10-29-2014

Telecommunication Network Survivability for Improved Reliability in Smart power Grids

Sankalp Mogla
University of South Florida, sankalpmogla@mail.usf.edu

Telecommunication Network Survivability for Improved Reliability in Smart Power Grids

by

Sankalp Mogla

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Electrical Engineering
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Nasir Ghani, Ph.D.
Zhixin Miao, Ph.D.
Lingling Fan, Ph.D.

Date of Approval:
October 29, 2014

Keywords: Electric transmission, failure analysis, disaster recovery, interdependent systems

DEDICATION

"Genius is one percent inspiration, ninety-nine percent perspiration "

- Thomas A. Edison

I dedicate my work to my loving Father and Mother, for their affection and encouragement, to make me capable of this accomplishment and follow my dreams.

With my deepest gratitude and warmest affection, I dedicate this thesis to my professor Dr. Nasir Ghani for being a constant source of knowledge and inspiration.

ACKNOWLEDGMENTS

I would like to acknowledge and extend my gratitude to my advisor Dr. Nasir Ghani for his countless hours of reflecting, reading, encouraging, and most of all, his expert guidance through the entire process. Thank you for your generosity and precious time.

I would also like to thank Dr. Zhixin Miao and Dr. Lingling Fan for agreeing to serve on my thesis committee.

I would also like to acknowledge my school, University of South Florida, for allowing me to conduct my research and providing the required resources.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Power transmission grid infrastructures deliver electricity across large distance and are vital to the functioning of modern society. Increasingly these setups embody highly-coupled cyber-physical systems where advanced telecommunications networks are used to send status and control information to operate power transmission grid components, i.e., "smart grids". However, due to the high interdependency between the communication and power grid network layers, failure events can lead to further loss of control of key grid components, i.e., even if they are undamaged. In turn, such dependencies can exacerbate cascading failures and lead to larger electricity blackouts, particularly under disaster conditions. As a result, a range of studies have looked at modelling failures in interdependent smart grids. However most of these designs have not considered the use of proactive network-level survivability schemes. Indeed, these strategies can help maintain vital control connectivity during failures and potentially lead to reduced outages. Hence this thesis addresses this critical area and applies connection protection methodologies to reduce communication/control disruption in transmission grids. The performance of these schemes is then analyzed using detailed simulation for a sample IEEE transmission grid. Overall findings show a good reduction in the number of overloaded transmission lines when applying network-level recovery schemes.

CHAPTER 1: INTRODUCTION

Power transmission grids play a vital role in delivering electricity from large generation sites to sub-stations serving end-user distribution networks. Now in recent years many utility providers have invested significant resources to revamp these infrastructures and improve their efficiency and reliability. Most notably, advanced telecommunication networking technologies are being extensively used to interconnect transmission grid components with large *network operating center* (NOC) sites, also termed as *system control centers* (SCC) [RAH13]. These networks are then used to build higher-level *supervisory control and data acquisition* (SCADA) systems that allow regional *balancing authorities* (BA) to send/receive regular field updates of critical grid measurements/parameters, i.e., to make crucial control decisions such as load-shedding [RAH13]. Note that these evolved setups are also termed as "smart" transmission grids and in a broader sense, represent coupled *cyber-physical systems* (CPS) [KIM12].

1.1 Background

A high-level view of a smart power grid is shown in Figure 1.1. This setup consists of the main utility power infrastructure, an overlying communication network, and well as a network of human operators. The main role of the communication network is to transfer information between remote monitoring and control agent systems [RAH13] and the main NOC site. Specifically, various types of networked *phasor measurement units* (PMU) and *phasor data*

concentrators (PDC) systems have been deployed in the field to collect information on the health of system components, loads, etc. SCADA systems and human operators at the main NOC site then use this distributed information to optimize power flow, and if necessary, initiate load shedding behaviors by transmitting control commands to control agents.

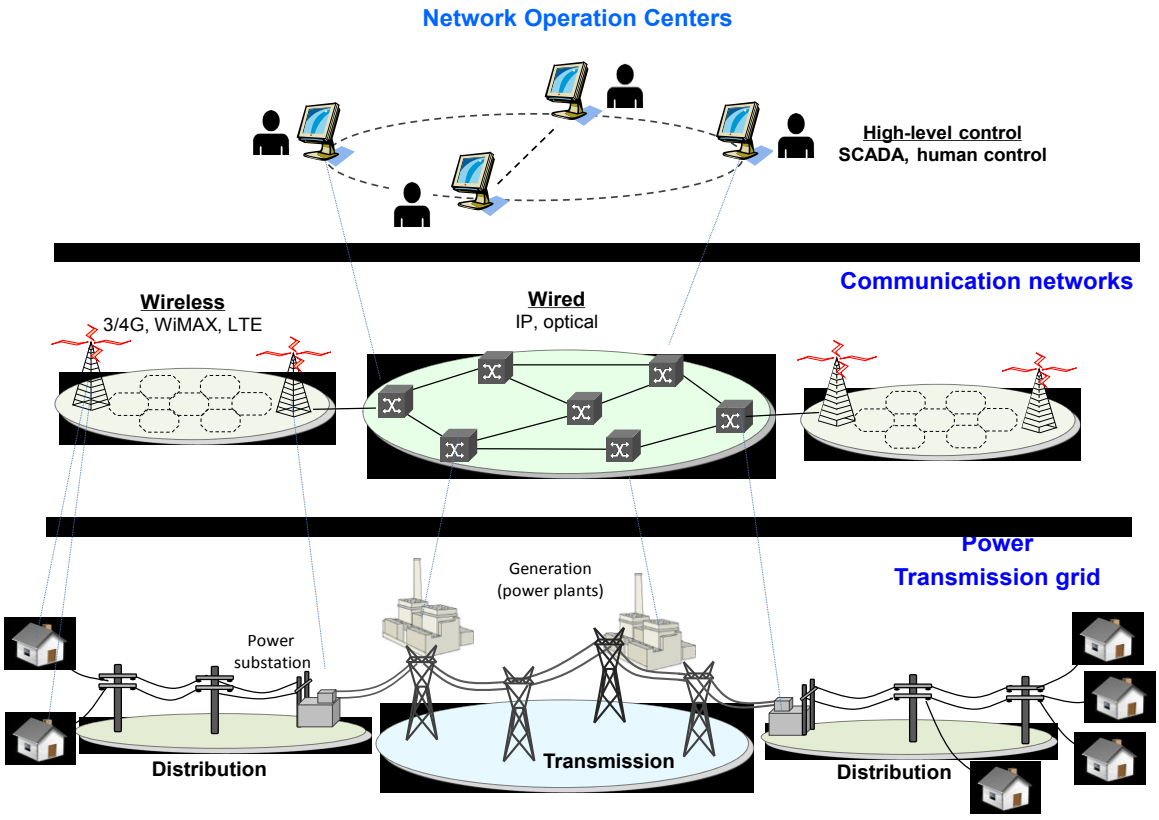

Figure 1.1: Overview of integrated "smart" transmission grid: power and networking mix

Now since transmission grids can span across wide geographic domains, a variety of communication technologies are being used today, i.e., including wired and wireless, see [YAN13] for a complete survey. However, for the most part, wireless technologies are being increasingly deployed on the *distribution* side, where communication distances are relatively small (under 10 km). Key examples here include wireless cellular, WiMAX (IEEE 802.16), and

even *long term evolution* (LTE), etc. Meanwhile, wired fiber-optic communications systems are much more common on the longer-haul transmission side. These systems are relatively cost-effective to deploy as most power utilities own the rights-of-way along their power line routes, i.e., and can either deploy air or ground fiber. Note that the latter case is also termed as "optical ground wire" [RAH13]. Overall, fiber transmission offers many saliencies here, including high-bandwidth capacity and immunity to electromagnetic emissions and corrosion. Furthermore, current state-of-the-art fiber-optic *wavelength division multiplexing* (WDM) networking technologies also provide a very flexible and cost-effective means of partitioning and provisioning abundant fiber bandwidth between network locations/sites. As a result, many utilities have deployed these and related technologies.

1.2 Motivations

Now clearly, the reliable functioning of transmission grids under a range of fault conditions is a major concern. For example, isolated power grid failures (lines, relays, switches, or generator sites) will affect many local users whose distribution networks are directly served by the faulty elements. Conversely, larger catastrophic events can be much more destructive, yielding multiple system failures with very high levels of spatial and temporal correlation, i.e., after natural disasters (such as hurricanes, floods, earthquakes, and solar storms) or malicious man-made attacks, such as those with *weapons of mass destruction* (WMD). As recent examples, hurricane Sandy (2012) and the Ontario ice storm (2013) resulted in widespread regional power outages that affecting millions of residents for extended durations (days).

In light of the above, there is critical need to address the reliability of smart grids under a range of failure conditions. Of particular concern is the mitigation of cascading failures, which can occur as utilities perform load-shedding actions to re-balance load across the remaining working grid components. Indeed, increased interdependency between the power grid and communication network can also worsen such cascading effects. Namely, power outages can end up causing more communication nodes to lose power and fail. In turn, these failures can disrupt control/communication to more transmission grid components (loads), resulting in more uncontrolled loads. For example, Figure 1.2 depicts the rapid onset of cascading failures during the large 2003 blackout event that affected the Northeastern United States and Canada [TFR04], i.e., multi-fold increase in failed lines (lost generation units) within minutes of the initial failure.

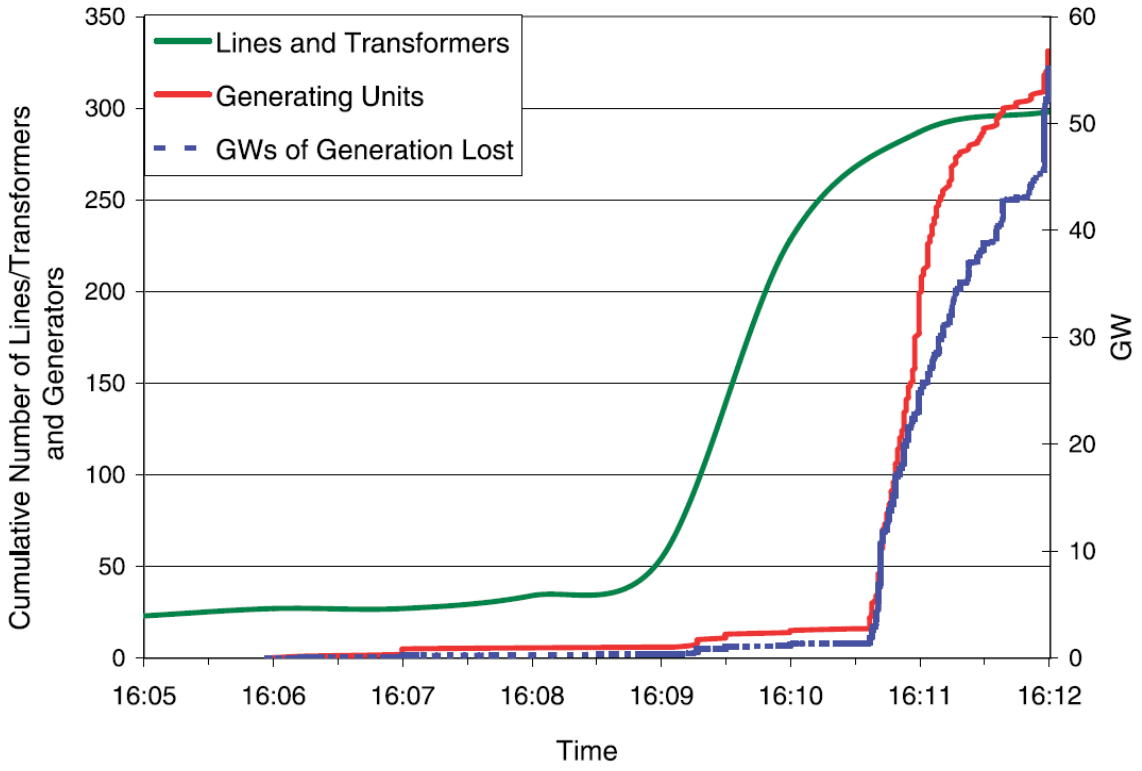

Figure 1.2: Cascading failure effects in 2004 US-Canada blackout event, from [TFR04]

In light of the above, many researchers are starting to study the impact of cascading failures in interdependent power-communication grids. By and large, most of these studies have taken a graph-theoretic approach towards analyzing the interdependencies (interplay) between the power transmission grid and data network topologies, see [BLD10],[CAR02],[CAS13],[KHA14], [NEU13],[PAR13],[RAH12],[RAH13],[ROS08]. Overall, these efforts provide a detailed modelling of cascading behaviors, which in turn can provide further design insights in to building improved data network topologies/overlays.

However, despite these contributions, there is still a pressing need to study the effect of *communication network survivability* schemes on failures in smart power-communication grids. For example, these strategies can help reduce communication/control disconnection in critical grid components, thereby limiting the number of un-controllable loads. In turn, these improvements have the potential to mitigate cascading failures and limit the size of blackout events. However there are no known studies along these lines. Perhaps the only related work is presented in [RAH12] and [RAH13], where the authors model the dependency of communication networks on the underlying transmission grid using random probabilities. Although this approach tries to incorporate communication network failures, fixed probabilities do not capture the response of complex network survivability schemes under varying (multi-failure) conditions. This forms the key motivation for this research.

1.3 Problem Statement

This thesis focuses on the use of advanced telecommunication network protection schemes in integrated communication/power smart transmission grids and analyses their detailed impacts on various power grid system failures.

1.4 Scope and Objectives

The objective of this effort is study the effect of network-level recovery schemes in smart transmission grids under varying failure conditions. The work focuses on realistic settings in which control network topologies use fiber-optic wireline communication and mirror their transmission grid counterparts. First, various protection algorithms are applied to help determine the transmission grid components (substations, lines) that will lose communication/control with the NOC site after a fault. Next, detailed power grid analyses are conducted to determine the resulting line failures (blackout sizes) from these component disconnections. All communication network simulations are done using the *OPNET Modeler*^{TM} toolkit, whereas the ensuing power analyses are done using the *MATLAB MATPOWER* package.

1.5 Research Approach

This overall research focuses on several key tasks. First, a detailed survey is done to review the existing work on analysis of integrated/coupled communication/power networks. The next step focuses on the selection and application of some well-known protection algorithms for

pre-provisioned network failure recovery. The goal here is to maintain vital connectivity between utility operation control centers and remote transmission grid components under stressor conditions. Several network recovery algorithms are then tested using the *OPNET Modeler*™ toolkit to determine post-fault connectivity for varying failure scenarios in a sample power grid topology. Finally, the above outputs are used to solve the resulting power flow models and identify the set of transmission line failures yielding uncontrollable (disconnected) loads.

1.6 Thesis Outline

The thesis is organized as follows. Chapter 2 first reviews the existing work in failure modelling of integrated smart transmission grids. Next, Chapter 3 details some network protection algorithms, including those for disaster recovery support, as well as a stochastic modelling approach for computing power grid blackout sizes. Finally, Chapter 4 presents some detailed analyses to quantify transmission grid failures (line outages) in a sample power grid experiencing a range of fault conditions. Conclusions and future work directions are then presented Chapter 5.

CHAPTER 2: BACKGROUND SURVEY

Survivability of integrated smart grids is a critical area of concern. Lately, a range of studies have emerged on this topic, with most focusing on modelling the nature of failure cascades between the two (power, data network) layers. Along these lines, this chapter reviews these contributions and also presents a high level summary of telecommunication network survivability schemes (itself an extremely broad area). The application of the latter within the context of smart grid survivability is the main focus of this research study.

2.1 Integrated Smart Grid Failure Modelling

Various studies have looked at survivability modelling and design of coupled power communication infrastructures. For example, [ROS08] gauges the impact of perturbations in the electrical grid on higher layer routing performance in data communication networks. Coupling factors are first introduced to model the degree of dependency between routing nodes and their feeding power node, i.e., higher coupling values imply that slight power losses in related power nodes can cause routing node outages. These factors are generally assigned based upon geographic proximity. Next, a load "re-dispatching" strategy is also presented to model utility load re-distribution to minimize departure from working state conditions after transmission line (link) failures. A detailed study is then conducted using the Italian national electrical grid and Internet backbone topologies. First, a detailed topological node-degree analysis is done for the

Italian electrical transmission grid, and the results indicate that it generally follows similar trends in the North American grid. Next, the effects of grid perturbations (faults) are tested on overlying routing performance. The findings here indicate a significant increase in packet routing delays, even with moderate coupling levels (orders of magnitude higher), termed in [ROS08] as an inter-layer amplification effect.

Meanwhile, [BLD10] looks at iterative cascading failures in interdependent power-communication networks. Namely, power outages are assumed to lead to node outages, which in turn lead to further power node outages. Now the model assumes an equivalent number of nodes in both layers, as well as bi-directional failure dependencies between respective-numbered nodes. Hence if a given layer node fails, then all its interconnected neighbors in the same layer and interdependent layer are removed. Based upon this, analysis is conducted to identify the critical number of failed nodes that can lead to complete fragmentation of the network (using percolation theory). Specifically, the work assumes Erdos-Renyi network/grid topologies and fails a random fraction of nodes in one of the layers to kick-start the iterative cascading process. These iterations are continued until the number of mutually-connected components in the largest sub-graph (cluster) stops changing. Using this method, the authors evaluate the performance of various abstract networks with varying node degrees and distributions, see [BLD10]. Albeit a good initial contribution, this work does not analyze realistic power grid/communication topologies. Moreover, the bi-directional failure dependency assumption is not very realistic as many networking sites will deploy backup power to prevent or delay node outages.

[NEU13] also studies the impact of power outages on communication networks. First of all, two-stage failure model is defined for power grid faults, i.e., where the first stage removes/fails power lines intersecting a given circular (fault) region and the second stage removes additional lines due to failure cascades. Here cascading line failures are computed by solving a iterative *direct current* (DC) power flow problem over the remaining (working) lines, i.e., versus a more complex/realistic *alternating current* (AC) model. Detailed simulations results show that failures correlated about a circular region actually give higher post-fault satisfied demand levels (yield) versus more dispersed independent failures, i.e., closer failure proximities can actually lower cascading effects. Next, the authors incorporate data network dependency concerns, i.e., by making network nodes fully-dependent upon their closest geographically-located power substation node. Findings show that cascading failures have a significant impact on data network connectivity levels as well, i.e., measured via average node connectivity and average connectivity probabilities between nodes (i.e., measure of post-fault disconnectivity). Hence the authors propose future efforts to augment data network topologies and algorithms to overcome cascading faults. However this work does not look at the further impact of communication node outages on power grid control capabilities, which can readily worsen cascades.

More recently [PAR13] has also studied robustness in interdependent power grid and communication network infrastructures. Here the authors focus on computing the minimum number of node outages that will result in total failure, i.e., *minimum total failure removals* (MTFR), and consider both uni-directional and bi-directional dependency between nodes in the respective layers. Furthermore, to achieve tractability, both infrastructures are also reduced to

simplified star topologies, i.e., one generator site connecting multiple sub-stations and one network control center router connecting to multiple sub-station routes. Now for the case of uni-directional dependency, the authors introduce the concept of cycles to show dependencies between nodes. The MTFR problem is then is likened to the NP-complete graph hitting cycle problem to determine the minimum number of removals, and several polynomial-time heuristics are proposed, i.e., cycle-based and degree-based. Meanwhile, the bi-directional dependency case is shown to be simpler (akin to vertex cover problem) and solvable in polynomial time, see [PAR13]. These solutions are then tested for sample networks and as expected, the bi-directional interdependency models are shown to be more robust. In addition, for the case of uni-directional dependency the degree-based heuristic gives better performance, i.e., higher MTFR values, see [PAR13] for details.

Meanwhile in [CAS13] the authors map heterogeneous networks to *interdependent multi-layer networks* (IMLN) and analyze their survivability. The proposed IMLN model consists of nodes, super-nodes, layers, intra-layer links, networked layers and inter-layer links. In particular, the nodes within each layer form a network, and interconnecting nodes form different layers represent different types of interdependencies. Furthermore, two failure propagation models are considered, i.e., kill effect and precursor effect. Now in order to evaluate these models, the authors estimate a function by generating the times to failure, propagating kill, and precursor failures. Finally, all of these effects are combined to calculate the probability that a node remains operational or becomes unavailable. In addition to evaluating the survivability of interdependent networks, the authors also examine the impact of the reliability of wireless links between the network nodes.

Finally, the work in [RAH12] presents one of the first studies on the effects of communication disconnectivity in smart transmission grids. Namely, an optimization formulation is used to compute load-shedding behaviors (distributions) after faults, with the goal of minimizing total cost (with load-shedding penalties) as introduced in [CAR02]. Communication vulnerabilities are directly coupled into this model by defining/assigning load controllability ratios for all loads, i.e., 0 meaning that the load is not controllable (disconnected). The formulation is solved using the *MATLAB MATPOWER* package for the well-studied IEEE 118 transmission grid and overall findings show that communication network vulnerabilities can greatly increase the probability of large-scale cascading failures.

In addition, [RAH13] also extends the above to model successive (cascading) failures between the power grid and communication network infrastructures. This work assumes that each substation node has an attached routing node and intelligent control agents sending/receiving measurement signals/commands to/from the control center. Several communication network layer topologies are also evaluated here, including a base topology matching the transmission grid as well as randomly-modified variations with increased and/or decreased link counts, i.e., node degrees. Furthermore, communication nodes are assigned failure probabilities to model their coupling/interdependency to nearby power facilities, i.e., higher probabilities imply increased vulnerability to power outages in the geographical proximity. These interdependencies are then inserted into the DC power-flow model of [CAR02],[RAH12] and solved iteratively until failures stop occurring. As expected, findings show that failures propagate faster when there is increased coupling between the two layers,

resulting in larger blackout sizes. However, increased node degrees (in the base topology) can notably lower the size of cascading line outages.

Although the above studies provide some good insights (and base references), in general, fixed probabilities do not accurately capture the post-attack recovery performance of complex network survivability schemes under multi-failure conditions. Moreover, to date few/no studies have actually looked at applying realistic communication network recovery schemes to improve post-attack power grid element connectivity (controllability). Some of these strategies are briefly surveyed next.

2.2 Network Protection Schemes

Telecommunication network survivability/recovery from faults is a very well-studied area and many different types of schemes have been developed over the years. However, given the depth and breadth of this area, a detailed survey is very much out of scope. As a result, only a subset of solutions are reviewed here, with a specific focus on those with more applicability to fiber-optic networks (see also high-level summary Figure 2.1). Interested readers are also referred to [CHL07] for more details.

2.2.1 Link Protection Schemes

Link protection is widely-deployed in fiber optic networks, and has its origins in earlier *synchronous optical network* (SONET) technologies [WU92]. The basic approach here is to

provision a dedicated backup physical link for each working network link. This backup link is usually routed along a geographically-diverse route in order to improve survivability, and may require switchover actions upon detection of failure on the main working/primary links.

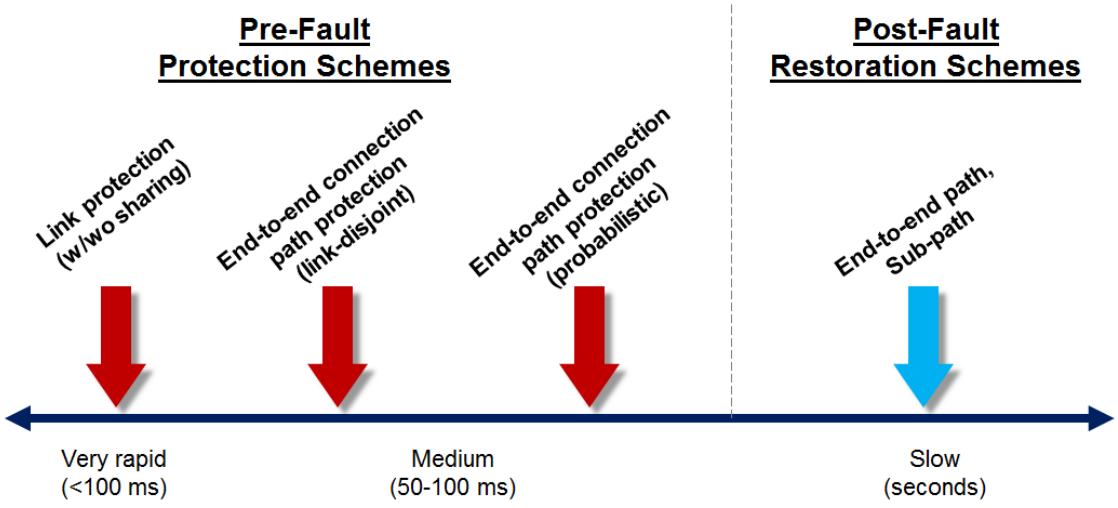

Figure 2.1: Overview of network recovery methods: pre- and post-fault

In particular, several key link protection schemes are in use today. The most basic scheme here is 1+1 protection, which transmits two copies of the data between the end point nodes, i.e., along primary and backup fiber routes. The receiving node simply selects from the fiber with the stronger signal, and hence failed link switchovers are almost seamless (within a few milliseconds). However, 1+1 protection is very wasteful of fiber resources, as data is essentially sent twice. To improve upon this, the 1:1 protection scheme oversubscribes the backup fiber by using it to send lower priority data during working conditions, i.e., shared link protection. Whenever a failure occurs on the primary route, this scheme pre-empts the lower priority traffic and performs a switchover to re-route working traffic onto the backup link. However, this scheme entails slightly more delays (10's of milliseconds) and added end-to-end signaling complexity to properly coordinate timely switchover events. Finally, some network operators

also use *M*:*N* link protection, which is a further generalization of 1:1 protection, i.e., where *M* working fibers share *N* working links. However, regardless of their design, all link-based protection schemes are very vulnerable to disaster-type events that can damage extensive parts of a network.

2.2.2 Path Protection Schemes

As noted above, link protection schemes are localized in nature will recover all traffic on a failed link, i.e., non-selective. In many cases network operators will want to differentiate between their clients and provide a higher grade of recovery to selected users. Along these lines, a range of end-to-end connection path protection schemes have been developed, see [ZHU00]. These designs pre-compute backup routes for working connections, and perform switchover actions upon detection of failures on primary routes. To overcome single link (node) failures, these backup routes are usually link (or node) disjoint from the primary routes.

Now akin to the case of link protection, path protection can be done in either a dedicated or shared manner [CHL07]. Namely, dedicated schemes pre-compute and reserve separate (non-shared) backup routes for all connections. Expectedly, these schemes yield lower resource efficiency. As a result researchers have also proposed many shared protection strategies to allow backup link resource sharing (of bandwidth, wavelengths) between multiple working paths as long as they are link disjoint. The latter condition ensures that two working paths cannot fail at the same time from a single link failure, preventing contention for backup bandwidth. However,

shared protection schemes are more complicated and all connection level strategies require additional end-to-end protocol signaling to perform working/backup switchovers.

In general, most protection schemes work well for single link failures, which are the most common types in most networks. However, under more rare disaster conditions, these schemes are very vulnerable since multiple failures can easily affect both working and backup connection routes. Along these lines, more recent efforts have proposed specialized *probabilistic* protection schemes [LEE10],[DIA12]. Unlike single failure recovery methods, these solutions do not try to guarantee any form of recovery, i.e., as that is generally not possible under probabilistic multi-failure scenarios. Instead, these strategies define a set of pre-existing (a-priori) probabilistic risk regions in the network and then compute path pair routes to minimize joint failure probabilities for the primary/working and backup routes. In particular, the work in [LEE10] proposes an iterative version of Dijkstra's shortest-path algorithm to compute disjoint path pairs, i.e., with link weights defined as functions of a-priori risk failure probabilities. Meanwhile, [DIA12] outlines a broader strategy that computes (multiple) k-shortest path pairs and selects the one which minimizes failure probabilities and reduces resource usages/costs. Findings here show improved performance over basic link-disjoint protection as well as the related scheme in [LEE10].

2.2.3 Restoration Schemes

Network protection schemes basically pre-reserve recovery resources to provide some level of guaranteed and rapid recovery. However, these schemes can be very resource inefficient

when backup resources are sitting idle/unused. As a result, many different *shared* protection schemes have also been proposed to oversubscribe (multiplex) backup resources between multiple working (non-failed) connection routes, see [CHL07]. However, these methods impose much more provisioning complexity and are only designed to handle single link failures.

As an alternative, flexible post-fault restoration schemes have also been proposed here to recover failed connections. Namely in these designs regular connections are simply provisioned in an unprotected manner at the time of their start. However, in case of a fault event, dynamic restoration algorithms are invoked to re-compute/re-establish failed working routes. In general, two further strategies are proposed here, i.e., sub-path segment recovery and complete end-to-end recovery [XU11]. Expectedly, these schemes give much better resource efficiencies as no resources (link routes) are reserved for backup connections. However, at the same time, these schemes cannot guarantee recovery (even for single node/link faults) as sufficient spare capacity may not be available. Finally, restoration strategies are also more latent since post-fault signaling can take 100 ms-seconds to re-establish a new route.

2.3 Open Challenges

Although the work surveyed in Section 2.1 presents some good analyses of coupled power-communication networks, these efforts do not take into account the further effects of *network survivability* schemes to overcome control disconnection between remote transmission grid agents (at PMU or PDC units) and SCC/NOC sites. This is a key concern as network designers have developed a range of advanced recovery schemes for single and even multiple failure

conditions. As a result, a detailed study is now proposed to incorporate/model the impact of network recovery techniques in smart transmission grids. Overall, given the fact that cascading failures can evolve within tens of seconds or minutes, rapid sub-second network recovery can play a vital role in minimizing power grid control disruption during such critical times.

CHAPTER 3: COUPLED TRANSMISSION GRID ANALYSIS

There is a critical need to incorporate network (control) connectivity when studying cascading failure effects in power grids. However this is a rather challenging task as the analytical methods used in the two fields are very different. For example, most networking studies focus on discrete events, e.g., such as connection requests, packet arrivals, link/node failures, etc. Meanwhile most transmission grid analyses treat continuous time-varying quantities, e.g., voltages, currents, phases. Hence it is very difficult to find or develop a single evaluation scheme that can provide an accurate analysis of interdependent power-communication grids under extreme failures.

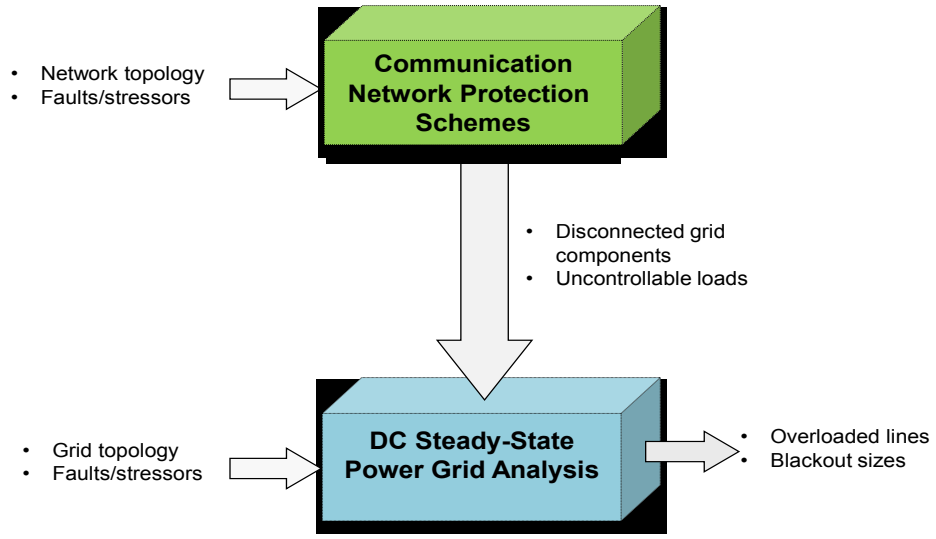

Figure 3.1: Overview of two-stage power-communication smart grid fault analysis

To address the above concerns, this thesis proposes a tractable two-step modelling approach by using a combination of network simulation and power-grid analysis, as shown in Figure 3.1. Namely, the first step uses *discrete event simulation* (DES) to determine connection failures in the communication network after a multi-failure event. Namely, this step identifies the networking nodes/links that are physically damaged by the event, and then computes the resultant grid components that lose connectivity to the NOC as a result of this damage. These disconnected components are then treated as non-controllable loads and provided as inputs (interdependencies) for the second step, which performs steady-state DC optimization analysis to compute the number of overloaded lines.

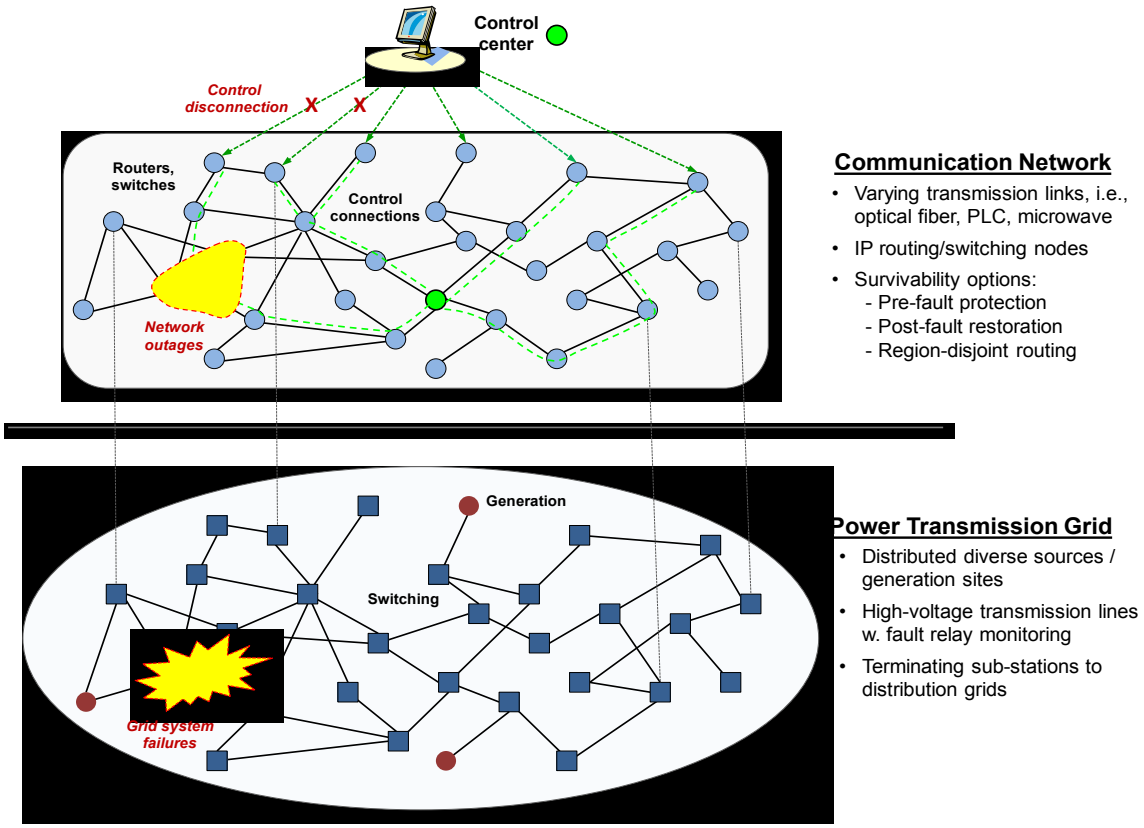

Figure 3.2: Failures in interdependent power-communication grids

Several important assumptions are noted for this solution framework. First, the fiber-based network is assumed to have the same topology as the transmission grid, i.e., switching/routing nodes placed at all transmission loads and fiber-optic cables routed along all transmission line routes. This symmetry is in-line with many of the studies noted in survey in Chapter 2. Next, it is assumed that all networking node and link failures are caused by physical damage from stressor events. Namely, further network outages (connection failures) resulting from power outages due to overloaded transmission lines (i.e., after initial damage) are not considered here, see Figure 3.2. This assumption simplifies the analysis and also facilitates an initial baseline solution against which to gauge future strategies. Moreover, this assumption is further justified by the fact that many utility operators are starting to install backup power supply units to maintain post-disaster communications. Hence the likelihood of additional network-layer outages being induced by non-physical damage will likely decline in the future, i.e., as most backup batteries will provide 2-3 days of operating power. Details on the two analysis steps in Figure 3.1 are now presented.

3.1 Network Survivability Schemes

As high-lighted in Chapter 2, many types of network survivability schemes have been developed. For the purposes herein, however, it is best to select those strategies that can provide some level of recovery guarantee and timescales. Overall, such saliencies will minimize the disruption of critical status/control information after a disaster event. As a result, proactive network *protection* schemes are chosen here to pre-compute/pre-reserve dedicated (link-disjoint) backup connection routes between all the remote transmission sites and the SCC/NOC. Namely,

upon detection of any connection failures after a physical stressor event, fast signaling/switchover actions are performed to switch communication to the backup routes, typically within sub-second timescales.

Now carefully note that some trace analyses of large-scale transmission grid blackouts have shown that cascading line failures tend to occur in the seconds-minutes range [ROS08],[TFR04]. Hence the use of rapid protection schemes will generally help minimize the occurrence of any race conditions between network (control connectivity) recovery and underlying power grid dynamics. However, transient post-fault analysis of power grids may reveal much faster dynamics (left for future study). Regardless, this would further justify the choice of faster protection strategies, i.e., as opposed to restoration methods. The various protection schemes are now presented.

3.1.1 No Protection (Baseline)

This approach routes working connections between the SCC/NOC site and all key transmission grid locations (housing buses, generators, etc). This is done in order to provide a "non-protected" baseline approach against which to compare the gains with more advanced protection schemes. Namely, the ubiquitous Dijkstra's shortest-path algorithm is used to compute the connection routes over the networking layer graph. Now shortest-path computation schemes typically require non-negative weights/costs for all links. Along these lines, two different link weighting strategies are chosen, *minimum hop count* and *load-balancing*. Consider the details.

In general, the bandwidth overheads for sending (receiving) grid statuses/commands are expected to be relatively low, i.e., in the sub-gigabit range. As a result there is very little likelihood of such overheads overloading a high-capacity control network. This further implies that all links can be treated the same here, and therefore a basic graph-based algorithm is used to find the shortest, i.e., *minimum hop count*, path between each transmission grid node and the main NOC site. In particular, let the graph $G(\boldsymbol{V},\boldsymbol{E})$ represent the communication network topology, where $\boldsymbol{V} = \{ v_i \}$ is the set of nodes (switches) and $\boldsymbol{E} = \{ e_{ij} \}$ is the set of links (C units of bandwidth capacity each). The minimum hop count path can be determined by running Dijkstra's shortest path algorithm with the link weights set to $\omega_{ij}=1$, i.e., for link e_{ij} between nodes i and j.

However, in many instances, utility providers may also re-use their fiber-optic networks to carry additional commercial bandwidth services, particularly in smaller regional markets. As these services will result in higher carried loads, more advanced "load-based" connection routing schemes can also be considered. In particular, these schemes compute *dynamic* link weights that are inversely-proportional to the bandwidth usage on the links. The aim here is to avoid links with higher weights (increased congestion levels). Again, this can be done by using Dijkstra's shortest-path algorithm with modified "load-aware" link weights computed as follows:

$$\omega_{ij} = \frac{1}{c_{ij} + \varepsilon} \qquad \text{Eq. 3.1}$$

where $c_{ij} \leq C$ is the residual (free) capacity on the link between nodes i and j, and ε is a small value chosen to avoid floating-point division errors. However, this approach also has a tendency to choose longer connection routes.

3.1.2 Basic Link-Disjoint Protection

This strategy uses a greedy approach to compute all working/backup connection pairs. Namely, a working connection route is first computed between two network nodes (e.g., NOC and grid location) using the standard Dijkstra's shortest-path graph algorithm. Subsequently, all the links along this route are pruned and then Dijkstra's algorithm is re-run to compute the link-disjoint backup path. As per Section 3.1.1 above, link weight selection can be done using either hop count minimization or load-balancing strategies.

3.1.3 Risk-Aware Link-Disjoint Protection

The link-disjoint protection scheme in Section 3.1.2 does not account for any separation between the working/backup paths. Now in general, if resource efficiency is not a major concern, it is best to choose longer path pairs with increased geographic (risk) separation. Along these lines, several "risk-based" path computation schemes have been developed in [LEE10] and [DIA12], as reviewed in Section 2.2.2. These solutions introduce and leverage the *probabilistic shared risk link group* (p-SRLG) concept to identify specific risk/vulnerability regions within a network. Namely, a p-SRLG is defined as a subset of nodes/links within a certain geographic region associated with a specific vulnerability/disaster threat. Here each such event is assigned a unique occurrence probability, along with further conditional failure probabilities for all of its associated nodes/links. For example, nodes/links closer to the epicenter of a disaster can be assigned higher conditional failure probabilities than those further towards the edge, etc. Based upon this model, various different path pair routing schemes are proposed to minimize joint

working/backup route failures. In particular, the scheme from [DIA12] is adopted here and is now detailed briefly.

Consider the requisite notation for probabilistic protection first. Foremost, a set of N mutually-exclusive stressor regions is defined for a communication network topology graph $G(\boldsymbol{V},\boldsymbol{E})$. This set is denoted as $\boldsymbol{F}=\{f_1, f_2, \ldots, f_n\}$, where each f_i represents a p-SRLG stressor. Furthermore, each p-SRLG is assigned a fixed occurrence probability ϕ_i and is comprised of a set of vulnerable links (or nodes) denoted by the set $\boldsymbol{X}_i$, usually co-located within a given geographical region. In addition, all links within $\boldsymbol{X}_i$ are also assigned independent conditional failure probabilities, i.e., p^i_{jk} for the link between nodes j and k. Using these p-SRLG definitions, the probabilistic protection scheme first computes the k-shortest paths between the NOC and each grid location/site. Again, these routes can be selected based upon minimum hop count or load-balancing objectives (as per Section 3.1.1). Next, each of these shortest paths is pruned and its corresponding link-disjoint backup path computed, i.e., thereby generating a set of k link-disjoint path pairs. Finally, the path pair with the minimum *joint* failure probability is chosen as the final working/backup connection pair to the particular grid site. Specifically, the joint conditional failure probability given stressor f_i is represented by:

$$Prob(failure|f_i) = \prod_{e_{jk}\in w}(1 - p^i_{jk}) \prod_{e_{mn}\in b}(1 - p^i_{mn}) \qquad \text{Eq. 3.2}$$

where $\boldsymbol{w}$ is the working path and $\boldsymbol{b}$ is the backup path. Namely, the end-to-end connection path failure probabilities can be written as two series product terms, i.e., due to the assumption of independent conditional link failure probabilities, see [DIA12] for more details.

3.2 Transmission Grid Fault Analysis

Transmission grid analysis takes the outputs from the previous network simulation stage, i.e., set of uncontrollable loads, and computes the final post-fault power flow and load shedding distributions, Figure 3.1. Now various algorithms have been developed to compute power flow distribution under normal working (non-failure) conditions, see [WOD96]. Further contributions have also proposed optimization schemes for failure load-shedding analysis [CAR02], and these have been applied in recent studies on interdependent grids [RAH12],[RAH13] (see Chapter 2). As a result, the work herein simply re-applies these techniques to obtain a realistic modelling of steady-state post-fault load shedding behaviors.

Consider a transmission system of a power grid with $\boldsymbol{V}$ nodes (sub-stations) interconnected by m transmission lines. The sets $\boldsymbol{L}$ and $\boldsymbol{G}$ are the set of load buses and the set of generator buses, respectively. In addition, L_j represents the demand at the load bus j. Now the well-known DC power-flow equation can be summarized as:

$$\tilde{\boldsymbol{F}} = \boldsymbol{A}\tilde{\boldsymbol{P}} \qquad \text{Eq. 3.3}$$

where $\tilde{\boldsymbol{P}}$ is a power vector whose components are the input powers of the nodes in the grid (except for the reference generator), $\tilde{\boldsymbol{F}}$ is a vector whose m components are the power flow through the transmission lines, and $\boldsymbol{A}$ is a matrix whose elements can be calculated in terms of the connectivity of transmission lines and their impedances. Since this system does not necessarily have a unique solution, an optimization approach is proposed in [CAR02] to minimize a cost function given by the following:

$$\boldsymbol{Cost} = \sum_{i \in G} w_i^g g_i + \sum_{j \in L} w_j^l l_j \qquad \text{Eq. 3.4}$$

where w^g_i and w^l_j are positive values representing the generation cost for every node in $\boldsymbol{G}$ and the load-shedding price for every node in $\boldsymbol{L}$, respectively. Now the solution to this optimization problem is given by the pair g_i and l_j (components of $\tilde{\boldsymbol{P}}$) that minimizes Eq. 3.4. Also note that $l_j = \theta_j L_j + b_j$, where b_j is determined by the optimization and θ is the load-shedding constraint, i.e., defined as the ratio of uncontrollable loads (i.e., loads that do not participate in load shedding) to the total power grid load. Namely, a value of θ=1 means load shedding cannot be implemented, whereas θ=0 means there is no constraint in implementing the load shedding. Furthermore, this formulation also assumes a high price for load shedding, i.e., loads are curtailed only due to generation inadequacy or transmission capacity limitations. Finally, various constraints are also added to bound/generate a valid solution, i.e.,

1) DC power flow equations: $\tilde{\boldsymbol{F}} = \boldsymbol{A}\tilde{\boldsymbol{P}}$
2) Limit generator powers to under G^{max}: $0 < g_i < G^{max}, \quad i \in \boldsymbol{G}$
3) Limit controllable loads: $(1 - \theta_j)L_j \leq b_j \leq 0, j \in \boldsymbol{L}, l_j = \theta_j L_j + b_j$
4) Limit power flow through lines: $F_k < C_k^{opt}$ (k=1, … , m)
5) Power balancing constraints (for power generated and consumed): $\Sigma\, g_i + \Sigma\, l_j = 0$

Note that in the above formulation, the l_j values are negative and the g_i values are positive by definition. In addition the power grid loading level—denoted by the ratio of total demand to total generation capacity—also affects the initial load (L_j values). Overall, the solution to this optimization problem determines the amount of load shedding, generation, and the power flow through the lines. Now when a failure occurs, the NOC will use the above optimization to redistribute power within the grid. If this new power flow distribution overloads certain lines,

more failures will occur, resulting in another round of re-optimization. Hence this process is iterated until no more failures occur in the system. Note that the overloading threshold of a line depends on many factors such as the capacity estimation error, which in turn can depend on the communication system efficiency.

CHAPTER 4: PERFORMANCE EVALUATION

Smart transmission grid performance under failure conditions is now tested using numerical software analysis techniques. First, the chosen network protection schemes (Section 3.1) are analyzed using DES analysis [PCH92]. These techniques are widely-used to evaluate complex networking behaviors as a series of responses to events, e.g., such a connection requests arrivals, control messages, link failures, etc. Although many network simulation tools are available, the state-of-the-art *OPNET Modeler*™ toolkit is used as it provides a complete development environment (with a full C/C++ backend) and an easy-to-use *graphical user interface* (GUI). Meanwhile, all power transmission grid analysis is done using the *MATLAB*® *MATPOWER* package. Specifically, the set of failed network connections after a failure (i.e., disconnected transmission grid loads) are inputted to the power analysis tool to determine the final DC steady-state load distributions, i.e., as per the load optimization model in Section 3.2 and [CAR02]. Full details are now presented.

4.1 Power Transmission Grid Topology

Performance analysis is conducted using the ubiquitous IEEE 118 bus transmission grid topology [IEEE118]. This topology represents a realistic regional power infrastructure in the Midwestern United States and has been widely used in many studies, as show in Figure 4.1. In particular, this configuration consists of 19 generators, 177 lines, 9 transformers, 91 loads, and

35 synchronous condensers. The latter elements either generate or absorb reactive power as needed to adjust voltages in the grid (and thereby improve the power factor) and are also treated as generators. As a result, the overall *MATLAB® MATPOWER* input case for this topology has 54 generators (i.e., 19 generators and 35 synchronous condensers), 186 lines (i.e., 177 lines and 9 transformers), and 118 buses. A revised illustration of the IEEE 118 grid showing these different components is also shown in Figure 4.2. Now as per the assumptions in Chapter 3, the fiber-optic communication network topology is also set to mirror that of the transmission grid, i.e., with routers/switches placed at all generator/bus locations and fibers routed along transmission line paths using rights-of-way. Further analysis shows that this network has a maximum (minimum) node degree of 12 (1) and an average node degree of 3.15 links/per node.

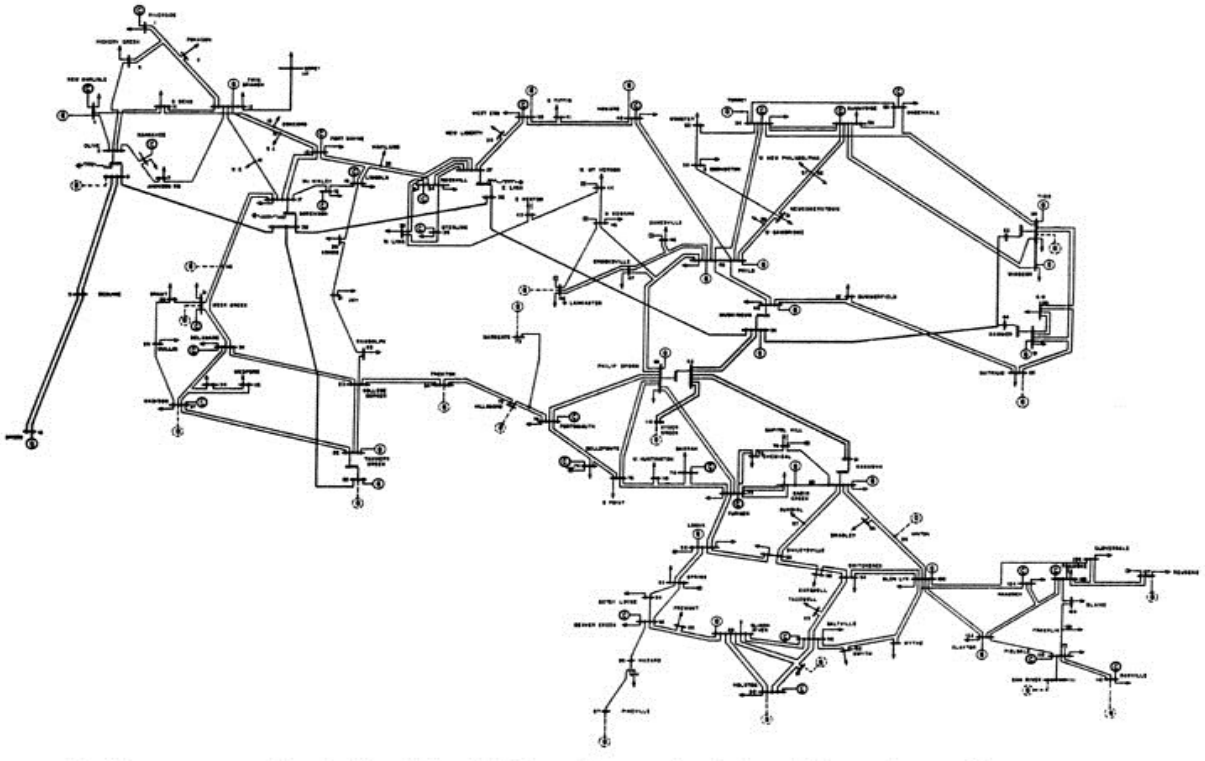

Figure 4.1: IEEE 118 transmission grid topology

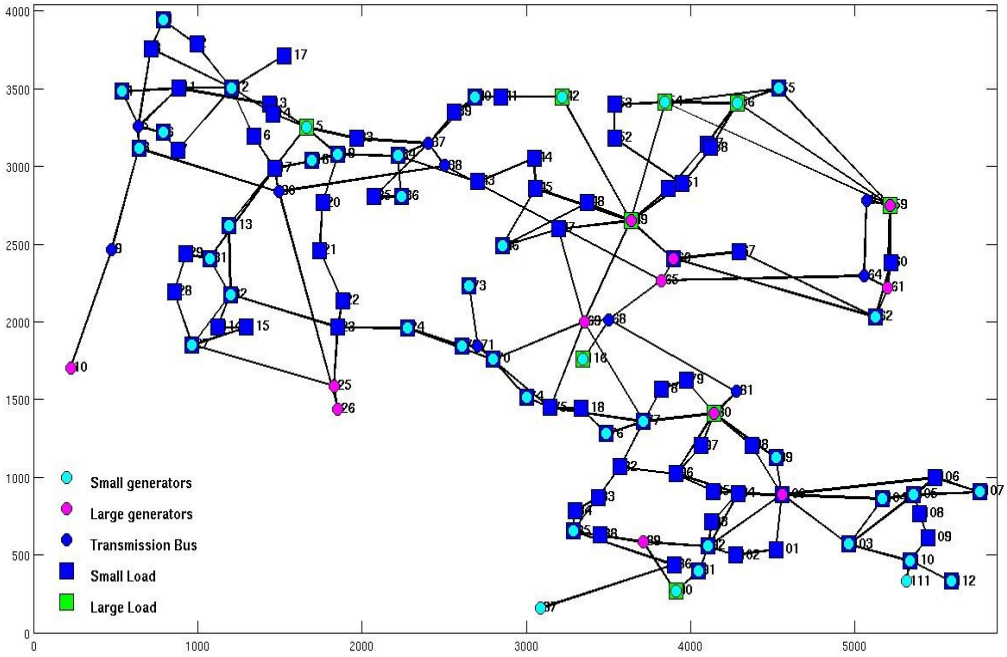

Figure 4.2: IEEE 118 transmission grid topology (alternate graphical view)

Now the overall goal of the failure mitigation strategy in Chapter 3 is to try to maintain as much control connectivity (with the centralized NOC site) after stressor events. As a result, the placement/location of NOC sites will have a direct impact on blackout sizes, along with the types of occurring multi-failure events. For example, if the NOC site is located in a high-risk region and a stressor occurs in that vicinity, then extensive blackouts will likely occur. This is treated as a rare degenerate case, and hence is not analyzed. Instead, it is reasonable to assume that the NOC locations will be placed in relatively safe regions, with minimal geographic or meteorological risk exposures. Along these lines, node 37 is chosen as the NOC location site and several probabilistic risk/vulnerability regions are defined with varying degrees of severity. Expectedly, the NOC is excluded from any of these risk regions.

4.2 Analysis Results and Findings

Sample results for the IEEE 118 transmission topology are now presented. The tests define three risk regions centered about sub-station nodes 15, 69, and 96, respectively, see Figure 4.3. Furthermore the probabilistic protection scheme [DIA10] is tested using two different a-priori failure region definitions, i.e., one in which all regions have a single node, Figure 4.3a, and another in which the regions have multiple nodes, Figure 4.3b. Note that this a-priori information is only used by the probabilistic protection scheme (Section 3.1.3) to compute protection routes.

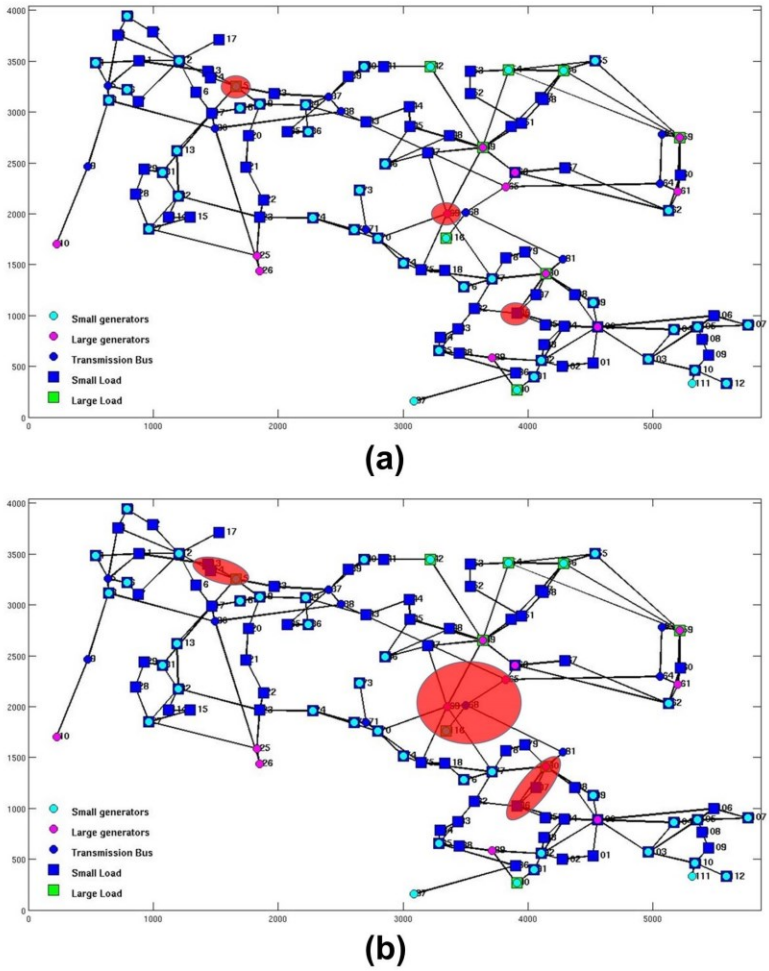

Figure 4.3: Testcase scenario with 3 failure regions

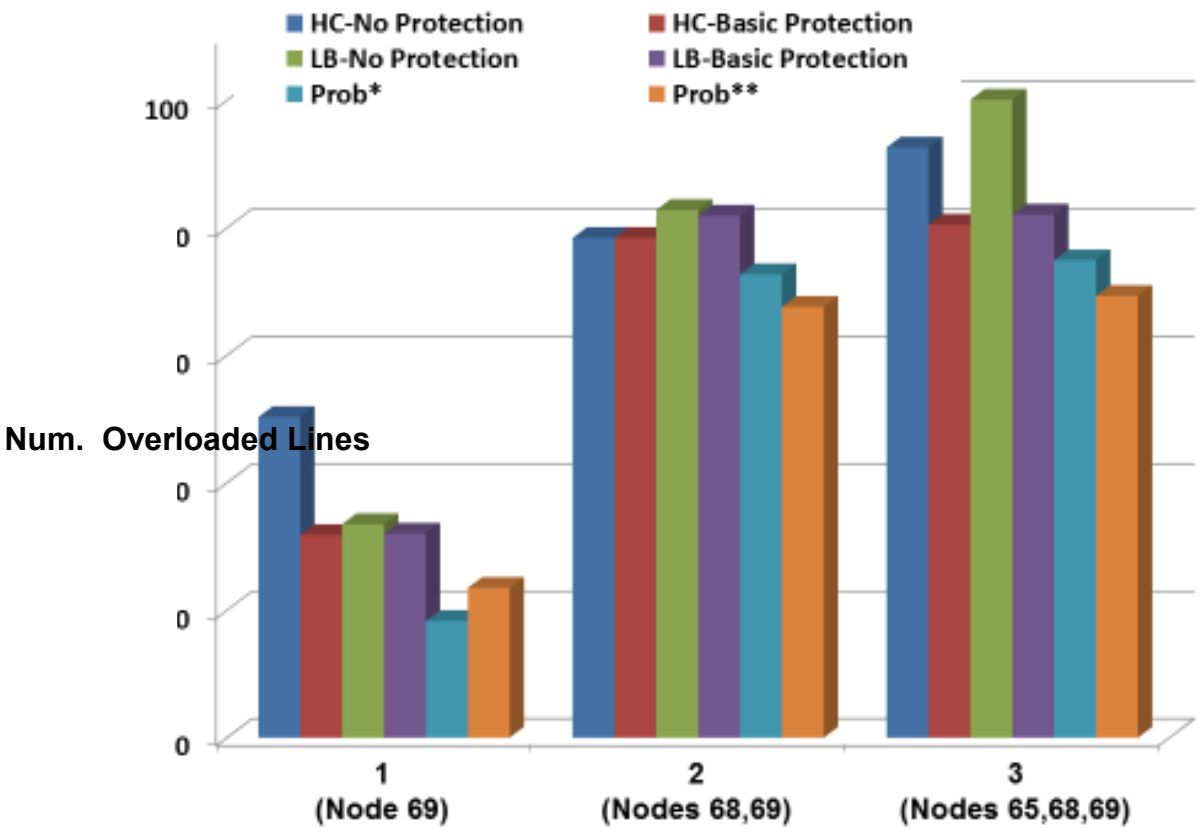

Figure 4.4: Average number of failed lines (fault center around node 69)

The first set of tests trigger failure(s) centered near sub-station node 69 with varying severity levels, i.e., 1-3 node failures. The two-stage analysis (Chapter 3) is then applied and the total blackout size measured by the resultant number of failed (overloaded) transmission lines. These findings are shown in Figure 4.4, where the labels "HC" and "LB" correspond to minimum hop count and load-balancing path computation (Section 3.1), respectively, and "Prob *" corresponds to probabilistic protection for single-node failure regions (Figure 4.3a) and "Prob **" corresponds to probabilistic protection for multi-node failure regions (Figure 4.3b). Overall, these results show a sizeable increase in the number of failed lines (load shedding) for 2 or 3 sub-station node failures, e.g., almost double those with single-node failures. In addition, these

findings also show that network protection gives some improvement. For example, basic link-disjoint protection (using both hop-count and load-balancing path computation) gives about 10-20% fewer failed lines. More importantly, the advanced probabilistic protection scheme gives the lowest load shedding results. In particular, the larger a-priori risk region definitions in Figure 4.3b (labelled as "Prob**") tend to give slightly fewer failed lines for double and triple node failures.

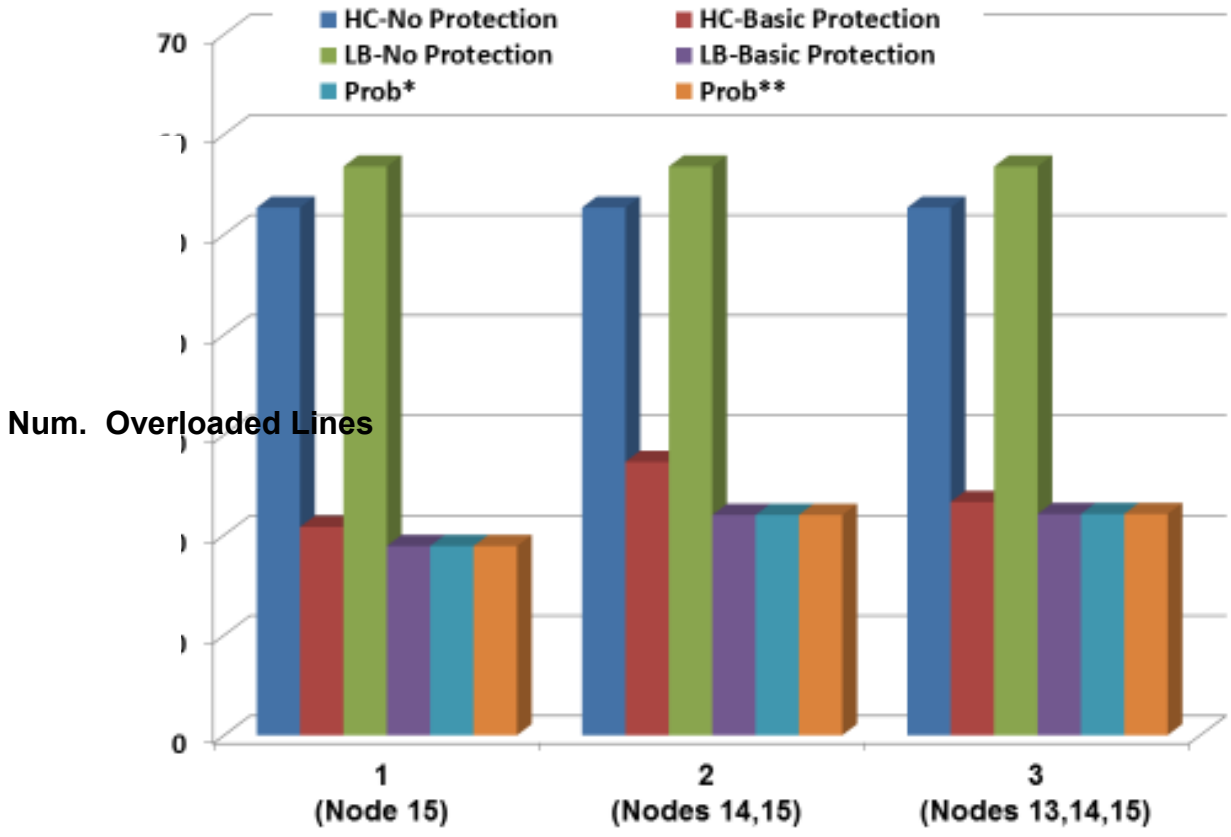

Figure 4.5: Average number of failed lines (fault center around node 15)

The above tests are now repeated for the failure region centered around node 15 with varying degrees of severity, as shown in Figure 4.5 In this case, the results show a much more

sizeable reduction in the number of failed/overloaded lines when using connection-level protection, i.e., more than 50% for single node failure. This gain is likely due to the reduced topological connectivity in this region, i.e., single node failure can affect many transiting network connection routes. However, for this very same region, the more advanced probabilistic protection scheme gives no improvements here.

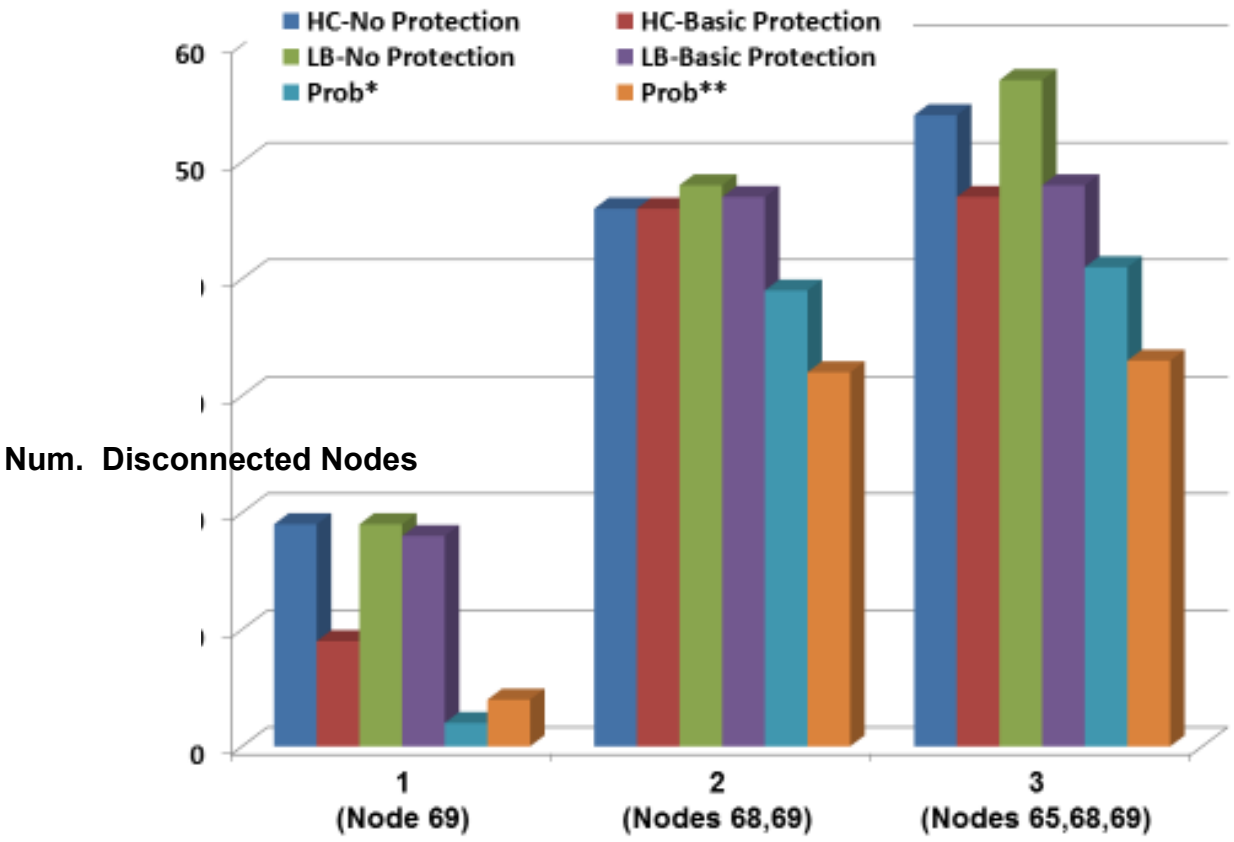

Figure 4.6: Number of failed connections (fault center around node 69)

Carefully note that the number of overloaded lines is related to the number of failed underlying communication control connections. Hence in order to get better insights of these network-level behaviors, Figure 4.6 and Figure 4.7 plot the number of failed connection routes

for the various protection schemes for failures centered about sub-station node 69 and sub-station node 15, respectively. Overall these findings reveal somewhat similar trends between the number of failed networking connections and number of overloaded transmission lines. However, expectedly there is no linear relationship here due to the highly complex nature of the interdependency between the communication and power transmission grid layers.

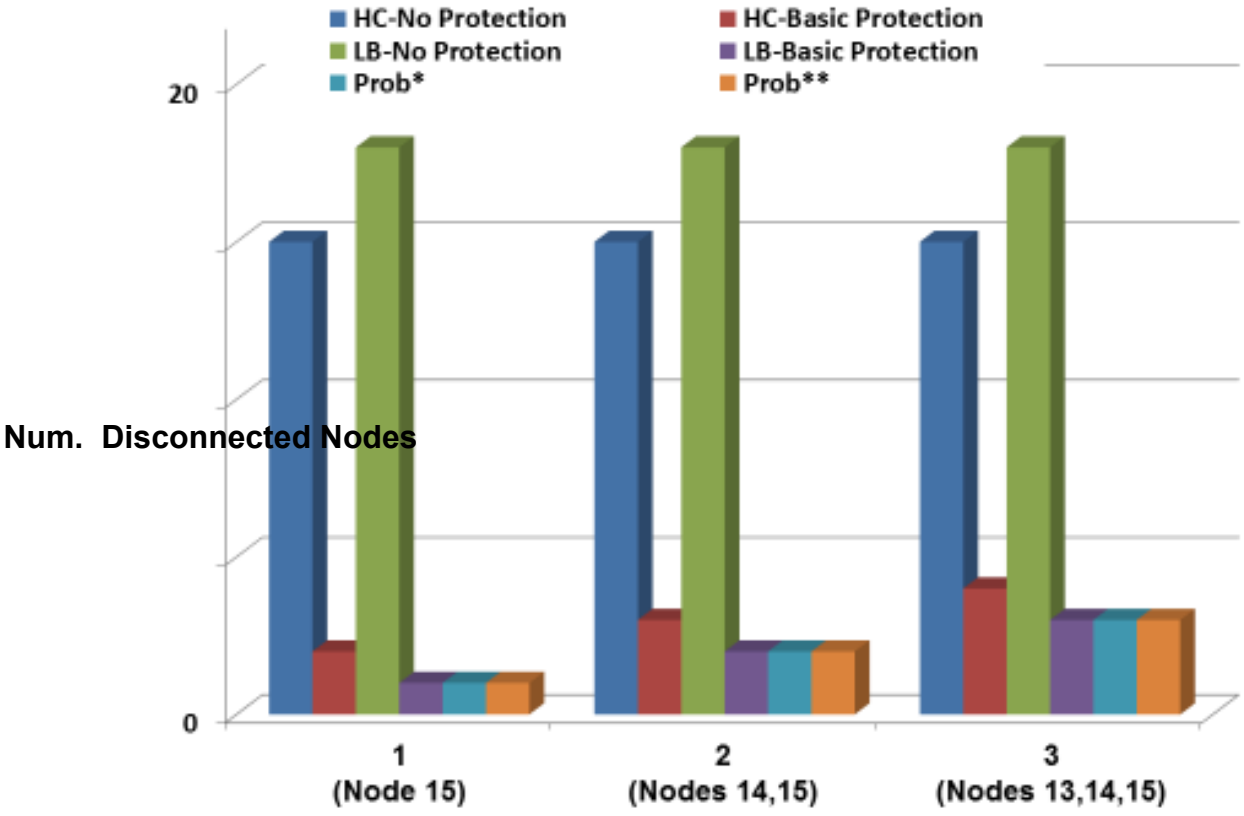

Figure 4.7: Number of failed connections (fault center around node 15)

CHAPTER 5: CONCLUSIONS AND FUTURE WORK

This thesis addresses the topic of failures in integrated smart transmission grids. The main objective here is to study the performance of various network recovery schemes in such settings and gauge their impacts on mitigating the number of overloaded lines (i.e., load shedding/blackout sizes). In general, this is a very difficult problem to study, and hence a combination of discrete-event network simulation and stochastic power-grid modelling techniques are used to provide an approximate steady-state analysis. The overall conclusions from this effort are now presented along with some directions for future work.

5.1 Conclusions

The overall findings of this study indicate that network-level protection schemes can reduce the impact of system failures in integrated smart grids. Specifically, these solutions can improve post-fault control connectivity and thereby achieve a reduction in blackout sizes, as measured via the number of failed transmission loads. In addition, more advanced probabilistic protection schemes can also be more effective here. However, these strategies require accurate pre-specification (a-priori knowledge) of randomized potential failure regions in order to provide meaningful improvements.

5.2 Future Directions

This research presents a good basis from which to extend into further studies on smart grid survivability design. Foremost, few studies have looked at modelling the detailed *transient* nature of cascading failures in power grids, i.e., at second or sub-second timescales. Hence it is important to study if rapid network recovery schemes (operating in the milliseconds-to-sub-seconds range) can affect such transient behaviors. In addition, broader studies can also look at designing more resilient networking topologies for smart transmission grids. In general, increased node degrees will provide better post-fault connectivity (and hence load controllability). However, in real-world settings one cannot arbitrarily change or expand network-layer topologies to increase node-level connectivity. Instead, such build-outs are usually deemed as longer-term undertakings and generally planned (optimized) according to a range of factors, i.e., such as cost, policy constraints, geographic settings, etc. Along these lines, future efforts can also look at constrained (and optimized) design of network control topologies design to minimize cascading behaviors. The use of mixed networking technology types, e.g., wireless and fiber-optic, can also be considered here.

REFERENCES

[BLD10] S. Buldyrev, *et al*, ``Catastrophic Cascade of Failures in Interdependent Networks", *Nature Letters*, Vol. 464, February 2010, pp. 1025-1028.

[CAR02] B. Carreras, V. Lynch, I. Dobson, D. Newman, "Critical Points and Transitions in an Electric Power Transmission Model for Cascading Failure Blackouts", *CHAOS*, Vol. 12 No. 4, 2002, p. 985-993.

[CAS13] J. Castet, J. Saleh, ``Interdependent Multi-Layer Networks: Modelling and Survivability Analysis with Applications to Space-Based Networks", *PLoS ONE*, Vol. 8, No. 4, April 2013.

[CHL07] P. Chołda, A. Mykkeltveit, B. Helvik, O. Wittner, A. Jajszczyk, "A Survey of Resilience Differentiation Frameworks in Communication Networks", *IEEE Communications Surveys and Tutorials*, Vol. 9, No. 4, 4th Quarter 2007.

[DIA12] O. Diaz, *et al*, ``Network Survivability for Multiple Probabilistic Failures", *IEEE Communications Letters*, Vol. 16, No. 8, August 2012, pp. 1320-1323.

[HP2012] D. McGhan, “Sandy: An Eye-Opener for the Power Grid”, *The Huffington Post*, Nov. 26, 2012, see http://www.huffingtonpost.com/daniel-mcgahn/power-grid_b_2192554.html.

[IEEE118] “Case 6 – IEEE 118 Bus Systems”, http://publish.illinois.edu/smartergrid/case-6-ieee-118-bus-systems/

[KHA14] S. Khaitan, J. McCalley, C. Liu, *Cyber Physical Systems Approach to Smart Grid Power Systems*, Springer, 2014.

[KIM12] K. Kim, P. Kumar, "Cyber-Physical Systems: A Perspective at the Centennial", *Proceedings of the IEEE*, Vol. 100, May 2012, pp. 1287-1308.

[LEE10] H. Lee, E. Modiano, Kayi Lee, “Diverse routing in Networks With Probabilistic Failures”, *IEEE/ACM Transactions on Networking*, Vol. 18, No. 6, December 2010, pp. 1895-1907.

[NEU13] S. Neumayer, E. Modiano, ``Assessing the Effect of Geographically Correlated Failures on Interconnected Power-Communication Networks", *IEEE SmartGridComm 2013*, October 2013, Vancouver, Canada.

[NP13] “Catastrophic Ice Storm’ Slams into Toronto, Strands Travellers Across the Province”, *National Post*, December 22, 2013.

[PAR13] M. Parandehgheibi, E. Modiano, ``Robustness of Interdependent Networks: The Case of Communication Networks and the Power Grid," *IEEE GLOBECOM 2013*, Atlanta, December 2013.

[PCH92] U. Pooch, *Discrete Event Simulation: A Practical Approach*, CRC Press, 1992.

[RAH11] M. Rahnamay-Naeini, *et al*, ``Modelling Stochastic Correlated Failures and Their Effects on Network Reliability," *IEEE ICCCN 2011*, Maui, Hawaii, August 2011.

[RAH12] M. Rahnamay-Naeini, Z. Wang, A. Mammoli, M. Hayat, ``Impacts of Control and Communication System Vulnerabilities on Power Systems Under Contingencies", *IEEE Power and Energy Society General Meeting*, San Diego, CA, July 2012.

[RAH13] M. Rahnamay-Naeini, M. Hayat, ``On the Role of Power-Grid and Communication-System Interdependencies on Cascading Failures", *IEEE Global Conference on Signal and Information Processing 2013*, Austin, TX, December 2013.

[RAM99] S. Ramamurthy, B. Mukherjee, "Survivable WDM Mesh Networks, Part II — Restoration," *IEEE ICC 1999*, pp. 2023–30.

[ROS08] V. Rosato, *et al*, ``Modelling Interdependent Infrastructure Using Interacting Dynamical Models", *International Journal of Critical Infrastructures*, Vol. 4, No. 1/2, 2008, pp. 63-79.

[TFR04] “Final Report on the August 14, 2003 Blackout in The United States and Canada: Causes and Recommendations”, *U.S.-Canada Power System Outage Task Force Report*, April 2004, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/ BlackoutFinal-Web.pdf.

[WOD96] A. Wood, B. Wollenberg, *Power Generation, Operation, and Control, 2nd Edition*, Wiley Press, New York, NY, 1996.

[WU92] T. Wu, *Fiber Network Survivability*, Artech House Publishers, 1992.

[XU11] F. Xu, M. Esmaeili, M. Peng, N. Ghani, “Multi-Domain Restoration with Crankback IP/MPLS Networks,” *Optical Switching and Networking*, Vol. 8, No. 1, January 2011, pp. 68-78.

[YAN13] Y. Yan, Q. Qian, H. Sharif, D. Tipper, ``A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges", *IEEE Communications Surveys and Tutorials*, Vo. 15, No. 1, 2013, pp. 5-20.

[ZHU00] D. Zhou, S. Subramaniam, “Survivability in Optical Networks”, IEEE Network, Vol. 14, No. 6, November/December 2000, pp. 16-23.

ABOUT THE AUTHOR

Sankalp Mogla graduated from Punjab Technical University with a Bachelor's of Technology in Electronics and Communication Engineering in 2011. He is currently pursuing his Master's of Science in Electrical Engineering at University of South Florida as a Graduate Research Assistant.