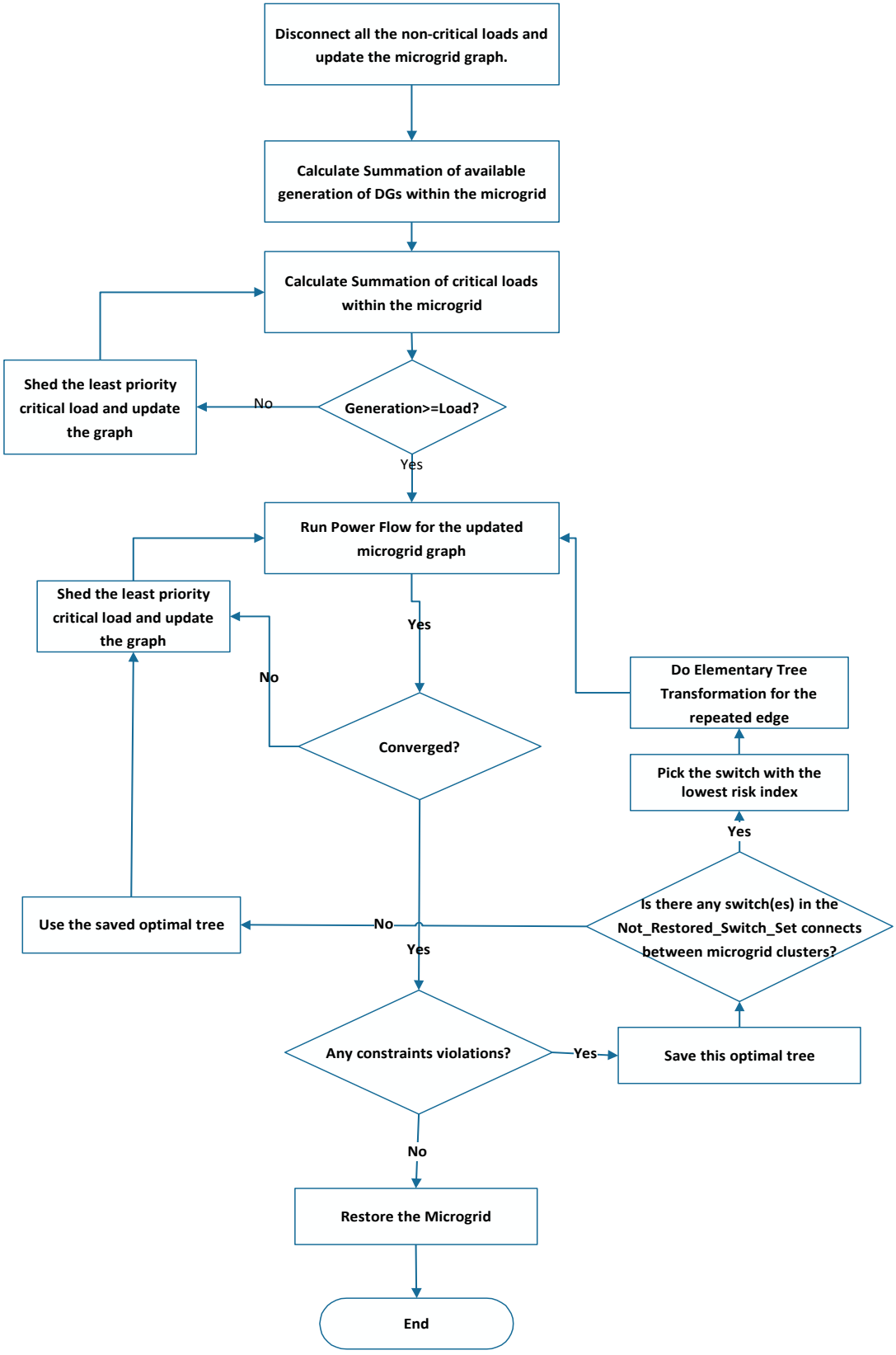


Figure 5.8 Microgrid formation Subroutine

Step 6) Check if the Candidate_Switches_Set is empty. If yes, then go to Subroutine #5 to form isolated microgrids. If there are Candidate switches available, go to Subroutine #3.

B. Subroutine #3: Minimum Spanning Tree Search

Step 7) Create the simplified graph *H* whose vertices are the clusters defined in Subroutine #1 and edges are the entries in the Candidate_Switches_Set.

Step 8) Find the MST for the graph *H* using Kruskal's algorithm, as discussed in Section 5.6.3.

Step 9) Save the tie switches to be restored in the Restored_Switches_Set and find Not_Restored_Switch_Set as (Candidate_Switches_Set - Restored_Switch_Set).

Step 10) Store the Clusters restored to the Root Cluster in the Restored_Clusters_Set and the clusters that could not be restored to the Root Cluster in the Not_Restored_Clusters_Set.

C. Subroutine #4: Updated Root Cluster Restoration Feasibility

If there are clusters to be restored,

Step 11) Update the Root Cluster in the graph by adding the clusters in the Restored_Clusters _Set using the switches in the Restored_Switches_Set.

Step 12) Send the updated root cluster to OpenDSS, run the three-phase unbalanced power flow, and send the results to MATLAB.

Step 13) If the power flow solution converges, check the operational constraints.

Step 14) If all the constraints are satisfied, restore the updated root cluster, and go directly to Subroutine#5.

Else, store this optimal tree configuration, then search for switches in the Not_Restored_Switch_Set that can connect to the Root Cluster. For all the switches found, start with the one that has the lowest risk index. Do EET for the repeated edge, then repeat Steps 12) through 14).

If there is no switch left, switch to the stored optimal tree configuration, shed the least priority loads, update the graph, and repeat Steps 12) through 14).

Step 15) If the power flow solution did not converge, shed the least priority load and update the graph. Then, repeat Steps 12) through 14).

D. Subroutine #5: Microgrid Formation Feasibility

For all the Clusters that could not connect to the root cluster (stored in the Not_Restored_Clusters_Set),

Step 16) Disconnect all the non-critical loads, update the microgrid (including tie switches to be restored).

Step 17) Check the DG(s) capacity constraints, given in Equations (5.9) and (5.10). If the DGs can supply all the critical loads belong to this microgrid, send the graph to OpenDSS, run the three-phase unbalanced power flow, and send the results back to MATLAB.

Step 18) If the power flow solution converges, check the operational constraints.

Step 19) If all the constraints are satisfied, restore the microgrid and end.

Else, store this optimal tree configuration, then search for switches in the Not_Restored_Switch_Set that can connect the microgrid clusters. For all the switches found, start with the one that has the lowest risk index. Do EET for the repeated edge, then repeat Steps 18) and 19).

If there is no switch left, switch to the stored optimal tree configuration, shed the least priority critical loads, update the graph, and repeat Steps 18) to 19)

Step 20) If the power flow solution did not converge, shed the least priority load and update the graph. Then, repeat Steps 18) through 20)

5.9 Test System Under Study and Simulation Results

In this study, the well-known IEEE 37-node distribution system [132], shown in Figure 5.9, is used as a test system to validate the proposed algorithm. The system is modified by adding normally-open tie switches (represented by the dotted lines in Figure 5.9) to simulate the restoration scenarios. A list of the tie switches is given in Table 5.1, and the critical load parameters are given in Table 5.2. The minimum and maximum allowable bus voltage are 0.95 pu and 1.05 pu, respectively. The proposed algorithm is implemented in MATLAB and OpenDSS on a PC with an Intel Core i7-8550U @1.80GHz CPU and 16.0 GB installed RAM.

Table 5.1 Normally-open Tie Switches for The IEEE 37-node Test Feeder System

No.	Switch Name	Node 1	Node 2	Weight
1	SW713-724	713	724	4
2	SW718-708	718	708	5
3	SW725-731	725	731	6
4	SW731-741	731	741	3
5	SW728-735	728	735	1
6	SW742-744	742	744	2

Table 5.2 Critical Load Parameters

Priority	Node Position.Phase	Pmax (kW)	Qmax (kVAR)
1	731.b	84	40
2	736.b	42	21
3	738.a	126	62
4	740.c	85	40
5	742.a	8	4

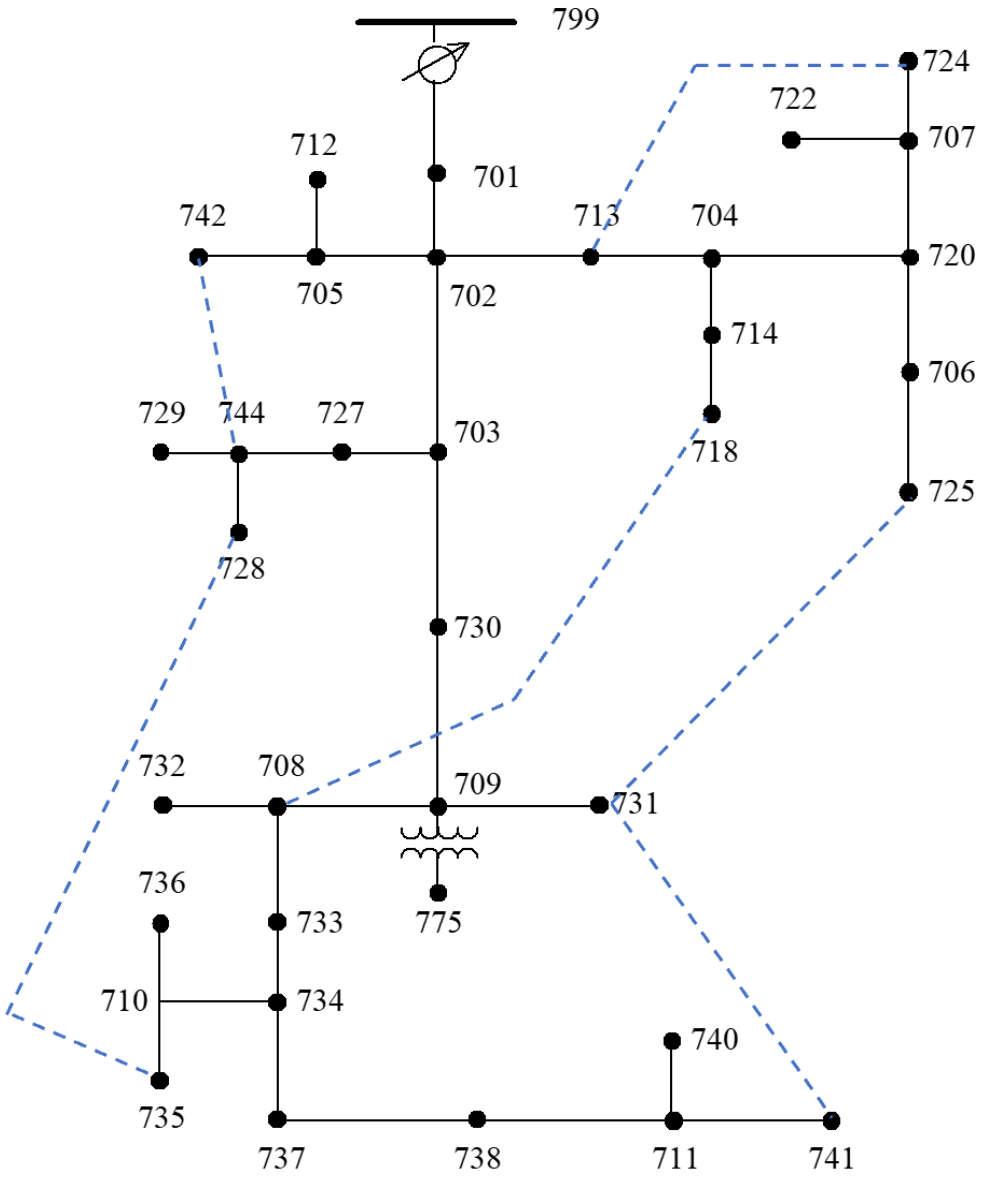


Figure 5.9 IEEE 37-bus Radial Distribution System with Tie Switches

The system under study is first converted to a graph with 37 nodes and 36 edges, as shown in Figure 5.10.

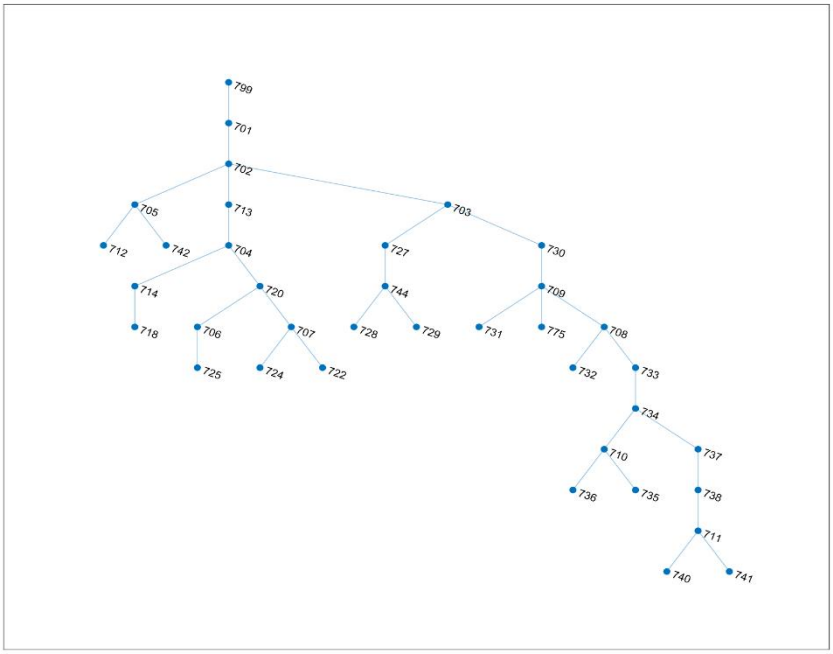


Figure 5.10 Graph Representation of The System Under Study

5.9.1 Case I: Single Faults

A. Scenario 1-I: Fault in line 713-704

Figure 5.11 (a) shows the graph of the system with the line with a fault in red. The sectionalizing switches are assumed to remove the line from the network, and the rest of the system becomes two separate components (clusters), as shown in Figure 5.11 (b) and (c). For this scenario, only three tie switches are candidate switches, listed in Table 5.3. The MST is first found for the system without graph simplification for the sake of comparison. The system graph with all the candidate switches is shown in Figure 5.12, whereas Figure 5.13 shows the MST formed highlighted over the system graph with candidate switches.

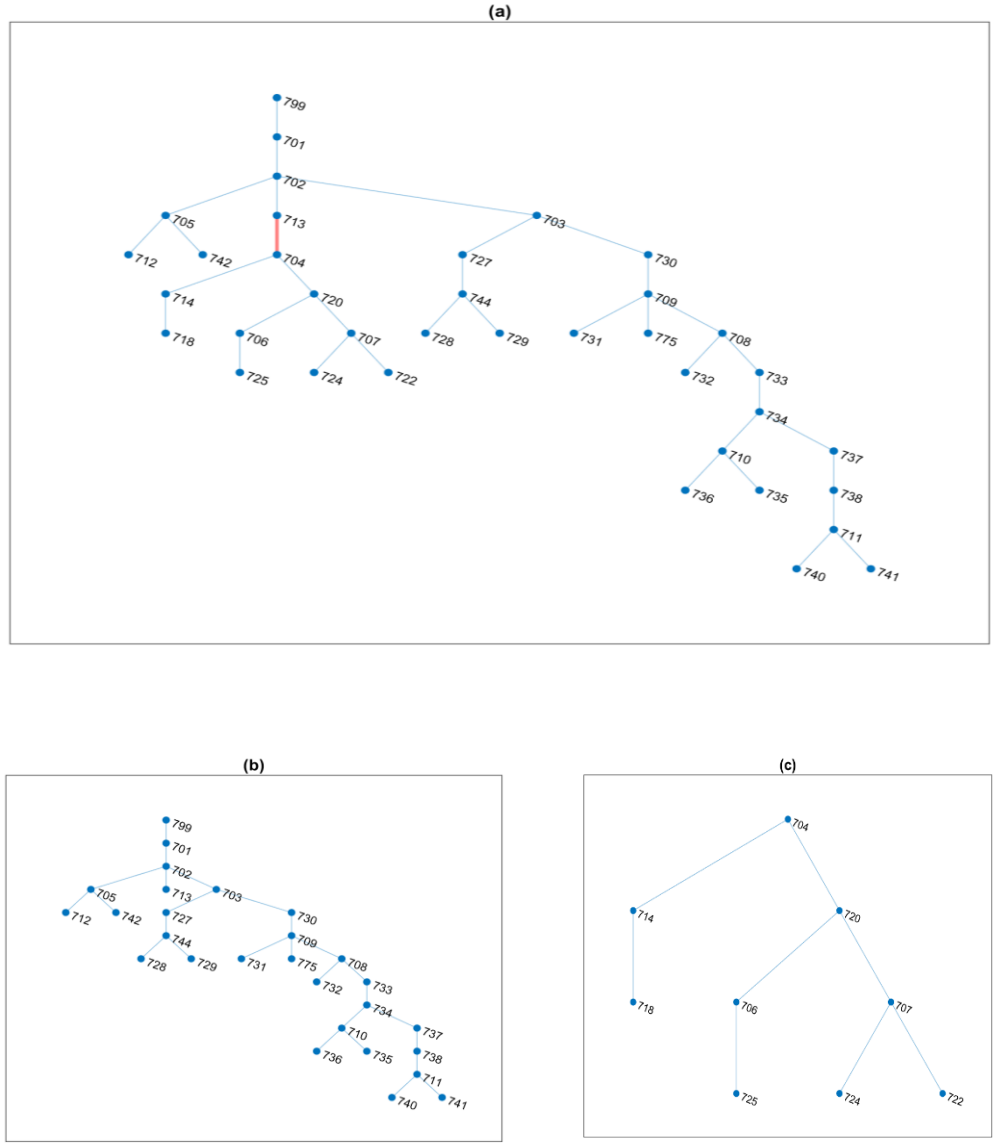


Figure 5.11 For Scenario 1-I: (a) Original System with Fault in Line 713-704, (b) First Component (Root Cluster), (c) Second Component.

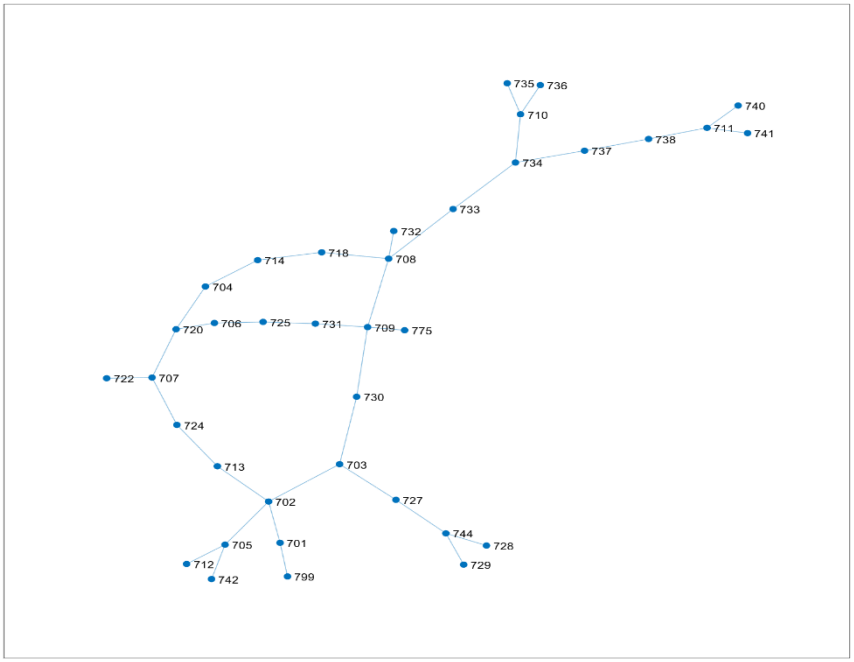


Figure 5.12 System Graph with Candidate Switches for Scenario 1-I

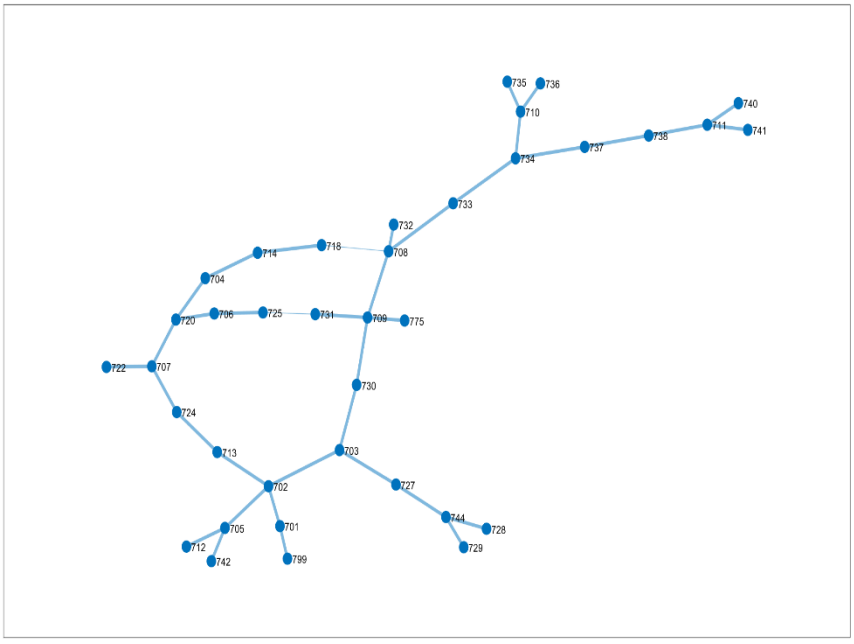


Figure 5.13 MST for Scenario 1-I

However, the post-fault network is converted to only a two-node graph with three edges after the graph simplification, as shown in Figure 5.14. Searching for the MST, the edge with weight w_1 representing SW713-724 has the minimum weight and forms the tree as shown in Figure 5.15.

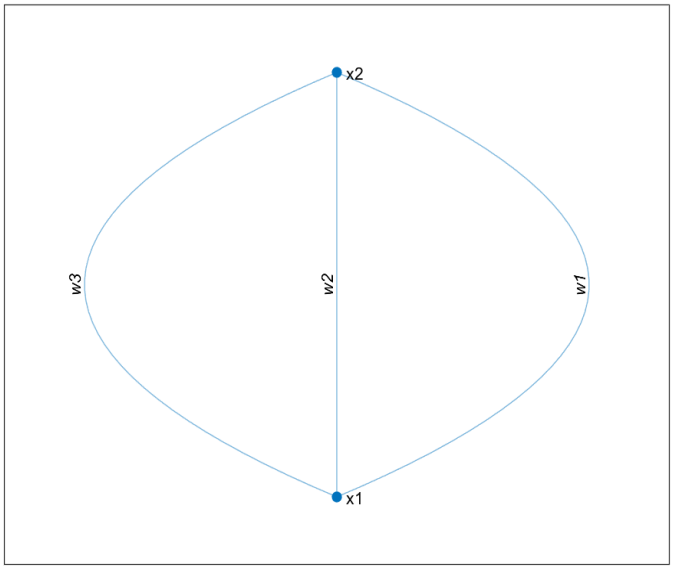


Figure 5.14 Simplified Graph for Scenario 1-I

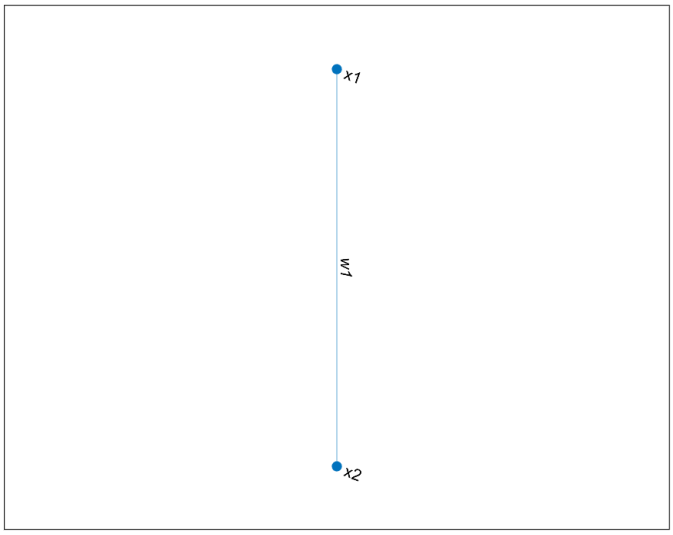


Figure 5.15 MST for Simplified Graph for Scenario 1-I

The power flow converges for this solution, and the voltage profile is given in Figure 5.16. No overcurrent or capacity limit violations for this scenario. This solution is hence feasible, and the computational time for the restoration solution is 0.3950 s.

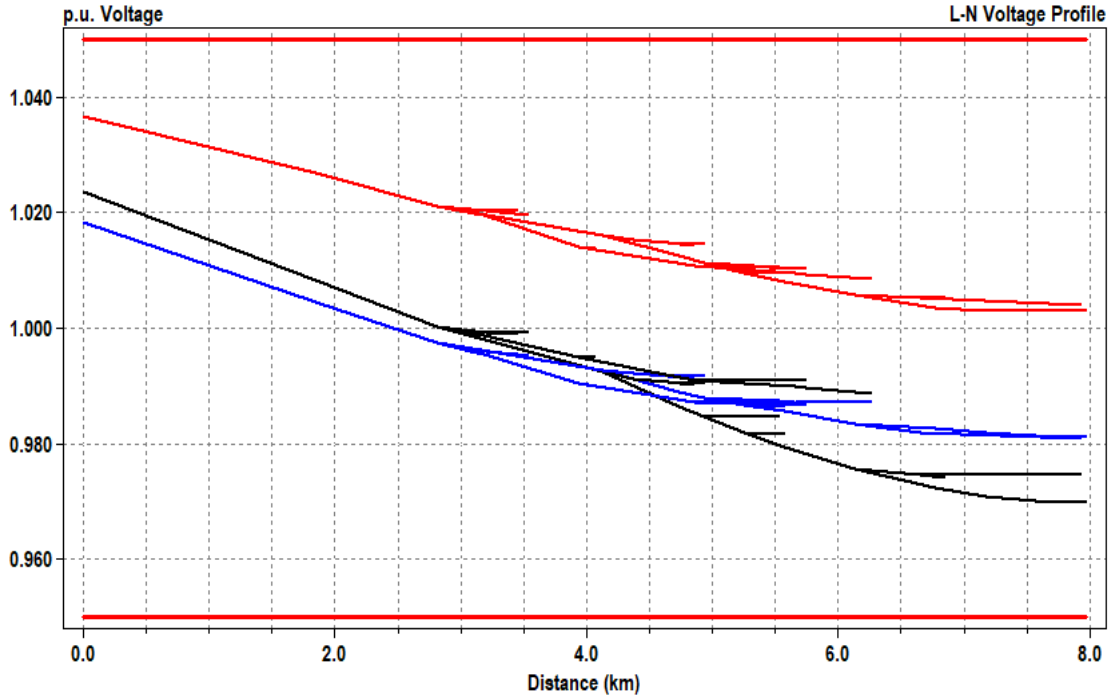


Figure 5.16 Post-restoration Voltage Profile for Scenario 1-I

Table 5.3 Tie Switches Info for Scenario 1-I

Switch no.	Switch Name	Candidate Switch	Switch Restored
1	SW713-724	Yes	Yes
2	SW718-708	Yes	No
3	SW725-731	Yes	No
4	SW731-741	No	N/A
5	SW728-735	No	N/A
6	SW742-744	No	N/A

B. Scenario 1-II: Fault in line 733-734

Similarly, Figure 5.17 (a) shows the location of the fault in the system, and the two clusters formed after fault isolations are shown in Figure 5.17 (b) and (c). The simplified graph is shown in Figure 5.18, and SW728-735 is selected to form the MST. When checking the solution feasibility, the power flow solution converged. Also, the bus voltage limits were satisfied, depicted in Figure 5.19, and line flows were within limits. However, the current in Line 703-727 (L5) exceeds the line ampacity as shown in the OpenDSS overload report provided in Figure 5.20. Therefore, the one switch found in the Not_Restored_Switch_set, i.e., SW731-741, replaced SW728-735 (by cyclic interchange operation). The power flow analysis has been performed for the new graph. The solution converged, and all the constraints were satisfied. Hence, the restoration should be done by closing SW731-741 in this scenario, as shown in Table 5.4. The computational time for this scenario is 0.4279 s.

Table 5.4 Tie Switches Info for Scenario 1-II

Switch no.	Switch Name	Candidate Switch	Switch Restored
1	SW713-724	No	N/A
2	SW718-708	No	N/A
3	SW725-731	No	N/A
4	SW731-741	Yes	Yes
5	SW728-735	Yes	~~Yes~~ No
6	SW742-744	No	N/A

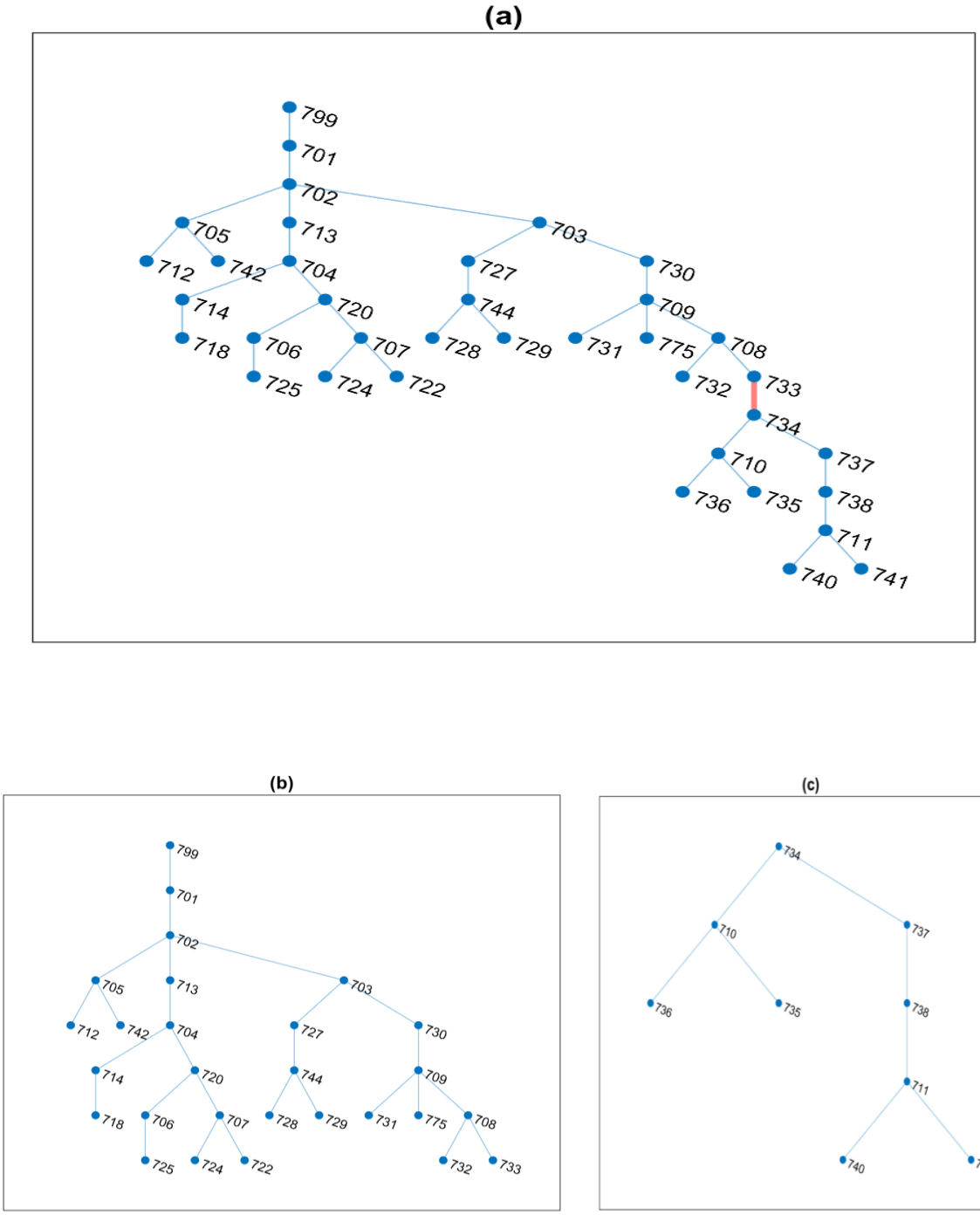


Figure 5.17 For Scenario 1-II: (a) Original System with Fault in Line 733-734, (b) First Component (Root Cluster), (c) Second Component.

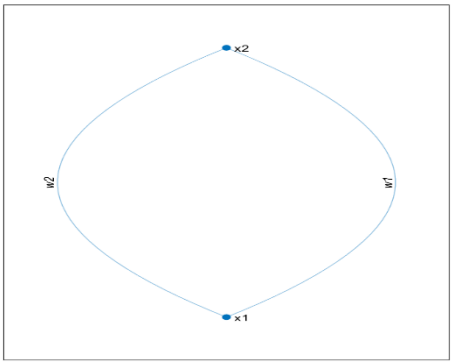


Figure 5.18 Simplified Graph for Scenario 1-II

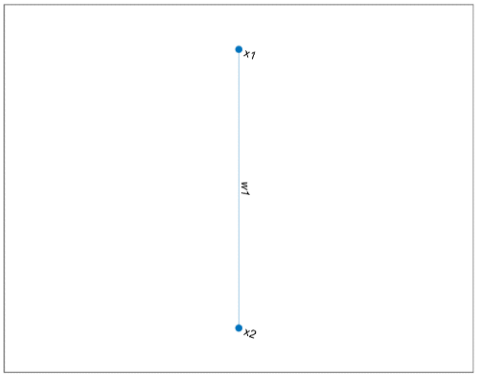


Figure 5.19 MST for Simplified Graph for Scenario 1-II

*ieee37_Overload - Notepad

File Edit Format View Help

Power Delivery Element Overload Report

SYMMETRICAL COMPONENT CURRENTS BY CIRCUIT ELEMENT

Element	Term	I1	IOver	%Normal	%Emerg	I2	%I2/I1	I0	%I0/I1
"Line.L5"	1	110.2	13.08	109.7	72.9	38.2	34.7	0.0	0.0

Ln 6, Col 20 100% Windows (CRLF) UTF-8

Figure 5.20 OpenDSS Overload Report for Scenario 1-II

C. Performance Evaluation

The algorithm was also used for additional three single-fault scenarios in lines (730-709, 703-727, and 709-708), and the candidate switches for these scenarios are given in Table 5.5

Table 5.5 Candidate Switches for Different Single Fault Scenarios

Switch Name / Faulted Line	SW718-708	SW718-708	SW725-731	SW731-741	SW728-735	SW742-744
730-709	No	Yes	Yes	No	Yes	No
703-727	No	No	No	No	Yes	Yes
709-708	No	Yes	No	Yes	Yes	No

To evaluate the performance of the proposed algorithm, the results obtained will be compared with two other algorithms: one based on spanning tree search in [130] and the other is a mixed-integer nonlinear programming algorithm in [131]. The comparison is shown in Table 5.6.

Table 5.6 Comparison of The Restoration Algorithms Performance of The Modified 37-node Test System

Scenario	Faulted Line	Proposed MST Search Algorithm		Spanning Tree Algorithm in [130]		MINLP in [131]	
		T(s)	Restoration Plan	T(s)	Restoration Plan	T(s)	Restoration Plan
1	713-704	0.3650	Close SW713-724	1.335	Close SW713-724	41	Close SW713-724
2	733-734	0.4279	Close SW731-741	0.484	Close SW731-741	30	Open 711-741 And close SW728-735 and SW731-741
3	730-709	0. 446	Close SW718-708	0.825	Close SW718-708	91	Open 708-733 and 738-711 And close SW728-735, SW725-731, and SW718-708
4	703-727	0.3358	Close SW728-735	0.805	Close SW728-735	3	Close SW742-744
5	709-708	0.4196	Close SW731-741	0.787	Close SW731-741	120	Open 734=737 and 711-741 And close SW728-735, SW731-741, and SW718-708

Compared to the algorithm in [131], our approach is significantly faster in finding the restoration plan for all the simulated scenarios. The fact that they put no limit on the number of interchanged tie switches, the algorithm keeps interchanging tie switches and sectionalizing switches to reach the optimal solution, which remarkably increased the number of switching operations, even sometimes resulted in constraints violation, e.g., the network is no longer radial in scenario 3 and 5. Also, our algorithm is notably faster than the one in [130] because the proposed graph simplification method made the graph size very small; hence the search process became much faster.

5.9.2 Case II: Multiple Faults

In this section, we simulate coordinated kinds of attacks that bring more negative consequences. For this purpose, we connect three DGs to the network with parameters given in Table 5.7.

Table 5.7 Parameters of the DGs

DGs	Node Position	P_{max} (kW)	Q_{max} (kVAR)
1	713	160	90
2	732	200	100
3	737	150	70

A. Scenario 2-I: Disconnecting Line 702-703 and Line 702-705

In this scenario, the attacker targets two lines that hold a significant portion of the system. These lines can be seen in Figure 5.21, with the resulting clusters bounded by dotted shapes. The graphs generated are then given in Figure 5.22 that show the faulted system and the three post-fault components. Table 5.8 gives the tie switches info for this scenario. From Figure 5.23, Figure 5.24, and Figure 5.25, SW718-708 and SW742-744 should be switched on to restore the disconnected clusters to the Root Cluster. When performing the power flow study, we found the bus voltages are within limits, shown in Figure 5.26. However, there are currents in multiple lines that exceed their capacity, as reported in Figure 5.27.

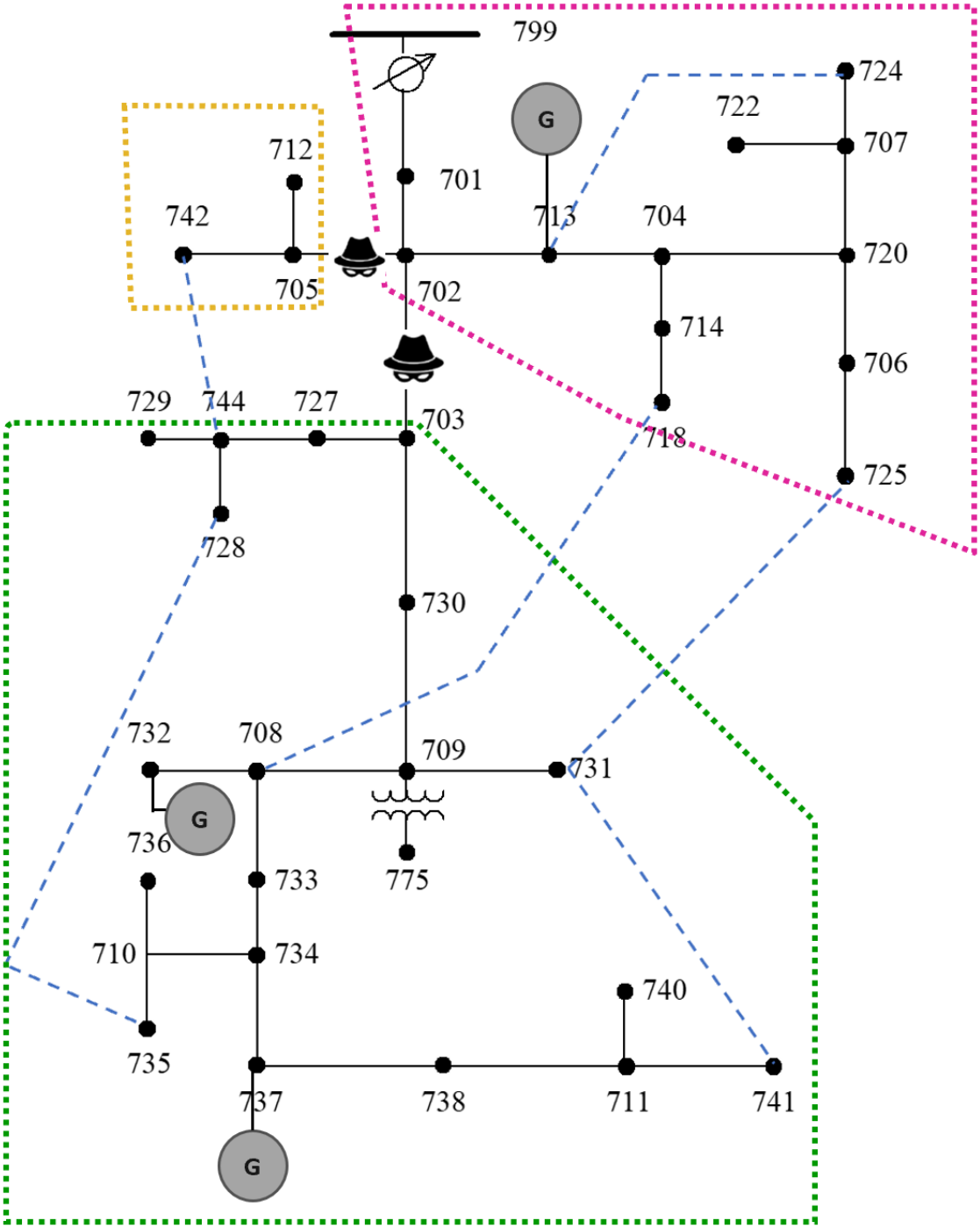


Figure 5.21 The Post-fault Network with Formed Clusters for Case II

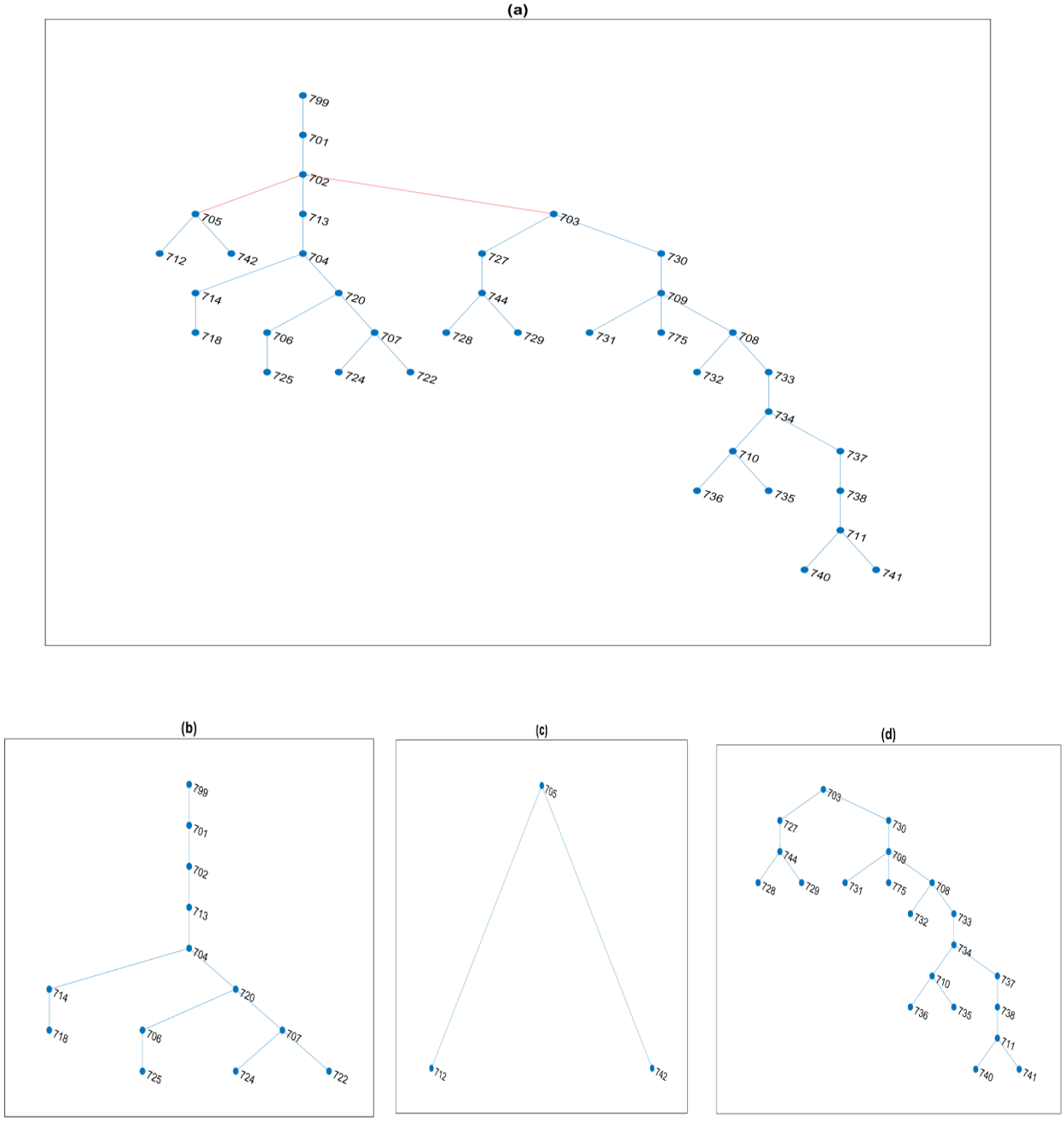


Figure 5.22 For Scenario 2-I: (a) Original System with Fault in lines 702-703 and 702-705, (b) First Component (Root Cluster), (c) Second Component. (d) Third Component.

Table 5.8 Tie Switches Info for Scenario 2-I

Switch no.	Switch Name	Candidate Switch	Switch Restored
1	SW713-724	No	N/A
2	SW718-708	Yes	~~Yes~~ Yes
3	SW725-731	Yes	Yes No
4	SW731-741	No	N/A
5	SW728-735	No	N/A
6	SW742-744	Yes	Yes

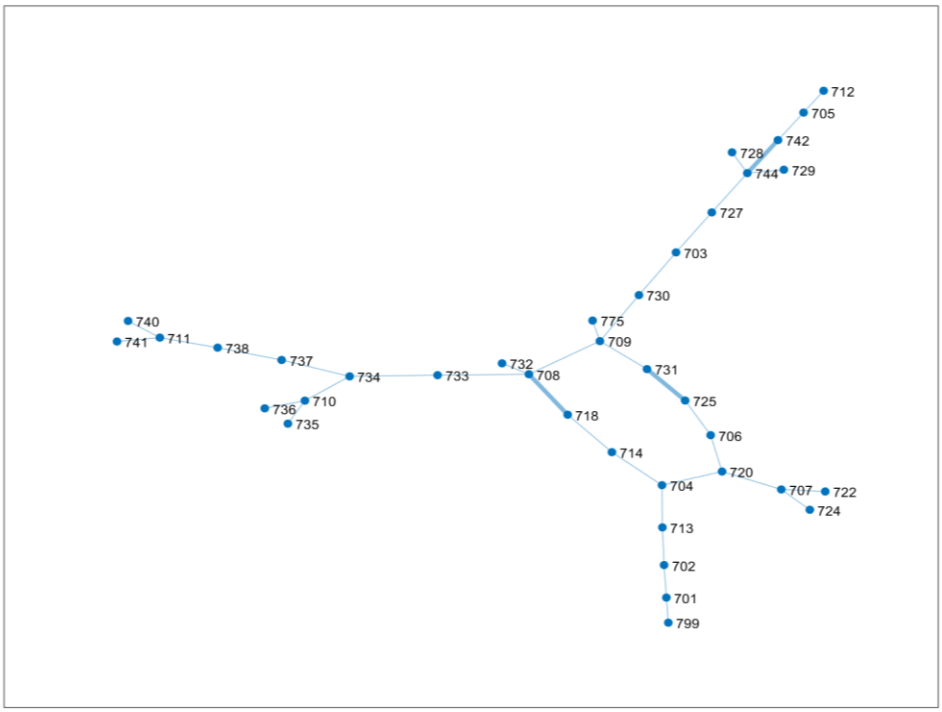


Figure 5.23 System Graph with Candidate Switches for Scenario 2-I

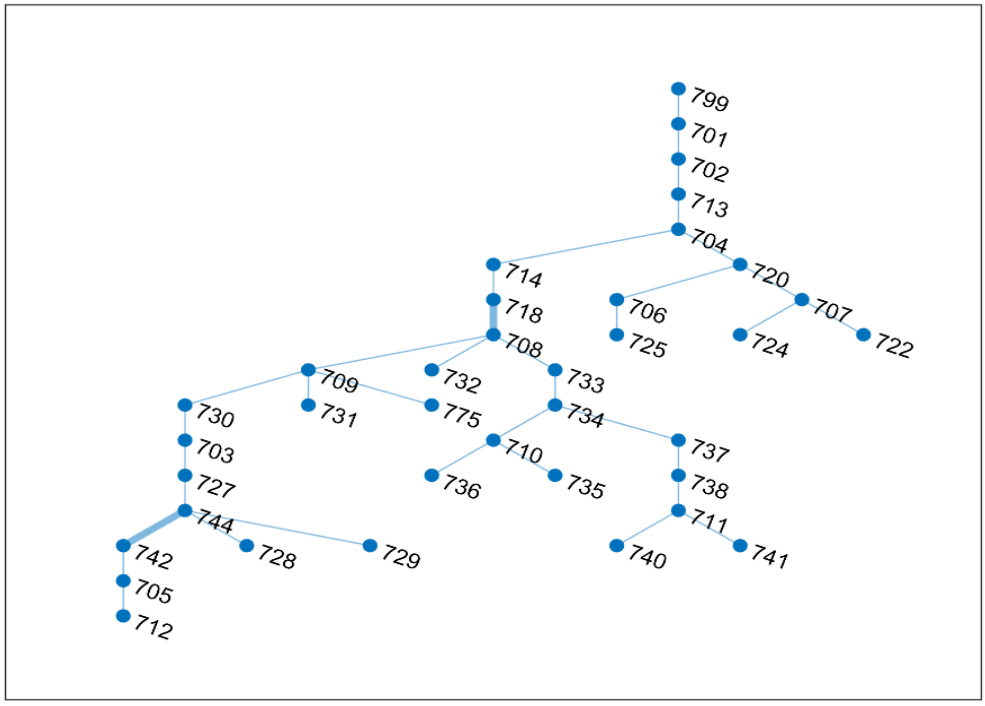


Figure 5.24 MST for Scenario 2-I

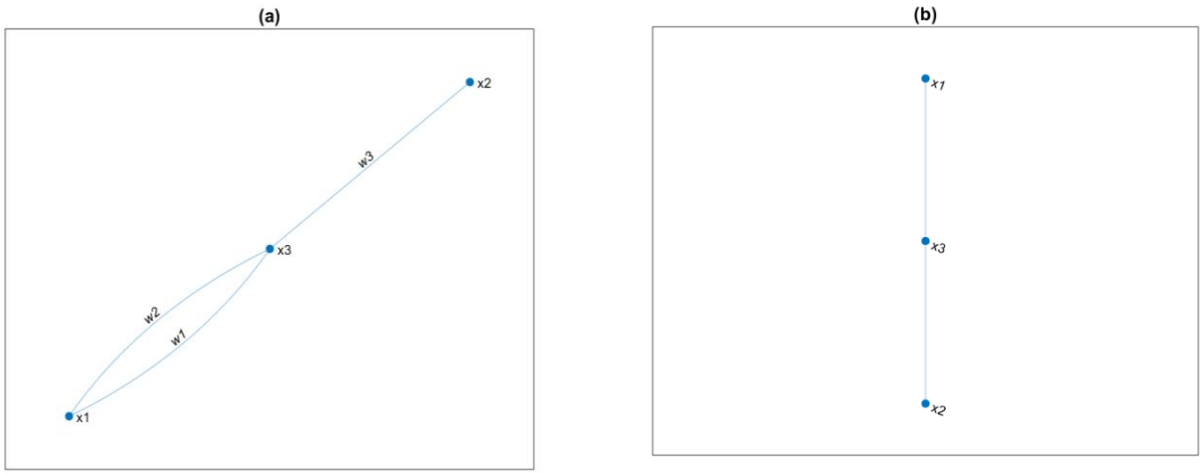


Figure 5.25 (a) Simplified Graph for Scenario 2-I and (b) Its MST

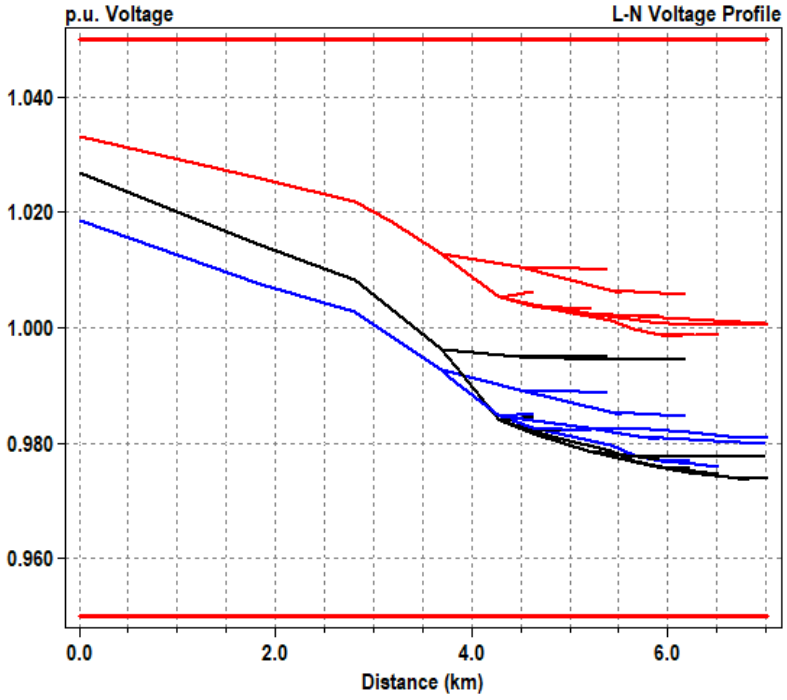


Figure 5.26 Post-restoration Voltage Profile for Scenario 2-I

*ieee37_Overload - Notepad

File Edit Format View Help

```
Power Delivery Element Overload Report

SYMMETRICAL COMPONENT CURRENTS BY CIRCUIT ELEMENT

Element             Term    I1    IOver %Normal  %Emerg     I2    %I2/I1    I0    %I0/I1

"Line.L7"             1   142.8   47.37   135.1    89.8    39.8    27.9     0.0     0.0
"Line.L22"            1   187.0    3.89   101.9    68.0    18.3     9.8     0.0     0.0
"Line.L23"            1   137.7   43.97   132.6    88.2    41.3    30.0     0.0     0.0
```

Ln 6, Col 21 | 100% | Windows (CRLF) | UTF-8

Figure 5.27 OpenDSS Overload Report for Scenario 2-I

Thus, according to the proposed algorithm, the other repeated switch (i.e., SW725-731) would replace SW718-708. The voltage profile for this case is given in Figure 5.28. However, the results in Figure 5.29 still show line flow violations.

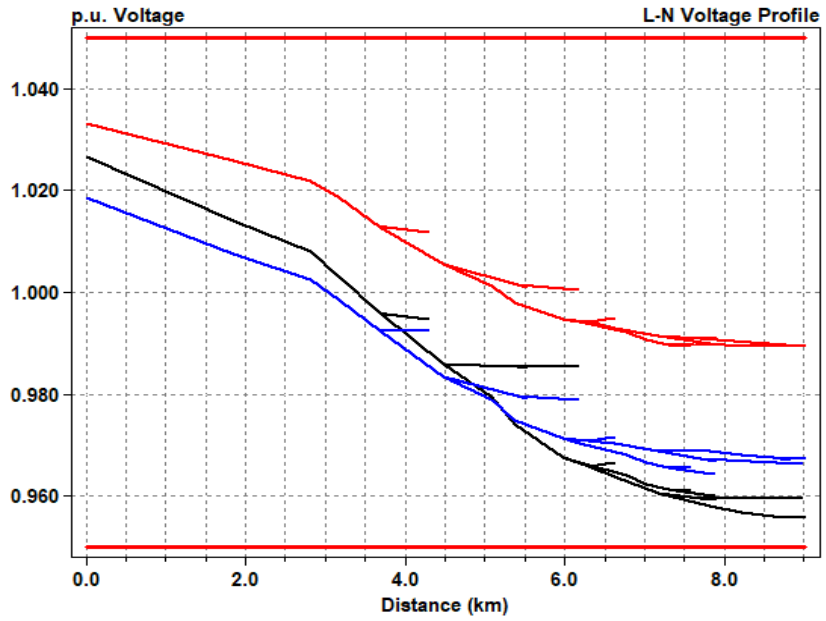


Figure 5.28 Post-restoration Voltage Profile Using SW725-731 for Scenario 2-I

ieee37_Overload - Notepad

File Edit Format View Help

```
Power Delivery Element Overload Report

SYMMETRICAL COMPONENT CURRENTS BY CIRCUIT ELEMENT

Element            Term    I1    IOver %Normal  %Emerg     I2    %I2/I1    I0    %I0/I1

"Line.L3"             1   176.9    0.36   100.2    66.8    28.7    16.2     0.0     0.0
"Line.L11"            1   132.4   27.85   120.6    80.2    31.3    23.6     0.0     0.0
"Line.L22"            1   187.5    4.63   102.3    68.2    18.7    10.0     0.0     0.0
```

Ln 6, Col 20 | 100% | Windows (CRLF) | UTF-8

Figure 5.29 OpenDSS Overload Report Using SW725-731 for Scenario 2-I

Accordingly, the algorithm switches back to the first solution (the more resilient configuration, and starts the load shedding process until the loading constraints are satisfied. After removing seven loads (the lowest prioritized seven loads) out of the existing thirty loads. The loads were shed in the following sequence: 727c, 720c, 722b, 744a, 732c, 741c, 733a. The currents in the lines are all within limits. The voltages at the buses are still within the allowable limits, too, as shown in Figure 5.30. The computational time is 1.09s.

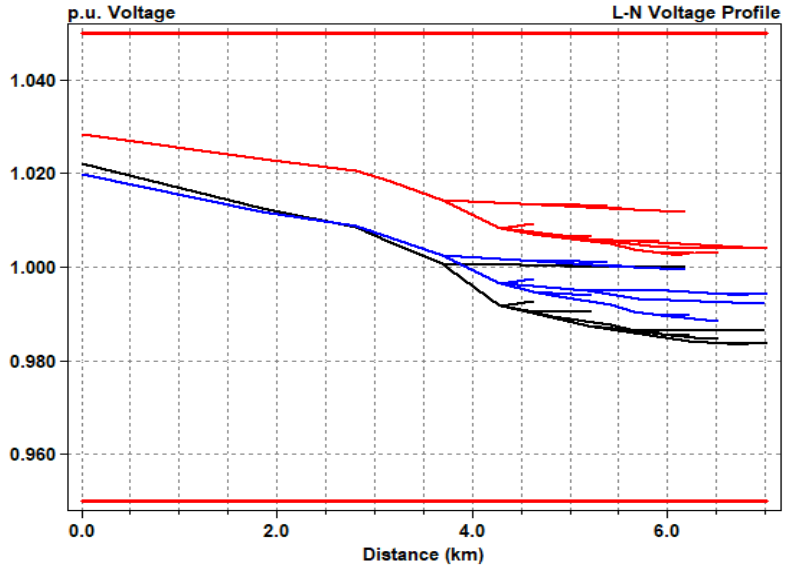


Figure 5.30 Voltage Profile after Load Shedding for Scenario 2-I

B. Scenario 2-II: Scenario 2-I with Attack on Switches SW718-708 and SW725-731

This scenario represents a more capable attack that can disable two switches, besides the two lines in Scenario 2-I, which forces a part of the system to entirely isolate from the main grid. Referring to Figure 5.22, we notice that the second and third components can be reconnected using SW742-744. However, there is no available switch that can connect them to the Root Cluster. The PRN is shown in Figure 5.31, and the restored MST is shown in Figure 5.32.

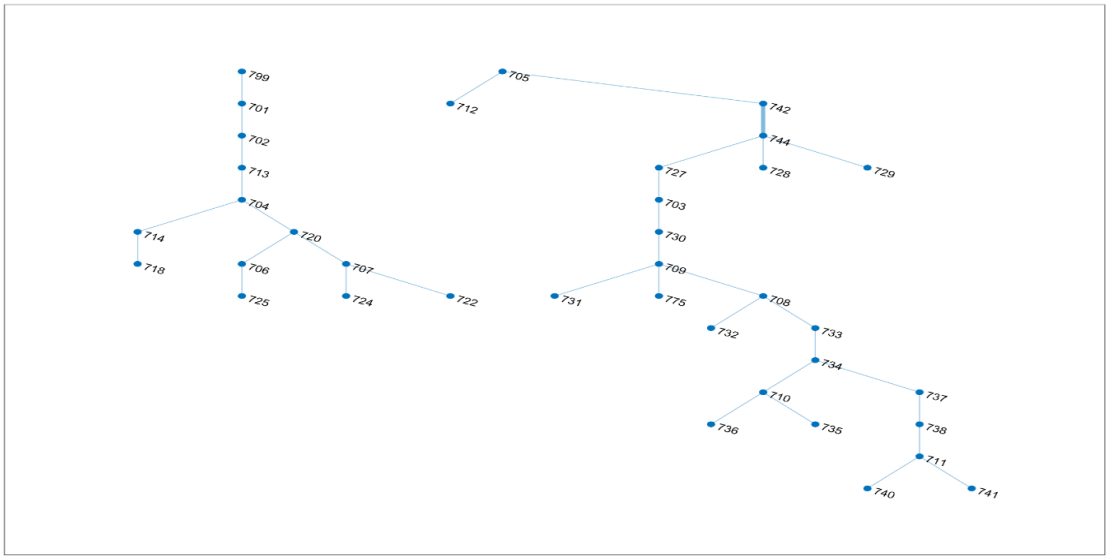


Figure 5.31 Post-restoration Network for Scenario 2-II

Figure 5.32 MST for System Clusters for Scenario 2-II

According to the proposed algorithm, the Root cluster will be connected to the main grid, and a power flow study will be conducted. The rest of the system will form a microgrid, in which only the critical loads are left connected, whereas all the non-critical loads are being disconnected. The overall power of the critical loads in the isolated microgrid was found to not exceed the total generation of the DGs within the same microgrid (Equations (5.9) and (5.10)). Thus, we checked the microgrid's power flow as well. All the constraints were satisfied. Figure 5.33 presents the voltage profile for this case.

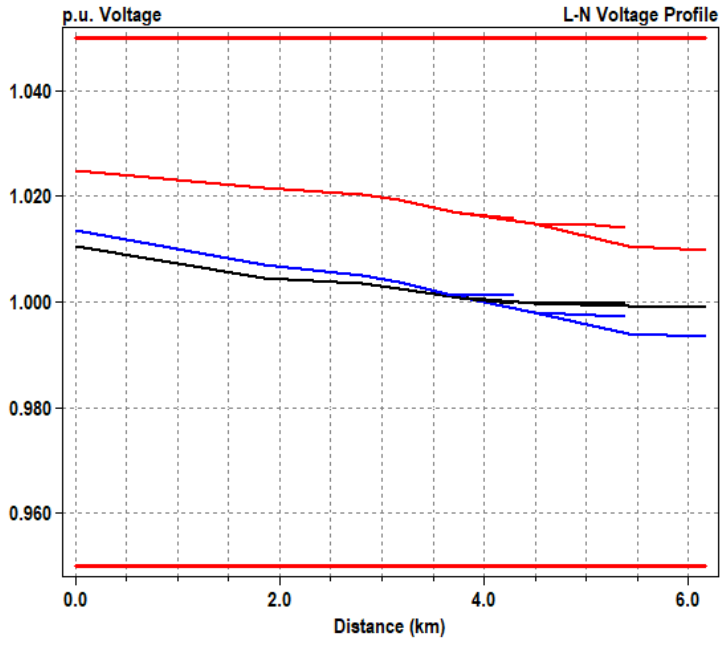


Figure 5.33 Post-restoration Voltage Profile for Scenario 2-II

Table 5.9 gives the post-restoration load status with their priorities. The computational time, in this case, is 0.64.

Table 5.9 Loads Parameters and Post-restoration Statuses for Scenario 2-II

Node Position.Phase	Load Priority	P_{max} (kW)	Q_{max} (kVAR)	Status
S701a	23	140	70	1
S701b	16	140	70	1
S701c	15	350	175	1
S712c	12	85	40	1
S713c	22	85	40	1
S714a	9	17	8	1
S714b	6	21	10	1
S718a	10	85	40	1
S720c	29	85	40	1
S722b	28	140	70	1
S722c	7	21	10	1
S724b	18	42	21	1
S725b	14	42	21	1
S727c	30	42	21	0
S728	13	126	63	0
S729a	11	42	21	0
S730c	8	85	40	0
S731b*	1	85	40	1
S732c	26	42	21	0
S733a	24	85	40	0
S734c	20	42	21	0
S735c	19	85	40	0
S736b*	2	42	21	1
S737a	17	140	70	0
S738a*	3	126	62	1
S740c*	4	85	40	1
S741c	25	42	21	0
S742a*	5	8	4	1
S742b	21	85	40	0
S744a	27	42	21	0

5.10 Summary and Conclusions

This chapter proposed a resilient multi-stage load restoration strategy through distribution system reconfiguration after disruptive events. An algorithm based on graph theory concepts and MST search has been developed to restore maximum load according to their priorities. It also aims to maximize the post-restoration resilience of the PRN while satisfying the operational and topological constraints. The algorithm's objective is to restore all the out-of-service loads as long as there is a connection to the utility network. If there are one or more areas completely isolated from the main grid, the objective would be to use the existing DGs' capacity to supply critical loads only until all the repair work is done, as discussed in Chapter 2.

The algorithm has been developed in sequential stages that check the available solutions and their feasibility for a PRN. With the help of the ETT and MST concepts, the network constraints could be maintained. Also, the power flow solution convergence and the operational constrained are considered. Load shedding according to load priority has been done for infeasible cases. Compared to the literature work, the proposed algorithm is generic and can tackle single or multiple faults in the system. Also, a novel simplification approach was proposed to deliberately simplify the graph, hence greatly affected the search domain of the MST. This technique clearly gives an advantage to the algorithm over the ones given in the literature when comparing the restoration plan and the computational time, especially because it uses an accurate three-phase unbalanced power flow simulation, not the linearized model. All these aspects validate the usefulness of the technique.

Chapter 6: Conclusions and Future Work

This chapter summarizes the main accomplishments and findings of this research and presents the recommended directions for future work.

6.1 Summary and Conclusions

This thesis set out to propose strategies to enhance the resilience of power networks against the growing cyber-physical attacks. These strategies aim at improving the preparedness and recovery potentials of the system. To enhance the system preparedness, first, a cyber-physical oriented risk analysis has been performed to identify the vulnerabilities and rank the substations and lines according to their importance in supplying the power to the loads. Second, a data-mining-based detection technique has been proposed for identifying compromised relay settings based on the electrical properties. For the recovery potential improvement, a graph-theoretic reconfiguration strategy for distribution networks has been proposed for restoring loads according to their priority. The following sections discuss the main research findings.

The first strategy is a quantitative cyber-physical-based risk analysis approach that investigates the risk of cyber attacks on power grids. The proposed approach is based on a threat/attacker-oriented model to identify threat sources for a substation and construct an attack tree to obtain the potential attack scenarios. The model also identifies potential grid attacker's profiles and adopts an adversary capability-based model that considers the attacker's motivations and resources to assess the likelihood of attack occurrence. The impacts of these attacks are quantified using the ratio of load interrupted in the network. This load interruption is calculated taking into consideration the network operational constraints. Three attacker models have been chosen based on attacker attributes to allow comprehensive coverage of possible grid attacks. A vulnerability analysis has been done using multiple centrality measures, and two strategies have been employed for formulating attacks. The system performance has been quantified based on topology information, and sets of vulnerable components have been extracted for the topological-based attacks. Risk quantification algorithms have been developed for the different attacker models that integrate the cyber and physical parts of the analysis. The results compare the system risk to different attack scenarios and attacker models. They also identify vulnerable substations and lines and rank them according to their contribution towards load interruption. Also, the results have confirmed that the evaluated risk index and the rank of a given target component change for different attacker attributes, which validates the hypothesis we made for which the risk should be quantified based on attacker models.

By comparing our approach to the prior studies in the literature, the salient features of this approach are

- Presenting detailed attacker modeling based on several attributes of the attacker: motivation, budget, and skills. Owing to the different amounts of accessible data for different grids, as explained in Chapter 1, the suitable attacker model should be considered in risk evaluation,
- Considering single and coordinated attacks, with the probability of attack occurrence affected by the number of targeted components. In addition, this approach takes into account the N-k criterion for cyber contingency requirements,
- Simulating different attack pathways to demonstrate the effect of different attack scenarios on the system risk, and
- Taking into account the indirect load interruption when calculating the attack impact due to the adequacy and line flow capacity constraints. The investigations showed that these operational constraints result in similar or even higher impacts in most cases.

Ranking critical assets is crucial for subsequent planning studies, e.g., determining which assets should be prioritized for reinforcement using the cost/benefit analysis, etc. The risk-informed assessment, in that way, help system planner to reinforce vulnerable assets and take better preventive and corrective actions. These activities can reduce the consequences of potential attacks. Therefore, accurate cyber-physical risk assessments help boost the system's preparedness, and hence the system's resilience.

The second strategy is a detection technique for the adaptive protective relay schemes based on Rough set theory. This technique aims to identify incorrect settings sent to overcurrent relays due to the integrity-related types of attacks. A probabilistic short-circuit analysis has been done to obtain the physical attributes needed in the Rough set analysis. The k-means clustering has been used to classify these attributes to have an adequate number of decision rules. An information table has been constructed for each relay in the network during the training stage. The specific relay's If-then rules have been generated and loaded to the relay during the preprocessing stage. Henceforth, relays only need to compare setting upon being received during the operational stage. The IEEE 34-bus system with DGs is used to evaluate the tool's performance. The assessment has been conducted using various performance measures, and the results demonstrate the tool's superior ability to classify settings in a rapid and efficient manner.

Since the intrusion detection and protection systems are one of the resilient system preparedness requirements according to NIPPs plans, as stated in Chapter 1, we claim that the proposed detection tool falls under this category. Incorrect relay settings can result in a broad range of negative consequences, from unnecessarily customer interruption and equipment damage to a cascading failure and grid stability problems, as discussed in Chapter 1. Thus, by monitoring and blocking incorrect relay settings, we believe that this tool goes a long way toward enhancing the grid cyber-physical resilience. This thesis focused on designing this tool for relays because we believe that relays are crucial elements in the network. According to the North American Electric Reliability Corporation (NERC) report, relay mal-operations are responsible for more than 70% of the major outages in the united states [133]. In essence, relays are responsible for giving opening commands for several network components, e.g., lines, transformers, generators. As seen from the risk analysis investigations, relays are located on the pathways of lots of attack scenarios, given that the probability of disconnecting switches or breakers directly from the control center is more complicated. In addition, cyber defense for protection applications is always challenging to

implement due to the limited overhead of the protocol used for these time-constrained applications. Hence, this tool is considered a useful line of defense for relays applications.

Compared to the methods presented in the literature, our tool and its analysis have the following merits,

- A probabilistic short-circuit analysis has been performed considering DG availability, renewable DG levels, different loading levels. It takes into account that loading varies for weekdays and weekends, also for different seasons of the year.
- This technique depends on only local measurements and pre-stored physical properties for detection, making it more reliable.
- The test dataset used has covered a broad range of settings that model different potential attacker profiles, i.e., script kiddies, cyber criminals, etc.
- Since detection happens in the relay itself, the tool proposed in this thesis can judge incoming settings regardless of the type of attack that affected them.
- The technique used for this tool makes it easy to be implemented in digital relays considering limited computational capabilities and the time-sensitivity of protection applications.

The third strategy is a resilient multi-stage distribution network reconfiguration for priority load restoration after cyber-physical disruptions. The proposed algorithm is mainly based on graph theory concepts and MST search in restoring maximum load according to their priorities. It principally aims to maximize the post-restoration resilience of the PRN while satisfying the operational and topological constraints. The objective of the proposed algorithm is to restore all the out-of-service loads as long as there is a connection to the upstream network. If there are one or more areas completely isolated from the main grid, the objective would be to use the existing DG(s) capacity to supply critical loads only until all the repair work is done, as discussed in Chapter 2. The algorithm is divided into different stages responsible for determining the topology of the optimal solution and checking its operational feasibility. A salient feature of this approach is that it can not only restore the critical loads in the network but also pick up the maximum possible critical load to the main grid according to their priority. Another important feature is that the restoration paths are selected based on their risk indices so that the post-restoration network becomes resilient against subsequent attacks.

Compared to the literature work, the proposed algorithm is generic and can tackle single or multiple contingencies in the system. Also, the novel simplification approach proposed greatly affected the search domain of the MST, hence the computational time. The optimization outcomes clearly give an advantage to the algorithm over the ones given in the literature when comparing the restoration plan and the computational time. These outcomes validate the usefulness of the technique. Although this algorithm has been developed to perform the network configuration for failed networks due to cyber-physical attacks, the same procedures can be applied for the case of natural disasters as well.

As a final conclusion, on the rise of cyber-physical attacks on modern power grids, the N-k criterion should be considered in system planning. Hence, it has become necessary to include a proper cyber-physical risk analysis side by side with the conventional risk assessment. This analysis helps the system operator identify critical assets within the network and plan

accordingly for preventive and corrective plans. The critical assets can be further reinforced, for example, by using the proposed detection tool for adaptive relays. Moreover, the critical lines can be avoided in restoration plans whenever possible using such a resilient restoration strategy proposed in this thesis.

6.2 Future Work

Although this research has achieved its goals, the work can be expanded in multiple ways as follows,

First, this work considers that the attacker's objective is to disconnect the maximum possible loads using their available resources and capabilities. Estimating actual costs is complicated since it is affected by several factors, including attack severity, customer types, outage duration, etc. Generally, the attack impact on power system can consider the following cost components:

- For industrial and commercial customers, they should consider the production opportunity cost for the forgone benefits, e.g., goods that would have been produced, since there are expenses of idle resources that have to be spent regardless of the plant is operating or not. Other costs due to material spoilage, equipment breakdown/repair, and restart costs have to be added to obtain the total cost of a power outage.

- For residential customers, one fundamental cost component is the out-of-pocket cost, including food spoilage, consumable goods (e.g., flashlights, candles), property/equipment damage, especially vital medical devices, hence threatening people's health or safety. Another cost component that should not be overlooked is customer inconvenience, lost leisure, anxiety, fear, stress, etc.

Second, better awareness of the realistic system can help better estimate the vulnerability of the lines and substations. Further information can be incorporated in the analysis for other factors which may affect the attacker's goals such as, considering vital nearby infrastructures such as water distribution systems and oil and gas pipeline systems.

Third, the N-2 coordinated attacks used in ranking the system components can be generalized to N-k attacks by investigating alternatives to brute-force search, which can be appropriate for this application. This extra step will enable the application of the algorithm to larger power systems.

Finally, the proposed restoration problem focuses on static constraints, i.e., voltage and current limits, power limits, and thermal loading capacities. Future work can consider the dynamic constraints as well. Dynamic performance of the DGs during the restoration and microgrid formation process affects the network stability. Such modeling can be achieved by incorporating additional constraints on the limits of frequency deviation and the limits of DGs transient voltages and currents.

Bibliography

[1] "U.S. DHS ICS CERT, 'ICS-CERT Year in Review,'" 2013. [Online]. Available: https://ics-cert.uscert.gov/sites/default/files/Annual_Reports/Year_In_Review_FY2013_Final.pdf.

[2] NCCIC and ICS-CERT, "ICS-CERT Year in Review-2014," 2014. Accessed: Sep. 22, 2020. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf.

[3] ICS-CERT, "Annual Assessment Report FY2016," 2017, Accessed: Sep. 22, 2020. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.

[4] H. Bilodeau, M. Lari, and M. Uhrback, "Cyber security and cybercrime challenges of Canadian businesses, 2017," *Statistics Canada*, no. 85, pp. 2–19, 2019, Accessed: Sep. 20, 2020. [Online]. Available: https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.htm#r5.

[5] K. Bissell, R. Lasalle, and P. Dal Cin, "2019 Cost of Cybercrime Study | 9th Annual | Accenture," *Ninth Annual Cost of Cybercrime Study*, 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (accessed Sep. 20, 2020).

[6] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 981–997, 2012, doi: 10.1109/SURV.2011.122111.00145.

[7] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016, doi: 10.1049/iet-cps.2016.0019.

[8] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid," *Electricity Journal*, 2017, doi: 10.1016/j.tej.2017.02.006.

[9] A. Gendron and M. Rudner, "Assessing Cyber Threats to Canadian Infrastructure Report," *Prepared for The Canadian Security Intelligence Service*, 2012.

[10] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015, doi: 10.1016/j.jisa.2014.09.005.

[11] G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*. 2015.

[12] Y. Liang and R. H. Campbell, "Understanding and Simulating the IEC 61850 Standard," *IEEE Transaction On Power Delivery*, 2007.

[13] H. Leon, C. Montez, M. Stemmer, and F. Vasques, "Simulation models for IEC 61850 communication in electrical substations using GOOSE and SMV time-critical messages," in *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*, 2016, doi: 10.1109/WFCS.2016.7496500.

[14] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *2012 IEEE Globecom Workshops, GC Wkshps 2012*, 2012, doi: 10.1109/GLOCOMW.2012.6477809.

[15] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC61850 substation automation system network," in *Conference Proceedings - 6th International Conference on Information Technology and Multimedia at UNITEN: Cultivating Creativity and Enabling Technology Through the Internet of Things, ICIMU 2014*, 2015, doi: 10.1109/ICIMU.2014.7066594.

[16] J. T. Sørensen and M. G. Jaatun, "An analysis of the manufacturing messaging specification protocol," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008, doi: 10.1007/978-3-540-69293-5_47.

[17] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32035–32053, 2018, doi: 10.1109/ACCESS.2018.2845378.

[18] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini, "Risk assessment of

malicious attacks against power systems," *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, vol. 39, no. 5, pp. 1074–1085, 2009, doi: 10.1109/TSMCA.2009.2020687.

[19] H. Cetinay, K. Devriendt, and P. Van Mieghem, "Nodal vulnerability to targeted attacks in power grids," *Applied Network Science*, vol. 3, no. 1, 2018, doi: 10.1007/s41109-018-0089-9.

[20] "Data - wiki.openmod-initiative.org." https://wiki.openmod-initiative.org/wiki/Data (accessed Nov. 09, 2020).

[21] "SMARD | Data use." https://www.smard.de/en/datennutzung (accessed Nov. 09, 2020).

[22] C. Arderne, C. Zorn, C. Nicolas, and E. E. Koks, "Predictive mapping of the global power system using open data," *Scientific Data*, vol. 7, no. 1, p. 19, Dec. 2020, doi: 10.1038/s41597-019-0347-4.

[23] J.-P. Van Belle, "The Status and Emerging Impact of Open Data in Africa," *African Data Revolution Report*, pp. 1–111, 2018.

[24] C. W. Ten, A. Ginter, and R. Bulbul, "Cyber-Based Contingency Analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3040–3050, Jul. 2016, doi: 10.1109/TPWRS.2015.2482364.

[25] C. Yoe, *Principles of Risk Analysis*. CRC Press, 2019.

[26] B. E. Biringer, E. D. Vugrin, and D. E. Warren, *Critical infrastructure system security and resiliency*. Taylor and Francis, 2013.

[27] V. Fthenakis, "The resilience of PV during natural disasters: The hurricane Sandy case," in *Conference Record of the IEEE Photovoltaic Specialists Conference*, 2013, pp. 2364–2367, doi: 10.1109/PVSC.2013.6744949.

[28] NIPP DHS, "National Infrastructure Protection Plan - DHS," *Dhs*, pp. 1–57, 2013.

[29] S. Poudel and A. Dubey, "Critical Load Restoration Using Distributed Energy Resources for Resilient Power Distribution System," *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 52–63, Jan. 2019, doi: 10.1109/TPWRS.2018.2860256.

[30] D. Luo *et al.*, "Evaluation Method of Distribution Network Resilience Focusing on Critical Loads," *IEEE Access*, vol. 6, pp. 61633–61639, 2018, doi: 10.1109/ACCESS.2018.2872941.

[31] A. Stankovic, "The Definition and Quantification of Resilience," *IEEE-PES Technical Report*, [Online]. Available: https://resourcecenter.ieee-pes.org/technical-publications/technical-reports/PESTR0065_04-18.html.

[32] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4732–4742, 2017, doi: 10.1109/TPWRS.2017.2664141.

[33] P. Dehghanian, S. Aslan, and P. Dehghanian, "Maintaining Electric System Safety Through An Enhanced Network Resilience," *IEEE Transactions on Industry Applications*, vol. 54, no. 5, pp. 4927–4937, 2018, doi: 10.1109/TIA.2018.2828389.

[34] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience," *IEEE Power and Energy Magazine*, vol. 13, no. 3, pp. 58–66, May 2015, doi: 10.1109/MPE.2015.2397334.

[35] Keith Bea et al., "Federal Emergency Management Policy Changes after Hurricane Katrina: A Summary of Statutory Provisions, RL33279, Washington, D.C.: Congressional Research Service."

[36] C. Robertson, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada," *Energy and Mines Ministers' Conference, Halifax, Nova Scotia*, Accessed: Jan. 10, 2020. [Online]. Available: https://www.readkong.com/page/after-the-blackout-implementation-of-mandatory-electric-7269695.

[37] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4732–4742, 2017, doi: 10.1109/TPWRS.2017.2664141.

[38] J. J. Plotnek and J. Slay, "Power Systems Resilience : Definition and Taxonomy with a View Towards Metrics," *IEEE PES Transactions on Power Systems*, no. September, 2019, doi:

10.13140/RG.2.2.22200.49926.
[39] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Power Systems Resilience Assessment: Hardening and Smart Operational Enhancement Strategies," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1202–1213, 2017, doi: 10.1109/JPROC.2017.2691357.
[40] R. P. Gupta and N. Srivastava, "Substation Automation Using IEC-61850," in *National Power Systems Conference (NPSC)*, 2004.
[41] C. R. Ozansoy, A. Zayegh, and A. Kalam, "A review of substation automation communication protocols," *Australian Journal of Electrical and Electronics Engineering*, vol. 1, no. 1. Institution of Engineers (Australia), 2004, doi: 10.1080/1448837x.2004.11464091.
[42] K. Heldman, *Project Manager's Spotlight on Risk Management*. San Francisco, Calif. ; London: SYBEX, 2005.
[43] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar. 2017, doi: 10.1109/TSG.2016.2545683.
[44] H. H. Goh *et al.*, "Assessment of Power System Risk in Cyber-Attacks in View of the Role Protection Systems," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 1, p. 184, Oct. 2017, doi: 10.11591/ijeecs.v8.i1.pp184-191.
[45] E. J. Oughton *et al.*, "Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks," *Risk Analysis*, vol. 39, no. 9, pp. 2012–2031, 2019, doi: 10.1111/risa.13291.
[46] A. Abedi, L. Gaudard, and F. Romerio, "Review of major approaches to analyze vulnerability in power system," *Reliability Engineering and System Safety*, vol. 183, no. November, pp. 153–172, 2019, doi: 10.1016/j.ress.2018.11.019.
[47] J. Yanbing, L. Ruiqiong, H. X. Shanxi, and W. Peng, "Risk assessment of cascading failures in power grid based on complex network theory," *2016 14th International Conference on Control, Automation, Robotics and Vision, ICARCV 2016*, vol. 2016, no. November, pp. 13–15, 2016, doi: 10.1109/ICARCV.2016.7838704.
[48] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in U.S. power grid," *GLOBECOM - IEEE Global Telecommunications Conference*, 2011, doi: 10.1109/GLOCOM.2011.6133788.
[49] Å. J. Holmgren, "A framework for vulnerability assessment of electric power systems," in *Advances in Spatial Science*, 2007.
[50] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, vol. 69, no. 2 2, pp. 1–4, 2004, doi: 10.1103/PhysRevE.69.025103.
[51] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the European power grid under errors and attacks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 7, pp. 2465–2475, 2007, doi: 10.1142/S0218127407018531.
[52] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 2013, doi: 10.1109/TIFS.2013.2249065.
[53] C. W. Ten, A. Ginter, and R. Bulbul, "Cyber-Based Contingency Analysis," *IEEE Transactions on Power Systems*, 2016, doi: 10.1109/TPWRS.2015.2482364.
[54] R. Bulbul, C. W. Ten, and A. Ginter, "Risk evaluation for hypothesized multiple busbar outages," *IEEE Power and Energy Society General Meeting*, vol. 2014-Octob, no. October, pp. 1–7, 2014, doi: 10.1109/PESGM.2014.6939782.
[55] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in U.S. power grid," *GLOBECOM - IEEE Global Telecommunications Conference*, pp. 1–6, 2011, doi: 10.1109/GLOCOM.2011.6133788.
[56] S. Sridhar, M. Govindarasu, and C.-C. Liu, "Risk Analysis of Coordinated Cyber Attacks on Power Grid," in *Control and Optimization Methods for Electric Smart Grids*, Springer New York, 2012, pp. 275–294.
[57] F. Farzan, M. A. Jafari, D. Wei, and Y. Lu, "Cyber-related risk assessment and critical asset

identification in power grids," *2014 IEEE PES Innovative Smart Grid Technologies Conference, ISGT 2014*, pp. 1–5, 2014, doi: 10.1109/ISGT.2014.6816371.

[58] Z. Mohajerani *et al.*, "Cyber-related risk assessment and critical asset identification within the power grid," in *2010 IEEE PES Transmission and Distribution Conference and Exposition: Smart Solutions for a Changing World*, 2010, doi: 10.1109/TDC.2010.5484417.

[59] S. Ward *et al.*, "Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee," 2007, doi: 10.1109/pes.2007.385583.

[60] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J. C. Tan, "An intrusion detection system for IEC61850 automated substations," *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010, doi: 10.1109/TPWRD.2010.2050076.

[61] U. Premaratne, C. Ling, J. Samarabandu, and T. Sidhu, "Possibilistic decision trees for intrusion detection in IEC61850 automated substations," in *ICIIS 2009 - 4th International Conference on Industrial and Information Systems 2009, Conference Proceedings*, 2009, pp. 204–209, doi: 10.1109/ICIINFS.2009.5429863.

[62] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011, doi: 10.1109/TSG.2011.2159406.

[63] Y. M. Khaw, A. Abiri Jahromi, M. F. M. Arani, S. Sanner, D. Kundur, and M. Kassouf, "A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2554–2565, May 2021, doi: 10.1109/TSG.2020.3040361.

[64] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4332–4341, 2019, doi: 10.1109/TII.2018.2884728.

[65] M. El Hariri, S. Faddel, and O. Mohammed, "An artificially intelligent physical model-checking approach to detect switching-related attacks on power systems," *2017 IEEE 7th International Conference on Power and Energy Systems, ICPES 2017*, vol. 2017-Decem, pp. 23–28, 2017, doi: 10.1109/ICPESYS.2017.8215914.

[66] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione, "A hybrid network IDS for protective digital relays in the power transmission grid," *2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014*, pp. 908–913, 2015, doi: 10.1109/SmartGridComm.2014.7007764.

[67] U. Shahzad, S. Kahrobaee, and S. Asgarpoor, "Protection of Distributed Generation: Challenges and Solutions," *Energy and Power Engineering*, vol. 09, no. 10, pp. 614–653, 2017, doi: 10.4236/epe.2017.910042.

[68] A. Girgis and S. Brahma, "Effect of distributed generation on protective device coordination in distribution system," *LESCOPE 2001 - 2001 Large Engineering Systems Conference on Power Engineering: Powering Beyond 2001, Conference Proceedings*, pp. 115–119, 2001, doi: 10.1109/LESCPE.2001.941636.

[69] P. A. Kumar and J. S. Y.NAGARAJU, "Protection Issues in Micro Grid," *International Journal of Applied Control, Electrical and Electronics Engineering (IJACEEE) Volume 1, Number 1*.

[70] A. Oudalov and A. Fidigatti, "Adaptive Network Protection in MIcrogrids," *ABB International Journal of Distributed Energy Resources* , 2009.

[71] U. Orji *et al.*, "Adaptive Zonal Protection for Ring Microgrids," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1843–1851, Jul. 2017, doi: 10.1109/TSG.2015.2509018.

[72] T. S. Ustun, R. H. Khan, A. Hadbah, and A. Kalam, "An adaptive microgrid protection scheme based on a wide-area smart grid communications network," in *2013 IEEE Latin-America Conference on Communications, LATINCOM 2013 - Conference Proceedings*, 2013, doi: 10.1109/LatinCom.2013.6759822.

[73] A. M. Ibrahim, W. El-Khattam, M. ElMesallamy, and H. A. Talaat, "Adaptive protection coordination scheme for distribution network with distributed generation using ABC," *Journal of Electrical Systems and Information Technology*, vol. 3, no. 2, pp. 320–332, Sep. 2016, doi: 10.1016/j.jesit.2015.11.012.

[74] F. Coffele, C. Booth, and A. Dyśko, "An Adaptive Overcurrent Protection Scheme for Distribution Networks," *IEEE Transactions on Power Delivery*, 2015, doi: 10.1109/TPWRD.2013.2294879.

[75] A. H. Osman, M. S. Hassan, and M. Sulaiman, "Communication-based adaptive protection for distribution systems penetrated with distributed generators," *Electric Power Components and Systems*, vol. 43, no. 5, pp. 556–565, Mar. 2015, doi: 10.1080/15325008.2014.992500.

[76] F. C. Souza and B. A. Souza, "Adaptive overcurrent adjustment settings: A case study using RTDS®," in *2013 IEEE PES Conference on Innovative Smart Grid Technologies, ISGT LA 2013*, 2013, doi: 10.1109/ISGT-LA.2013.6554469.

[77] G. D. Rockefeller, C. L. Wagner, J. R. Linders, K. L. Hicks, and D. T. Rizy, "Adaptive transmission relaying concepts for improved performance," *IEEE Transactions on Power Delivery*, 1988, doi: 10.1109/61.193943.

[78] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient Distribution System by Microgrids Formation after Natural Disasters," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 958–966, 2016, doi: 10.1109/TSG.2015.2429653.

[79] Z. Tan, R. Fan, Y. Liu, and L. Sun, "Microgrid black-start after natural disaster with load restoration using spanning tree search," *IEEE Power and Energy Society General Meeting*, vol. 2016-Novem, 2016, doi: 10.1109/PESGM.2016.7741866.

[80] A. Kumar and S. Grijalva, "Graph Theory and Critical Load-Based Distribution System Restoration using Optimal Microgrids Formation," *Clemson University Power Systems Conference, PSC 2018*, pp. 1–6, 2019, doi: 10.1109/PSC.2018.8664074.

[81] C. Ju, S. Yao, and P. Wang, "Resilient post-disaster system reconfiguration for multiple energy service restoration," in *2017 IEEE Conference on Energy Internet and Energy System Integration, EI2 2017 - Proceedings*, Jun. 2017, vol. 2018-Janua, pp. 1–6, doi: 10.1109/EI2.2017.8245559.

[82] F. Wang *et al.*, "A multi-stage restoration method for medium-voltage distribution system with DGs," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2627–2636, 2017, doi: 10.1109/TSG.2016.2532348.

[83] A. Arif and Z. Wang, "Service restoration in resilient power distribution systems with networked microgrid," in *IEEE Power and Energy Society General Meeting*, Nov. 2016, vol. 2016-Novem, doi: 10.1109/PESGM.2016.7741533.

[84] Y. Xu, C. C. Liu, K. P. Schneider, F. K. Tuffner, and D. T. Ton, "Microgrids for service restoration to critical load in a resilient distribution system," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 426–437, 2018, doi: 10.1109/TSG.2016.2591531.

[85] Y. Xu *et al.*, "DGs for Service Restoration to Critical Loads in a Secondary Network," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 435–447, Jan. 2019, doi: 10.1109/TSG.2017.2743158.

[86] S. Ghasemi, A. Khodabakhshian, and R. Hooshmand, "Active distribution networks restoration after extreme events," *Journal of Operation and Automation in Power Engineering*, vol. 8, no. 2, pp. 152–163, 2020, doi: 10.22098/joape.2019.5803.1435.

[87] J. P. Brans and P. Vincke, "Note—A Preference Ranking Organisation Method," *http://dx.doi.org/10.1287/mnsc.31.6.647*, vol. 31, no. 6, pp. 647–656, Jun. 1985, doi: 10.1287/MNSC.31.6.647.

[88] H. Gao, Y. Chen, Y. Xu, and C. C. Liu, "Resilience-Oriented Critical Load Restoration Using Microgrids in Distribution Systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2837–2848, Nov. 2016, doi: 10.1109/TSG.2016.2550625.

[89] F. Wang *et al.*, "A multi-stage restoration method for medium-voltage distribution system with DGs," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2627–2636, 2017, doi: 10.1109/TSG.2016.2532348.

[90] A. Arif, Z. Wang, J. Wang, and C. Chen, "Power Distribution System Outage Management with Co-Optimization of Repairs, Reconfiguration, and DG Dispatch," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4109–4118, 2018, doi: 10.1109/TSG.2017.2650917.

[91] Rebecca M. Blank. Patrick D. Gallagher, "NIST Special Publication 800-30 Revision 1 - Guide

for Conducting Risk Assessments," *NIST Special Publication, Sept. 2012*, p. 95.
[92] J. Hong, C. C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1643–1653, 2014, doi: 10.1109/TSG.2013.2294473.
[93] Y. Fan, J. Li, D. Zhang, J. Pi, J. Song, and G. Zhao, "Supporting sustainable maintenance of substations under cyber-threats: An evaluation method of cybersecurity risk for power CPS," *Sustainability (Switzerland)*, vol. 11, no. 4, p. 982, Feb. 2019, doi: 10.3390/su11040982.
[94] X. Ji, H. Yu, G. Fan, and W. Fu, "Attack-defense trees based cyber security analysis for CPSs," *2016 IEEE/ACIS 17th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2016*, pp. 693–698, 2016, doi: 10.1109/SNPD.2016.7515980.
[95] J. Hong, "Cybersecurity OF SUBSTATION AUTOMATION SYSTEMS," *Thesis (Ph.D.), School of Electrical Engineering and Computer Science, Washington State University*, 2014, Accessed: May 23, 2021. [Online]. Available: https://research.libraries.wsu.edu:8443/xmlui/handle/2376/5164?show=full.
[96] T. R. Ingoldsby, "Attack Tree Threat Risk Analysis," *Amenaza Technologies Limited*, p. 36, 2013, Accessed: May 15, 2021. [Online]. Available: www.amenaza.com.
[97] M. Hajizadeh, T. V. Phan, and T. Bauschert, "Probability Analysis of Successful Cyber Attacks in SDN-based Networks," *2018 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2018*, no. November, pp. 1–6, 2018, doi: 10.1109/NFV-SDN.2018.8725664.
[98] W. Shang, T. Gong, C. Chen, J. Hou, and P. Zeng, "Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees," *Security and Communication Networks*, vol. 2019, 2019, doi: 10.1155/2019/3574675.
[99] NIST, "NVD - CVSS v3 Calculator," 2017. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (accessed May 30, 2021).
[100] "IEEE 30-Bus System - Illinois Center for a Smarter Electric Grid (ICSEG)." https://icseg.iti.illinois.edu/ieee-30-bus-system/ (accessed Jun. 14, 2021).
[101] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione, "A hybrid network IDS for protective digital relays in the power transmission grid," in *2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014*, Jan. 2015, pp. 908–913, doi: 10.1109/SmartGridComm.2014.7007764.
[102] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *IEEE PES General Meeting, PES 2010*, 2010, doi: 10.1109/PES.2010.5590115.
[103] A. Chakrabortty and M. D. Ilić, *Control and optimization methods for electric smart grids*. Springer New York, 2012.
[104] B. Chen, Z. Yang, Y. Zhang, Y. Chen, and J. Zhao, "Risk Assessment of Cyber Attacks on Power Grids Considering the Characteristics of Attack Behaviors," *IEEE Access*, vol. 8, pp. 148331–148344, 2020, doi: 10.1109/ACCESS.2020.3014785.
[105] J. Liu, M. Zhou, S. Wang, and P. Liu, "A comparative study of network robustness measures," *Frontiers of Computer Science*, vol. 11, no. 4, pp. 568–584, 2017, doi: 10.1007/s11704-016-6108-z.
[106] P. De Meo, E. Ferrara, G. Fiumara, and A. Ricciardello, "A novel measure of edge centrality in social networks," *Knowledge-Based Systems*, vol. 30, pp. 136–150, 2012, doi: 10.1016/j.knosys.2012.01.007.
[107] M. Ouyang and K. Yang, "Does topological information matter for power grid vulnerability?," *Chaos*, vol. 24, no. 4, p. 043121, Oct. 2014, doi: 10.1063/1.4897268.
[108] M. Wakefield and M. Mcgranaghan, "Achieving smart grid interoperability through collaboration," in *IET Conference Publications*, 2009, no. 550 CP, doi: 10.1049/cp.2009.0620.
[109] P. A. Kumar, J. Shankar, and Y. Nagaraju, "PROTECTION ISSUES IN MICRO GRID," *International Journal of Applied Control, Electrical and Electronics Engineering*, vol. 1, no. 1, 2013.
[110] N. A. Mohamed and M. M. A. Salama, "A review on the proposed solutions to microgrid

protection problems," in *Canadian Conference on Electrical and Computer Engineering*, 2016, doi: 10.1109/CCECE.2016.7726697.

[111] F. Yang, A. P. S. Meliopoulos, G. J. Cokkinides, and Q. B. Dam, "Effects of protection system hidden failures on bulk power system reliability," *2006 38th Annual North American Power Symposium, NAPS-2006 Proceedings*, no. October, pp. 517–523, 2006, doi: 10.1109/NAPS.2006.359621.

[112] P. Saini, N. Sethi, M. T. Scholar, and M. T. Scholar, "Decision Support in Data Mining," *International Journal of Innovative Research in Technology and Science*.

[113] J. Komorowski, L. Polkowski, and A. Skowron, "Rough sets: A tutorial," *Rough fuzzy hybridization: A new trend in decision-making*, pp. 3–98, 1999, [Online]. Available: http://secs.ceas.uc.edu/~mazlack/dbm.w2011/Komorowski.RoughSets.tutor.pdf.

[114] Y. Yao and Y. Zhao, "Discernibility matrix simplification for constructing attribute reducts," *Information Sciences*, vol. 179, no. 7, pp. 867–882, 2009, doi: 10.1016/j.ins.2008.11.020.

[115] A. Skowron and C. Rauszer, "The Discernibility Matrices and Functions in Information Systems," in *Intelligent Decision Support*, Springer Netherlands, 1992, pp. 331–362.

[116] C. Grigg and P. Wong, "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*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999, doi: 10.1109/59.780914.

[117] M. E. Nassar and M. M. A. Salama, "A novel probabilistic load model and probabilistic power flow," in *Canadian Conference on Electrical and Computer Engineering*, Jun. 2015, vol. 2015-June, no. June, pp. 881–886, doi: 10.1109/CCECE.2015.7129391.

[118] M. E. Nassar and M. M. A. Salama, "Probabilistic power flow using novel wind and solar probabilistic models," in *IEEE Power and Energy Society General Meeting*, Nov. 2016, vol. 2016-Novem, doi: 10.1109/PESGM.2016.7741568.

[119] Q. Yue, F. Lu, W. Yu, and J. Wang, "A novel algorithm to determine minimum break point set for optimum cooperation of directional protection relays in multiloop networks," *IEEE Transactions on Power Delivery*, vol. 21, no. 3, pp. 1114–1119, Jul. 2006, doi: 10.1109/TPWRD.2005.861333.

[120] "Distribution Test Feeders - IEEE Distribution System Analysis Subcommittee." https://www.ewh.ieee.org/soc/pes/dsacom/testfeeders.html (accessed Jun. 27, 2021).

[121] "OpenDSS." https://www.epri.com/pages/sa/opendss (accessed Jan. 22, 2021).

[122] "ROSETTA. A Rough Set Toolkit." http://bioinf.icm.uu.se/rosetta/ (accessed Aug. 05, 2021).

[123] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014, doi: 10.1109/TSG.2014.2298195.

[124] J. Zhang and C. A. Gunter, "Application-Aware Secure Multicast for Power Grid Communications," in *2010 First IEEE International Conference on Smart Grid Communications*, Nov. 2010, pp. 339–344, doi: 10.1109/smartgrid.2010.5622066.

[125] R. Q. H. Feng Ye, Yi Qian, *Smart Grid Communication Infrastructures: Big Data, Cloud Computing, and Security*, no. c. John Wiley& Sons, 2018.

[126] D. Bernardon, A. P. C. de Mello, and L. Pfitscher, "Real-Time Reconfiguration of Distribution Network with Distributed Generation," in *Real-time Systems*, K. Jian, Ed. Rijeka: IntechOpen, 2016.

[127] Y. Xu, C.-C. Liu, K. Schneider, and D. Ton, "Placement of Remote-Controlled Switches to Enhance Distribution System Restoration Capability," *IEEE Transactions on Power Systems*, vol. 31, pp. 1–12, 2015, doi: 10.1109/TPWRS.2015.2419616.

[128] S. Chanda and A. K. Srivastava, "Defining and Enabling Resiliency of Electric Distribution Systems With Multiple Microgrids," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2859–2868, Nov. 2016, doi: 10.1109/TSG.2016.2561303.

[129] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on Resilience of Power Systems under Natural Disasters - A Review," *IEEE Transactions on Power Systems*. 2016, doi: 10.1109/TPWRS.2015.2429656.

[130] J. Li, X. Y. Ma, C. C. Liu, and K. P. Schneider, "Distribution system restoration with microgrids using spanning tree search," *IEEE Transactions on Power Systems*, vol. 29, no. 6, pp. 3021–3029, 2014, doi: 10.1109/TPWRS.2014.2312424.
[131] S. Khushalani, J. M. Solanki, and N. N. Schulz, "Optimized restoration of unbalanced distribution systems," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp. 624–630, May 2007, doi: 10.1109/TPWRS.2007.894866.
[132] "Resources | PES Test Feeder." https://site.ieee.org/pes-testfeeders/resources/ (accessed Jan. 22, 2021).
[133] J. Chen, S. Thorp, and I. Dobson, "Cascading Dynamics and mitigation assessment in power system disturbances via a hidden failure model," *International Journal of Electrical Power and Energy Systems*, vol. 27, no. 4, pp. 318–326, 2005.
[134] R. Shirey, "Internet Engineering Task Force's Internet Security Glossary, Version 2," *RFC*, vol. 4949, pp. 1–365, 2007.
[135] "Quadrennial Energy Review:Chapter Ii Increasing The Resilience , Reliability , Safety , And Asset Security of TS & D," *QER Report: Energy Transmission, Storage, and Distribution Infrastructure*, [Online]. Available: https://www.energy.gov/sites/prod/files/2015/04/f22/QER-ALL FINAL_0.pdf.
[136] Maryland Energy Administration, "Resiliency through Microgrids Task Force Established," 2014, [Online]. Available:http://energy.maryland.gov/documents/ResiliencyThroughMicrogridsTaskForceEstablished.pdf.
[137] Office Of Electricity Delivery And Energy Reliability, "Hurricane Katrina Situation Report #6," *U.S. DEPARTMENT OF ENERGY*, pp. 7–8, Accessed: Sep. 19, 2020. [Online]. Available: https://www.oe.netl.doe.gov/docs/katrina/katrina_090405_1200.pdf.
[139] J. Celestial, "Ferocious windstorm leaves over 900,000 without power in Quebec, Canada," *The Watchers*. https://watchers.news/2019/11/04/ferocious-windstorm-leaves-over-900-000-without-power-in-quebec/ (accessed Sep. 19, 2020).
[139] *Enhancing the Resilience of the Nation's Electricity System*. National Academies Press, 2017.
[140] NERC, "2019 State of Reliability." Accessed: Sep. 17, 2020. [Online]. Available: https://www.nerc.com/pa/RAPA/PA/Performance Analysis DL/NERC_SOR_2019.pdf.
[141] NERC, "2020 State of Reliability An Assessment of 2019 Bulk Power System Performance," 2014.
[142] Y. Sattarova Feruza and T. H. Kim, "IT security review: Privacy, protection, access control, assurance and system security," *International Journal of Multimedia and Ubiquitous Engineering*, 2007.
[143] W. Stallings, *Cryptography and Network Security: Principles and Practices Fifth Edition*. Pearson, 2011.
[144] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. B. Varnado, and G. Wyss, "Risk assessment for physical and cyber attacks on critical infrastructures," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2005, doi: 10.1109/MILCOM.2005.1605959.
[145] G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann, 2015.
[146] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," *Defcon 22*, pp. 1–90, 2014, Accessed: Sep. 25, 2020. [Online]. Available: https://ioactive.com/a-survey-of-remote-automotive-attack-surfaces/.
[147] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach," in *Proceedings - 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012*, 2012, pp. 55–62, doi: 10.1109/ISRCS.2012.6309293.
[148] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017, doi: 10.1109/TSG.2017.2702125.
[149] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," *Electricity Information Sharing and Analysis Center*, p. 36, 2016,

Accessed: Sep. 17, 2020. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
[150] NERC, "Lesson Learned Risks Posed by Firewall Firmware Vulnerabilities," 2019. Accessed: Sep. 22, 2020. [Online]. Available: https://www.nerc.com/pa/rrm/ea/Lessons Learned Document Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf.
[151] C. S. Holling, "Resilience and Stability of Ecological Systems," *Annual Review of Ecology and Systematics*, vol. 4, no. 1, pp. 1–23, Nov. 1973, doi: 10.1146/annurev.es.04.110173.000245.
[152] M. Bruneau *et al.*, "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," *Earthquake Spectra*, vol. 19, no. 4. pp. 733–752, Nov. 2003, doi: 10.1193/1.1623497.
[153] C. Perrings, "Resilience and sustainable development," *Environment and Development Economics*, vol. 11, no. 4, pp. 417–427, 2006, doi: 10.1017/S1355770X06003020.
[154] W. N. Adger, "Social and ecological resilience: Are they related?," *Progress in Human Geography*, vol. 24, no. 3, pp. 347–364, 2000, doi: 10.1191/030913200701540465.
[155] National Academy of Science, *Disaster Resilience : A National Imperative Disaster Resilience : A National Imperative Committee on Increasing National Resilience to Hazards and Disasters*. 2012.
[156] A. R. Berkeley Iii, M. Wallace, and NIAC, "A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations," *Final Report and Recommendations by the Council*, pp. 1–73, 2010.
[157] T. The National Academies, "Improving Power System Resilience in the 21st Century," *Meeting in Breif-- Resilient America Roundtable*, Accessed: Jan. 07, 2020. [Online]. Available: https://sites.nationalacademies.org/PGA/ResilientAmerica/PGA_146736.
[158] Y. Lin, Z. Bie, and A. Qiu, "A review of key strategies in realizing power system resilience," *Global Energy Interconnection*, vol. 1, no. 1, pp. 70–78, 2018, doi: 10.14171/j.2096-5117.gei.2018.01.009.
[159] A Akhikpemelo, N. Eyibo, and A. Adeyi, "Reliability Analysis of Power Distribution Network," *Continental J. Engineering Sciences*, vol. 11, no. 2, pp. 53–63, 2016, doi: 10.5707/CJENGSCI.2016.11.2.53.63.
[160] E. Vugrin, A. Castillo, and C. Silva-monroy, "Resilience Metrics for the Electric Power System : A Performance-Based Approach," *United States. https://doi.org/10.2172/1367499*, p. 49, [Online]. Available: https://www.osti.gov/servlets/purl/1367499.
[161] A. Lippert, "Hardening and Resiliency: U.S. Energy Industry Response to Recent Hurricane Seasons," *United States. Office of Electricity Delivery & Energy Reliability*, pp. 1–71, [Online]. Available: https://www.hsdl.org/?abstract&did=4496.
[162] P. Zahodiakin, "Making distribution grids stronger, more resilient," *EPRI Journal*, no. 4, pp. 4–8, 2016.
[163] P. A. Kuntz, R. D. Christie, and S. S. Venkata, "Optimal vegetation maintenance scheduling of overhead electric power distribution systems," *IEEE Transactions on Power Delivery*, vol. 17, no. 4, pp. 1164–1169, 2002, doi: 10.1109/TPWRD.2002.804007.
[164] R. Brown, "Literature Review and Analysis of Electric Distribution Overhead to Underground Conversion," *Undergrounding assessment phase 1 final report*, vol. 1019, no. V, pp. 1–59, 2007.
[165] A. R. Berkeley Iii, M. Wallace, and NIAC, "A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations," *Final Report and Recommendations by the Council*, pp. 1–73, 2010.
[166] Y. Lin and Z. Bie, "Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding," *Applied Energy*, vol. 210, pp. 1266–1279, 2018, doi: 10.1016/j.apenergy.2017.06.059.
[167] EPRI Staff, "Electric Power System Resiliency," *Electric Power System Research Institute (EPRI)*, vol. 2, pp. 1–56, 2016, [Online]. Available: https://www.naseo.org/Data/Sites/1/resiliency-white-paper.pdf.
[168] A. Hussain, V. H. Bui, and H. M. Kim, "Optimal operation of hybrid microgrids for enhancing resiliency considering feasible islanding and survivability," *IET Renewable Power Generation*,

vol. 11, no. 6, pp. 846–857, 2017, doi: 10.1049/iet-rpg.2016.0820.
[169] H. Farzin, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Enhancing Power System Resilience Through Hierarchical Outage Management in Multi-Microgrids," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2869–2879, 2016, doi: 10.1109/TSG.2016.2558628.
[170] B. Chen, C. Chen, J. Wang, and K. L. Butler-Purry, "Multi-time step service restoration for advanced distribution systems and microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6793–6805, Nov. 2018, doi: 10.1109/TSG.2017.2723798.
[171] D. E. Olivares, C. A. Cañizares, and M. Kazerani, "A centralized optimal energy management system for microgrids," *IEEE Power and Energy Society General Meeting*, pp. 1–6, 2011, doi: 10.1109/PES.2011.6039527.
[172] C. M. Colson, M. H. Nehrir, and R. W. Gunderson, "Distributed multi-agent microgrids: A decentralized approach to resilient power system self-healing," in *Proceedings - ISRCS 2011: 4th International Symposium on Resilient Control Systems*, 2011, pp. 83–88, doi: 10.1109/ISRCS.2011.6016094.
[173] K. Butler-Purry and S. Nuthalapati, "Self healing reconfiguration for restoration of naval shipboard power systems," in *IEEE Power Engineering Society General Meeting, 2004.*, vol. 2, pp. 40–40, doi: 10.1109/PES.2004.1372745.
[174] C. J. Zapata, S. C. Silva, H. I. González, O. L. Burbano, and J. A. Hernández, "Modeling the repair process of a power distribution system," *2008 IEEE/PES Transmission and Distribution Conference and Exposition: Latin America, T and D-LA*, 2008, doi: 10.1109/TDC-LA.2008.4641852.
[175] Y. Xu, Y. Wang, J. He, M. Su, and P. Ni, "Resilience-Oriented Distribution System Restoration Considering Mobile Emergency Resource Dispatch in Transportation System," *IEEE Access*, vol. 7, pp. 73899–73912, 2019, doi: 10.1109/ACCESS.2019.2921017.
[176] N. Petrovic, D. L. Alderson, and J. M. Carlson, "Dynamic resource allocation in disaster response: Tradeoffs in wildfire suppression," *PLoS ONE*, vol. 7, no. 4, 2012, doi: 10.1371/journal.pone.0033285.
[177] S. Lei, J. Wang, C. Chen, and Y. Hou, "Mobile Emergency Generator Pre-Positioning and Real-Time Allocation for Resilient Response to Natural Disasters," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 2030–2041, 2018, doi: 10.1109/TSG.2016.2605692.
[178] H. Mo, M. Xie, and G. Levitin, "Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks," *European Journal of Operational Research*, vol. 243, no. 1, pp. 200–210, 2015, doi: 10.1016/j.ejor.2014.12.006.
[179] Z. Wang, B. Chen, J. Wang, and C. Chen, "Networked microgrids for self-healing power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 310–319, 2016, doi: 10.1109/TSG.2015.2427513.
[180] Z. Wang and J. Wang, "Self-Healing Resilient Distribution Systems Based on Sectionalization into Microgrids," *IEEE Transactions on Power Systems*, vol. 30, no. 6, pp. 3139–3149, 2015, doi: 10.1109/TPWRS.2015.2389753.
[181] E. Elgqvist, W. Becker, D. Gagne, K. Krah, and C. Kurnick, "Energy Exchange Pre-Conference Workshop: Distributed Energy Technologies for Resilience and Cost Savings," *the 2019 Energy Exchange Conference, 19-22 August 2019, Denver, Colorado*.
[182] R. Arghandeh *et al.*, "The local team: Leveraging distributed resources to improve resilience," *IEEE Power and Energy Magazine*, vol. 12, no. 5, pp. 76–83, 2014, doi: 10.1109/MPE.2014.2331902.

Appendix-A: Understanding Resilience from A Power Grid Perspective

A.1 Introduction

The devastating impacts of the latest high-impact, low-probability events are a motive for making power systems more resilient. In the light of this motivation, the different kinds of these events are defined, and their vulnerabilities to power grids were discussed, with real incidents provided. In addition, the definition of the resilience concept is investigated. The differences between resilience and reliability will be thoroughly studied. A wide range of grid enhancement solutions provided in the literature can be classified as hardening measures and smart/operational measures. Both kinds will be further classified and reviewed.

A.2 Power Grid Vulnerability to Disruptive Events

Since modern societies are becoming more and more dependent on power grids, these grids, in turn, have become more complex and interconnected. Hence, these widespread grids become more vulnerable to both natural and man-induced disasters. The following subsections will discuss these events and the vulnerabilities of power grids towards them. They will also present real examples and discuss their impacts on the grids. While on the subject, the term "Vulnerability" can be defined as a weakness in a system's design, implementation, or operation that could be exploited to violate the system's security and/or operation [134].

A.2.1 Vulnerability to Natural Disasters

Power grids are becoming more vulnerable to natural disasters such as hurricanes, earthquakes, regional storms, floods, Tsunami, ice storms. Due to global climate change, numerous weather events have increased both in severity and frequency [135]. As stated by National Oceanic and Atmospheric Administration (NOAA) [136], the average number of storms the Atlantic produced per year, between 1975-1994, increased 67% in the period between 1995-2012. Additionally, the average annual number of severe hurricanes is more than doubled during the same period. Still, during the period 1985-2012. Thus, climate change is a serious threat to power systems. It will increase the risk of more violent weather events. Such growing events result in more frequent damage to the grid components and cause large-scale power outages affecting hundreds of millions of people.

- **Hurricane Katrina**

In August 2005, Hurricane Katrina, a large Atlantic hurricane, resulted in over 1,800 deaths and $125 billion in damage. The hurricane left more than 2.5 million people in different American states without electricity[137]. It caused extensive flooding to and around the city of New Orleans, which was the main cause of the loss of lives. It also resulted in physical

damage to a number of utilities, which significantly slowed down the efforts of electricity restoration. According to the Homeland Security Secretary, at that time, Hurricane Katrina, plus the resulting flooding of New Orleans, is the worst catastrophe in the country's history.

- **Quebec's 2019 Windstorm**

Quebec has always been prone to severe windstorms. In November 2019, Montreal and several surrounding areas were hit by high winds with speeds as strong as 100 km/h. It also resulted in flooding in some areas wherein people were evacuated. Several electrical towers collapsed, and trees were knocked out. According to Hydro Quebec, this violent storm left more than 900,000 customers without power [138].

A.2.2 Vulnerability to Man-induced Disasters

The second kind of disruptive events —the man-induced— encompass physical attacks, cyber and cyber-physical attacks, and operation errors. The rest of this section will discuss the power grid vulnerability to each kind of these events and explain the attack causes and consequences with real-life examples.

- **Vulnerability to Operation Errors**

Operation errors are considered one of the main causes of historical blackouts in power grids. A substantial number of potential sources of operation errors can be found in both control rooms and the field. The good part is that, because all important grid components are protected using various protective devices that disconnect them before damage occurs, the cascading blackouts normally do not lead to serious physical damage to system components beyond the initiating failure [139].

a. Northeast Blackout of 2003

One example is the Northeast blackout of 2003, which affected about 10 million people in Ontario and 45 million in 8 American states. This blackout was initiated by a simple fault caused by tree branches touching power lines in Ohio. The situation was then complicated by human errors and software/equipment issues since grid operators were not aware of the need for load redistribution of the overload lines. This incident should have been a typical local blackout but unexpectedly was escalated to be the most widespread blackout in North America's history.

b. Southwest Blackout of 2011

Another example is the 2011 Southwest blackout, known as the Great Blackout of 2011. It is the largest power outage in California's history. Owing to a mistake by a technician, a 500kV line was accidentally shut down. Instead of a quick reconnection, the line opening had caused a large phase difference in the grid and could not be reconnected until the next day. Power was re-routed through another stations' switchyard, but the demand was more than it could supply. Hence, multiple transformers were sequentially overloaded and disconnected, leaving 7 million people without power.

- **Vulnerability to Physical Attacks**

Power grids feature substantial amounts of elements that are widely scattered all over the network, hence vulnerable to physical attacks. Physical attacks can target several grid

elements, including transmission and distribution lines, generators, sensors, transformers, actuators, etc. Physical security denotes the procedures required to prevent an attacker from obtaining unauthorized physical access to energy facilities or equipment and cause damage such as espionage and theft [7]. Power utilities always endeavor to guard their facilities by applying appropriate surveillance and access control practices such as closed-circuit television (CCTV) and protective barriers. According to the Electricity Information Sharing and Analysis Center (E-ISAC) [140], 207 physical security incidents were reported in 2018, as shown in Figure A.1, with a 5.3% increase from 2017. Unexpectedly, they reported that 2019 saw a significant increase (536%) in physical security incidents compared to 2018 [141].

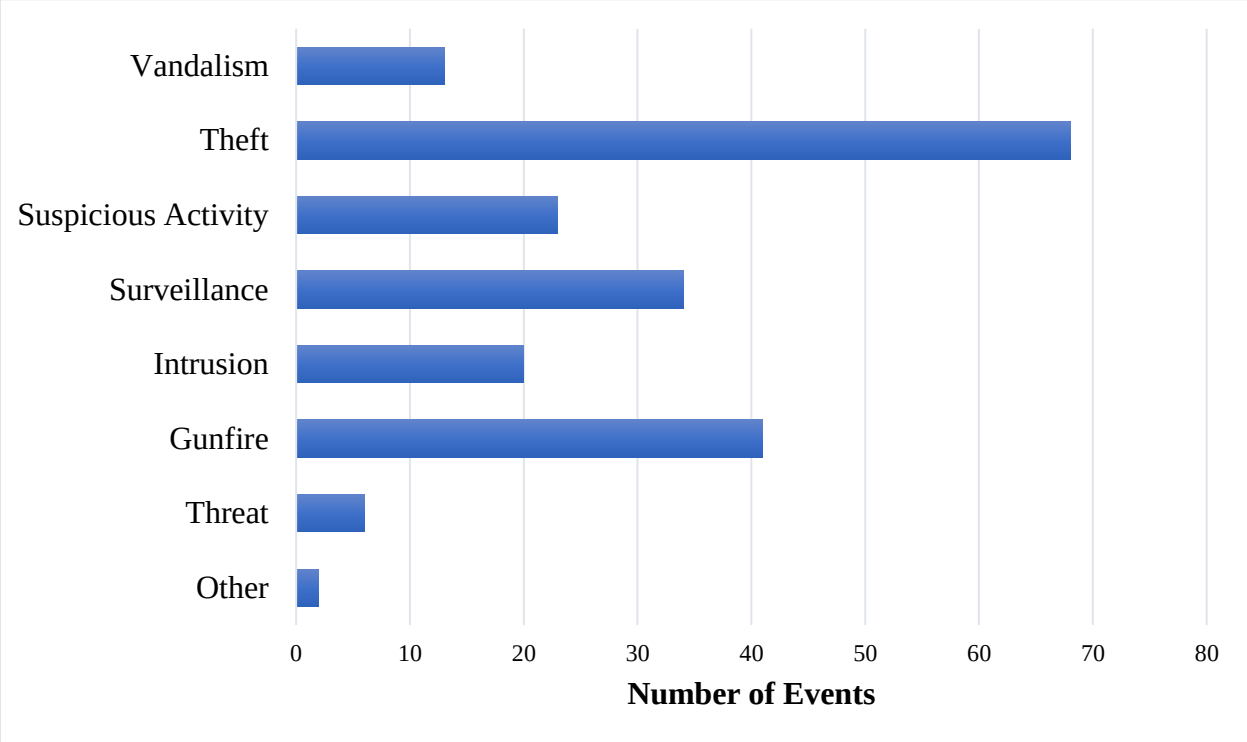


Figure A.1 Physical Security Incidents reported in 2018 according to E-ISAC

a. Metcalf Transmission Substation Attack

In April 2013, the Pacific Gas and Electric (PG&E)-owned Metcalf Transmission Substation near San Jose, California, was attacked by a team of gunmen. This well-planned attack is considered the most significant domestic terrorism incident ever happened involving power grids. Prior to the attack, the communication lines (fiber optic cables) were cut. Using rifles, attackers opened fire on and seriously damaged 17 giant transformers that transferred power to Silicon Valley. Grid operators were able to re-route power from nearby stations, so no major outages occurred. However, the attack caused more than $15 million worth of equipment damage, and it took weeks to replace the damaged parts. Although the effect of this assault on power outage was minor, it rather raised the alarm about the potential for coordinated attacks on multiple key substations.

b. Arkansas Transmission Line Attack

In September 2013, the attacker(s) climbed a 100- ft tower and cut a line using a hacksaw. They also loosened the bolt at the tower base, then tied one end of a steel cable to the bottom of the tower and the other end to a tree across the railroad tracks, with the intention that a train would run into the cable and pulling down the entire tower (possibly tumbling nearby towers as well). The damage in this incident was $550,000. Even though no injuries resulted from the incident, the act created a potential danger to the community.

- **Vulnerability to Cyber and Cyber-physical Attacks**

The need for communication technologies to help monitor and collect data from all over the smart grid has added new cyber vulnerabilities to the grids. According to the Internet Engineering Task Force (IETF) [134], a cyber attack is an "intentional act by which an entity attempts to evade security services and violate the security policy of a system". Likewise, cybersecurity refers to IT security, and it can be defined as the techniques used to protect data and cyber network assets from damage or unauthorized access. Confidentiality, integrity, and availability, known as the CIA triad, are the three security objectives of any information system[142]. Data confidentiality aims to restrict system data access and privileged communications to authorized people only to protect personal privacy and system information. Data integrity refers to protecting system data against improper modification or destruction by unauthorized users or entities. These illegal modifications can be applied during processing, in transit, or even in storage. Thus, data integrity helps ensure data accuracy and consistency. Finally, data availability can be defined as the guarantee of timely and reliable access to system data by authorized users when needed. The CIA triad was originally proposed for cyber paradigms and is useful when being considered for the security of cyber-physical systems.

According to the intent, cyber attacks are classified into two categories: passive attacks and active attacks [143]. Passive attacks are limited to eavesdropping and monitoring communication channels. In other words, the attacker does not aim at modifying any transmitted information or affecting system resources. Instead, the main objective is the disclosure of confidential information, i.e., privacy attacks. However, the attacker can make use of that information in order to prepare for an active attack. On the other hand, in active attacks, an adversary attempts to alter the content of the original message or system resources or to affect system operation. There are four different active attacks types: denial of service (DoS), modification, replay, and fabrication attacks.

c. Cyber-physical Vulnerability

The integration of the cyber layer into power grids makes it easy to cause physical damage to grid elements through cyber attacks. As mentioned earlier, cyber-physical attacks are replacing physical attacks since the attackers can cause the same damage they cause by physical means, without the different risks associated with physical attacks. Fundamentally, cyber-physical attacks (also known as cyber-enabled physical attacks [144]) are a kind of cyber attacks which adversely affect the physical components of power grids [145], attacks that result in physical control of various aspects [146], or the cyber attacks that have a physical effect propagation (the effect propagates from the cyber domain to the physical domain) [147].

a. Ukraine Power Grid Cyber Attack

The Ukraine cyber attack incident —that occurred in December 2015— is considered the first known successful cyberattack on a power grid. [148]. This attack was able to compromise three different energy distribution companies wherein malicious commands were sent to trip the critical lines by switching off 30 substations remotely. In addition, they succeeded in disabling important IT–components such as the uninterruptible power supplies (UPSs). Moreover, they launched denial-of-service attacks on call centers to prevent customers from providing feedback information on the blackout and delay the restoration process. This sophisticated attack caused a widespread power outage disconnecting 225,000 customers. Although power was restored in about six hours, it took several months for control centers to be fully operational [149]. This incident has put the governments on notice because nothing about this attack was intrinsically specific to Ukrainian infrastructure. In other words, the same methodology, techniques, and procedures used in this attack can be easily employed in any other country with unpredictable impacts. Therefore, this attack highlighted the importance of enhancing cyber resilience in the worldwide power grid infrastructure.

b. U.S. Grid Cyberattack (March 2019)

According to the Department of Energy (DOE), on March 5th, 2019, attackers managed to exploit firewall vulnerabilities which enabled them to cause blind spots for the grid operators for about 10 hours between a low-impact control center and multiple remote small power generation sites and between equipment in these sites in the Western area United States (specific location has not been disclosed). Although this attack has not affected the actual flow of electricity, it was significant enough to urge the victim utility to report it to the (DOE). It is the first known cyber attack that results in this kind of disruption. A NERC document named "Lesson Learned" discussing the attack details was posted to the grid regulators' website [150].

A.3 Resilience Definitions and Fields of Application

Although the concept of grid resilience has been studied over the past decade and is currently ongoing, a formal definition for resilience is still being investigated. Various definitions have been presented in several disciplines. Back in 1973, in Ecology, resilience was defined as "a measure of the ability of systems to absorb changes and disturbance and still maintain the same relationships between populations or state variables"[151]. In [152], Bruneau et al. defined community seismic resilience as "the ability of social units to mitigate hazards, contain the effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future earthquakes". They proposed a resilience framework comprises four interrelated dimensions: technical, organizational, social, and economic. In economic systems, resilience is "the ability of the system to withstand either market or environmental shocks without losing the capacity to allocate resources efficiently" [153]. In social systems, it is "the ability of groups or communities to cope with external stresses and disturbances as a result of social, political and environmental change" [154].

According to the National Infrastructure Protection Plan (NIPP) [28], a document developed by the U.S. Department of Homeland Security, resilience is defined as "the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack

or another incident". The National Academy of Sciences (NAS) defined Disaster Resilience as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [155]. One salient feature of this definition is its ability to capture the temporal dimensions of resilience, as discussed in Chapter 2. Since modern power grids are classified as critical cyber-physical infrastructure, according to the National Infrastructure Advisory Council, grid resilience can be defined as "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" [156].

Finally, in April 2018, the IEEE Power and Energy Society (PES) published a technical report to define electric grid resilience. The task force has adopted the following definition and considered it a somewhat general description. As stated, electric grid resilience is "The ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event."[31]. This definition is adequate and hence will be adopted in this thesis as well.

A.4 Resilience Cycle

As aforementioned, resilience specifically handles high-consequence, low-probability events. Indeed, the key to understanding resilience is realizing that disruptions cannot be prevented; instead, we can 1) prepare and plan for, 2) ride through, 3) recover from an event, and 4) observe and learn during this process. Therefore, this process involves four fundamental concepts, as illustrated in Figure A.2 [157], [158]. These concepts form the resilience cycle, as proposed by the National Infrastructure Advisory Council. The incident-focused stage can be seen as three steps reflecting measures taken prior to, during, and after a disruptive event. The post-incident stage focuses on the learning process by modifying plans and revising procedures and measures.

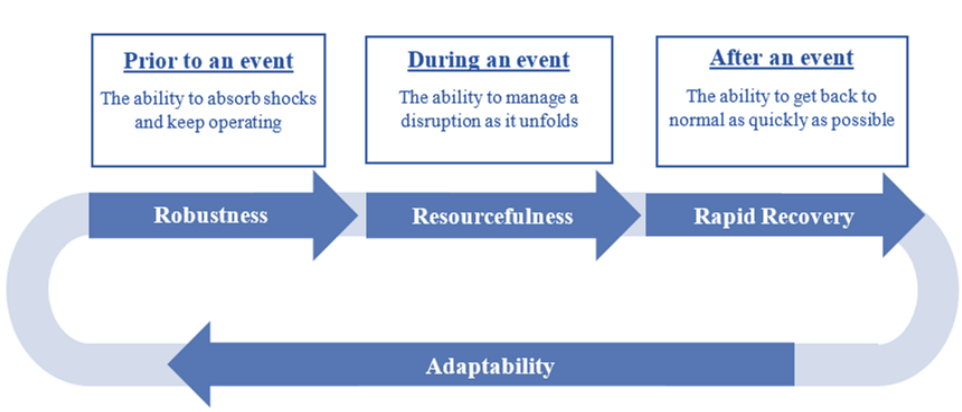


Figure A.2 Resilience Cycle

A.5 Power System Reliability Vs. Resilience

Resilience is often mistakenly used as a synonym for reliability. Power systems reliability is a well-established concept. It is defined as "a measure of the ability of a system to deliver power to all points of utilization within acceptable standards and in amounts desired"[159]. Grid Reliability features adequacy and security. Adequacy denotes the capability of the power system to meet the electric power and the energy requirements of its customers in all the steady states in which the power system may exist considering standards conditions. Security refers to the system's ability to survive sudden disturbances such as electric short circuits or unexpected losses of system components. Power grids are designed to sustain such typical outages.

Those typical power outages that reliability is concerned with are classified as high probability, low impact events such as line faults, device failure, insulation failure, etc. On the other hand, resilience is concerned with extreme events with low probability but high impacts, such as natural disasters, cyber-physical attacks, and human errors [39]. Such kind of events is less predictable and less controllable. They can cause multiple system components to fail, affecting large geographic regions as opposed to typical outages. In addition, because the system is designed to meet the N-1 criterion, single outages leave the network intact in opposed to extreme events, which cause multiple faults, probably in multiple locations, and hence need lots of resources and longer time to recover. Therefore, a power system can be reliable but not resilient to such extreme events. The Ukraine attack is again a typical example of such a coordinated attack, i.e., attacks in which various commands are employed and various components are targeted. Therefore, the N-1 criterion can no longer satisfy the new requirements of modern power grids. Hence, for contingency analysis, there is a need for a more comprehensive framework that takes into account cyber contingencies along with the physical ones [24]. First, a set of combinations of system components that can be compromised should be obtained. Within this extremely large solution space, elimination methods based on power flow are used to assess each combination. Combinations that result in worst-case scenarios will be only considered, while the rest will be discarded.

Another difference is that disruptive events may also affect other infrastructures interdependent with power grids such as telecommunications, transportation, water supply, etc., which affect the restoration process. Such an example is when call-centers were attacked during the Ukraine attack to prevent customers from providing feedback information on the blackout, making the restoration process even harder and slower.

Finally, unlike resilience, reliability analysis does not encompass the adaptation phase, which helps enhance the infrastructural and operational resilience. For example, the reliability-oriented studies do not identify the extra resources and costs required to reduce outage consequences [160].

A.6 Grid Resilience Enhancement

A.6.1 Grid Hardening Measures

Grid hardening is the physical reinforcement of the system infrastructure to improve its ability to sustain the impacts of disruptive events, enhancing the infrastructural resilience. The following are examples of hardening-related measures:

1) Vegetation management near power lines [161]–[163]: During severe weather conditions, falling trees and branches result in excessive damage to power lines. Vegetation management includes two activities. The first is tree trimming and removal programs, which target all trees and bushes within a specified distance from conductors. The second is Tree-Growth Regulators (TGRs). TGRs are chemicals that are injected into trees to control their growth. Since those activities are costly, optimal vegetation maintenance scheduling is done, considering tree growth, weather studies, and crew availability.
2) Undergrounding transmission and distribution lines [164]: The conversion of overhead lines to the underground to lower damage and restoration during storm events. It also helps lower tree trimming cost. However, this conversion must be planned carefully because of the high initial and maintenance expenses.
3) Upgrading utility poles and adding guy wires, and replacing existing conductors with low-temperature, low-sag conductors [161], [165],
4) Relocating network key assets to areas less prone to external shocks, for example, elevating substations and control rooms to protect against flooding [165],
5) Adding redundant transmission routes and installing additional lines, breakers, and transformers [166], and
6) Installing black-start capabilities [167].

Hardening measures primarily aim to reduce the physical impact of disruptive events. Although those measures are more resilience-effective when compared to the operational measures, they must be planned wisely. The measures effective to a specific threat may have a negative effect on a different occasion. For instance, as aforementioned in Chapter 1, undergrounding is an effective solution in the face of storm events. However, underground cables are then vulnerable to flooding and storm surges.

A.6.2 Smart Operational Measures

Smart operational measures denote the adaptive control strategies which can boost system performance in the face of disruptive events. Smart operational measures are more affordable than hardening measures, yet they might not be as effective [17]. Examples of operational-oriented measures are advanced energy management system, allocation and dispatch of emergency response resources, microgrid networking, leveraging distributed energy resources, in addition to risk analysis for disruptive events, adaptive protection and control schemes, optimal reconfiguration and DG islanding, which fully reviewed in Chapter 2.

- **Advanced Energy Management System**

The energy management system (EMS) function is to monitor, control, and optimize the network's performance, considering the required criteria for system stability, reliability, and safety. For microgrids, the EMS is responsible for resource scheduling and coordinating with the distribution network operator (DNO) regarding electricity trading with the main grid. The EMS is basically a system of computer-aided tools which can apply either a centralized or decentralized control scheme.

a. Centralized EMS

Ref. [168] is an example of using a Centralized EMS (CEMS) for enhancing the hybrid microgrid resilience, wherein optimization problems are formulated to be used during normal and emergency operations. During normal operation, it revises the unit commitment status of dispatchable generators and battery scheduling to guarantee feasible islanding after a disturbance event can be realized. During emergency operation, it maximizes the service reliability to local loads according to load priority. Another example of employing CEMS is Ref. [169], which presents a novel hierarchical outage management scheme (OMS) to boost the resilience of a smart distribution system with multi-microgrids against natural hazards. First, it develops a framework for a resilient OMS based on requirements and features identified. Then, using a Model-Predictive-Control (MPC) based algorithm, the microgrid can schedule its available resource. Finally, a DNO coordinates the possible power transfer among microgrids. Ref. [170] aims to generate a sequence of control actions for controllable switches and DERs to help the system operator with decision-making for service restoration. The problem is formulated as an MILP that minimizes the unserved loads by energizing the system step by step, considering the operational constraints at each time step.

The centralized EMS (CEMS) allows for broader observability of the microgrid and appropriateness for optimization techniques application. However, it needs modifications to embrace new elements. In addition, the optimization, in this case, is a computer-intensive function [171]. Another critical downside is the vulnerability of communication infrastructure between microgrid elements. If communication is compromised, the optimization results will be affected. Hence, in the case of uncertain communication environments, a decentralized EMS (DEMS) is more suitable to use wherein each microgrid element is able to communicate with the other elements.

b. Decentralized EMS

In decentralized schemes, as opposed to centralized ones, each entity is responsible for optimizing its operation. Ref. [172] develops a decentralized multi-agent control framework for self-healing in power systems with microgrids. It develops the agent protocols and performs a microgrid multi-agent system simulation that investigates performance during disturbances. Ref. [173] presents a self-healing strategy for shipboard power systems. The system is modeled as a graph. The objective is to optimize the post-event system configuration with priority loads while considering the unavailable equipment and system constraints.

- **Allocation and Dispatch of Emergency Response Resources**

For typical outages, repair resources are always assumed to be unlimited, and repair crews are always assumed available when restoring any grid component [174]. Consequently, the repair time can be predetermined. However, for the outages due to widespread high-impact

events, these assumptions are no longer realistic. Emergency response resources (ERR) are composed of mobile power sources (MPSs) and repair crews (RCs). The MPSs are usually needed to facilitate the restoration of critical loads, and they include mobile diesel generators, mobile photovoltaics, mobile energy storage systems, and spare components. Thus, pre-allocation and pre-positioning of MPSs should be studied. In addition, RCs need to make trips to the affected sites. The crews may experience traffic congestion because the transportation system, as an interdependent system, may also be affected by the disruptions. Hence, a dynamic traffic state for RC mobilization should be considered for accurate dispatch of ERR.

Ref. [175] considered the ERR dispatch in their critical load restoration framework after extreme events. They formulated a weighted dynamic traffic assignment problem as a linear program for transportation using the cell transmission model to minimize the total travel time of the ERR. Ref. [90] proposes a two-stage method for outage management that improves computational efficiency and makes it suitable for applying to large distribution systems. First, it clusters the repair tasks of damaged elements based on their distances from the central crew stations and the availability of resources. The second stage maximizes the picked-up loads and minimizes the repair time by formulating an MILP that considers both systems and routing RCs constraints. The wildfire phenomenon is a type of disaster where delays in response efforts can result in a dramatic escalation in the disaster severity and the demand for resources accordingly. Ref. [176] introduces a dynamic resource allocation method to handle wildfires. First, the wildfire progression was represented by a minimal stochastic process. Then, optimal strategies for decision-making scenarios that arise in fire response policy were computed based on the introduced framework. Ref. [177] proposes forming microgrids to restore critical loads during natural disasters by dispatching truck-mounted mobile emergency generators (MEGs) as a flexible kind of DGs in distribution systems. The dispatch framework is composed of two stages for pre-positioning and real-time allocation problems to minimize the outage duration of critical loads. The vehicle routing problem is also used to address the traffic issue. Finally, considering intentional cyber attacks, Ref. [178] develops a dynamic resource distribution strategy to decide on increasing the protection of components or adding redundant components in parallel systems. The objective is to minimize the system destruction probability by using the best resource allocation. The most probable attack time, considering uncertainties is considered for the vulnerability model.

- **Microgrid Networking**

A series of recent studies have been dedicated to investigating the coordination of islanded microgrids to optimize the operational performance and enhance grid resilience by sharing power among each other when the power from the main grid is not available. Ref. [179] supports two modes of operation for networked microgrids. In the normal operation mode, the objective is to minimize the operation costs and maximize the supply adequacy of each microgrid. In the self-healing mode, an average-consensus algorithm is used to allocate the needed power among the microgrids operating in normal modes to provide the requested power support to the on-fault microgrid. Ref. [180] introduces another strategy with operational and self-healing modes using dispatchable and non-dispatchable DGs. During emergencies, the on-outage portion of the distribution system will be optimally sectionalized into multiple microgrids, and the outputs of the dispatchable DGs will be rescheduled to provide reliable power supply to the maximum loads continuously.

- **Leveraging Distributed Energy Resources (DERs)**

The Federal Energy Management Program (FEMP) is working on a comprehensive framework for resilience planning and implementation. The FEMP discusses, in [181], the role of DER technologies for Resilience and Cost Savings with a focus on solar photovoltaic (PV), energy storage, and combined heat and power (CHP). They designed a web tool, called REopt Lite, that can help obtain the most cost-effective and resilient energy solution for a specific site taking into account the economic viability of the DERs at the site. It can also estimate the time a system can supply a critical load during the main grid outage. Ref. [182] thoroughly discusses the relation of the DERs and grid resilience, including DGs, energy storage, standby generators. It also discusses current industry practices of DER usage during outage conditions. It concludes that DERs can offer ancillary services that central resources can provide.