Towards a Smarter Power Grid: Vulnerability Assessment and Security Metric Deployment

Parisa Akaber

A Thesis

in

The Department

of

Concordia Institute for Information and System Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of

Master of Applied Science (Information System Security) at

Concordia University

Montréal, Québec, Canada

July 2017

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Parisa Akaber**

Entitled: **Towards a Smarter Power Grid: Vulnerability Assessment and Security Metric Deployment**

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science (Information System Security)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

______________________________ Chair
Dr. Amr Youssef

______________________________ External Examiner
Dr. Anjali Agarwal

______________________________ Examiner
Dr. Lingyu Wang

______________________________ Supervisor
Dr. Chadi Assi

______________________________ Co-supervisor
Dr. Mourad Debbabi

Approved by ______________________________
Rachida Dssouli, Chair
Department of Concordia Institute for Information and System Engineering

____________ 2017

____
Amir Asif, Dean
Faculty of Engineering and Computer Science

Abstract

Towards a Smarter Power Grid: Vulnerability Assessment and Security Metric Deployment

Parisa Akaber

Smart Grid is considered as one of the most critical cyber-physical infrastructure; leveraging the advanced coupled communication infrastructure, it is designed to address the limitations and drawbacks of the current power grid and offer a more available, reliable, and efficient power delivery system. Despite its promised advantages, coupling a cyber system with the power grid would increase the grid attack surface by adding known cyber vulnerabilities and threats. Furthermore, security solutions proposed for the traditional power system may not be applicable for the smart grid since they do not consider all smart grid added characteristics (e.g., synchronization). Therefore, it is crucial to lay out a study for the smart grid vulnerabilities and propose corresponding security evaluation and mitigation techniques.

In this thesis, our objective is to model the smart grid as a cyber-physical network considering all the characteristics of power and communication networks as well as the interdependencies among their component. We first propose a contingency analysis security evaluation framework for the smart grid considering concurrent failures resulting from malicious compromises. The proposed framework enables the utility to quantify and monitor the criticality level of the system under study from the security perspective, and decide on proper mitigation/protection actions to avoid catastrophic power outages.

Then, we investigated the critical link (power or communication) identification problem in the smart grid. We highlight the importance of considering the interdependencies among the power and communication network components by showing how a single failure in one side of the grid (cyber or physical) could cascade through both sides and disrupt the power delivery service for a large area immediately. We study the minimum number of links whose removal would have the largest impact on the system in terms of unserved load. The result of this study is beneficial for efficient and optimal resource allocation while designing protection mechanisms for the grid.

Finally, we address the power service restoration problem through network reconfiguration in the presence of distributed energy storage systems. Service restoration is a mandatory procedure which should be performed after any failure occurrence in order to increase the consumer satisfaction and decrease the penalty paid by utility. In this chapter, an optimal restoration approach is devised which is a combination of minimizing the restoration time, unserved load, and energy storage usage cost.

Acknowledgments

I would never have been able to finish my dissertation without the inspiration and support of a number of wonderful individuals.

First and foremost, I would like to express my sincere gratitude to my supervisors, Professor Chadi Assi and Professor Mourad Debbabi, for their continuous support of my Master's study, for their patience, motivation, and immense knowledge. Professor Assi, I want to thank you for your kindness, helpful discussions, constructive and timely feedbacks, and for pushing me to work harder and harder. Professor Debbabi, I am grateful for your support, insightful comments, and valuable and meticulous feedbacks.

I would like to acknowledge the financial supports from Concordia University, My supervisors, and donors of Clara Strozyk Scholarship and Power Corporation Of Canada Graduate Fellowship.

I would like to thank my lab-mates and friends, Heyam, Sara, Mahsa, Reem, Bassam, Ribal, Elie, Mohaned, Houssem, and Tushar, for their support and companionship. Thank you for all the great times that we have shared!

Special thanks goes to my parents, including my in-laws, for their continuous support through my studies far away from home.

This last word of acknowledgment I have saved for my beloved husband, Hamed, who has been standing beside me all along this journey and has made it the best time of my life. Hamed, I am truly thankful for having you in my life.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.0.1 Why Do We Need a Smarter Power Grid?

Today, the reliable delivery of electricity is mandatory to maintain and facilitate the life in modern communities. Electricity delivery is the most vital precondition for world's economy growth and, more importantly, for public safety and health provision. In addition, the power delivery system is considered as the backbone of other important services such as water delivery, gas delivery, digital communication, and the Internet. Indeed, imagining only a couple of minutes of power outage might better highlight the significant role of electricity in our life.

While the current power infrastructure has been aging, the global population growth is demanding the power delivery system to outperform its original capability. According to the U.S Department of Energy report, there is an annul increase of 2.5% in U.S. power demand over the past 20 years [1]. On the other hand, keeping a balance between generation and consumption is a challenging task, since utilities do not have accurate information to predict the dynamic demand. Consequently, in order to meet the consumers' demand, utilities always over-generate power to guarantee smooth power supply even at peak demand [1]. Over-generation is inefficient and costly; in addition, it results in extra Green-house Gas emissions [1]. Moreover, increasing the dependency of the discussed services on the power system because of their expansion will highlight more the importance of designing a reliable power delivery system.

[1] https://www.eia.gov/outlooks/ieo/world.cfm

Table 1.1: Existing Grid and Smart Grid Comparison.

Existing Grid	**Smart Grid**
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors throughout
Manual monitoring	Self-monitoring
Manual restoration	Self-healing
Failures and blackouts	Adaptive and islanding
Limited control	Pervasive control
Few customer choices	Many customer choices

The idea of deploying a Smart Grid as a next generation power delivery system has been introduced to address the discussed drawbacks of the current power grid [2]. The Smart Grid system is a cyber-physical network consisting of a tightly coupled power and communication network which has been evolved to provide a more available, reliable and efficient power delivery service [3]. Smart Grid utilizes the emerging communication and information technologies to provide a comprehensive situational awareness [2]. Hence, the power utilities could rely on real time accurate information about the grid situation to balance the generation and demand, detect failures, and take proper actions to promptly restore the service in case of any disruption. Table 1.1 gives a brief comparison between the smart grid and the traditional power grid [1].

1.0.2 Smart Grid as a Cyber-Physical system

If we look at the smart grid as a cyber-physical system, the physical part of the grid consists of generation, transmission, distribution, and consumption components while the cyber part consists of smart measurement devices (sensors) called Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs), routers, databases, controllers, and a Control Centre. PMUs measure the phasor values such as voltage magnitude, phase angle, current, and frequency. PDCs collect the measurements and send these information to the Control Centre though a Wide Area Network [4]. The control centre will monitor the collected values, perform protection and control analysis (e.g., state estimation) and send back the proper actuation commands (e.g., closing a circuit breaker, increase or decrease the generation) to the power grid. Fig. 1.1 shows an abstract architecture of

[2] Situational awareness could be defined as having the right information at the right time to make the right decisions.

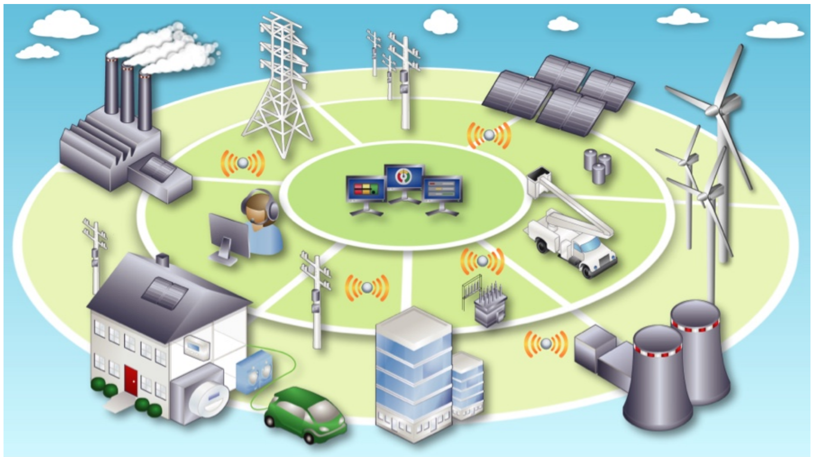

Figure 1.1: Smart Grid architecture. Sensors are deployed in different components of the grid such as generation, transmission, distribution, and consumption.

the smart grid [3]. There is a bidirectional information flow (sensing data and actuation commands) between the control center and the grid.

1.0.3 Smart Grid Vulnerabilities and Security Challenges

The Smart grid is known as a complex cyber-physical network [5] composed of millions of interconnected power and communication network components. Coupling the power network with a communication network makes the grid vulnerable to large number of cyber threats [6],[7]. On the other hand, due to the interdependencies between the power and communication network components, any failure in the power grid could propagate easily to the communication network and vice versa which will lead to cascade of failure [8]. Studying the catastrophic historical blackouts such as 2003 Northeast Blackout [9] and more recently, 2015 Ukrainian Blackout [10] is one of the important resources for power utility to better understand the cyber-physical interdependencies, as well as smart grid vulnerabilities and threats. On the other hand, catastrophic historical blackouts are the main initiatives for the power utilities to try to model and simulate the smart grid as a cyber-physical system while respecting all its characteristics [8],[11], investigate the possible attack scenarios considering cascading effects, quantify the impact and propose protection mechanisms to prevent catastrophic power blackout occurrence [12],[11],[13], quantify the grid resiliency against

[3] https://naea.today/paving-way-newer-smarter-energy-grid/

malicious compromises, and propose security metrics in order to quantify the criticality level of the power system in real time and take actions in emergency situations [14],[15].

1.1 Thesis Organization

In this thesis, we aim at addressing three security challenges in the context of smart grid. Below are the problems investigated in this research:

1.1.1 Contingency Analysis Based Security Metric Deployment

In general, security evaluation techniques (known also as security metrics/indices) are deployed to quantify the security/criticality level of the grid at any instance of time. Taking advantage of security metrics would enhance the situational awareness and help the utility decide upon proper mitigation/restoration strategies to avoid catastrophic power blackouts. In addition, by utilizing security metrics, utilities can identify the critical cyber and physical assets and pinpoint vulnerable threat vectors which are crucial in protection system design. A power security metric deployment is investigated in this chapter [14],[15].

In this chapter, we propose a contingency analysis based security evaluation framework (CASeS) for smart grid systems considering the concurrent power contingencies as well as the power flow dynamics and communication network characteristics. CASeS leverages the Markovian Decison Processes (MDP) model for system security states discretization and provides a novel solution for concurrent power contingency consideration. We evaluate the performance of CASeS on different standard IEEE Bus systems and report on the collected results.

1.1.2 Cascading Link Failure Analysis in Interdependent Networks

Smart grid leverages the high-tech IT infrastructure capabilities to address the drawbacks of the current power delivery system. We could think about smart grid as an interdependent power-communication infrastructure in which communication network components functionality relies on reliable power delivery and power network components operation depends on receiving accurate real-time command and control from the communication side. These interdependencies make the grid more vulnerable to cascading effects in a sense that even a single failure in one side of the grid could easily propagate to both sides immediacy and result in a large-scale outage.

In this chapter, we introduce a vulnerability analysis based on the dynamics of the power grid, and the associated communication network, by reproducing the power flow conditions and the interdependency between the two components to evaluate the impact of attacks on the system in the form of lines and links removal. We formulate this system in a mathematical model and present an algorithm for the analysis of the model output. Numerical experiments of the proposed model and algorithm on the IEEE 14-Bus system and an associated communication network are presented as well.

1.1.3 Automated Post-Failure Service Restoration

Component failures are unavoidable in the power delivery system resulting from natural disasters (e.g., trees falling on power lines because of storm) or malicious compromises (e.g., DoS on access point). After a failure occurs, the utility should identify the faulty components, isolate the fault, and restore the service. Since, customer satisfaction and service reliability are of primary concerns in the smart grid systems, immediate automated service restoration is mandatory after any interruption in the power delivery service. Service Restoration (SR) through Network Reconfiguration (NR) in power systems is a highly investigated problem [16],[17]. To restore the power delivery service after a failure through network reconfiguration, utilities reconfigure the transmission and distribution networks to supply the consumer load demands. However, the advancements in distributed energy storage (DES) systems at the consumer side define a new dimension for SR.

In this chapter, we approach the network reconfiguration for SR in the presence of DES through mathematical modeling. We present a mathematical model that captures the properties of the power system, and reconfigures the network to supply consumer demand over available lines. The presented model considers power supply from DES, and proposes the least cost service restoration plan. We evaluate the proposed approach on different standard IEEE Bus systems, and report on the collected results. The collected results demonstrate the importance of available DES in power service restoration.

Chapter 2

Contingency-analysis Based Security Metric Deployment

2.1 Introduction

Today, our power grid is witnessing a major evolution to a smarter and more capable grid. The idea of *Smart Grid* has been introduced with a goal of enhancing the current state of the electric grid by providing more reliable, available, and efficient power generation, transmission, and distribution network [2]. The smart grid could be defined as a Cyber-Physical network with a tight coupling and interdependencies between the cyber and physical components including the power network components such as generation units, transmission lines and circuit breakers,transformers, and loads, and communication network infrastructure such as sensors, routers, relays, databases, communication links, and control center [18].

The cyber side of the grid is expected to work closely with the power network to monitor the system in real time and respond to the dynamic changes in the electricity demand. In addition, the cyber side is responsible for mitigation/protection decision making in case of any emergency. However, in addition to the advantages provided by cyber-physical coupling, integrating the cyber infrastructure with the power grid will increase their common cyber-threats and vulnerabilities to cyber compromises [19],[20]. Moreover, the increased cyber connectivity of the infrastructure and the interdependency of cyber and physical components prevent the deployment of traditional protection/security solutions.

While the security evaluation techniques have been deployed extensively in IT domain over the past decade, the constraints and characteristics of the cyber-physical systems such as the smart grid in terms of security are different and more complex. In other words, traditional security solutions may not be directly utilized since the smart grid has its own requirements. For instance, any proposed technique should consider the real-time requirements of the smart gird. To evaluate the security of the smart grid, it is important to consider constraints and requirements of both power and communication networks as well as their interdependencies. This has motivated a large body of research in deployment of effective and appropriate security evaluation techniques [21], [12], [15], [14].

Zonouz et al. in [15] introduces a cyber-physical contingency analysis framework called SOCCA to quantify the physical impact, in terms of transmission line overload as a result of different malicious cyber-attacks. At any time, SOCCA estimates the current security state (criticality level) of the system considering the privileges gained by the attacker and the possible physical impact. The same group of researchers extended the idea behind SOCCA [3], by proposing an online security evaluation technique which utilizes the system log to extract the dependencies among cyber assets through a learning phase, and also consider the critical objectives of the system under study indicated by the admin to translate the intrusion detection alerts to something meaningful for intrusion response system. However, none of them considered the impact of *Concurrent Power Contingencies* while performing the security evaluation. Such study can be used to predict and prevent the possible power outages, such as the Ukrainian blackout [22] which occurred as a result of multiple concurrent compromises.

In this research, we present CASeS, a contingency analysis based security evaluation framework. CASeS is designed to evaluate the criticality level of a smart grid in real-time from a security perspective given the alerts produced by intrusion detection systems. It will enable the utility to predict the possible consequences of concurrent power contingencies on the system (for instance probable power outage in an area) that will be served in the protection/mitigation decision making process in case of emergency. Moreover, the proposed framework could be utilized for critical component identification in the grid in order to allocate protection resources in an efficient way. The novelty of CASeS can be summarized as follows:

- Concurrent power contingency identification
- Formulation and implementation of an optimization based AC power simulator designed to quantify the amount of unserved load due to component failures
- MDP tree deployment for system state discretization considering the identified concurrent contingencies

In the remainder of this chapter, we present concurrent contingency consideration impact in Section 2.2. CASeS architecture is described in Section 2.3. A mathematical proof for the proposed security metric is provided in Section 2.4. The numerical results are discussed in Section 2.5. Concluding remarks and future work are provided in Chapter **??**.

2.2 Concurrent Contingency: A Motivation

Contingency analysis in general, is one of the fundamental tools for smart grid monitoring/control which could be defined as a set of if/else scenarios in order to quantify the impact of each component on overall system functionality. An ideal smart gird operates according to the $(N-1)$ security measure to ensure secure power supply even in case of a failure of single grid components. In this section, we provide a motivational example to emphasize the impact of concurrent contingency consideration to better predict the criticality level of the system. Consider a situation in which multiple relays are compromised. Consequently, a catastrophic blackout might occur if the transmission lines controlled by those relays are critical links carrying power flow for a large area. Fig. 2.1 presents an illustrative example in which the circle represents an area receiving its power demand through two

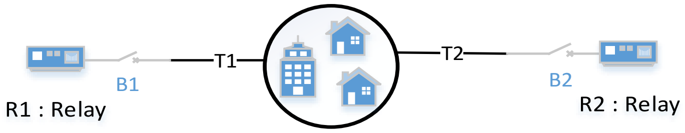

Figure 2.1: Multiple link contingency analysis example.

main transmission lines $T1(T2)$. Circuit breaker $B1(B2)$ is controlled by relays $R1(R2)$. Consider an attack scenario in which $R1$ is compromised, then the attacker has the control over circuit breaker $B1$ and could trip the transmission line $T1$. Consequently, power flow would be rerouted through $T2$ (if it has enough capacity) to prevent any power outages. The same scenario could be considered for compromising $R2$. However, if the attacker could compromise $R1$ and $R2$ concurrently, the utility could not redistribute the power and consumers in the area would experience a power blackout.

Therefore, to better protect the system against malicious compromises, we should identify and avoid the system to enter a state with $R1$ and $R2$ (or other set of relays with similar scenarios) being compromised concurrently. In a large network, concurrent contingency identification is indeed not a straight forward step because of cascading effects [23].

2.3 CASeS Architecture

CASeS will evaluate the security level of the power network in two phases: offline and online phase.

- Offline Phase: an exhaustive search is performed to identify concurrent contingencies. In other words, to identify the transmission lines whose removal would have a large impact on the power delivery system. In addition, given the topology of the communication network and the access control policies, a connectivity matrix is produced. The details are provided in Section 2.3.2.

- Online Phase: Taking the communication network components (e.g., databases, web servers, hosts, controllers, and relays) connectivity matrix as an input, to enumerate the possible security states the system could be in, a Stochastic Markovian Decision Process [24] model is deployed (similar to [15]). However, the MDP tree alone could not capture states with multiple compromised components (concurrent contingencies). Therefore, complementary state generator is designed to add the concurrent contingency states to the MDP. And finally, a security metric is defined and calculated.

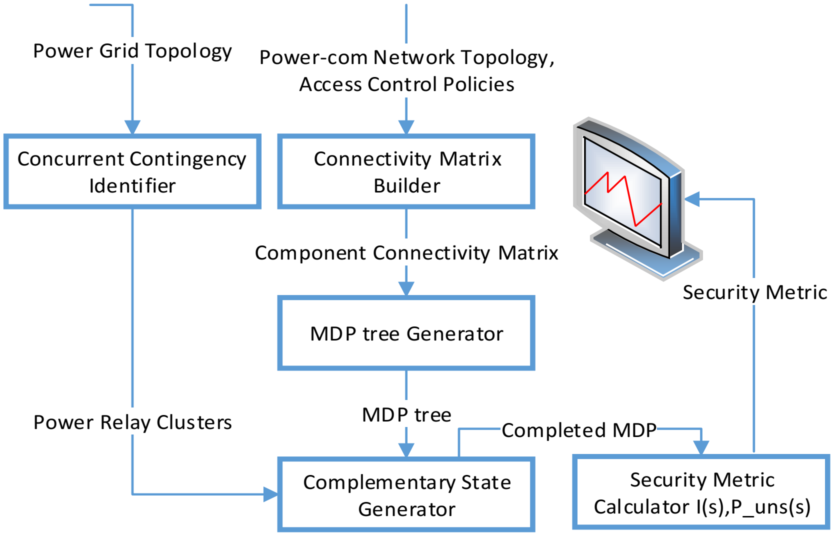
Power Grid Topology
Power-com Network Topology, Access Control Policies
Concurrent Contingency Identifier
Connectivity Matrix Builder
Component Connectivity Matrix
MDP tree Generator
Security Metric
Power Relay Clusters
MDP tree
Completed MDP
Complementary State Generator
Security Metric Calculator I(s),P_uns(s)

Figure 2.2: CASeS architecture.

The main components of CASeS are presented in Fig. 2.2 and described in the following.

2.3.1 Connectivity Matrix Builder

Given the topology of the communication network (devices such as databases, web servers, hosts, routers, controllers, and relays are the communication network components) and access control policies, Connectivity Matrix Builder will produce matrix $C[D \times D]$ in which C_{ij} is 1 if component j is accessible through component i and 0 otherwise; D is the total number of components. Accessibility could be defined as the possibility for the attacker to compromise component j while he already compromised component i.

As an example in Fig. 2.3, relay controllers C_1 and C_2 are accessible through database DB. Therefore, if an attacker compromise DB there is a possibility for him to compromise these controllers as well. Fig. 2.3 (a) presents a simple connectivity graph with the assumption that components W and DB are connected to a network which is accessible by a remotely connected attacker. Since attacker's entry points are critical nodes to generate the MDP, if component i is accessible for the attacker to initiate the attack, C_{ii} is set to 1.

2.3.2 Concurrent Contingency Identifier

As discussed before, to perform a complete contingency analysis, it is important to take into account concurrent contingencies since the failure the of multiple grid components concurrently has occurred in some historical blackouts and affected a large area [22]. Therefore, it is not enough to consider only the states with single compromised power component (relay) in our MDP generation. To address this problem, the first step is to identify clusters k ($k \in \{2, 3, 4, ..\}$) of power transmission lines for which the impact (i.e. unserved load) of concurrent failure is much larger than the summation of their single failure impact. Eq.2.1 is a mathematical representation for concurrent contingency identification (k=2):

$$P_{uns}(\{t_i\}, P) + P_{uns}(\{t_j\}, P) < P_{un}(\{t_i, t_j\}, P) \tag{2.1}$$

where $P_{uns}(T, P)$ function would return the amount of unserved load calculated by the AC power simulator (discussed in section 2.3.6) given the power network toplogy P and the set of compromised transmission lines T. For instance, in Fig. 2.3 although the impact of compromising $R1$ $(or\ R2)$ is zero as the power flow could be redistributed over the other lines, attacking both would result in a power service disruption for the circled area. Therefore, $R1$ and $R2$ would create a cluster.

Indeed, the analysis could be done for clusters of two, three, or more power links. However, there is no need to consider large clusters as the success rate for attacking large number of components successfully is so small [11]. In [11], we studied the smart grid critical link identification problem and showed that even in a big grid removal of small number of links could result in a catastrophic power outage since the interdependencies between component would cause a cascaded failure. Therefore, in this research an exhaustive search is done for the clusters of size $k \in \{2, 3, 4\}$. Indeed, for each possible set of relays with size k, if Eq. 2.1 satisfies, we consider the set as one cluster. The output of this block is a set of clusters which will be used by Complementary State Generator.

2.3.3 MDP State Tree Generator

Given the connectivity matrix C generated in the previous block, MDP Tree Generator enumerates all the possible states and transitions among them.To deploy any MDP the below elements should be defined:

- S a finite set of states
- A a finite set of actions
- $P_a(s, s')$ transition probability
- $R_a(s, s')$ reward function
- $\gamma \in [0, 1]$ discount factor

From which S, A, and $P_a(s, s')$ are mandatory components to build the MDP tree. These components are discussed below in details ($R_a(s, s')$ and γ are discussed in Section 2.3.5):

- S is a finite set of system states. Any attack scenario could be divided into a finite number of actions followed by an attacker or a group of attackers with pre-defined objectives. In this research, we define a ”security state” for the system as a set of compromised power-communication network components.It is worth mentioning that high-tech power components used in smart grid such as circuit breakers and switches has a cyber part (application running on them) which could be compromised through a cyber attack.

- A is a finite set of actions: A_s is a set of possible actions in state s (i.e., SQL injection and DoS attack)

- $P_a(s, s')$ a probability that tacking an action a results in going to state s' while the current state is s. In our case, this probability could be defined as the attacker success rate for a specific scenario. Common Vulnerability Scoring System [25] is employed to assign these probabilities.

To generate the MDP tree, we start from an initial state ($\emptyset$) in which there is no compromised component and we follow the Algorithm 1 to create the states and transitions. Fig. 2.3 (b) presents

Algorithm 1 MDPGenerator(int[][] componentsConnectivity)

```
Output: Array<State> $states$;
        Array<Transition> $transitions$;
State $emptyState$ =new State()
$states.add(emptyState)$;
for ($i$:$componentsConnectivity$) do
    if ($i$ is an attacker's entrypoint) then
        State $initial$ =new State($i$);
        $states.add(initial)$;
        $transitions.add(emptyState, initial)$;
    end if
    for ($j$ : $componentsConnectivity[i]$) do
        if ($i$ is not connected to $j$) then
            continue;
        end if
        if ($i$ and $j$ mutually connected) then
            if ($s_{ij}$ does not exist) then
                State $s_{ij}$ = new State($i, j$);
                $states.add(s_{ij})$
                $transitions.add(initial, s_{ij})$;
                $createReachableStates(s_{ij})$;
            else
                $transitions.add(initial, getState(i, j))$;
            end if
        else
            State $s_{ij}$ = new State($i, j$);
            $states.add(s_{ij})$
            $transitions.add(initial, s_{ij})$;
            $createReachableStates(s_{ij})$;
        end if
    end for
end for
```

a MDP tree created based on the Fig. 2.3 (a) connectivity matrix. To produce this MDP based on Algorithm. 1 we follow the below steps:

- Creating the initial state ($\emptyset$). Lines (3 - 4)
- Creating entry points states as states reachable from the initial state (states Db and W). Lines (6 - 8)
- For each state s adding the reachable states based on the connected components to s's components. For instance, $C1$ is connected to Db so a combinatorial state s_DbC1 would be added to the state Db. Lines (17 - 20)

$createReachableStates(s)$ function is a recursive function which returns all the possible states reachable from state s considering all the components in this state and their connectivities to other components.

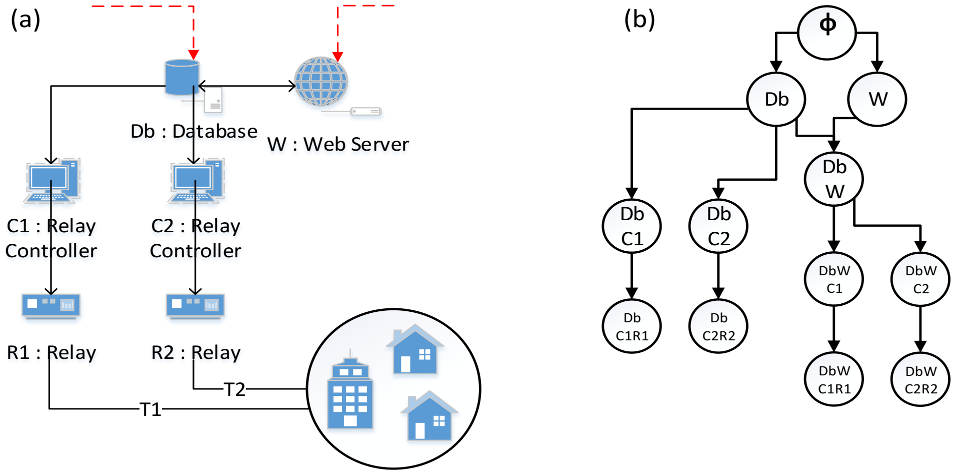

Figure 2.3: MDP generation example. (a) connectivity matrix developed based on the network topology, connections, firewalls, access control policies. (b) MDP deployed given the connectivity matrix.

2.3.4 Complementary State Generator

To address the problem discussed in the previous block, after clustering the power components (e.g., relays), Complementary State Generator will add the required additional states covering the concurrent contingencies. Therefore, this block will receive the set of clusters (each cluster is a finite set of power network relays) identified by concurrent contingency identifier block and the tree generated by MDP generator and the output would be the completed MDP tree. The following steps are performed by Algorithm. 2:

(1) For each cluster we consider all the possible combinations of states called $subSt$ including relays which their combinatorial state would have all the components belonging to the cluster. Line (5)

(2) For each subset of states $subSt$, we find the root node using the function $getRoot$. Line (7)

(3) For each state $s \in subSt$, we find the path from the $root$ to s. Line(9)

(4) We combine all the paths for $subSt$ states in order to build one combinatorial path $combPath$ including new states and transitions from the $root$ to the complementary state covering all the relays belong to the cluster. Line(11)

(5) We assign transition probability for the added transitions and calculate it according to: $Pr(A \cap B) = Pr(A) \times Pr(B)$

(6) We add the new states and transitions to the completed MDP tree. Lines (12, 13)

Algorithm 2 MDPComplete(MDPtree)

```
 1: Given Array <Cluster> $clusters$;
 2: Output Array <State> $completedSt$;
 3:        Array <Transition> $completedTr$;
 4: for ($cluster$ : $clusters$) do
 5:     for ($subSt$ :$MDPtree.states.getSubSt(cluster)$) do
 6:         Array <Path> $paths$;
 7:         State $root$ = $subSt.getRoot()$;
 8:         for ($clusterState$ : $subSt$) do
 9:             $paths.add(getPath(root,clusterState))$;
10:         end for
11:         Path $combPath$ = $paths.combine()$;
12:         $completedSt.addAllSt(combPath.states)$;
13:         $completedTr.addAllTr(combPath.transitions)$;
14:     end for
15: end for
```

Fig. 2.4 presents the completed MDP tree, assuming that R_1 and R_2 belong to one cluster. If we consider the $subSt$ $sub = \{DbC1R1, DbC2R2\}$, the $getRoot$ function would return the state

Db and the final combinatorial state containing $R1$ and $R2$ would be $DbC1R1C2R2$ for which the combinatorial path would be created, as shown in the figure.

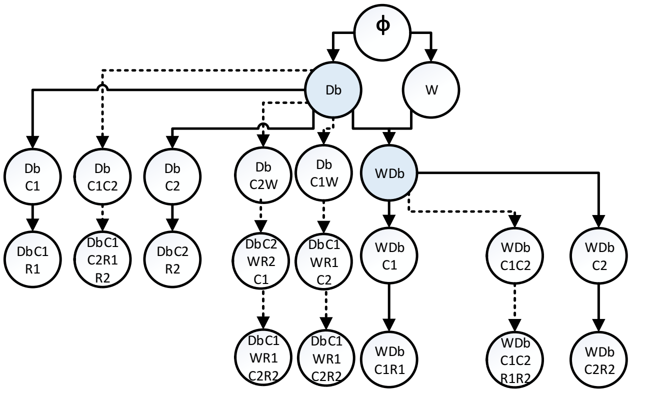

Figure 2.4: Completed MDP tree produced by Algorithm. 2

2.3.5 Security Metric Calculator (MDP solver)

In the MDP generation block S, A, and $P_a(s, s')$ are discussed. In this section, we define other required variables and calculate the security metric $I(s)$ for each system state s. $R_a(s, s')$ is the received reward after transitioning from state s to s', due to action a. In CASeS, the reward function is defined by:

$$R_a(s, s') \ = \ P_{uns}(PowComp(s'), P) - P_{uns}(PowComp(s), P) \tag{2.2}$$

in which $P_{uns}(T, P)$ is an impact index quantified as the amount of unserved load calculated considering the compromised power components in state s ($PowComp(s)$ function will return the set of compromised transmission line relays in state s) and the power network topology P. In other words, $R_a(s, s')$ is the excessive power impact that an attacker could achieve by going from state s to state s'. Impact index would be assigned states with power components (e.g., relay).

Assuming that we could estimate the current security state by analyzing the alerts received from intrusion detection systems, the Bellman Equation (Optimal Value Function) could be followed to quantify the criticality level of the current state from the security perspective.

γ is the discount factor which represents the difference in importance between future rewards and present rewards.

Bellman equation is an iterative equation that connects a state (value/reward) to its predecessor written as follows:

$$I(s) = \max_{a \in A(s)} \sum_{s' \in S} P_a(s,s')[R_a(s,s') + \gamma I(s')] \tag{2.3}$$

The main objective behind this representation is to find the state with the maximum impact (reward) accessible from the current state with the minimum budget (maximum success probability) from the attacker point of view. In this research, value iteration technique is implemented to compute the $I(s)$ from the Bellman Equation.

2.3.6 AC power simulator

We presented the power network as graph $G(N_p, E_p)$ in which N_p is a set of nodes including substations N_s, generation units N_g, and loads N_l. And E_p is a set of power lines. $A[Np \times Ep]$ is an adjacency matrix in which a_{ij} is 1 if node i is one of the ends of link j and 0 otherwise. d_{ij}^{out}/d_{ij}^{inc} is a binary variable indicates of there is a power flow on links j from/toward node i. For each generator g, we present the amount of generated power by gen_g and the capacity by cap_g. For each transmission line j, the capacity is presented by cap_j, the injected power by p_j^{in} , power loss by p_j^{loss}, and the outgoing power by p_j^{out}. δ_j^{gn} is a fraction of load from generator g to load n on link j and r_j^{gn} is a binary shows if link j is on the path between generator g to load n. The objective of the proposed mathematical model is to minimize the unserved load given the available power links and with respect to the constraints discussed in the following.

$$\text{Minimize } P_{\text{uns}}$$

subject to:

$$d_{ij}^{out} = a_{ij}\ ,\ d_{ij}^{inc} = 0 \quad \forall i \in N_g,\ j \in E_p \tag{2.4}$$

$$d_{ij}^{out} = 0\ ,\ d_{ij}^{inc} = a_{ij} * t_j \quad \forall i \in N_l,\ j \in E_p \tag{2.5}$$

$$d_{ij}^{out} + d_{ij}^{inc} = a_{ij} * t_j \quad \forall i \in N_s,\ j \in E_p \tag{2.6}$$

$$P_{\text{uns}} = \sum_{i \in N_l} (q_i - s_i^{total}) \tag{2.7}$$

$$s_i^{total} = \sum_{j:(si) \in E_p} p_j^{out} \quad \forall i \in N_l, s \in N_s \tag{2.8}$$

$$p_j^{in} = p_j^{out} + p_j^{loss} \quad \forall j \in E_p \tag{2.9}$$

$$p_j^{loss} = I_j^2 (R_j \cos(\phi) + X_j \sin(\phi)) \quad \forall j \in E_p \tag{2.10}$$

$$p_j^{in} = I_j (V_{i_1}.\, d_{i_1 j}^{out} + V_{i_2}.\, d_{i_2 j}^{out}) \quad \forall j : (i_1 i_2) \in E_p, i_1 i_2 \in Np \tag{2.11}$$

$$0 \leq p_j^{in} \leq t_j * cap_j \quad \forall j \in E_p \tag{2.12}$$

$$\sum_{g \in N_g} gen_g = \sum_{j:(il) \in E_p} p_j^{out} + \sum_{j \in E_p} p_j^{loss} \quad \forall i \in N_p, l \in N_l \tag{2.13}$$

$$gen_g = \sum_{j:(gi) \in E_p} p_j^{in} \quad \forall g \in N_g, i \in N_s \tag{2.14}$$

$$0 \leq gen_g \leq cap_g \quad \forall g \in N_g \tag{2.15}$$

$$\sum_{j:(is) \in E_p} p_j^{out} * d_{sj}^{inc} = \sum_{j:(si) \in E_p} p_j^{in} * d_{sj}^{out} \quad \forall i \in N_p, s \in N_s \tag{2.16}$$

$$\sum_{j:(i_1 i_2) \in E_p} \delta_j^{gn} * d_{i_1 j}^{out} - \sum_{j:(i_1 i_2) \in E_p} \delta_j^{gn} * d_{i_1 j}^{inc} \begin{cases} \leq 1 & \text{if g is at } i_1 \\ \geq -1 & \text{if n is at } i_1 \\ = 0 & \text{otherwise} \end{cases} \tag{2.17}$$

$$\forall n \in (N_p - N_g),\ \forall g \in N_g$$

$$r_j^{gn} \leq \delta_j^{gn} \, * \, d_{i_1 j}^{out} \, * \, M \quad \forall j : (i_1 i_2) \in E_p, g \in N_g, n \in (N_p - N_g) \tag{2.18}$$

$$r_j^{gn} \geq \frac{\delta_j^{gn} \ * \ d_{i_1j}^{out}}{M} \quad \forall j : (i_1 i_2) \in E_p, g \in N_g, n \in (N_p - N_g) \tag{2.19}$$

$$t_j \leq \sum_{g \in G} \sum_{n \in N_l} r_j^{gn} \tag{2.20}$$

$$t_j \geq \frac{\sum_{g \in G} \sum_{n \in N_l} r_j^{gn}}{M} \tag{2.21}$$

In the presented mathematical model, we assume that voltage regulators are available at all nodes to fix the voltage and reactive power compensator are installed before the loads. The objective function is to minimize the unserved load to deploy the optimal power flow. Eq. (2.4),(2.5), and (2.6) are responsible for power direction, although power transmission lines are bi-directional, power will flow on one direction simultaneously. Eq. (2.7) is calculating the amount of unserved load given the requested by each load q_i and the amount of power delivered to the load through the power network s_i^{total}. Eq. (2.8), (2.9), and (2.10) are responsible for calculating the current and the power loss associated to each transmission line. Eq. (2.12) represents the power line capacity. The total generation should be equal to the total power delivery plus the total loss over all transmission line which is captured by Eq. (2.13). Eq. (2.14) is to make sure that all the power generated by generation units are injected to the grid. Eq. (2.15) is the generation capacity constraint. Eq. (2.16) handles the power balance in each substation. Eq. (2.17) represents the multi-commodity flow constraint. Eq. (2.18), (4.21), (2.20), and (2.21) are responsible for constructing the power delivery path.

2.4 Metric Proof

Function $f(x, y)$ is a metric if it satisfies the following properties ($\forall x, y$) [26]:

(1) Non-negativity $\quad f(x, y) \geq 0$

(2) Triangle inequality $\quad f(x, y) + f(y, z) \geq f(x, z)$

(3) Symmetry $\quad f(x, y) = f(y, x)$

(4) Identity $f(x, y) = 0 \iff x = y$

If all the above mentioned properties except (4) are satisfied we would have a pseudo-metric. In this section, we will prove that the proposed security metric is mathematically a pseudo-metric [26]. Suppose in each state (s) only one state (s') is accessible by taking action (a) (if we prove the properties for this case, the proof would be valid as well for the general case). The proposed security metric could be written as :

$$I(s) - \gamma I(s')P_a(s, s') = P_a(s, s')\; R_a(s, s') \tag{2.22}$$

If we consider $I(s) - \gamma I(s')P_a(s, s')$ as a metric and call it $f(s, s')$, the below steps could be followed in order to prove the satisfaction of the discussed properties for f:

(1) Non-negativity: First, a probability is always a non-negative value. Second, the generated MDP is a history tree, so if s' is followed by s, s' contains all the components in s plus one. Assume that $R_a(s, s')$ would take a negative value (proof by contradiction) then:
$P_{uns}(PowComp(s'), P) > P_{uns}(PowComp(s), P)$
which means that more components are compromised ,however, the result is the smaller amount of unserved, which is a contradiction. As a result, $R_a(s, s')$ could not be negative. Therefore, $f(s, s')$ would always take non-negative values.

(2) Triangle inequality: Let P be the existence of triangle in the graph ($s \rightarrow s' \rightarrow s" \implies s \rightarrow s"$) and Q be the triangle inequality
$f(s, s') + f(s', s") \geq f(s, s")$
Now we should prove that $P \implies Q$ is always $True$. In our case, since state generation is accumulative, if ($s \rightarrow s"$) exist, starting from state s there is no other path reaching state $s"$. Therefore, (P) is $False$. However, based on *Vacuous Proof*, $P \implies Q$ is still $True$.

(3) Symmetry: Since the generated MDP is a tree, there is no loop. Therefore, if $f(s, s')$ is defined $f(s', s)$ does not exist. The same approach discussed in triangle inequality proof could be followed (Vacuous Proof).

(4) Identity: There are many middle states for which the difference between $P_{uns}(s')$ and $P_{uns}(s)$

is zero since s' and s are the states without any power compromised components. As a result $f(s, s') = 0$, however, s and s' are two different states. Therefore, $f(s, s')$ is a pseudo-metric.

2.5 Numerical Results

Fig. 2.5 presents the power-communication network architecture for the IEEE 14 bus system. We consider the buses as nodes and transmission lines as edges in the power network graph. Power network consists of generation units presented by G, substations presented by S, and loads presented by L and each load stands for a neighborhood. Power transmission lines are bidirectional links, however, they can carry the power flow only on one direction at the same time. For each transmission line we associated a relay (R) which controls the status of the circuit breaker. We assume that each substation contains one controller (C) which is controlling the relays on transmission lines connected to that substation. As an example, we showed on the figure, $C7$ (which is a controller inside substation $S7$) is controlling relays $R8$, $R29$, $R15$ and $R14$ which are located on transmission lines connected to $S7$. From the attacker's point of view, compromising $C7$ would result in going one step toward changing the status of circuit breakers associated to those transmission lines. In the communication network, we associate databases presented by D connected to the controllers and centralized databases presented by CD connected to those databases. Each centralized database has web server presented by W. Centralized databases and web servers are connected to the network accessible by a remotely connected attacker (entry point presented by double lines).

The simulations were executed on a windows machine with Intel Core i7 CPU running at 2.67GHZ and equipped with 12 GB of RAM.

Table 2.1 shows the results for different IEEE bus systems for which communication network is designed following the same approach discussed for IEEE 14 bus system. The results show that adding the complementary state generation block to the security evaluation framework increases the number of produced states in MDP less than 6% in all test cases. Table 2.2 presents the run time for different blocks of CASeS. Since, the identified power component clusters depend on the topology of power network (which is fixed), concurrent contingency identification would be performed in an offline manner. The running time for different blocks are reported in milliseconds. Values reported

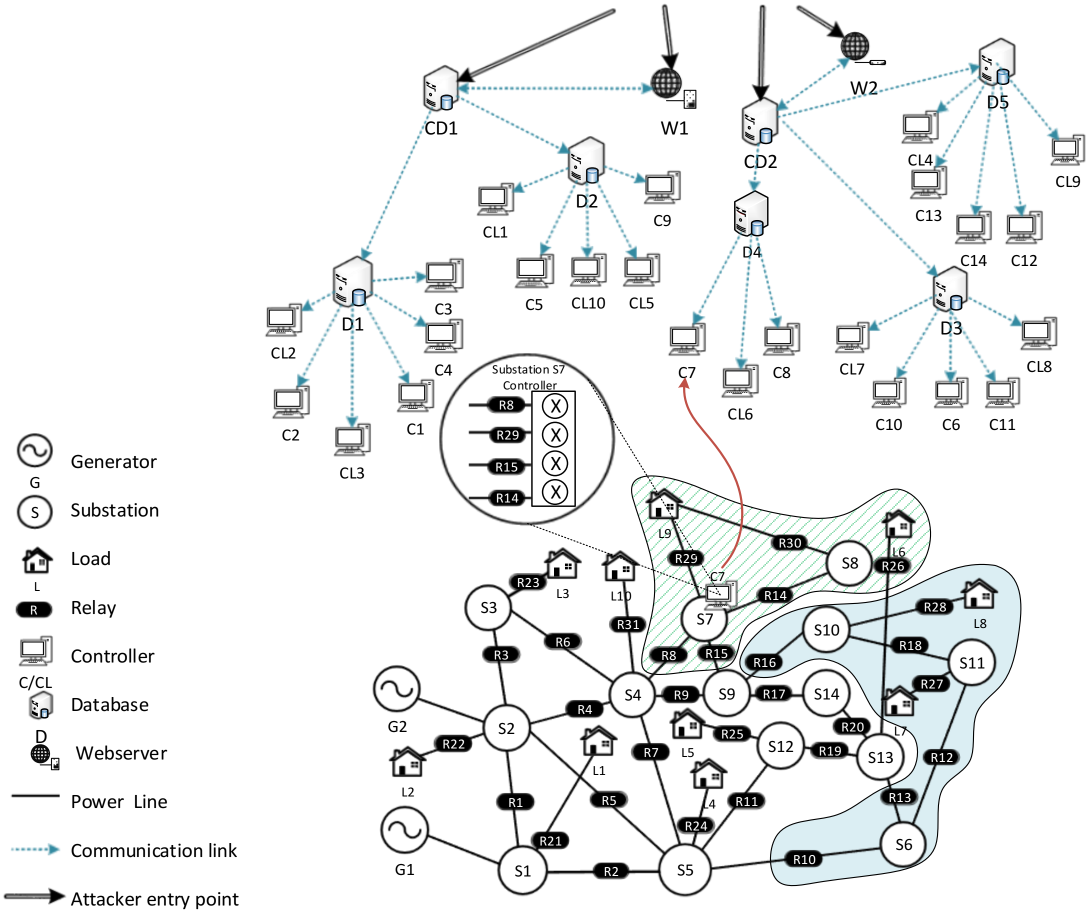

Figure 2.5: IEEE 14 bus system Power-Communication network.

in Table 2.2 and 2.1 prove the scalability of the proposed security evaluation framework. Since, the whole MDP for the system under study is a big tree, we show a part of it in Fig. 2.6 to emphasize how adding the concurrent contingencies would impact the calculated security index. We assume that $CD2$ and $D4$ are already compromised by the attacker. Therefor we calculate the security index for state $CD2D4$ with and without complementary states. First, the security index is calculated for the generated MDP. The only state with non-zero value of P_{uns} is $CD2D4CL6R26$. The calculated security index is $I(CD2D4) = 0.43$ (the framework proposed in [15] will calculate the same number since it does not consider concurrent contingencies). Second, we run the framework with concurrent contingency identifier and MDP completion block. The identified clusters are shown in blue, red, and green color and additional states and transitions are added with dashed colored

Table 2.1: Network and MDP tree size (Number of nodes) for different test systems.

	Power	**Communication**	**MDP**	**CompletedMDP**
14 Bus	26	61	341	363
30 Bus	60	126	875	921
57 Bus	101	268	1164	1291

Table 2.2: MDP tree runtime(ms) for different test systems.

	Power Analysis	**MDP Gen**	**MDP Comp**	**Index(avg)**
14 Bus	155	2	3	12
30 Bus	194	28	9	45
57 Bus	264	173	104	114

lines. In this case, the added states would have the $P_{uns} = 22$ which is equal to $L9$ demand and the security index would take a positive value $I(CD2D4) = 0.79$. The dashed states are the one with positive P_{uns} value.

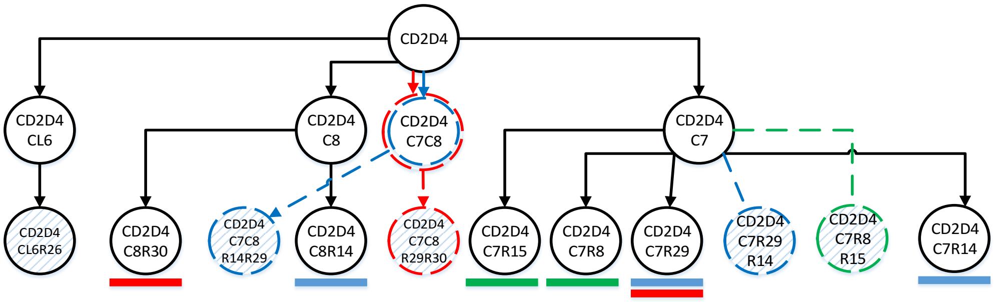

Figure 2.6: Index calculation example with and without concurrent contingency consideration

To compare, we preform the same exercise with the current state $CD2D3$. In this subtree, $R12$ and $R16$ belong to one cluster since removal of these two transmission line from the system would disconnect $L7$ and $L8$ ($P_{uns} = 38$). The calculated security index for state $CD2D3$ is equal to 1.71. Comparing the security index values for $CD2D4$ and $CD2D3$ will show that compromising database $D3$ would have a larger impact on the power delivery. The value for the security metrix is larger since the demand of the area affected following state $CD2D3$ (blue area) is larger compared to state $CD2D4$ (dashed green area). In addition, the proposed security framework could be also utilized to rank the system component based on their criticality and allocate the protection resources for based on the ranking.

Chapter 3

Cascading Link Failure Analysis in Interdependent Networks

3.1 Introduction

Recent power grid failures have exposed hidden vulnerabilities in the power system that need thorough investigation. The cascade of failures in the famous North American 2003 blackout, the 2003 Italy blackout, and the most recent 2015 Ukrainian blackout demonstrate that our critical infrastructure are susceptible to faults and attacks that can bring the power system down along with all the other dependent systems [10].

Today, the robust operation and the availability of the power grid is a critical requirement [19]. The grid is exposed for more threats both on its cyber and physical sides. Cyber-attacks are a consistent threat that is intensified with advances in the deployment of the smart grid. The increased dependency on the communication network and the integration of both systems present a potential attack surface for cyber-attacks. Further, the physical components of the grid are subject to attacks targeting their functionality, such as the reported attack on the high voltage transmission line in the United States in 2013 [27] and Canada in 2014 [28]. The presence of these threats call for an innovative analysis of the functionality of the grid that results in a robust design of a smarter grid: a grid capable of restraining the effects of attacks and survive the loss of any of its components.

Typically, networks in the power system are operated according to the (N-1) security measure to ensure secure power supply even after the failure of any of the grid components[29]. However, the analysis of the above mentioned blackouts indicate that the root cause of the failure was the loss of a single line which cascaded and resulted in the loss of power over large geographical regions [30]. To expose more system vulnerabilities, in the case of the Italian blackout, the cascade of the failure was enlarged by the failure of dependent systems namely the communication network [31]. This highlights the interdependency between systems in the critical infrastructure, the need for a new understanding of these systems and the way they function, and an analysis of this interdependence and its role in any upcoming challenges.

The vulnerability analysis of power systems received much attention from the research community especially the problem which seeks the identification of a small set of power lines whose failures will result in the total failure of the system [32], [33], [34], [35]. This problem is known under a variety of names: vulnerability evaluation problem, network interdiction, network inhibition, and most commonly as the (N-k) problem [36]. The problem at hand can be generalized into the case of failure of a set of components rather than just power lines. In our work, we will target the problem of identification of lines only. However, the interdependency between the power grid and the communication network plays a major role in the start and development of failures in both systems. A malicious actor can target the communication network to prevent the collection of needed measurements for load shedding and prevent appropriate load management [37]. This serves in favoring power system cascade of failures. Moreover, the effect of such threats escalates if executed in the presence of a natural disaster or terrorist attack. Thus, we will add a new dimension to the problem by considering the interdependency between the power system and the communication network.

In this research, we aim at analyzing the vulnerability of the interdependent power-communication system to the removal of a small set of links. The aim of this analysis is to identify critical links in both parts of the system whose failure result in severe damage. The induced damage is quantified in terms of the loss of unrestorable power load. We are interested in minimizing this set of links as to make the failure feasible and possible through a coordinated attack on both systems. We will present a model of the power-communication system that captures the characteristics of both systems, abides by the interdependency across power and communication domains, and an algorithm to identify the required set of critical links.

The main contributions of this study are:

- Presentation of a power-communication system model.
- Modeling the interdependency between the two systems.
- Identification of a critical set of links whose failure leave a deep impact on the system.
- Validation of the approach on the IEEE bus system.

The remainder of this chapter is structured as follows. Section 3.2 introduces the problem definition. System model is presented in Section 3.3. Section 3.4 covers the experimental setup and the collected results.

3.2 Problem Definition

The functionality of the future smart grid relies on the availability of advanced measurement technology, information tools, and operational infrastructure for control and management of the power system. These advanced measurement tools are dispersed across the domains of the grid allowing for better observability and control of the smart grid. Their functionality depends on the availability of a reliable communication network, and sufficient power supply. Thus, the survivability of these measurement units and the communication network is critical for power delivery during normal operations of the grid and in the case of failures as well.

The system resulting from the combination of power grid, communication network, measurement units, electric devices, among other equipment, is a highly complex and interdependent system. The analysis of such a system results in complex models that are hard to handle. To make this analysis possible, there is a need for abstraction and a high level description of this smart system. Thus, we will present a high level abstraction of the smart grid comprising of the power and communication networks and the interactions between them as in the upcoming scenario.

Fig. 3.1 represents a schema of a power and communication network. Power and communication nodes and links along with the associated loads and capacities are depicted. G and S represent generators and substations respectively. CC and Ci represent the control center and routers at the communication side. For each power transmission line, the current power flow and maximum capacity C are indicated. The power consumption of the regions where the communication routers reside are indicated next to these loads and routers. For the system to function properly, we assume that each power node should receive power flow from a generator and each router should be directly or indirectly connected to the control center. The interdependency between the two systems is restricted by the need of communication nodes to receive power, and the need of power nodes for command and control [13]. Thus, each communication node should be connected to at least one power node and vice versa.

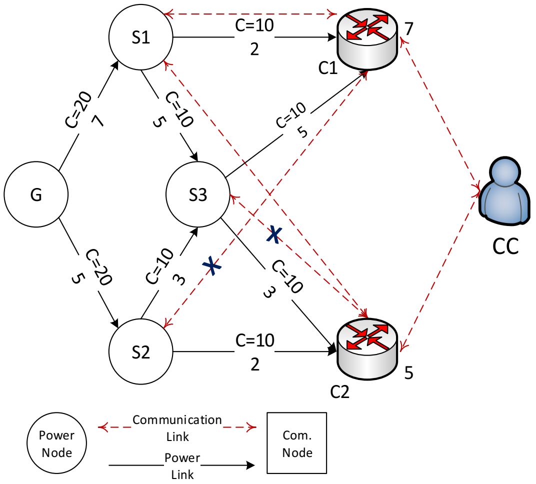

Figure 3.1: A schema of power-communication system under study.

Assume that the links that are directly connected to generators and the control center are well protected and resilient to failure. Then, the presented schema abides by the (N-1) design both on the power and communication sides. The removal of any link will not disrupt the functionality and availability of the system. Moreover, due to the redundancy available in the system, this system is capable of functioning with a smaller number of links. If an attacker targets the links $S3 - C1$, $S2 - C2$, and $C1 - S1$, the system will continue to function with zero outage whereas the attacker spend his budget without any outcomes. Hence, an attacker should be smart in his choices to impact the system with a loss in the served load.

Now, consider an attack on the links in the system where the attacker targets only two links out of the fourteen links available. The links targeted are the communication links connecting (C1, S2), and (C2, S3). The attack is indicated using a **X** in the figure. This is a relatively small number of links targeted. However, if we look at the resulting schema after this attack as depicted in Fig. 3.2, we can evaluate the effect of the attack on the system. Due to the interdependency in the system, the attack on the communication links results in the failure of communication/power links and nodes. Indeed, the failure of the two mentioned links result in the failure of S2 and S3 due to the loss of connectivity to the control center. Thus, all the transmission lines originating or terminating at S2 and S3 are lost. Due to cascade of failures, C2 fails along with the associated communication and power lines due to the loss of power supply.

We quantify the effect of this failure on the system in terms of the load lost. Making use of the characteristics of the lost power and communication nodes, the attack on two links resulted in the loss of more than 40% of the served load in the system.

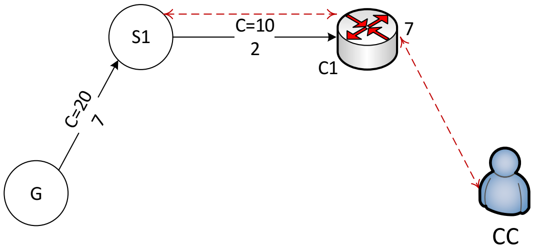

Figure 3.2: Power-communication system after attack on links.

The above scenario illustrates the vulnerability of the interdependent power-communication system to attacks targeting a limited number of links. We aim at identifying a small set of links that leave a large impact on the system. However, we want to avoid the traditional bi-level optimization model [32] used to handle this problem where an attacker tries to minimize the number of links while maximizing the damage to the system. The literature is already rich with approaches to handle this hard to solve problem [36], [32], [38], [39], [40]. Moreover, researchers have shown that the selection of k-critical links in the system is NP-Complete [41]. Thus, we will approach this problem from a new perspective to avoid its hardness. We will target this vulnerability to quantify the losses in the system due to attacks/failures of selected links. This quantification is presented as a percentage of loss in the loads served. This relaxation of the problem allows modeling the system along with the above mentioned interdependency, identifying a critical set of links that leaves a big impact on the system availability, and pointing out hidden vulnerabilities in the system design.

3.3 Power-Communication Network Model

3.3.1 System Model

The system under study is formed of the interdependent power and communication networks. The power system is composed of generators, substations and loads. The communication network is formed of the control center and intermediate routers connecting the control center to the components in the power system. We represent this system as a graph of vertices and edges, $G = (N, E)$. The set of vertices N is defined as $N = N_p \cup N_c$, where N_p is the set of power nodes, and N_c is the set of communication nodes. While the set of edges E is defined as $E = E_p \cup E_c$, where E_p is the set of power links, and E_c is the set of communication links.

To analyze the power dynamics in the system, we use the well known DC power flow model presented in equation (3.1). We select this model as it is widely used in the literature and presents a linearization of the power flow in the power grid.

$$Af = P \tag{3.1a}$$

$$A^T\theta = Xf \tag{3.1b}$$

In this model, $A[n \times m]$ represents the node-arc incidence matrix or the adjacency matrix in the network where $n = Card(N_p)$ and $m = Card(E_p)$. For each $a_{ij} \in A$, a_{ij} = 1 if link j starts from node i, -1 if link j ends at i, and 0 otherwise. f is the vector of power flows in the transmission lines. P and θ are vectors holding the power injections and voltage phase angles at all power nodes respectively. $X[m \times m]$ is a matrix having non-diagonal elements of zeroes, diagonal element X_{ii} represents the reactance of the i^{th} power line.

The conservation of power flow in the network is presented by constraint (3.1a). On the other hand, constraint (3.1b) is a replication of Ohm's law applied to a resistor carrying a dc current where the amount of flow is equal to the difference in phase angles at the line ends divided by the line reactance. Using the power flow model allows to capture the dynamics of the system and hence the effect of attacks or link failures on the entire system. The redistribution of power flows over the links maintains the power delivery and affect saturated links in the network. This may lead to further failures in the system due to violation of link capacities and results in what is known as cascading failures in the power grid.

Our system model captures the change in the availability of power links and nodes in the system. Through the analysis of available generation, loads, and links, the power flow is directed over the links to serve the requested loads. Moreover, due to the loss of links and as a result of attacks, the power flow is adjusted to balance the demand to supply and abide by the power links capacity constraints. On the other hand, the availability of communication nodes and links is essential for the availability of the system. Our model secures this interdependency by forcing the rules described in Section 3.2 where a communication node should be receiving power from an active power node and a power node is connected to the communication network through an active communication node. An active power node is that connected to a generation unit, and an active communication node is that connected to the control center.

We distinguish between two types of link failures. The first type of failure is a direct result of an attack where a specific link is disconnected from the network. This attack can be two fold: a physical attack targeting a transmission line [28] or a communication cable, a cyber attack that trips the breakers at the ends of a transmission line in case of a power link; modifying routing tables at intermediate routers, or flooding the targeted communication link to render it unavailable. The second type of failure is an indirect effect of the attack. This type results from breaking the survivability rules of links which can be summed up as follows:

- both end nodes of a link should be online
- power flow on a transmission line should not exceed its capacity

For the node failure, we do not consider attacks on nodes as we are trying to identify critical links only. However, nodes fail as an indirect consequence of the attacks on links. Nodes failure results from:

- A load not receiving the required power
- A power node not connected to a generating unit

- A generator not connected to the network
- A communication node not connected to the control center
- A violation of the interdependency constraints

Our objective is to identify a critical set of links that an attacker should target given a limited budget. We assume that the attacker has knowledge of the system topology and the various characteristics of its nodes and links. Our attacker is interested in a small set of links whose failure induce significant damage to the system. To reduce the load served by a pre-specified percentage, the attacker has to smartly choose which links to attack. Thus, he will first run the model to identify a minimum set of links whose failures fulfill the attack's aim. This is possible by solving the dual problem presented below and finding the maximum number of non-failing links. A maximum number of surviving links identifies the set of links that attacker has to target wisely with minimum effort. Next, he will run algorithm 3 to identify the critical links to attack. Depending on his budget, the attacker can vary the attack impact factor α and identify different subsets of links to attack. The attack on these identified critical links makes use of the dynamic nature of the power system and the interdependency between the power and communication systems to fail the set of links identified by the model. The attack on these critical links reveals hidden vulnerabilities in the system and the model serves as a first step in approaching these vulnerabilities and improving the system resiliency against such attacks.

3.3.2 Mathematical Model

3.3.3 Notations

g: generator l: load

C: control center

$o(j)$: origin of link j $t(j)$: terminal of link j

3.3.4 Parameters

N: set of all power and communication nodes

N_p: set of all power nodes

N_g: set of all generators

N_l: set of all nodes with an associated power load

N_c: set of all communication nodes

E_p: set of all power links

E_c: set of all communication links

E_g: set of all power links directly connected to a generator

E_{cc}: set of all communication links directly connected to the control center

A[$N_p \times E_p$]: power network adjacency matrix

$$a_{ij} \in A = \begin{cases} 1 & \text{if link j starts from node i} \\ -1 & \text{if link j ends at node i} \\ 0 & \text{otherwise} \end{cases}$$

B[$N_c \times E_c$]: communication network adjacency matrix

$$b_{ij} \in B = \begin{cases} 1 & \text{if node i is vertex for link j} \\ 0 & \text{otherwise} \end{cases}$$

f[$E_p \times 1$]: vector of power flows

θ[$N_p \times 1$]: vector of voltage phases at power nodes

P[$N_p \times 1$]: vector of power injections at nodes

X[$E_p \times E_p$]: reactance matrix of power lines

P_g: generation capacity of generator g

c_j: capacity of power link j

$Load_{init}$: Initial load served

α: loss factor

M: a large number P_g: power generation capacity of generator g

3.3.5 Decision Variables

k: the total number of surviving links

$$x_j = \begin{cases} 1 & \text{if link } j \in E_p \text{ is available} \\ 0 & \text{otherwise} \end{cases}$$

$$y_j = \begin{cases} 1 & \text{if link } j \in E_c \text{ is available} \\ 0 & \text{otherwise} \end{cases}$$

$$z_i = \begin{cases} 1 & \text{if node } i \in N_p \text{ is online} \\ 0 & \text{otherwise} \end{cases}$$

$$t_i = \begin{cases} 1 & \text{if node } i \in N_c \text{ is online} \\ 0 & \text{otherwise} \end{cases}$$

$$s_{o(j)t(j)}^{Cn} = \begin{cases} 1 & \text{if link } j \text{ is on a path from } C \text{ to } n \\ 0 & \text{otherwise} \end{cases}$$

$\delta_{o(j)t(j)}^{gn}$: fraction of power supplied by $g \in G$ to $n \in N_p \cup N_c$ on link $j \in E_p$

$$r_{o(j)t(j)}^{gn} = \begin{cases} 1 & \text{if link } j \text{ is on a path from } g \text{ to } n \\ 0 & \text{otherwise} \end{cases}$$

$A[N_p \times E_p]^{up}$: power network adjacency matrix after attack

$$a_{ij}^{up} \in A^{up} = \begin{cases} 1 & \text{if link j starts from node i} \\ \text{-1} & \text{if link j ends at node i} \\ 0 & \text{otherwise} \end{cases}$$

$B[N_c \times E_c]^{up}$: communication network adjacency matrix after link removal

$$b_{ij}^{up} \in B^{up} = \begin{cases} 1 & \text{if node i is vertex for link j} \\ 0 & \text{otherwise} \end{cases}$$

3.3.6 Mathematical Model

Our objective function is to maximize the number of links surviving the attack on the system.

$$\text{Maximize } k$$

This selection is subject to the following constraints:

$$\sum_{j\in E_p} x_j \; + \sum_{j\in E_c} y_j \; = \; k \tag{3.2}$$

$$\sum_{i=1}^{|N_l|} l_i * z_i \le \alpha * Load_{init} \tag{3.3}$$

$$A^{up} f = P \tag{3.4}$$

$$A^{upT}\theta = Xf \tag{3.5}$$

$$0 \le f_j \le x_j * c_j \quad \forall j \in E_p \tag{3.6}$$

$$x_j \le z_{o(j)} * z_{t(j)} \quad \forall j \in E_p \tag{3.7}$$

$$y_j \le t_{o(j)} * t_{t(j)} \quad \forall j \in E_c \tag{3.8}$$

$$a_{ij}^{up} = a_{ij} * x_j \quad \forall a_{ij}^{up} \in A^{up} \tag{3.9}$$

$$b_{ij}^{up} = b_{ij} * y_j * t_i \quad \forall b_{ij}^{up} \in B^{up} \tag{3.10}$$

$$z_i \le \sum_{j}^{|E_p|} |a_{ij}^{up}| \quad \forall i \in N_p \tag{3.11}$$

$$t_i \le \sum_{j}^{|E_c|} b_{ij}^{up} \quad \forall i \in N_c \tag{3.12}$$

$$\sum_{\substack{j \\ j:(i_1 i_2)\in E_p}} \delta_{i_1 i_2}^{gn} - \sum_{\substack{j \\ j:(i_2 i_1)\in E_p}} \delta_{i_2 i_1}^{gn} \begin{cases} \le 1 & \text{if g is at } i_1 \\ \ge -1 & \text{if n is at } i_1 \\ = 0 & \text{otherwise} \end{cases} \quad \forall i_1 \in N, n \in (N - N_g),\ \forall g \in N_g \tag{3.13}$$

$$r_{i_1 i_2}^{gn} \le \delta_{i_1 i_2}^{gn} * M \; \forall j : (i_1 i_2) \in E_p, g \in G, n \in (N_p - N_g) \tag{3.14}$$

$$r_{i_1 i_2}^{gn} \ge \frac{\delta_{i_1 i_2}^{gn}}{M} \quad \forall j : (i_1 i_2) \in E_p, g \in G, n \in (N_p - N_g) \tag{3.15}$$

$$z_n \le \sum_{g\in N_g} \sum_{\substack{j \\ j:(i_1 i_2)\in E_p}} r_{i_1 i_2}^{gn} \quad \forall n \in (N_p - N_g), j : (i_1, i_2) \in E_p \tag{3.16}$$

$$\sum_{g \in G} \sum_{\substack{j \\ j:(i_1 n) \in E_p}} \delta^{gn}_{i_1 n} = 1 * z_n \quad \forall n \in N_l \tag{3.17}$$

$$\sum_{n \in (N-G)} \sum_{\substack{j \in E_g \\ g=o(j)}} \delta^{gn}_{gt(j)} = P_g \quad \forall g \in N_g \tag{3.18}$$

$$s^{Cn}_{i_1 i_2} \leq y_j \quad \forall j : (i_1 i_2) \in E_c, n \in N - (N_g \cup \{C\}) \tag{3.19}$$

$$t_n \geq s^{Cn}_{i_1 i_2} \quad \forall j : (i_1 i_2) \in E_c, n \in N - (N_g \cup \{C\}) \tag{3.20}$$

$$\sum_{\substack{i_2 \\ j:(i_1 i_2) \in E_c}} s^{Cn}_{i_1 i_2} - \sum_{\substack{i_2 \\ j:(i_2 i_1) \in E_c}} s^{Cn}_{i_2 i_1} \begin{cases} \leq 1 & \text{if C is at } i_1 \\ \geq -1 & \text{if n is at } i_1 \\ = 0 & \text{otherwise} \end{cases} \quad \forall i_1, n \in N - (N_g \cup \{C\}) \tag{3.21}$$

$$t_n \leq \sum_{\substack{j \\ j:(i_1 i_2) \in E_c}} s^{Cn}_{i_1 i_2} \; \forall j : (i_1 i_2) \in E_c, \; n \in N - (N_g \cup \{C\}) \tag{3.22}$$

Where constraint (3.2) represents the number of surviving links from the power and communication network as k. The attack effect on the system is presented by a fractional loss in the load served as indicated by constraint (3.3). Constraints (3.4) and (3.5) represent the DC power flow model as previously described. The power flow on the transmission lines is restricted by the capacity and availability of these lines as illustrated in constraint (3.6). The availability of transmission lines and communication links in the network is governed by constraints (3.7) and (3.8) respectively. The power and communication adjacency matrices are updated in constraints (3.9) and (3.10) respectively. Constraints (3.11) and (3.12) control the availability of power and communication nodes in the system respectively. Constraints (3.13), (3.14), (3.15), and (3.16) are for power flow and represent the connectivity of nodes to the generating units. Constraint (3.17) ensures that each node receives the needed amount of power to be available in the system, while constraint (3.18) restricts the flow out of a generator to its generation capacity. Constraints (3.19), (3.20), (3.21), and (3.22) represent the nodes connectivity to the control center. It is worth noting that constraints (3.4), (3.7), (3.8), (3.10),and (3.11) are non-linear, however these constraints can be easily linearized.

The set of failing links and nodes identified by the model are input to algorithm 3. This algorithm outputs a subset of these links to be attacked. Thus, combining the model with algorithm 3 and based on the attack budget, the attacker is capable of identifying a critical set of links to be attacked.

Algorithm 3 Algorithm to select critical links to attack

```
1:  Given: $L = L_p \cup L_c$: set of failed links, $N$: set of failed nodes
2:  Result: $A \subseteq L$: set of links to attack
3:  $F$: set of failed links;
4:  $L_1$ & $L_2$: temporary sets of size $|N|$;
5:  $n_i$: node in $N$;
6:  $n_i$: node in $N$;
7:  $A = \phi$;
8:  $\forall i \in N$, define:
9:  $p_i$= number of incoming power links to $i$;
10: $c_i$= number of communication links passing through $i$;
11: while ($L \neq \phi$) do
12:     $L_1$ = $N$ sorted based on $p_i$;
13:     $L_2$ = $N$ sorted based on $c_i$;
14:     $n_i$ = min(min($L_1$),min($L_2$));
15:     assume $n_i \in L_1$;
16:     add incoming power links of $n_i$ to $A$;
17:     add other links of $n_i$ to $F$;
18:     remove all links connected to $n_i$ from $L$;
19:     remove $n_i$ from $N$;
20:     remove affected nodes from $N$;
21:     add affected links to $F$;
22:     remove affected links from $L$;
23: end while
```

The set of failing links and nodes are denoted by L and N respectively. Each node i in N is characterized by the number of incoming power links and communication links to i. In lines 12 & 13, we sort the set N into two temporary sets L_1 and L_2 as indicated. The node with minimum number of communication or incoming power nodes is selected in line 14. This minimum number of links is attacked and added to the set A, line 16. Due to this attack, the links connected to n_i fail, line 17. Sets L and N are updated in lines 18 and 19 respectively. Nodes affected in line 20 are the ones who lost all their communication or incoming power links due to failures in lines 16 and 17. Links affected in line 21 are those failed due to the removal of the nodes in line 20. The set L is updated and the algorithms iterates until all links are either attacked or fail due to the attack.

As an alternative to this algorithm, the attacker may choose to do exhaustive search to identify the minimum set of links to be attacked. However, algorithm 3 is a low complexity algorithm

$O(n^2 logn)$ that runs in polynomial time and provides near optimal solution. Thus, it is more efficient to use.

3.4 Numerical Results

setup our system, we used Java and IBM CPLEX concert technology to develop the model and related simulation programs. The simulations were executed on a windows machine with Intel Core i7 CPU running at 2.67GHZ and equipped with 12 GB of RAM.

The first set of tests were run on the system presented in Figure 3.1. We set $\alpha = 0.8$ to determine the failing links. The model identified 7 links as failing ones along with nodes $S2$, $S3$ and $C2$. Algorithm 3 was run using the model output. The links to be attacked, as identified by the algorithm, are communication links $S3 - C2$ and $S2 - C1$. This attack results in the loss of control at substations $S2$ and $S3$ and thus their failure. The failure cascade over all the links connected to those substations. Thus, $C2$ will fail due to loss of power supply along with all its connected links. The cascade of failure terminates as shown in Figure 3.2. Therefore, the combination of the model with algorithm 3 identified the two critical links in Figure 3.1 as the ones to be failed which is the optimal solution for this case-study.

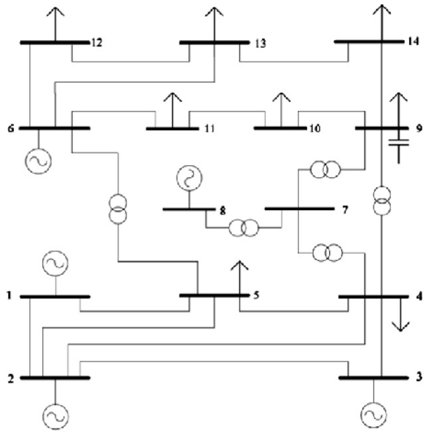

Figure 3.3: IEEE 14-bus system case.

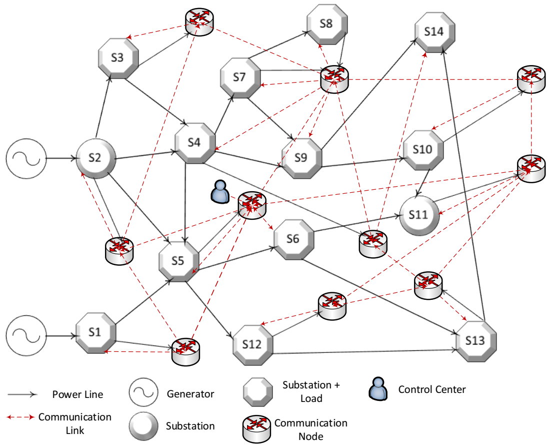

Figure 3.4: Graph representing the IEEE 14-bus system coupled with a communication network.

The second set of numerical experiments were run on the IEEE 14-Bus system. System topology is presented in Fig. 3.3. The power related data of this system is publicly available. Each bus is represented as a node in our graph apart from the bus that has a generator and load connected to it. For such a bus, we created two nodes: a generator and a substation assigned the bus load. On the other hand, to build the corresponding communication network, we followed the approach presented by Wu et al. in [42] to add communication nodes based on the system topology. The resulting topology is presented in Figure 3.4. Moreover, we coupled each of the power nodes we added with a communication node that represents its command and control component. The power consumption of the communication nodes is considered as part of the power nodes consumption to avoid violations to the power generation and consumption balance in the system. The total number of nodes in the resulting graph is 51 nodes while that of the edges is 62 edges. The run-time of the model was in order of seconds.

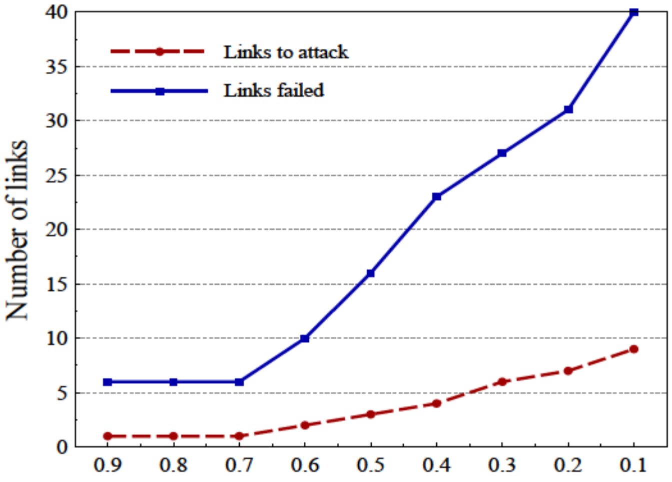

Figure 3.5: Comparison between number of critical links to attack and total number of failed links.

We run our model for different values of α to identify the minimum number of links that should fail to achieve this fractional loss in the served load, and we used algorithm 3 to decide on a smaller subset of links to attack. The collected results are plotted in Figure 3.5 where α is varied from 0.9 to 0.1. The number of failing links ranged from 6 to 40 while the critical links to be attacked varied from 1 to 9. We notice that an attacker needs to attack a small number of links to achieve the desired target. Moreover, depending on the system topology, with the same number of links attacked, an attacker can cause varying damage to the system due to the interdependency between the components and the cascading effects. We also note that, as shown in Figure 3.5, attacking 1 link results in a varying damage from 0.9 to 0.7. This is due to the fact that the model attempts the isolation of a load to cause the damage in the system. Thus, with the same number of links, a varying damage can be induced depending on the targeted load and how much it resembles of the total system load. Thus, running the model and the algorithm with different values of α enables the attacker to induce more damage to the system within his allocated budget.

As a countermeasure for such attacks, the best practice will be to introduce redundant links to improve the resiliency along with smart mitigation plans based on intentional islanding. Such islands should enjoy decentralized control to limit the interdependency effect.

Chapter 4

Automated Post-Failure Service Restoration

4.1 Introduction

In the past few decades, reliability and robustness of power distribution networks have become major concerns for power utilities as power systems experienced severe outages [43]. Equipment failure, bad weather conditions, vehicle accidents, and in some cases intentional cyber-attacks could be counted as main initiatives for massive power outages. The recent India blackout (2012), the largest historical blackout based on the number of people affected, started by tripping a circuit breaker and affected over 300 million people [44]. Such incidents emphasize the need for effective and timely recovery strategies as part of the self-healing characteristic of the next generation Smart Grid.

Smart grid self-healing is realized through the collection and analysis of real-time data. Using measurements from phasor measurement units dispersed across the grid, operators and control systems fully observe the power network and act immediately to restore the service upon disruption. This allows faster and more intelligent self-recovery for power system protection and restoration compared to traditional Supervisory Control and Data Acquisition (SCADA) systems [45], [2]. This procedure is currently referred to as Automated Service Recovery (ASR). ASR is expected to replace the time-consuming manual restoration procedure of traditional power grids. Through ASR, utilities increase customer satisfaction, reduce compensation, and decrease the duration of system interruption [46].

Due to the critical nature of the grid, any ASR approach should restore services in a reasonable time. Such service restoration can be achieved through Network Reconfiguration (NR) [16]. NR modifies the topology of the power transmission/distribution network by changing the status of switches on power lines, meeting several objectives, including minimization of the set of out-of-service consumers, active power loss, the voltage instability, etc.[46]. However, NR is rather complex to solve as the solution space grows exponentially with respect to the available switching gears in the network [47].

Service restoration through NR for transmission and distribution networks is one of the much investigated problems in the literature [46],[48], [49]. Researchers propose heuristic [48], [50],[51] and meta-heuristic methods including tabu search [52],[53], ant colony optimization [47],[54], genetic algorithm and fuzzy optimization [49] for network reconfiguration. Graph-based approaches are available in the literature as well as in [51],[55] where Dimitrijevic et al. proposes an approach based on the logic of a modified minimum spanning forest in order to address the requirements of optimal service restoration. These algorithms are generally characterized by their simplicity and speed, however they do not guarantee a global optimal solution.

Another view of the problem for the future smart grid is presented by Pournaras et al. in [56] where they study service restoration in the form of self-repairable Smart Grid. They aim at mitigating the effect of cascading failures through the use of smart transformers in an online and automated way. Two optimization strategies are presented to coordinate the functionality of smart transformers in response to disruptive actions. Their approach is centered around applying load shedding, generation balancing, and optimization of flow distribution through the coordinated smart transformers.

Service restoration through network configuration in the smart grid is recently studied by Rodriguez et al. in [57]. The authors propose a distributed approach that adapts the open shortest path first (OSPF) routing protocol to minimize power losses, balance loads, and improve reliability in distribution networks through automatic network reconfiguration.

The availability of plug-in hybrid electric vehicles (PHEV) in the smart grid, and the role played by their stochastic behavior in distribution feeder reconfiguration (DFR) is studied by Rostami et al.

[58]. However, the main interest of the authors is the stochastic behavior of those electric vehicles and the integration of these vehicles in the network through DFR. Different behavioral models are considered, and the reconfiguration is examined to model PHEV charging behavior under different strategies and penetration levels. Although the authors consider a form of DES, PHEV, their study deviates from ours in that we are interested in the usage of those DES to support the grid in case of failure rather than studying the charging behavior of PHEV.

In this research, we aim at solving the service restoration problem in smart grid through an optimal NR-based methodology in the presence of DES systems. Optimal restoration approaches are proposed to minimize the restoration time, maximize the served load, minimize the active power loss, or a combination of those objectives. However, in this study, we add a new dimension to the problem by considering the availability of distributed energy storage (DES) systems and their impact on service restoration as in the smart grid. The presence of DES systems affects the amount of power to be routed over reconfigured paths, presents a reduced cost alternative for utilities, and allows for faster restoration times with less disturbance in the system. Thus, the availability of DES systems affects the restoration plans set by utilities, and presents a new challenge of advising the optimum NR approach for service restoration. In this chapter, A linear programming approach will be presented to describe the network dynamics and the decisive factors in the NR approach. Our objective is to minimize the restoration-time and DES utilization cost while maximizing the served load for consumers in de-energized areas by solving the power flow equations.

The main contributions of this study are:

- Presentation of a meshed format power transmission/distribution system model.
- Defining the NR-based service restoration problem with the availability of DES systems.
- Formulation of the NR-based approach in presence of DES systems.
- Proposing an optimal solution for NR-based service restoration in presence of DES systems.
- Validation of the approach on different IEEE bus system.

The remainder of this manuscript is structured as follows. Section II introduces an illustrative example. The research problem is defined in section III. The system model is presented in section IV. Section V covers the experimental setup and the collected results. Section VI presents the related work. Concluding remarks and future work are provided in section VII.

4.2 Illustrative Example

Consider a simple power distribution network that consists of two feeders supplying power to the connected loads as shown in Fig. 4.1. Redundant power lines are available to improve system resiliency to failures. A failure or attack on the link connecting loads 5 & 6 will propagate through the network and results in extending the de-energized area to include loads 6 & 9. To restore power to this area through NR, several options are available for the operator as closing switches 8-9 & 6-9 (Fig. 4.1(c)), closing switches 2-6 & 6-9, or fixing switch 5-6 and closing switch 6-9. However, each of these options incurs different costs and restoration times. Restoration cost depends on the number of switching actions performed, nature of the switching action, and active power loss. While restoration time depends on the number of switching operations and the time required for changing the status of each switch in the restoration path (switching cost) [59]. In addition to that, smaller number of switching status modification could be translated into less frequency and voltage deviation and thus better power quality [60]. Moreover, sensitive protection devices may respond to voltage and frequency variations and cause tripping of the equipment, thereby weakening the system and possibly leading to system instability [61].

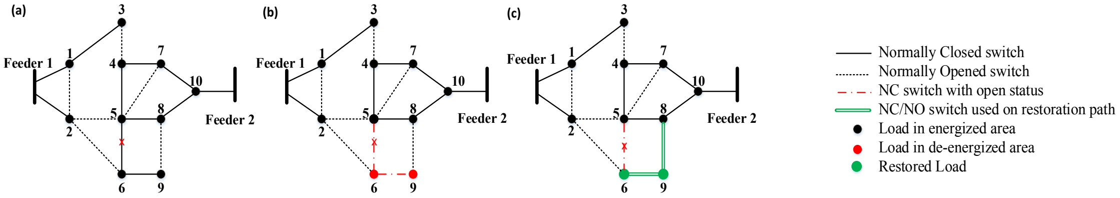

Figure 4.1: Power distribution network and service restoration through NR in traditional power grid.

Now considering the same network but in the presence of DES systems as shown in Fig. 4.2. Various network reconfiguration plans could be followed to restore the power to the consumers in de-energized areas by taking into consideration the different load priorities, performance, capacity, and pricing for the available DES systems. Those plans are illustrated in Fig. 4.2(b), (c), and (d) by green double-lines. The utility may decide to purchase power from none 4.2(b), one 4.2(c), or multiple DES systems 4.2(d) for each load in the de-energized area. Thus, the presence of those DES systems extends the solution space of the service restoration problem through network reconfiguration, and affects the optimal choice for power restoration to de-energized zones. Nonetheless, importing energy from DES systems incurs additional cost, as well as power delivery cost, and therefore deciding on the best contingency plan is of utmost importance to a utility.

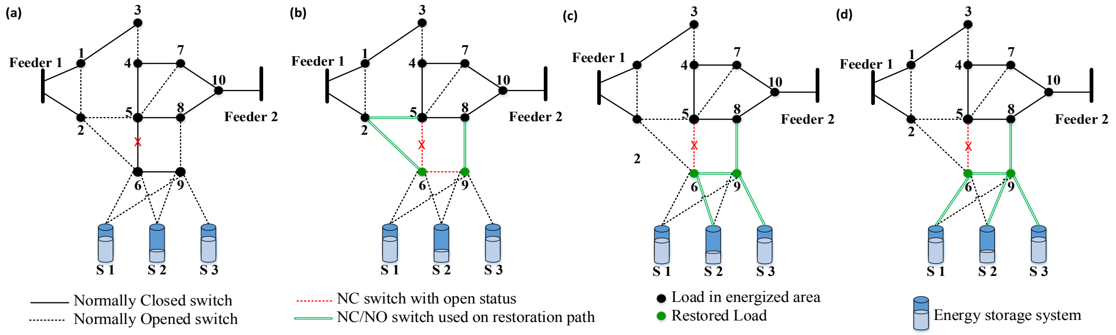

Figure 4.2: Power distribution network and service restoration through NR considering multiple DES systems in smart grid.

4.3 Problem Definition

In our study, we model the power grid as a graph, $G_p = (N_p, E_p)$ in which N_p is a set of power nodes and E_p is a set of power lines. Power nodes include generating units with defined generation capacity, substations, and loads with specific demand. Loads are composed of neighborhoods containing multiple households and their demands are served by the utility over the grid during normal operations. However, in case of a failure, demands might be partially served depending on the availability of resources.

To narrow down the gap between power demand and supply, and fully restore the service after a failure, several factors are taken into consideration. Those factors include the updated topology of the network, the availability of power generating units and their capacity, and active power loss over power lines. Taking into consideration that increasing the generation capacity of power generators is time consuming, utilities will consider purchasing power from the available DES systems.

In order to reduce the impact of power outages, reduce the time of service interruption, and avoid extra costs paid by utilities, ASR is mandatory after a failure. ASR through network reconfiguration is the main candidate for service restoration in smart grid. However, as mentioned earlier, NR for service restoration can be achieved through various means each associated with a cost to be paid by the utilities. This cost is mainly decomposed into the switching cost [59], the unserved load cost, and the cost incurred by the use of DES systems.

The switching cost is associated with the number of switching actions, where an action changes the state of a switch from open to close or vice versa. Minimizing the number of switching operations is an important objective in service restoration as mentioned earlier. Moreover upon repairing the faulty equipment, switches will revert to their initial status. Hence, minimizing the number of switching actions during ASR will result in little changes needed to return to the network topology under normal conditions.

Thus, the switching cost can be formulated as

$$C_{switching} = \sum_{i=1}^{q} c_i * \ c_{i,a} \tag{4.1}$$

where $C_{switching}$ is the total service restoration cost, c_i is the cost to change the status of the i^{th} switch, q is number of switches in the network, and $c_{t,a}$ is a binary variable representing the change in the status of the t^{th} switch.

Moreover, we distinguish between two types of costs for a switching operation. Upon detection of a failure, the root cause of the failure can be identified by applying line outage detection and performing post attack analysis on the collected phasor measurements[62, 63]. Then, this is followed by device repair to enable power flow over the damaged line. This incurs a high cost for the utility, which we represent by c_f. On the other hand, updating the status of non-damaged switches is less costly from the utility perspective and we represent this cost by c_r. Thus, the switching operation cost $c_t \in \{c_r, c_f\}$ where $c_f \gg c_r$.

The unserved load cost, $L_{unserved}$, is determined by the mismatch in the demand from the costumer premises and the supply from the utilities.

However, purchasing power from DES systems such as a parking lot containing hundreds of electric vehicles (EV) incurs an additional cost denoted by $C_{storage}$ to the utility as it purchases power from the customers. This cost is determined by the amount of power purchased.

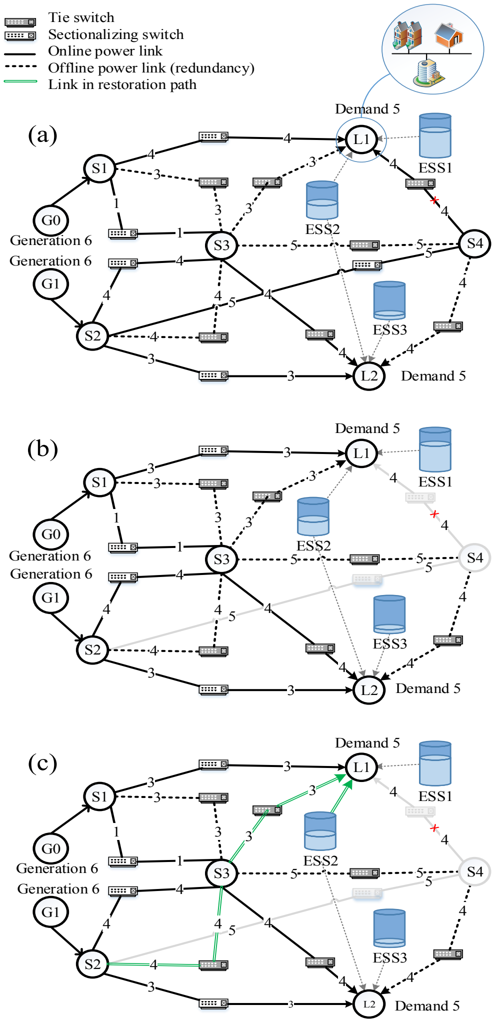

Figure 4.3: Graph representation of power network. (a) network before failure, (b) Failure on link S4L1 affects load L1, (c) service restoration path through NR (green lines).

Fig. 4.3 (a) represents our view of the system under study. The network includes power lines being used for power delivery represented by single solid lines. While the dotted lines represent redundant power lines to be used in network reconfiguration in the presence of failures or attacks on the power system. The system includes two types of switches. Closed switches on the lines in use, referred to as sectionalizing switches. And open switches on the redundant lines, referred to as tie switches. Energy storage systems are randomly located close to the customer premises. A failure is introduced on the link connecting S4 to L1 as Figure 4.3(a) shows. This failure affects the switch status on this link and thus it changes its state from closed to open. As a result, L1 can not receive all its requested power from the power grid. Consumers in area L1 will experience service disruption until the utility restores the service through other available paths or repairs the failed line which is more time consuming.

Through ASR, several network reconfigurations are possible to supply L1 with the required power. L1 can receive power through:

(1) Routing all needed power on link S1L1

(2) Closing S4L1

(3) Closing S3L1

(4) Closing S1S3 and S3L1

(5) Closing S2S3 and S3L1

Taking into consideration the power flow constraints such as power line capacity limit, generators supply capacity, network connectivity, infeasibility to increase generation in real time, we infer that not all the listed solutions are suitable for ASR. For example, solution 1 results in violation of the line capacity, and solutions 3&4 result in violation of generators generation capability. Moreover, other solutions include the failing line which are time consuming. Therefore, closing S2S3 and S3L1 is the best solution. However, in the presence of power loss over the lines, such a solution may not satisfy all the requested power by L1. In this case, the utility will supply the needed power by utilizing distributed energy storage systems. This will introduce more solutions associated with different network reconfiguration and costs depending on the availability of DES systems, and their associated power cost.

Thus, we define the service restoration through network reconfiguration as an optimization problem governed by various constraints. The problem objective is to restore the power service through network reconfiguration while minimizing the overall operational cost. This problem is mathematically formulated in the next section along with a description of all the rules that determine the optimal network reconfiguration for the system under study.

4.3.1 Notations

g: generator l: load s: substation

4.3.2 Parameters

N_p: set of all power nodes

N_l: set of all nodes with an associated power load

N_s: set of all substations

N_g: set of all generators

N_e: set of all distributed energy storage systems

E_p: set of all power links

E_g: set of all power links directly connected to a generator

$A[N_p \times E_p]$: power network adjacency matrix

$$a_{ij} \in A = \begin{cases} 1 & \text{if link } j \text{ starts from node } i \\ 0 & \text{if node } i \text{ is one of the vertices of link } j \end{cases}$$

$R[E_p \times E_p]$: resistance matrix of power lines

$X[E_p \times E_p]$: reactance matrix of power lines

$LS[E_p]$: vector of initial power links status after a failure

$$ls_j \in LS = \begin{cases} 1 & \text{if link } j \text{ is online} \\ 0 & \text{otherwise} \end{cases}$$

$Q[N_l]$: vector of power requested by loads

cap_j : capacity of power link $j \in E_p$

cap_g : capacity of generator $g \in N_g$

cg_e : amount of power charge of storage $e \in N_e$

cg_e^{min} : minimum amount of power charge of storage $e \in N_e$

$N[N_l \times N_e]$: load-storage connectivity matrix

$$n_i^e \in N = \begin{cases} 1 & \text{if load } i \text{ is connected to storage } e \\ 0 & \text{otherwise} \end{cases}$$

M: large real number

per_i^e: loss factor for serving load i through storage e

p_i^e: power price per unit for serving load i through storage e

V_i: voltage at power node i

4.3.3 Decision Variables

$C_{switching}$: total switching cost

$C_{storage}$: total storage cost

$$L_{unserved} = \begin{cases} 1 & \text{if link } j \in E_p \text{ is available} \\ 0 & \text{otherwise} \end{cases}$$

$$t_j = \begin{cases} 1 & \text{if link } j \text{ is online after restoration} \\ 0 & \text{if node } j \text{ othewise} \end{cases}$$

$$d_{i_1 j}^{inc} = \begin{cases} 1 & \text{if flow on link } j : (i_1 i_2) \text{ is from node } i_1 \text{ to node } i_2 \\ 0 & \text{otherwise} \end{cases}$$

$$d_{i_1 j}^{out} = \begin{cases} 1 & \text{if flow on link } j : (i_1 i_2) \text{ is from node } i_2 \text{ to node } i_1 \\ 0 & \text{otherwise} \end{cases}$$

p_j^{in}: amount of power injected to power link j

p_j^{out}: amount of power leaving power link j

p_j^{loss}: amount of power loss for power link j

s_i^{total}: amount of total power delivered to load i from the grid and storage systems

gen_g: amount of power generated by generator g

m_i^e: amount of power delivered to load i from storage e

$$r_j^{gn} = \begin{cases} 1 & \text{if link } j \text{ is on the path from generator } g \text{ to load } n \\ 0 & \text{otherwise} \end{cases}$$

δ_j^{gn}: the fraction of power supplied from generator g to load n on link j

4.3.4 Mathematical Model

Our objective is to determine the optimal network reconfiguration to restore services to de-energized zones. The optimal configuration aims at finding the least cost strategy in terms of switching actions taken and the use of DES systems while fulfilling most of the demand available in the system.

Hence, the objective function can be presented as

$$\text{Minimize } \alpha C_{\mathit{switching}} + \beta C_{\mathit{storage}} + \gamma L_{\mathit{unserved}} \tag{4.2}$$

where $C_{\mathit{switching}}$ is the total switching cost, C_{storage} is DES systems usage cost, and L_{unserved} is the cost of unserved load. While α, β, and γ are weights assigned to those loads to favor one over the other while satisfying ($\alpha + \beta + \gamma = 1$).

This objective is subject to the following constraints:

$$C_{\mathit{switching}} = \sum_{j \in E_p} (t_j - ls_j) \tag{4.3}$$

$$t_j \geq ls_j \quad \forall j \in E_p \tag{4.4}$$

$$d_{ij}^{\mathit{out}} = a_{ij}\ ,\ d_{ij}^{\mathit{inc}} = 0 \quad \forall i \in N_g,\ j \in E_p \tag{4.5}$$

$$d_{ij}^{\mathit{out}} = 0\ ,\ d_{ij}^{\mathit{inc}} = a_{ij} * t_j \quad \forall i \in N_l,\ j \in E_p \tag{4.6}$$

$$d_{ij}^{\mathit{out}} + d_{ij}^{\mathit{inc}} = a_{ij} * t_j \quad \forall i \in N_s,\ j \in E_p \tag{4.7}$$

$$L_{\text{unserved}} = \sum_{i \in N_l} (q_i - s_i^{\mathit{total}}) \tag{4.8}$$

$$\begin{gathered} s_i^{\mathit{total}} = \sum_{j:(si) \in E_p} p_j^{\mathit{out}} + \sum_{e \in N_e} m_i^e \\ \forall i \in N_l, s \in N_s \end{gathered} \tag{4.9}$$

$$p_j^{in} = p_j^{out} + p_j^{loss} \quad \forall j \in E_p \tag{4.10}$$

$$p_j^{loss} = I_j^2 (R_j \cos(\phi) + X_j \sin(\phi)) \quad \forall j \in E_p \tag{4.11}$$

$$\begin{gathered} p_j^{in} = I_j (V_{i_1}.\, d_{i_1 j}^{inc} + V_{i_2}.\, d_{i_2 j}^{inc}) \\ \forall j : (i_1 i_2) \in E_p, i_1 i_2 \in Np \end{gathered} \tag{4.12}$$

$$0 \leq p_j^{in} \leq t_j * cap_j \quad \forall j \in E_p \tag{4.13}$$

$$\sum_{g \in N_g} gen_g = \sum_{j:(il) \in E_p} p_j^{out} + \sum_{j \in E_p} p_j^{loss} \quad \forall i \in N_p, l \in N_l \tag{4.14}$$

$$gen_g = \sum_{j:(gi) \in E_p} p_j^{in} \quad \forall g \in N_g, i \in N_s \tag{4.15}$$

$$0 \leq gen_g \leq cap_g \quad \forall g \in N_g \tag{4.16}$$

$$\sum_{j:(is) \in E_p} p_j^{out} * d_{sj}^{inc} = \sum_{j:(si) \in E_p} p_j^{in} * d_{sj}^{out} \;\; \forall i \in N_p, s \in N_s \tag{4.17}$$

$$C_{\text{storage}} = \sum_{e \in N_e} \sum_{i \in N_l} (m_i^e * (1 + per_i^e) * p_i^e) \tag{4.18}$$

$$m_i^e \leq n_i^e * M \quad \forall e \in N_e, i \in N_l \tag{4.19}$$

$$\sum_{i \in N_l} m_i^e \leq cg_e - cg_e^{min} \quad \forall e \in N_e \tag{4.20}$$

$$\sum_{j:(i_1 i_2) \in E_p} \delta_j^{gn} * d_{i_1 j}^{out} - \sum_{j:(i_1 i_2) \in E_p} \delta_j^{gn} * d_{i_1 j}^{inc} \begin{cases} \leq 1 & \text{if g is at } i_1 \\ \geq -1 & \text{if n is at } i_1 \\ = 0 & \text{otherwise} \end{cases} \tag{4.21}$$
$$\forall n \in (N_p - N_g), \quad \forall g \in N_g$$

$$r_j^{gn} \leq \delta_j^{gn} \; * \; d_{i_1 j}^{out} \; * \; M \quad \forall j : (i_1 i_2) \in E_p, g \in N_g, n \in (N_p - N_g) \tag{4.22}$$

$$r_j^{gn} \geq \frac{\delta_j^{gn} \; * \; d_{i_1 j}^{out}}{M} \quad \forall j : (i_1 i_2) \in E_p, g \in N_g, n \in (N_p - N_g) \tag{4.23}$$

$$t_j \leq \sum_{g \in G} \sum_{n \in N_l} r_j^{gn} \quad \forall j \in E_p \tag{4.24}$$

$$t_j \geq \frac{\sum_{g \in G} \sum_{n \in N_l} r_j^{gn}}{M} \qquad \forall j \in E_p \tag{4.25}$$

where Eq (4.3) determines the number of switching actions performed in the reconfiguration. Eq(4.4) restricts switching actions possible to closing an open switch. The direction of power flow is controlled by Eq (4.5)-(4.7). Based on these equations, generating units only inject power to the system, loads consume power, and flow on a power link can only be in one direction simultaneously. The total amount of unserved load is presented in Eq (4.8). While Eq (4.9) balances the total amount of power consumed by each load to the summation of that received from the generating units and supplied by distributed energy storage systems. Power loss constraints over the power lines are presented in Eq (4.10)-(4.12). In these equations, we use the AC power flow equations with the assumption that the system is enabled with sufficient reactive power compensator in the form of capacitor banks at the substation level [64],[65]. Thus, only the active power consumptions should be taken into consideration. The amount of power flow over the network lines is ruled by their capacity as specified in Eq (4.13). Power generation/consumption balance in the system is presented in Eq (4.14). The power flow from one generator to the loads in the system does not exceed the power generated by this generator as specified in Eq (4.15). The power generated by generators is constrained by Eq (4.16). Balancing the power flow into and out of a substation is handled by Eq (4.17). The cost of usage of distributed energy storage systems is presented in Eq (4.18). The presence of a link between a DES system and a load allows the power supply from this DES system to the load as specified in Eq (4.19). The storage system charge constraint is presented in Eq (4.20). Finally, power flow and connectivity between power nodes and the generating units are presented in Eq (4.21)-(4.25). It is worth mentioning that Eq(4.11), Eq(4.12), Eq(4.17), Eq(4.18), Eq(4.21), Eq(4.22), and Eq(4.23) are non-linear, however these constraints can be easily linearized. To linearize the quadratic term in Eq(4.11), we first discretized the constraint interval into a number of sub-intervals and then assuming a linear constraint for each sub-interval. To linearize the other nonlinear constraints (product of a binary and a continuous variable) we used the following technique:

suppose $a = B \times c$ in which $B \in [0, \bar{B}]$ is a continues and c is a binary variable. Then the production could be linearized as following:

$$\begin{aligned} a &\leq \bar{B} \times c \\ a &\leq B \\ a &\geq B - (1-c)\bar{B} \\ a &\geq 0 \end{aligned} \tag{4.26}$$

4.4 Numerical Results

To setup our system, we used Java and IBM CPLEX concert technology to develop the model and related simulation programs. The simulations were executed on a windows machine with Intel Core i7 CPU running at 2.67GHZ and equipped with 12 GB of RAM.

We evaluated our approach on the IEEE 14, 30, & 57-Bus systems. The power related data of these systems is publicly available. We randomly added redundant power lines to the system representation to enable power restoration using those lines. The total number of lines for each system is presented in Table 4.1. We represent each bus as a node in the graph apart from the bus that has a generator and load connected to it. For such a bus, we create two nodes: a generator and a substation assigned the bus load.

To simulate a cascading failure in the system, we used our previous work [11] to identify failing links in the system. We distinguished between the links affected by a direct failure(or targeted by an adversary, see [11] for details), and the one failed as a consequence of the cascade of failure. For the former ones, manual switching and repairs are needed. However, automatic switching is allowed for the latter set to enable power delivery over those links.

Table 4.1: Test Systems Data

	14 Bus	**30 Bus**	**57 Bus**
Basic Power Links	34	71	139
Redundant Power Links	18	36	71
Total Power Links	52	107	210

For the first set of experiments, we did not consider the availability of storage systems. We ran the model taking into consideration the switching cost only. We attempted to restore service to the system with a varying amount of tolerable unserved load. This tolerance varies from 10% to 90% of the post failure unserved load. The load loss due to the failure constitutes 30% of the initial load in the system. The collected results for the different experiments are presented in Table 4.2.

Table 4.2: Switching Operations needed for SR

Tolerance	**14 Bus**	**30 Bus**	**57 Bus**
10%	No solution	No solution	No solution
20%	No solution	No solution	No solution
30%	No solution	10	18
40%	5	9	13
50%	3	8	12
60%	3	8	8
70%	2	5	4
80%	2	3	3
90%	1	1	1

The collected results shows that there is a varying cost (number of switching operations) to be paid by utilities for service restoration. This cost is directly dependent on the tolerable amount of unserved load. Based on the network topology, and the availability of redundant links, utilities need to perform the indicated number of switching actions to restore service to the affected loads. The switching actions are directly related to the tolerance level of load loss. As the tolerance level decreases, more switching actions should be performed to restore the service as can be seen from Table 4.2. However, for some scenarios, when the tolerance level is 10% or less, service restoration is unachievable due to the inability of routing power to the affected loads. Thus, network reconfiguration is not sufficient to restore power in case of failures and there is need to introduce supplementary elements in the network to attain a 0% tolerance level for unserved loads.

For illustration purposes, we present a more detailed view of the 14-Bus system for the case of 30% tolerance in the absence of supplementary distributed storage systems. The system schema after attack is presented in Fig. 4.5. The attacked power links are presented by dashed red lines and the offline power links as a result of cascading effects are presented by dotted blue lines.

The system schema after service restoration is presented in Fig. 4.6, and is detailed in Table 4.3. The power demand for the disconnected loads after the failure can be partially met with network reconfiguration. Indeed, closing the switches on the indicated links (see Table 4.3) restores power

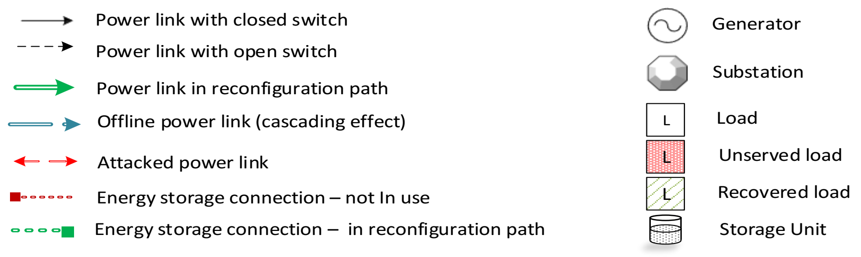
Power link with closed switch
Power link with open switch
Power link in reconfiguration path
Offline power link (cascading effect)
Attacked power link
Energy storage connection – not In use
Energy storage connection – in reconfiguration path
Generator
Substation
L
Load
L
Unserved load
L
Recovered load
Storage Unit

Figure 4.4: IEEE 14-Bus system figure legend.

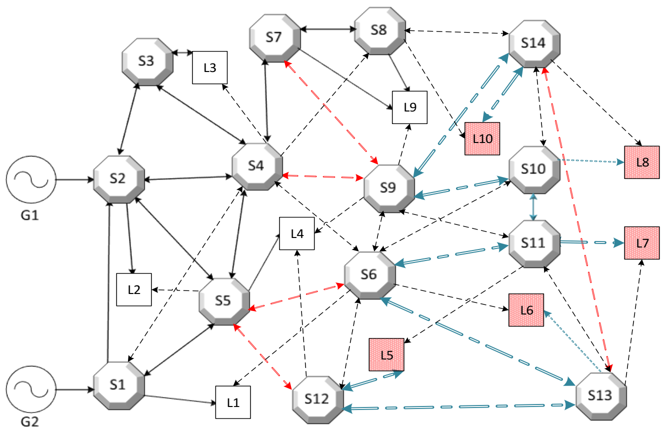

Figure 4.5: IEEE 14-Bus system schematic after attack (30% load loss tolerance). Figure legend provided in Fig. 4.4.

to loads L6, L8, & L10. However, loads L5 & L7 remain disconnected.

Another instance of the problem is studied in the presence of DES systems. In this aspect, we randomly distribute storage systems in the power network. Those systems are randomly located within physical proximity of the loads as they take the form of electric vehicles, or photovoltaic cells at the customer premises. DES systems are assigned random availabilities of stored power, different efficiency and pricing for their power supply.

In this instance, we restrict the number of switching actions by utilities to a pre-defined value. This restriction forces the model to provide solutions for service restoration depending on the availability of DES systems, and the power stored at those systems. We run the model with a varying number of switching actions, while minimizing the cost of DES systems usage for a certain load loss tolerance level. The collected results demonstrate the usefulness of DES in service restoration.

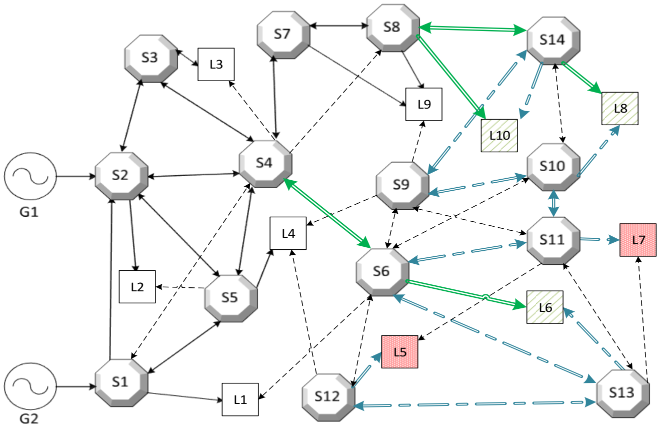

Figure 4.6: Service restoration for 14 Bus system with 30% load loss tolerance. Figure legend provided in Fig. 4.4.

Table 4.3: 14 Bus System SR

Failed Links	Lost Links		Power Demand(MW)	Switched Links
S7-S9	S9-S14	S12-L5	L5: 11	S6-L6
S4-S9	S9-S10	S12-S13	L6: 12	S8-L10
S5-S6	S6-S11	S13-L6	L7: 8	S8-S14
S5-S12	S6-S13	S10-L8	L8: 30	S14-L8
S13-S14	S14-S10	S11-L7	L10: 15	S4-S6

The detailed results for the 14-Bus system with a 30% tolerance level are presented in Table 4.4 for a varying number of switching actions. Those results demonstrate that with the availability of sufficient power at the DES, utilities can restore services to the lost loads with any changes to the network configuration and thus avoiding unwanted disruptions in the system. Indeed, even without rerouting energy from the utilities (0 switching actions), the requested load can be served through the available storage systems.

Moreover, we present a detailed view of the system for the 10% tolerance level and 2 possible switching actions in Fig. 4.7. This figure details the used DES and the affected links in the network reconfiguration. It is worth noting that multiple solutions in terms of switching actions and usage of DES systems are possible for some blackouts. However, the model presents the best solution in terms of balancing the cost of DES power in the presence of restricted number of switching actions.

Table 4.4: 14 Bus system with 30% load loss tolerance with DES

Number of Switching actions	**Closed Switched**	**DES Usage (MW)**
5	S6-L6	E6-L5: 3.40
	S8-L10	E6-L6: 8.0
	S8-S14	
	S14-L8	E8-L7: 8.0
	S4-S6	
4	S8-L10	E6-L5: 3.40
	S8-S14	E6-L6: 12.0
	S14-L8	E8-L7: 8.0
2	S8-S14	E6-L5: 3.40
		E6-L6: 12.0
	S14-L8	E8-L7: 8.0
		E5-L10: 14.99
1	S8-L10	E6-L5: 3.40
		E6-L6: 12.0
		E8-L7: 8.0
		E7-L8: 29.8
		E8-L8: 0.2
		E5-L10: 2.52
0		E6-L5: 3.4
		E6-L6: 12.0
		E8-L7: 8.0
		E7-L8: 29.8
		E8-L8: 0.2
		E5-L10: 15.0

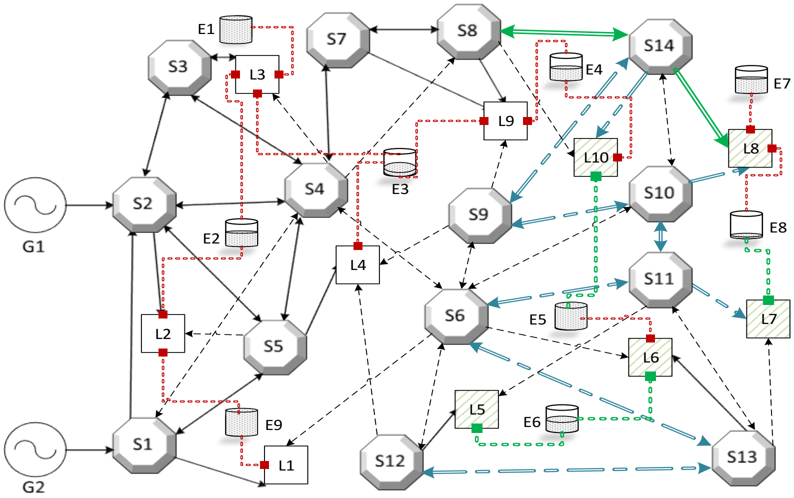

Figure 4.7: Service restoration for 14 Bus system with 30% load loss tolerance in presence of distributed energy storage systems.Figure legend provided in Fig. 4.4.

Based on those results, the availability of DES presents a potential solution for SR. This motivates the utilities to provide customer-based incentives for usage of DES systems. The presence of those DES systems improves the resiliency of the system to failures and provides utilities with various options for SR.

Chapter 5

Conclusion

5.1 Summary of Thesis Findings

In conclusion, in this thesis, we modeled the smart grid as a cyber-physical network and investigated different security challenges and proposed protection/mitigation mechanism in order to increase the smart grid resiliency against malicious compromises.

In Chapter 2, we demonstrated the importance of security evaluation mechanism which should be performed by power utility to quantify the criticality level of the grid from the security point of view. The results provided by security evaluation frameworks such as CASeS could be utilized by control/protection mechanism for decision making process during emergency situations. CASeS is a contingency analysis based security evaluation framework which considers the concurrent power contingencies while quantifying the security level. Given the current security of the system, CASeS would calculate a security index in real time with respect to the dynamic changes in the electric demand. In addition, CASeS could be utilized in efficient protection resource allocation. To validate our approach we test the approach for different benchmark IEEE bus systems.

In Chapter 3, we targeted the interdependency between the power and communication systems to expose the system vulnerabilities induced by this interdependency. Through the introduced model and algorithm, we exposed those vulnerabilities in the form of critical links in the smart grid as attack targets. The attack on these links leads to blackouts quantified in terms of the drop in the load served by the system. The validity of the approach is demonstrated through a mathematical model, and test results on the IEEE 14-Bus system.

And finally, in Chapter 4, we studied automatic service restoration through network reconfiguration which plays a major role in fulfilling the self healing capability of the envisioned smart grid. In this chapter, we presented our analysis of the service restoration in the presence of distributed storage systems. We followed a mathematical modeling approach where the problem was modeled as an optimization problem. The presented model identifies the optimal solution in terms of cost incurred by the utility to restore service to affected consumers, and highlights the importance of the availability of distributed energy storage systems for service restoration.

5.2 Future Work

As a future work, for enhancing the security metric proposed in Chapter 2, we aim at deploying energy storage systems in the power network and examine their impact on the security evaluation. In addition, optimal energy storage localization could be investigated to improve the system security in case of malicious compromises. Moreover, we aim at enhancing the MDP generation and completion blocks to capture coordinated attacks. For performing a more comprehensive study on critical link identification approach proposed in Chapter 3, we aim at building on the presented model to identify attacks on the smart grid that result in more severe outcomes. The fractional loss in the served load is the first step towards more elaborate attacks. And as a continuation of the study performed in Chapter 4, we are planning to extend the proposed model to study the optimal placement of distributed energy storage systems to allow utilities to minimize outage times and restoration costs. We believe such an objective is of high importance to utilities to improve the availability and reliability of the smart grid.

Bibliography

[1] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart gridthe new and improved power grid: A survey,” *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[2] H. Farhangi, “The path of the smart grid,” *IEEE power and energy magazine*, vol. 8, no. 1, pp. 18–28, 2010.

[3] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, “Cpindex: cyber-physical vulnerability assessment for power-grid infrastructures,” *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2015.

[4] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, “Communication security for smart grid distribution networks,” *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42–49, 2013.

[5] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, “Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid,” *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[6] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[7] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, “Smart-grid security issues,” *IEEE Security & Privacy*, vol. 8, no. 1, 2010.

[8] S. Pahwa, A. Hodges, C. Scoglio, and S. Wood, “Topological analysis of the power grid and mitigation strategies against cascading failures,” IEEE, pp. 272–276, 2010.

[9] J. Minkel, “The 2003 northeast blackout–five years later,” *Scientific American*, vol. 13, 2008.

[10] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the cyber attack on the ukrainian power grid,” *SANS Industrial Control Systems*, 2016.

[11] P. Akaber, B. Moussa, M. Debbabi, and C. Assi, “Cascading link failure analysis in interdependent networks for maximal outages in smart grid,” IEEE, pp. 429–434, 2016.

[12] A. Hahn and M. Govindarasu, “Cyber attack exposure evaluation framework for the smart grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, 2011.

[13] M. Parandehgheibi, E. Modiano, and D. Hay, “Mitigating cascading failures in interdependent power grids and communication networks,” in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*. IEEE, 2014, pp. 242–247.

[14] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, “Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures,” *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[15] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, “Socca: A security-oriented cyber-physical contingency analysis in power infrastructures,” *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[16] D. Shirmohammadi, “Service restoration in distribution networks via network reconfiguration,” *IEEE Transactions on Power Delivery*, vol. 7, no. 2, pp. 952–958, 1992.

[17] K. L. Butler, N. Sarma, and V. R. Prasad, “Network reconfiguration for service restoration in shipboard power distribution systems,” *IEEE Transactions on Power Systems*, vol. 16, no. 4, pp. 653–661, 2001.

[18] R. Baheti and H. Gill, “Cyber-physical systems,” *The impact of control technology*, vol. 12, pp. 161–166, 2011.

[19] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber–physical security of a smart grid infrastructure,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[20] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[21] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Military Communications Conference, 2010-MILCOM 2010*. IEEE, 2010, pp. 1830–1835.

[22] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," 2016.

[23] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 46, no. 1, pp. 101–107, 2005.

[24] J. Filar and K. Vrieze, *Competitive Markov decision processes*. Springer Science & Business Media, 2012.

[25] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, 2006.

[26] I. Kramosil and J. Michálek, "Fuzzy metrics and statistical metric spaces," *Kybernetika*, vol. 11, no. 5, pp. 336–344, 1975.

[27] Terrorism Research & Analysis Consortium, "Attacks on Electrical Grids," http://www.trackingterrorism.org/article/attacks-electrical-grids, 2013.

[28] P. Behr, "Outage on Quebec power grid traced to airborne attacker," http://www.eenews.net/stories/1060020352, 2015.

[29] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Communications Magazine*, vol. 50, no. 8, 2012.

[30] US-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf, 2003.

[31] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 63–79, 2008.

[32] A. Pinar, J. Meza, V. Donde, and B. Lesieutre, "Optimization strategies for the vulnerability analysis of the electric power grid," *SIAM Journal on Optimization*, vol. 20, no. 4, pp. 1786–1810, 2010.

[33] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 12, pp. 2340–2354, 2014.

[34] J. Yan, Y. Tang, Y. Zhu, H. He, and Y. Sun, "Smart Grid Vulnerability under Cascade-Based Sequential Line-Switching Attacks," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–7.

[35] V. Donde, V. Lopez, B. Lesieutre, A. Pinar, C. Yang, and J. Meza, "Identification of severe multiple contingencies in electric power systems," *Lawrence Berkeley National Laboratory*, 2008.

[36] D. Bienstock and A. Verma, "The nk problem in power grids: New models, formulations, and numerical experiments," *SIAM Journal on Optimization*, vol. 20, no. 5, pp. 2352–2380, 2010.

[37] Department of Homeland Security Office of Cyber and Infrastructure Analysis (DHS/OCIA), "The Future of Smart Cities: Cyber-Physical Infrastructure Risk," https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf, 2015.

[38] J. M. Arroyo and F. J. Fernández, "Application of a genetic algorithm to n-k power system security assessment," *International Journal of Electrical Power & Energy Systems*, vol. 49, pp. 114–121, 2013.

[39] T. N. Dinh, M. T. Thai, and H. T. Nguyen, “Bound and exact methods for assessing link vulnerability in complex networks,” *Journal of Combinatorial Optimization*, vol. 28, no. 1, pp. 3–24, 2014.

[40] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “Bilevel model for analyzing coordinated cyber-physical attacks on power systems,” 2015.

[41] S. Soltan, D. Mazauric, and G. Zussman, “Cascading failures in power grids: analysis and algorithms,” in *Proceedings of the 5th international conference on Future energy systems*. ACM, 2014, pp. 195–206.

[42] Y. Wu, L. Nordström, and D. E. Bakken, “Effects of bursty event traffic on synchrophasor delays in ieee c37. 118, iec61850, and iec60870,” in *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*. IEEE, 2015, pp. 478–484.

[43] M. Amin, “Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid,” in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*. IEEE, 2008, pp. 1–5.

[44] Y. Tang, G. Bu, and J. Yi, “Analysis and lessons of the blackout in indian power grid on july 30 and 31, 2012,” in *Zhongguo Dianji Gongcheng Xuebao(Proceedings of the Chinese Society of Electrical Engineering)*, vol. 32, no. 25. Chinese Society for Electrical Engineering, 2012, pp. 167–174.

[45] S. M. Amin and B. F. Wollenberg, “Toward a smart grid: power delivery for the 21st century,” *IEEE power and energy magazine*, vol. 3, no. 5, pp. 34–41, 2005.

[46] M. H. Camillo, R. Z. Fanucchi, M. E. Romero, T. W. de Lima, A. da Silva Soares, A. C. B. Delbem, L. T. Marques, C. D. Maciel, and J. B. A. London, “Combining exhaustive search and multi-objective evolutionary algorithm for service restoration in large-scale distribution systems,” *Electric Power Systems Research*, vol. 134, pp. 1–8, 2016.

[47] C.-T. Su, C.-F. Chang, and J.-P. Chiou, “Distribution network reconfiguration for loss reduction by ant colony search algorithm,” *Electric Power Systems Research*, vol. 75, no. 2, pp. 190–199, 2005.

[48] R. S. Rao and S. Narasimham, “A new heuristic approach for optimal network reconfiguration in distribution systems,” *International Journal of Applied Science, Engineering and Technology*, vol. 5, no. 1, 2009.

[49] Y.-C. Huang, “Enhanced genetic algorithm-based fuzzy multi-objective approach to distribution network reconfiguration,” *IEE Proceedings-Generation, Transmission and Distribution*, vol. 149, no. 5, pp. 615–620, 2002.

[50] A. Morelato and A. Monticelli, “Heuristic search approach to distribution system restoration,” *IEEE Transactions on Power Delivery*, vol. 4, no. 4, pp. 2235–2241, 1989.

[51] S. Dimitrijevic and N. Rajakovic, “An innovative approach for solving the restoration problem in distribution networks,” *Electric Power Systems Research*, vol. 81, no. 10, pp. 1961–1972, 2011.

[52] A. Y. Abdelaziz, F. Mohamed, S. Mekhamer, and M. Badr, “Distribution system reconfiguration using a modified tabu search algorithm,” *Electric Power Systems Research*, vol. 80, no. 8, pp. 943–953, 2010.

[53] N. Rugthaicharoencheep and S. Sirisumrannukul, “Feeder reconfiguration with dispatchable distributed generators in distribution system by tabu search,” in *Universities Power Engineering Conference (UPEC), 2009 Proceedings of the 44th International*. IEEE, 2009, pp. 1–5.

[54] C. F. Chang, “Reconfiguration and capacitor placement for loss reduction of distribution systems by ant colony search algorithm,” *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1747–1755, Nov 2008.

[55] S. Dimitrijevic and N. Rajakovic, “Service restoration of distribution networks considering switching operation costs and actual status of the switching equipment,” *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1227–1232, 2015.

[56] E. Pournaras and J. Espejo-Uribe, “Self-repairable smart grids via online coordination of smart transformers,” *IEEE Transactions on Industrial Informatics*, 2016.

[57] F. J. Rodriguez, S. Fernandez, I. Sanz, M. Moranchel, and E. J. Bueno, “Distributed approach for smartgrids reconfiguration based on the ospf routing protocol,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 864–871, 2016.

[58] M.-A. Rostami, A. Kavousi-Fard, and T. Niknam, “Expected cost minimization of smart grids with plug-in hybrid electric vehicles using optimal distribution feeder reconfiguration,” *IEEE Transactions on Industrial Informatics*, vol. 11, no. 2, pp. 388–397, 2015.

[59] D. S. Sanches, T. W. de Lima, J. B. A. L. Junior, A. C. B. Delbem, R. S. Prado, and F. G. Guimarães, “Multi-objective evolutionary algorithm with discrete differential mutation operator for service restoration in large-scale distribution systems,” in *International Conference on Evolutionary Multi-Criterion Optimization*. Springer, 2015, pp. 498–513.

[60] M. Kleinberg, K. Miu, and H.-D. Chiang, “Service restoration of power distribution systems incorporating load curtailment,” in *Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on*. IEEE, 2009, pp. 1709–1712.

[61] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor *et al.*, “Definition and classification of power system stability ieee/cigre joint task force on stability terms and definitions,” *IEEE transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, 2004.

[62] J. E. Tate and T. J. Overbye, “Line outage detection using phasor angle measurements,” *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1644–1652, 2008.

[63] ——, “Double line outage detection using phasor angle measurements,” in *2009 IEEE Power & Energy Society General Meeting*. IEEE, 2009, pp. 1–5.

[64] M. E. Baran and M.-Y. Hsu, “Volt/var control at distribution substations,” *IEEE Transactions on Power Systems*, vol. 14, no. 1, pp. 312–318, 1999.

[65] G. Ozdemir, S. Emiroglu, and M. Baran, “Supervisory control for coordinating volt/var control devices on a distribution system,” in *Innovative Smart Grid Technologies Conference (ISGT), 2016 IEEE Power & Energy Society*. IEEE, 2016, pp. 1–5.