Dynamic Probabilistic Network Protection in Large-Scale Failure Scenarios

By

Alireza Izaddoost

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of

Doctor of Philosophy

in

Computer Science

Faculty of Business and Information Technology

University of Ontario Institute of Technology

January 2015

Abstract

Large-scale failure resulting from natural disasters or intentional attacks is now considered a serious risk for communication network infrastructure. In these events, simultaneous damages in several links and nodes may cause substantial loss of information, which can be very costly for governments, subscribers and businesses. The impact of natural disasters generally is probabilistic in nature. Geographical characteristics and the distance of the components to the centre of the disaster may change the failure probability. Considering the probabilistic failure feature in natural disasters and the possible vast area coverage, we aim to develop a probabilistic dynamic model to protect data from failure and maintain undisrupted network services in large-scale failure scenarios. For this purpose, we develop a preventive protection model, which is able to estimate the potential destruction of all the network components in different locations. Using this information, the proposed model has a holistic view of the failure probabilities for the different paths to make a decision to reroute traffic from the endangered routes through the more reliable paths prior to the failure. As the proposed model protects data before failure, the size of damaged traffic will decrease and fewer connections need to be restored. The proposed preventive model is able to adjust rerouting decision parameters in a dynamic way by considering the disaster expansion and available network resources at each decision interval. Our findings show that the proposed preventive protection model significantly reduces the average number of disrupted connections and successfully decreases the required network restoration time. The performance of the proposed model has been examined in software defined networking (SDN), which is one of the emerging technologies in communication

networks. We studied the performance of a SDN controller instructed with a considerable amount of data flow updates and the best method of applying preventive rerouting is indicated.

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Prof. Shahram Shah Heydari, for his supervision, guidance, and continued support throughout my research. I would like to thank him for his motivation, immense knowledge and insightful discussions that helped me to accomplish this thesis.

I would like to extend my appreciation to my committee members; Prof. Khalil El-Khatib, Prof. Miguel Vargas, Prof. Walid Morsi and Prof. Isaac Woungang for evaluating my thesis and providing their invaluable comments and feedbacks.

I also wish to thank the University staff for their assistance and generous help and administrative support.

I gratefully thank Ericsson Canada, NSERC, Mitacs Canada, Feddev Ontario and Esri Canada for their financial support during my study.

I would like to thank my friends Roozbeh Jalali, Eduardo Luengo, Chris Weber, Dr.Saeed Astaneh and Dr.Kevork Hacatoglu for their encouragement and support throughout my research.

Finally, I would like to express my greatest gratitude to my mother, my sister and my dearest “Merida” for their unconditional love and support during my study.

TABLE OF CONTENTS

List of figures

List of tables

Abbreviations

MPLS	Multiprotocol Label Switching
WDM	Wavelength-Division Multiplexing
SDN	Software Defined Network
SRLG	Shared Risk Link Group
PDR	Packet Delivery Ratio
QoS	Quality of Service
SLA	Service Level Agreement
CBR	Constraint Based Routing
LSP	Label Switched Path
MLW	Modified Link Weight
MTR	Multi-Topology Routing
EON	Elastic Optical Network
ILP	Integer Linear Programing
INLP	Integer Non-Linear Problem
IQP	Integer Quadratic Programming
LLDP	Link Layer Discovery Protocol
BFD	Bidirectional Forwarding Detection
OSI	Open System Interconnection
LSR	Label Switching Router

Chapter 1: Introduction

Over the last few years, the exponential growth of network services has provided connectivity for hundreds of millions of systems, devices and users. The original purpose of the Internet for remote system access has expanded with emerging important applications such as social networking, e-commerce, voice over IP and many more, making it part of our daily lives. Many of those applications such as online banking and online trading are time-sensitive and critical to businesses and governments. The widespread and growing online demand reveals the importance of having a fast communication network to provide high quality data transport at minimum time. To achieve this target, data transfer in the Internet backbone is mainly relying on fiber optic technology because of features that make it an ideal platform for this purpose. The current optical technology allows transferring a massive amount of data (up to 100 Gbps) in each lightpath [1]. Besides the widespread fiber optic connections on land, the world's continents are connected together using submarine communication cables to transfer huge amounts of data all over the world (Figure1). The combination of all these mediums together forms the backbone of Internet infrastructure in large-scale geographical areas.

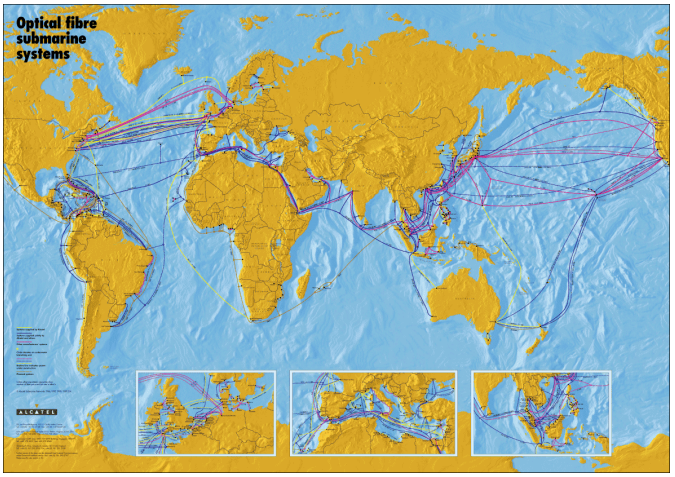


Figure1. Long-haul submarine cable maps.

Several factors such as accidental cable cuts, natural disasters or explosions can cause damage to physical links. Such damage may affect lightpaths carried by the link and result in substantial losses of information that can be catastrophic, affecting banking, business operations, health care, air lines and more. As a result, industry and the public who rely on the Internet infrastructure require a high degree of reliability in the backbone network. A resilient network should be able to provide and maintain an accepted level of service and operation continuity in face of failures.

1.1 Background and Motivation

Network failure recovery has been the subject of many research efforts in the past three decades and several models have been proposed to address this issue. Most studies regarding network resiliency in the past focused primarily on network restoration in cases of single or double failures. However with ever-increasing reliance on network-based services in today's society, the issue of network resilience in large-scale failure scenarios has started to gain a great deal of attention. Natural disasters such as earthquakes or power outages may cover a vast area and the impact of such disasters on the physical communication infrastructure would cause large-scale network service failures. In this event, simultaneous damages to several links and nodes may cause substantial loss of data, which can be very costly for governments, subscribers and businesses. For example, the Taiwan earthquake in December 2006 [2] resulted in several simultaneous undersea cable cuts, causing a major communication disruption in parts of Asia for several weeks. Another research project studied network service disruption and its consequent effects after Hurricane Katrina – one of the most destructive Atlantic hurricanes ever [3]. This study measured the impact of Hurricane Katrina by analyzing network services disruption

caused by the disaster. For this reason, survivability of critical infrastructure systems and continued, undisrupted network operations in the presence of large-scale failures has become a major concern for communication network operators.

Although IP routing protocols are able to compute alternative paths and reroute traffic in failure scenarios, they are too slow for carrier-grade restoration. To reduce required network restoration time and reroute traffic as fast as possible, recovery approaches should be applied to the network backbone, where routing mostly relies on methods such as Multiprotocol Label Switching (MPLS) or Wavelength-Division Multiplexing (WDM) lightpaths. In this research we assumed, without loss of generality, an MPLS-based network, however this model is applicable to many other connection-based or flow-based routing protocols such as software defined network SDN, which we discuss in further detail later in this thesis

While there have been a number of studies on large-scale failures in communication networks, most of these works have taken a static view of failures. A common assumption among previous studies is that the failures are independent and consecutive failures will not happen at the same time [4-7]. However, the above assumption is not valid in large-scale failure scenarios. For instance in natural disasters such as earthquakes or large-scale power outages, failure may cover a vast geographic area. These types of failures are geographically correlated, where the failure event usually starts from an epicentre and expands during a limited time across the region. Figure 2 shows an example of regional, dynamically expanding large-scale failures. The failure risk of a network component in these events depends on the distance of the component to the epicentre and also the intensity of the disaster. In this situation, simultaneous failures in network components can happen in the vicinity of the epicentre. The impact of natural disasters is probabilistic

in nature.

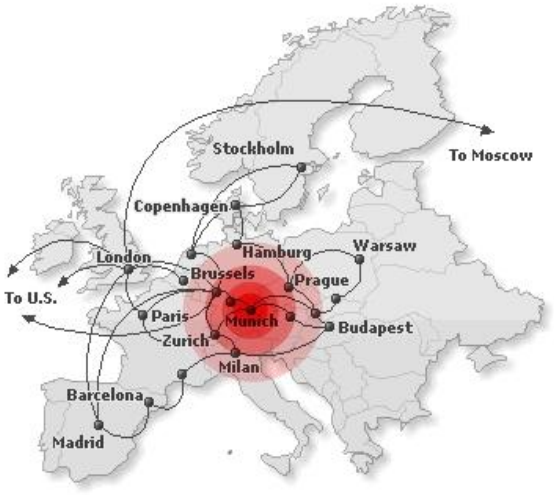


Figure 2. Large-scale regional failure.

Geographical characteristics and the distance of the components to the centre of the disaster may change the failure probability. This means that the failure risk for different components may not be equal and therefore the failure model should take into account the likelihood of component failure. Considering the probabilistic nature of failures and the wide area vulnerable to disasters in large-scale failure scenarios, we need a restoration framework that provides guidelines to network operators and supplies appropriate solutions to reduce the damaging effects of disasters.

The lack of reported results in large-scale failure scenarios motivated us to examine network survivability issues in backbone networks with a dynamic probabilistic model that not only considers the time-varying dynamics of regional disasters (for example the expanding impact zone of earthquake as it spreads), but also takes into account the probabilistic nature of failures resulting from such events. To develop such an approach, the first step is to answer an essential question as to how to fortify the network to withstand failures caused by disasters. To answer this question, we will provide the

detailed problem statements and the targeted objectives in the next sections.

1.2 Problem Statement

Damaged critical infrastructures in the regions affected by natural disasters or nuclear explosions require fast recovery action to restore the disrupted services. Since the failures caused by disasters do not follow a deterministic pattern, the damage may be different from one to another. This characteristic reveals a need for dynamic methods to protect network services and prevention of data destruction corresponding to the severity of disasters. In any proposed solution, it should be considered that network components in the impact range would not all necessarily become nonfunctional, and that failures may happen with different probabilities. In this situation, the problem is to develop a dynamic network protection model based on a set of initial information such as regional geographical data and disaster intensity, which should be able to evaluate the risk of disruption continuously and dynamically and take appropriate actions

To address this issue, the proposed model should be able to use information derived from the network to calculate the probability of failure for each network components and reach a pattern that can be used to determine the degree of vulnerability to the ongoing disaster in each network region. This kind of model should not rely merely on static information such as earthquake prone zones, but should take into account dynamic information such as disaster impact epicentre location and its velocity of expansion as the disaster is unfolding. We believe the typical disaster expansion times – from between 20-80 seconds for earthquakes [8] to longer times for hurricanes and other natural disasters – would give sufficient time to at least salvage some endangered network connections before they are disrupted. Eventually, a clear decision can be employed to reroute traffic

of the endangered locations through more reliable paths with less failure probability and protect them against upcoming failures. Thus the number of network components involved with transferring data that are going to be destroyed by the disaster will be reduced and the size of the affected traffic will be minimized.

An appropriate decision making approach to detect endangered or safe areas in the network topology should consider network infrastructure availability at the time of study. Based on available resources on the network, decision parameters should be able to adjust themselves to provide adequate levels of protection without extra burdens on network performance. Along with disaster expansion and changes in the network topology, the above parameters should be adaptable in tune of network requirements. By decreasing the size of affected traffic, fewer flows will be damaged that would need recovery. Fewer flow failures means less restoration time and decreasing network disruption time, which is one of the most important objectives in designing a resilient network.

Furthermore, the emerging SDN technology shows a clear lack of an effective protection method in large-scale failure scenarios. Our approach is particularly suitable for SDN networks as there are included features such as central network controller and OpenFlow protocol, which can facilitate implementation of proactive flow rerouting as a result of data flow risk analysis. Implementing the proposed approach as a specific software (application) for disaster events to instruct the controller to apply protection policies and proactive rerouting patterns may improve network resiliency in large-scale failure scenarios.

1.3 Methodology

Given the described shortcomings of current protection approaches, the selected method should be able to protect network flows in large-scale failure scenarios. The proposed method in this research is capable of calculating failure probability for network components in a disaster zone. Based on this ability, the proper action to protect high risk flows will be taken. Our proposed algorithm can be implemented in a manner that coincides with widespread destruction and damage to the network as well as likelihood of future damages and adapts itself to improve network resiliency in large-scale failure scenarios. To evaluate the effectiveness of the proposed algorithms, the selected methods are simulated on real-world topologies using MATLAB software. The focus of this research is to reduce the number of disrupted connections and decrease the required restoration time rather than evaluating network efficiency in a packet level view. MATLAB is fully capable of studying the aforementioned metrics with high precision and is therefore a suitable tool to simulate our proposed methods. In simulation models, network performance is evaluated at discrete time intervals and at each inspection time, the deviation of metrics such as the number of disrupted connections and the required restoration time are investigated. To evaluate such metrics, topological properties at each inspection interval time are taken into account to update involved parameters in the simulated algorithm by MATLAB.

1.4 Research Objectives

The main goal of designing a survivable model in large-scale failure scenarios is to maintain the network service undisrupted. To achieve this goal we are looking to meet these objectives:

- Design and develop a probabilistic preventive protection technique to protect information by rerouting traffic from endangered locations prior to the failure in large-scale failure scenarios.
- Develop a probabilistic failure model to calculate the failure probability, considering wave-like behaviour as a common attribute among disasters.
- Conduct sensitivity analysis with regard to risk decision parameters assignment in a preventive model and examine network behaviour under different values.
- Design and develop a self-adaptive mechanism to adjust risk parameters dynamically in tune with network requirements and resources availability and validate the proposed model by simulating real-world networks.
- Study network performance such as restoration time and disruptive connections in deterministic and probabilistic large-scale failure scenarios and provide a comparison to show how the selected failure model can affect network performance. Design a preventive protection model for SDN architecture to enhance network protection in large-scale failure scenarios and study the proposed protection approach in an experimental test-bed.

1.5 Research Contributions

Our contributions in this thesis are as follows:

- A comprehensive study of network protection in large-scale failure scenarios is provided. Protection approach considering deterministic and probabilistic failures in different disaster scenarios have been studied and network performance for each protection approach is evaluated.
- A wave-like model to estimate failure probability for network components in disaster scenarios is developed. The proposed model is able to determine risk failure probability for links and nodes in the network that encounter a disaster.
- A proactive approach to prevent damage of endangered traffic in a disaster zone is elaborated. Considering this approach as a main contribution in this thesis, the proposed preventive protection model is able to protect high risk flows using a dynamic proactive mechanism to reroute traffic through safe areas prior to failure.
- Risk decision parameters associated in preventive protection model are examined and an analysis for different risk decision parameter assignments is provided.
- An automated approach to assign risk parameters for a preventive model is developed. In this way, the proposed protection model is able to adjust rerouting risk parameters based on the required level of protection and the potential risk failure in each interval inspection.
- A proactive protection model in large-scale failure scenarios for an SDN network is designed and an experimental model to study network performance through instructing the controller with a considerable number of required preventive rerouting is developed.

1.6 Thesis outline

In chapter two we present an extensive study of previous works in network protection and failure recovery. The reviewed literature is studied under four different categories; deterministic failure models, probabilistic failure models, enhancing network resiliency using topological parameters and proposed recovery approaches in SDN. Chapter three explains network protection and failure models. In this chapter, the effect of probabilistic approach on the network and restoration mechanism is explained and a model to assign failure probability in wave-like disasters is examined. Network performance using several simulation models studies the effect of deterministic and probabilistic failure in different disaster scenarios. In chapter 4, we present a preventive protection model to enhance network resiliency in large-scale failure scenarios. Rerouting strategy and risk decision parameters are discussed in this chapter and the performance of the proposed model is evaluated under different failure scenarios. Chapter 5 investigates the effect of risk parameters adjustment on network performance and provides a procedure to study an extensive range of possibilities in risk decision parameters adjustment and the effect of each model on network is evaluated. In chapter 6, we improve the preventive protection model by providing a self-adaptive approach to keep network decision adaptable with network conditions. We describe a model that adjusts risk decision parameters dynamically in tune with network requirements. Design a protection model in SDN network using the preventive protection mechanism is discussed in Chapter 7 and the controller performance in response time to update a number of considerable data flow paths is evaluated. Chapter 8 concludes the research and presents possible future works.

Chapter 2: Literature review

To improve the stability of a network and enhance network resilience, it is necessary to increase the ability of the network to cope with failures, which is commonly termed "network survivability". For this purpose, many approaches have been proposed in the literature over the past three decades. We focus primarily on network survivability in large-scale failure cases.

In general, the prior work can be grouped into two different aspects of spreading failures and outcome damages in the network. One approach is a deterministic view of failures in which all network components in the affected region will become definitely inoperative and will not have any chance of maintaining functionality. In the other approach, a probabilistic destruction view is applied in which a network component has a chance to survive the disaster and continue operation. Depending on how failure behaviour is considered, the proposed method to improve network protection may be different. Both approaches have provided valuable results and will be reviewed in the following.

As software defined networking (SDN) is an emerging technology and of interest to researchers in both academia and industry, we have dedicated a separate subsection to review and discuss some recent works in SDN and its contribution to network survivability.

2.1 Network resiliency with deterministic failure view

A number of restoration methods and recovery time studies in large-scale scenarios have been presented in the literature. Path restoration performance in large-scale failure scenarios have been studied in [9]. In that work, a basic regional large-scale failure model

was developed and network capacity requirements and failure notification time were analyzed using simulation. The authors noted that in a highly mesh network, a fairly small extra spare capacity in the network could provide a high ratio of restoration for affected demands in regional large-scale failures. The study used a circular impact with fixed radius as a model for regional failures.

Categorizing links in a Shared Risk Link Group (SRLG) is an attempt to provide a measure of failure dependency into the scenarios. The SRLG model attempts to group together links or nodes that share common failure risks. Such risks can be shared ducts, power sources, or geographical area. SRLG disjoint path pairs is an approach to improve network resiliency by reducing the risk of a backup path failure. In this case, there is no bandwidth sharing between protection paths. The proposed models intend to solve a min sum problem [10, 11].

In [12] the authors considered one type of shared resource called "region." All links in a region belong to one SRLG and failure in this region causes failure of all of the links. The authors applied this approach to model the impact of earthquakes. The divided regions in the network topology were mapped to the different seismic zones. The seismic map was used in the SRLG assignment and each zone formed its own risk. Because individual seismic zones were large, the authors expected an earthquake to affect one region only, and they divided each zone to have multiple SRLGs. This method was applied to minimize the number of shared SRLGs between the working and backup paths, using a seismic map of an earthquake as an example of a natural disaster scenario that created large-scale correlated component failures. However, pre-planned protection methods required a substantial amount of spare capacity in case of large-scale failure.

In studying the damage levels caused by large-scale failures, packet delivery ratio is

one of the metrics to evaluate degradation of network performance. The authors in [13] showed that increasing the number of impacted network devices in a large-scale failure scenario and deterministically eliminating them significantly decreases the ratio of the number of packets sent from the source to the packets received on the destination side. The authors examined three area-based failure scenarios named scaling circle, moving circle, and scaling polygon. The failure scenarios were simulated using the NS-3 network simulator [14]. The authors introduced a regional large-scale scenario called "scaling circle" to model electromagnetic pulse attacks. The failure of components started from a centre and expanded with a constant velocity in every simulation time. The results showed how the type and strength of the impact, such as the number of damaged network equipment and the coverage of the affected area in large-scale failure directly affects network performance. The authors simulated scaling circle by expanding the failure impact radius and calculating the lost aggregate packet delivery ratio (PDR). In this study it was assumed that as the impact radius increased, all nodes and links within the impact area are failed. PDR was computed and the relationship between the PDR drop and the number of failed links and nodes in the circle was studied.

Assessing network vulnerability was studied in [15] and failures were modeled as a line segment or disk shape. This study indicated the most vulnerable locations in the network where disasters could have maximum damage and degrade network efficiency significantly. The authors employed a polynomial-time algorithm to identify the worst-case line segment and circular cut where any network components intersected by the failure would be destroyed.

A design for survivable networks with multi-path routing was developed in [16]. The authors developed an end-to-end protection switching called self-protecting multi-path,

which used several disjoint paths to carry traffic between the source and destination. This approach allowed for load distribution in failure events. In the proposed model, if the network failure affected a partial path, only traffic on the affected path should be rerouted. In the normal situation, the traffic was distributed according to a load balancing function through available parallel paths that might have different lengths. In a failure event, another load balancing function redistributed the traffic of the affected path among the other available working paths. The authors measured required spare capacity and showed that the proposed model improved network resiliency with less extra capacity requirement in failure scenarios. The proposed load balancing function was optimized by minimizing the maximum link utilization of all protected failure scenarios [17].

Connection availability can be considered an important metric to calculate Quality of Service (QoS) in a survivable network [7]. The authors assumed that different connections may have different availability requirements, which are typically based on the agreement between a service provider and a customer. Considering this requirement, they developed a dynamic connection provisioning for single-failure scenarios, where network component failures might happen independently. The proposed model based on Service Level Agreement (SLA) requirement provided three service models: no protection, shared-path protection, or dedicated protection to an incoming connection. The authors mentioned that maximizing backup-sharing could decrease the value of the cost function but could also decrease connection availability. To address this issue they limited backup sharing to improve availability.

Random regional failure was modeled as a disk shape cut to study network survivability in geographically correlated failure scenarios in [18]. The authors developed a model based on region-disjoint, self-protecting, multipath routing based on a load

balancing mechanism. The proposed model sets up two or more working paths in an MPLS network and route traffic with a different ratio between them. The available spare capacity in each working path could be used to backup each other in failure scenarios. Numerical results studied in two real network topologies, the U.S network and NFSNET, and a comparison was provided for three different disjoint routing models: multiple node-disjoint paths routing, multiple region-disjoint paths routing, and self-protecting multi region-disjoint paths routing. Network throughput as a metric of network efficiency was studied in multipath routing in both protected and unprotected forms.

Multiple region fault models were studied in [19] for connectivity issues in a wireless environment. The authors mentioned that failures in a network could be considered locally and they developed a model based on region-disjoint paths. The maximum number of region-disjoint paths and minimum region cut were found by two heuristic algorithms. The authors employed region-based connectivity as a new metric in [20] to involve the concept of locality in network fault-tolerance ability and extended the resiliency study from single-region failure to multiple regions.

Authors in [21] proposed a measurement of network resiliency to develop a model in computer network management. The proposed resilience factor considers network topology aspects such as number of redundancies and also the amount of traffic losses in failure scenarios. The proposed metric can be used by network managers to support decision making regarding the design of a new network or improve the performance of the operational network. The proposed model was simulated in the Brazilian National Research Network (RNP), and by employing a resilience factor, they analyzed how changes in the topology affect the network and its traffic.

A path restoration solution with quality of service consideration and label constraints

in MPLS networks was developed in [22]. The authors considered constraint based routing (CBR), which is a combination of shortest path first algorithm and network resource information such as link capacity or available bandwidth. The proposed model maximized network operation in different classes of traffic in both 1+1 and 1:1 protection mechanisms. In 1:1 method, low priority traffic (in this case best effort) was routed through the backup path prior to the failure events. The optimization problem in this article considered traffic engineered Label Switched Paths (LSPs).

MPLS fault management consists of three methods: global backup, reverse backup and local backup. Some factors in quality of services such as packet loss, restoration time and resource consumption could be considered to select an appropriate recovery method in an MPLS network [23]. In different scenarios with varying traffic classes based on Diffserv, different weights can be assigned to the packet loss, restoration time, and resource consumption. A function of these parameters was employed to compute and recommend the best backup protection approach.

Path diversification is a mechanism to achieve maximum flow reliability between source and destination nodes using a diversity measure [24]. The idea of using path diversification is extended to develop the path geo-diversification approach [25]. The proposed model considered geographical diversity of physical network topology to route traffic. The main objective in this research is to route the traffic around the endangered area by determining vulnerable locations in the network and estimating the disaster boundaries. The authors assumed that there is available exact information about the damage or some sort of estimation. To select an alternative path with acceptable distance as the backup path, the proposed algorithm considered different possibilities. If the disaster boundary is known, traffic would be routed through a path outside the challenge

area. If only an estimate of the disaster location is available, an ack request field which is added to the routing header, will be employed to route traffic through the nearest geographically diverse path. If there is no estimation about disaster and only occurrence of disaster just been notified, the ack request is set to true for all the packets sent out for next-hop acknowledgment.

The above approach is improved by providing two heuristics for solving the path geodiversity problem [26] and reduce the complexity of the proposed model in [25]. The WayPoint Shortest Path (iWPSP) algorithm selects viewpoints with a specific distance to a middle node on the shortest path between source and destination and employs Dijkstra's algorithm to find the geodiverse path. In the Modified Link Weight (MLW) heuristic, the algorithm modifies the link weights and using Dijkstra's algorithm determines the geodiverse path. The distance value *d* would be provided as a user value, and during the disaster events, users can modify *d* based on determined disaster models to pass traffic around disaster zone. In a simulated model, it is assumed that the disaster zone is 50 km and the proposed model can reroute traffic outside the danger zone. The results of PDR and delay compared to standard OSPF.

Backup path selection in our proposed model compared to [25, 26] is independent of user interaction, alternative paths for traffic rerouting are selected dynamically, and adjustable protection parameters are provided based on the network status at each time. Additionally, our proposed model only considers the epicentre as a starting point for the disaster, dynamically monitors disaster expansion, and is not limited to a pre-assigned disaster boundary. Estimating a boundary for natural disasters with varieties in destructive power and damage behaviour may be hard or infeasible. The probabilistic time-varying approach that is taken in our proposed model distinguishes it from the above research

when it needs to consider network components as operational or faulty.

Routing instability caused by multiple failures in large-scale failure challenges can lead to shortest path first throttling and a longer convergence time. Multi-Topology Routing (MTR) has been employed as a solution to mitigate failure effects caused by large-scale events [27]. Using MRT extension in OSPF, pre-determined virtual topologies are used to reroute traffic in failure events and isolate the affected part of the network. The authors developed two MRT-based algorithms called Geographic Coverage MTR (gcMTR), which creates a set of topologies to provide coverage across the network and Geographic Targeted MTR (gtMTR) to generate virtual topologies using pre-knowledge of likely disaster events. Another proposed algorithm in this study was developed to detect a geographical challenge and select a topology for traffic rerouting.

In the above approach, for each vulnerable location in the network, a topology will be generated assuming a specific radius for each potential disaster. In the generated topology, link weights for the vulnerable area are increased to keep the shortest path tree away from that disaster area. Thus, geographical challenges have less impact, such as OSPF routing convergence delay time. The authors considered deterministic failures within a fixed pre-determine radius for the challenge area. The results indicated that if the selected topology radius is bigger than the event size, it could reroute traffic around the vulnerable area. However, for an event size larger than the selected topology radius, the proposed algorithm was not able to reroute traffic to a suitable distance outside the vulnerable area. Although IP routing protocols are able to compute alternative paths and reroute traffic in failure scenarios, they are too slow for large-scale failure cases. The proposed preventive protection model in this thesis is not limited to a disaster boundary in order to reroute traffic out of a danger zone as it adjusts itself in tune with disaster

expansion through a probabilistic dynamic approach. The proposed recovery approach is also suitable for the network backbone, where routing mostly relies on methods such MPLS or WDM for fast recovery.

Dedicated path protection as a solution in survivable elastic optical network (EON) was studied in [28]. Routing and spectrum allocation in dedicated path protection was formulated in Integer Linear Programing (ILP) problem and two metaheuristic optimization algorithms based on Tabu search were developed to address optimal solution in large size networks.

In geographic routing, each node determines its location and the destination location to send packets without knowledge of network topology. Failure in a network may cause a dead end problem in geographic routing. To address this issue in geometric routing, recovery mechanisms are discussed in [29]. Tree-based greedy embedding was considered in this research and connection availability of geometric routing evaluated for a single failure problem. Component availability is another metric that has been used to study network performance and it is defined as the probability that a component is operational at any random time.

A developed model in multiple link failures using link-based restoration with MPLS Fast Re-route (FRR) is discussed in [30]. Three approaches to improve network protection in multiple failures are proposed such as: a collection of spanning trees where a spanning tree is added for each possible edge failure, parallel edges that create a backup path for each edge, and disjoint spanning cycles. The proposed network designs can address multiple failures by adding a small number of edges to the current topology without causing disconnection or congestion.

It is a common assumption in deterministic failure models that network components

will fail with certainty as long as the failure event occurs. However, natural disasters in most large-scale failure events are probabilistic in nature.

2.2 Network resiliency with probabilistic failure view

Probabilistic failure models can be used to design a survivable network using pre-planned backup paths with minimum mutual failure probability [31]. Joint failure probability can be minimized by formulating the backup path selection as an Integer Non-Linear Problem (INLP). As explained earlier, a pre-planned protection mechanism could be costly and may be infeasible in the case of large-scale failures.

Improved network survivability in overlay networks was studied in [32]. A model was developed to find a backup route with the minimum joint path failure probability with the working path. Although it is possible that the selected backup path is disjointed from the working path in overlay layer, they may share some physical links. The authors assumed that overlay link failure probabilities are small and employed exponential physical link failure models. They calculated overlay link failure probability based on independent physical link failure probabilities and the backup path routing problem was formulated as an Integer Quadratic Programming (IQP).

Identifying vulnerable network locations in the event of probabilistic failure scenarios can be used to redesign connectivity or add extra capacity to improve network resiliency. To assess vulnerable locations in the network, failure probability can be calculated using a grid partitioned-based model as in [33]. In a related study in network vulnerability [34], regional failure events such as earthquakes or floods were modeled as random line-segment cuts. The authors applied geometrical probability theory to develop a grid partitioned-based estimation model to locate vulnerable network parts and developed a

model to determine single and pairwise link failure probabilities.

Survivability in layered networks in the event of a failure in the physical layer and its effect on the logical links as multiple failures was discussed in [35]. The authors developed a polynomial-time approximation algorithm for the failures and eliminated resampling for different values of link failure probabilities. Random failures were assumed for physical links with low-failure probability. The proposed model, however, did not sufficiently model the impact of a large-scale failure event in which failure probability can be considerably high in the epicentre.

Correlated link failures with a probabilistic approach were presented in [36]. The authors developed a model to study stochastic disasters, considering that they could be spatially correlated. Failure correlation may be used to assign higher failure probability in specific areas to implement more failure events. The main contribution of this model was to identify vulnerable network locations.

Probabilistic geographical failure has been discussed in [37]. The authors studied probabilistic approaches and developed algorithms considering pre-computed protection plans. The proposed model makes it possible to indicate the vulnerable locations in the network. However, the pre-planned protection scheme is infeasible in cases of large-scale failure.

A number of different network failures and their impacts were studied in [38]. The authors introduced a taxonomy of the variety of network challenges and developed a framework to evaluate the effect of different failure scenarios such as probabilistic uncorrelated random failures in non-malicious problems and deterministic failure in large-scale scenarios. The framework simulates different challenge scenarios using NS3 to evaluate network performance.

In [24], path diversification was employed to design and evaluate survivable networks. The proposed algorithm was able to select a set of alternative paths with different diversities while meeting performance constraints. The authors also explained a measure of diversity that takes into account physical distance as opposed to a measure that solely relies on node or link disjointness. For this purpose, several networks were studied with different ranges of effective path diversity (EPD) thresholds. The metric in this study to indicate the level of topology survivability was flow robustness while it was computed with increasing link and node failure probability. The authors improved network resiliency by applying a path diversification scheme. The proposed model was simulated in different topologies and the results were used to evaluate the network survivability degree.

For a selected set of paths between the source and destination, path diversities were aggregated and shown as the effective path diversity [39]. The average of effective path diversity of all node pairs within the graph was considered as a metric for total graph diversity and employed to estimate network survivability in case of simultaneous failure of nodes and links in probabilistic failure scenarios. The authors simulated a probabilistic failure model using 51 failure probabilities evenly distributed over the range of 0-0.5. The failure probability incremented until the range of all values was complete. Using the proposed metric, connected nodes in each failure scenario were computed.

A risk-based model was studied in [40]. The authors developed a model to design survivable networks based on managing risk. The main goal of this study was to spend a fixed budget in the best part of the network to enhance network resiliency. Different risk management based approaches for survivable network design were proposed.

Network survivability with prioritizing connections in restoration and protection

approaches was studied in [41]. The authors proposed a model that does not transfer all of the data flow to the backup path during a failure event but only reroutes high priority traffic through available resources. They considered a differentiated recovery mechanism taking into account different priorities. This approach was able to increase the recovery ratio of traffic with higher priorities. The failures were generated with a random distribution function and only single failures were assumed at each time.

Considering prior knowledge regarding link failure probability, end-to-end path failure probability can be computed. With this knowledge, it is possible to select working and backup paths with the minimum joint path failure probability. Using risk minimization and employing traffic engineering, a path pair protection can be developed in multi-failure scenarios [42].

Network protection in WDM networks for the case of multiple link failure was discussed in [43]. The authors proposed a protection mechanism by developing two algorithms for path selection and connection unavailability determination. The protection scheme was developed by providing a list of protection paths while having optimum load balancing in the network.

2.3 Enhancing network resiliency using topological parameters

Node and link betweenness are among the parameters that are of concern to network researchers to evaluate network performance or estimate network vulnerability. Authors in [13] showed that selecting links and nodes with higher betweenness in an intentional-failure scenario had a higher impact on the network efficiency compared to random links and nodes failure. Failures in a few nodes with high node betweenness could reduce

network efficiency significantly.

Betweenness centrality and resistance distances can be used in the design and control of communication networks [44]. A weighted random-walk path criticality routing algorithm may be able to select the best backup path with minimum total cost in a shared backup protection approach. Betweenness centrality and its relationship to random walks were discussed in [44] to develop the proposed routing algorithm.

Assessing network vulnerability and detecting vulnerable locations in the network for further improvement has also been a goal in the research on network resiliency in the face of failures [15, 36, 45, 46]. A metric to study network vulnerability using normalized average edge betweenness as a vulnerable index is discussed in [46] and the vulnerability of several networks was studied using this metric.

Betweenness centrality can also be employed to assess network vulnerability for random damage or malicious attack in a complex network [47]. The authors introduced link-based multi-scale vulnerability with integrating power and link betweenness for complex networks. The proposed approach was employed for link placement in a network that produces the maximum resistance in case of malicious attack

Node and link betweenness and other centrality metrics can be used to develop a framework to analyze the robustness of multilevel networks [48]. The authors discussed the impact of removing network components (nodes and links) on network performance and flow robustness.

Node betweenness and other node centrality parameters can be employed to design heuristics for node removal strategies to efficiently determine and remove important nodes from a complex network to minimize network performance [49]. This approach is commonly used in a situation when the objective is to eliminate specific nodes in a

complex network such as disease or criminal organizations.

In a cascade failure, damage in one part of the network can lead to failure of the other successive parts. Authors in [50] examined vulnerability in power grids network in the case of cascading failures. The proposed model in this approach employed an extended betweenness metric, which is a combination of power-flow with network structure to define the load of power grid to analyze network stability. By simulating selective attack strategies the vulnerability of different grid networks were evaluated.

Optimizing a current network or improving the design of future networks requires an understanding of the impact of network challenges. The framework presented in [38] is a simulation-based approach to study network performance in face of failures. In this approach, critical nodes and links are determined using nodes degree connectivity and links and nodes betweenness centrality. The authors argued that the impact of failures on the network is influenced by the period of disaster, the number of network components in the impact zone and the importance of damaged parts.

Node betweenness can be used to specify the average loaded traffic on a node. A connected link to the node with high betweenness needs more capacity to deal with more encounter traffic. Considering link capacity as the bandwidth of the link, the effect of the traffic utility and utilization ratio of bandwidth was examined under random and intentional attacks in complex network in [51].

Network management in complex networks can be improved by quickly locating the fault point in the network. Authors in [52] discussed that in the event of failure on a node with higher betweenness, the possibility of failure occurring on the other nodes within the shortest path of the failed node is higher. The proposed algorithm based on node betweenness centrality acts faster in fault locations compared to other classical

algorithms.

Network criticality is defined as the ratio of random-walk betweenness of a node or link to its weight, which shows the same value for all links or nodes in the network. This factor can be used as a metric to evaluate network robustness [53]. A shared backup path selection approach based on using weighted random-walk path criticality routing can be a solution to address network survivability issues. In this case, a path with minimum effect on the network criticality is considered as a robust path that can be a good candidate for the primary or backup path [53].

A measurement to evaluate network robustness under multiple failure scenarios is discussed in [54]. Random and targeted attacks were examined to determine the level of network robustness. Several metrics were selected to form targeted attacks such as node degree, betweenness centrality, clustering coefficient and spreaders. The results indicated that some networks are more robust based on the selected attack parameter than other networks. A lower betweenness centrality value in some simulation models indicates less centrality for the network components and decreases vulnerability on targeted attacks.

2.4 Network resiliency in software defined networking (SDN)

Software defined networking technology is considered one of the latest approaches in network developments. Here, we study some recent protection approaches and proposed methods using this technology. Network resiliency has been studied in several different ways, such as improvement in fast notification to the controller, development in dynamic restoration, or pre-planned protection mechanisms.

A comparison of the current forwarding algorithm in POX controller [55] has been

discussed in [56]. Evaluating current forwarding algorithms in POX controller can help network researchers study SDN reliability issues with better understanding. In the case of failures, adjacent nodes to the failed link are able to detect the failure and find another link in parallel of the failed link to transfer traffic through. If a secondary link is not available, the adjacent nodes try to find a common node in their adjacency list to reroute traffic. Traffic received by the common node is then sent to the destination. It is possible that a common node cannot be found in their adjacency list. At that point, the adjacent nodes to the failed link try to find a path with a two-hop distance between each other, where each hop is connected directly to each adjacent node. The selected path temporarily transfers traffic to provide protection against packet loss until the controller determines the shortest path and establishes it. Monitoring link status in POX controller is done by a discovery module that sends and monitors link layer discovery protocol (LLDP) packets. The authors mentioned that the recovery process with this mechanism consumes about 4-5 seconds [56].

SDN Controller is responsible for processing LLDP messages in a restoration mechanism. Although increasing the LLDP interval may speed up the recovery process, it can increase overload on the controller significantly [57]. To accelerate the recovery process without increasing the burden on the controller, it is possible assign this job to OpenFlow switches [57]. In this case, probe packets are sent from the tunnel entry point (source node) to the destination in each path. If the destination node fails to receive the probe packets, it is possible that some nodes or links in the path will face problems. In the proposed mechanism, the destination node switches to an alternative path that is selected from table group entries.

In another approach, backup paths for each single failure scenario are determined and

upon the failure event, the flow is transferred through the computed backup path [58]. Working and backup paths are assigned different priorities in this approach. To keep pre-established backups path alive and prevent them from deletion by the controller as unused paths, renew packets are designed to be periodically sent through these paths. The pair nodes involved to detect failure will remove flow entry from the failed link from the switch by an auto-reject mechanism and transfer flow to the backup path. If the failed link is physically repaired, the adjacent switches inform controller by sending port status messages.

Adding recovery action to OpenFlow switches using the group table concept is proposed in [59]. Group table includes group entries to perform different actions. A protection mechanism is implemented in each group entry. Each group entry has an action bucket with alive status. If one action bucket is indicated as unavailable, the next available bucket executes the appropriate actions. The status of each bucket is determined through port state monitoring or bidirectional forwarding detection (BFD). The proposed approach could apply to fast recovery in failure events without involving the controller.

The above studies respond to failure events through a reactive approach and are mainly focused on a single link failure scenario. Our objective in this research is to develop a proactive protection approach with pre-knowledge of potential failures that may affect a part of network. The proposed model is not limited to a single failure problem and can improve network resiliency in large-scale failure scenarios such as natural disasters or power outages. Considering SDN technology and its features, preventive protection model [60]is fully appropriate and consistent within this concept.

Previous research shows a lack of a comprehensive model capable of taking topological properties of the disaster zone into account and dynamically adjusting the

protection approach to enhance the network resiliency level. Although in probabilistic protection approaches failure probability of network components is employed to develop a protection model, this factor has not been used to improve network resiliency against upcoming failures. Moreover, in most probabilistic failure research the method of determining failure probabilities for network components is not dynamic. The studied literature also does not provide an efficient protection model capable of adapting its strategy in a proactive and dynamic way, considering changes on the network topology caused by failures. The literature also shows a shortage of proactive models that can reduce network damage simultaneously with the development of regional devastation. In addition, previous studies do not provide an approach to predict the upcoming damage on network components caused by large-scale disasters.

Considering these shortcomings of previous studies, we aim to enhance the network resiliency level by developing a dynamic, proactive and predictive protection model.

Chapter 3: Network protection and failure models

3.1 Background

Several models in the past three decades have been proposed for network failure recovery [61-64]. The proposed techniques can be roughly divided into two main categories [6]: protection methods where an alternative disjoint path is pre-established along with the primary path to reroute traffic in case of failure, and dynamic restoration methods where an alternative route is established after detecting a failure. A data path from source to destination node in a network may consist of several links. Both dynamic restoration and protection techniques can be applied to improve link or path failure recovery.

In a pre-planned link protection, for each link in the primary path, a backup path with enough resources is considered. In a dynamic link restoration approach, the end nodes of the failed link participate to discover a route around the failed link.

In a path protection scheme, end-to-end backup path for each connection (from source to destination nodes) is determined and adequate resources are allocated. It is also possible to share the allocated resources among backup paths. In an end-to-end dynamic path restoration mechanism, the source and destination nodes of each connection participate to calculate and establish a backup route once a failure is detected. In this case we will have a complete traffic rerouting between the origin and destination nodes.

Dynamic restoration methods are more efficient to utilize network resources and applicable in different failure scenarios. However, pre-planned protection methods are faster than dynamic restoration methods as the backup paths are pre-established and restoration is guaranteed. All possible failure scenarios should be considered when

allocating adequate network resources for each one (required more cost). Path and link protection methods are illustrated in Figure 3.

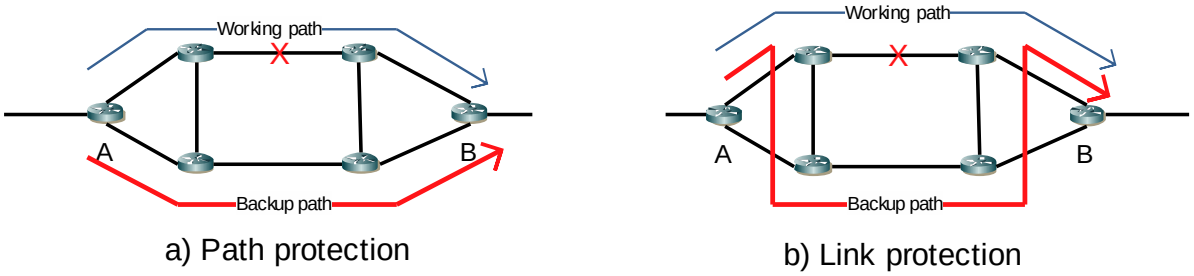


Figure 3. Path and link protection.

In the case of single failure scenarios, recovery is possible using pre-planned disjoint backup paths; however this approach may not be feasible in dynamic large-scale failure scenarios. Although establishing several disjoint backup paths may enhance the probability that at least one of the paths survives, it significantly increases the total cost of additional network resources required for network survivability. This issue is studied in [65] and an analysis of multiple failure restorability for pre-planned link protection is provided. Therefore, in large-scale failure scenarios, our focus is on a dynamic response that allows us to salvage as much traffic as possible and reroute the affected traffic using the available paths in the post-failure network. Considering the characteristics of the large-scale failure, the restoration technique could be an appropriate approach to enhance network resiliency.

We recall here, in general, disasters can be modeled in two different aspects of spreading failures and outcome damages in the network; a deterministic view of failures or a probabilistic view.

This thesis considers the destruction produced by a natural disaster as expanding

dynamically and gradually decreasing to zero. Our focus is therefore on probabilistic failure models, which are more realistic compared to deterministic failure approaches. In this regard, we explain the network model and associated failure probabilities for the network components in this chapter. We will also study the restoration mechanism as a dynamic approach that is able to protect data flow when the network encounters an unpredictable probabilistic phenomenon such as natural disasters. In order to provide a model to assign possible failure probability for network components, we will study earthquake destructive behaviour, which has the strongest destruction effect among natural disasters. In the rest of this chapter, we will provide a comprehensive study of network protection by examining deterministic and probabilistic failure models.

3.2 Our network model

In this section, we explain our network model and the method to estimate the probability of failure in large-scale failure scenarios and describe characteristics of network components that are involved in a failure scenario. The proposed model also will be employed to study the restoration mechanism and explain a method to compute required restoration time.

3.2.1 Network and failure probability model

To model an impacted network by a disaster, we assume that the range of the disaster follows a circular pattern that expands with time. Besides the affected nodes and their connected links, some crossing links may be affected too while their end nodes remain intact. Here we describe how the dynamic failure probability is calculated in our model.

We consider a network graph $G= (V,E)$ where V is a set of nodes and E is a set of links. A link from node i to node j is represented by e_{ij}. A crossing link e_{ij}^{c} is considered

as a link where the end nodes i, j are out of the impact area but parts of the link e_{ij}^{c} have been impacted. In a time-varying model, the failure probability tends to vary with time. Let the impact radius at $time = t$ be R_t. We denote failure probability of link $e_{ij} \in E$ as $P_f^{ij}(R_t) \in [0,1]$ and for node $n_i \in V$ as $P_f^{n_i}(R_t) \in [0,1]$.

In this thesis, R_t for a node is the distance R from the epicentre at time t. We assume that the impact radius increases with time, which is a valid model for disasters such as earthquake or nuclear explosion. To compute probability failure for a link (e_{ij} and e_{ij}^{c}), the minimum Euclidean distance from the epicentre to the link is R_t. Figure 4 shows an example that illustrates crossing links and nodes within the impact area.

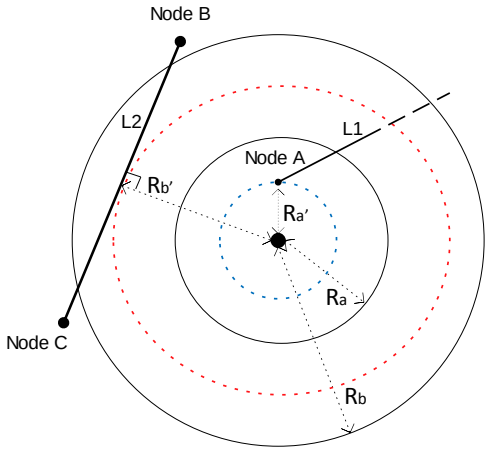


Figure 4. Network with crossing link and an impacted node.

In Figure 4, node A is connected to link L_1. Impact radius at $t = t_a$ is R_a and at $t = t_b$ is extended to R_b. Node A is impacted at $t = t_{a'}$. The failure probability for Node A and the connected link can be shown as $P_f(R_{ta'})$. This failure probability is applied to link L_1 for further end-to-end path failure probability in the preventive routing model. The crossing link L_2 between node B and C has been affected at $t = t_{b'}$ at the distance

$R = R_{b'}$ from the epicentre.

The closest point of the link to the disaster epicentre has been used in calculation of the failure probability of the crossing link. In this example, the failure probability of the crossing link, L_2, can be shown as $P_f(R_{tb'})$.

We define the set Q as failure events caused by expanding the impact radius. Each failure event $P_f(R(t)) \in Q$ occurs at t and once a failure event happens, node $n_i \in V$ may fail with probability$P_f^{n_i}(R_t) \in [0,1]$. We assume that $P_f^{n_i}(R_t) = 0$ if n_i is outside the impact range R_t and all nodes and links outside of the impact area remain in working status. At each simulation time step, a probabilistic engine will determine whether each node will fail or not. We further assume that all connected links to a failed node will be failed and unable to carry network traffic, as they have lost one end node. Network restoration will be applied to the new network topology after removing all failed links and nodes.

An important difference between the single failure restoration approach and large-scale scenarios is that in the latter, the post-failure demand matrix is different from the original demand matrix, because demands from/to failed nodes should be removed from the matrix as they become un-routable [9].

Given that the area affected by natural disasters may have a great extent, the selected strategy to cope with the problem is different with single or double failure scenarios. On the other hand, we assume that the proposed protection model is applicable to backbone networks where the transmission media is mostly relay on fiber optics. As this technology can handle substantial amounts of traffic, the required capacity for data transfer is not a concern. We also emphasize here that, in a large-scale failure scenario, full restoration

(100%) of all network demand is infeasible because some demand originates from or destined for nodes that are damaged and thus are no longer in the network. Removing demands of the damaged nodes in the network actually releases extra capacity for rerouting other connections. However the required spare capacity may be different in each large-scale failure scenario, corresponding to the severity of the damage.

To simulate disaster models and evaluate the performance of our proposed approach, we assume some possible failure probabilities in selected distances away from the epicentre. Selecting values for the probability of failure are such that to simulate a model, close to natural disasters behaviour. The assigned value to failure probability parameters can also be replaced with any other desired values.

3.3 Travelling wave concept in failures

One of the main factors in creating large-scale failures in communication networks is an earthquake, which has the highest destructive effect among natural disasters. The destruction caused by an earthquake is due to the release of energetic waves that decrease gradually over time. In this section, the characteristics of the generated waves by earthquakes are studied in order to provide a model to compute failure probabilities of network components. In the proposed model, impact ranges and failure probabilities vary with time. Considering the similarity of damage among nuclear explosions, earthquakes, hurricanes or floods, the proposed model can be calibrated or extended to identify required resources to provide the expected level of reliability.

3.3.1 Destructive wave attributes

Waves travel through space and time and transfer energy from one place to another. The released energy of natural disasters or nuclear attacks can generally be modeled as a

travelling wave, where energy decreases as the wave expands.

Travelling waves can be grouped as transverse or longitudinal. In a transverse wave, the medium displacement is perpendicular to the direction of propagation of the wave and causes the medium to move up and down. A type of seismic wave called secondary wave or shear wave is known as a transverse wave. In a longitudinal wave, the movement in the medium is in the same direction to the motion of the wave, which means that the wave is seen as the motion of the compressed region. Seismic waves called P-type and explosion waves are examples of longitudinal waves. Figure 5 shows transverse and longitudinal waves.

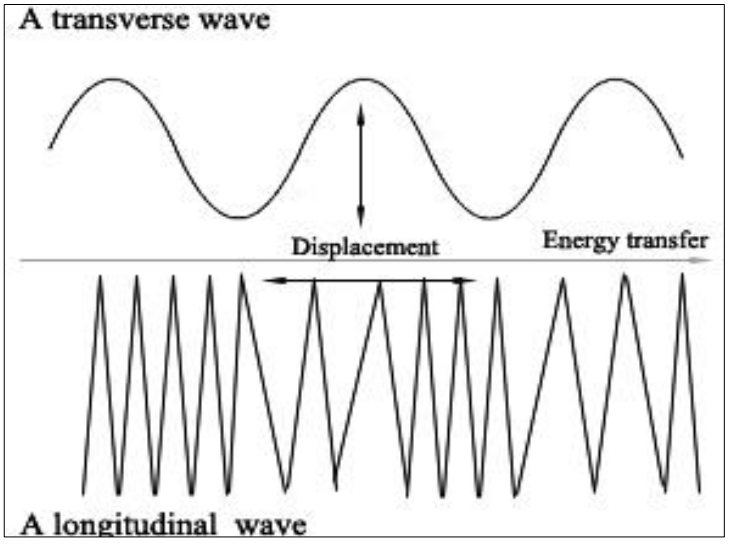


Figure 5. Transverse and longitudinal waves.

A one-dimensional wave equation with amplitude y can be shown as [66]:

$$y(x,t) = A\sin(kx - \omega t) \tag{1}$$

In equation (1), *A* is the maximum amplitude of the wave and *x* is the space coordinate. *k* is defined as the wave number, which is $k = \frac{2\pi}{\lambda}$ and λ is the wavelength. *t* is the time coordinate and ω is the angular frequency which is $\omega = 2\pi f$.

Total energy (kinetic and potential) carried by one wavelength in a travelling wave is:

$$E_\lambda = \frac{1}{2}\mu\omega^2 A^2 \lambda \tag{2}$$

μ is the mass per unit length.

As $v = \lambda f$, the associated power carried by the wave is:

$$P = \frac{1}{2}\mu\omega^2 A^2 v \tag{3}$$

We model a large-scale failure scenario by assuming that the failure starts from an epicentre with the highest degree of damage, and expands across the region at a constant velocity during a limited time. Destructive energy in the earthquake originates in an underground point, which is called the focus. An epicentre is the point on the earth's surface, directly above the focus. The released energy at the epicentre propagates through the surface and causes failure. Figure 6 shows the seismic waves and the epicentre.

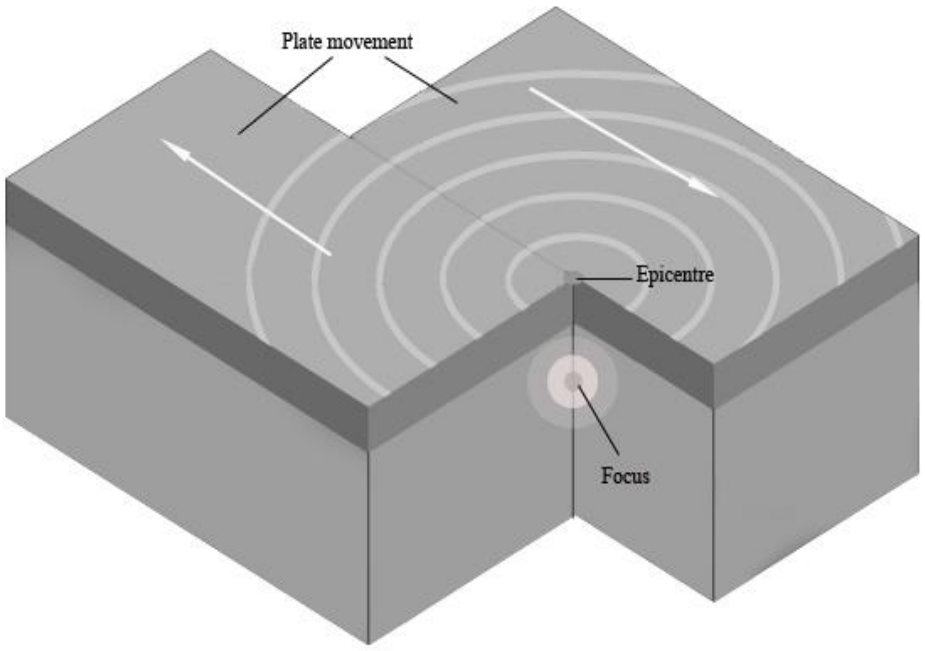


Figure 6. Seismic waves and epicentre.

3.3.2 Failure probability estimation

The damage caused by the earthquake depends on the amount of the initial wave energy. As the seismic waves travel farther away from the epicentre, the amplitude of the waves decrease because of geometric spreading. The geographical area also has a damping capacity known as material damping. A combination of them can be shown as following:

$$A_2 = A_1(r_1/r_2)^n e^{[-\alpha(r_2-r_1)]} \quad (4)$$

A_1 and A_2 are amplitudes of motion at distances r_1 *and* r_2 from the source. α is the *attenuation coefficient* and depends on the type of material through which the wave passes. *n* is the power depending on the type of wave (can be 0.5,1 or 2) [67].

Considering (2), the relationship between wave energy and amplitude is $E \propto A^2$ which can be employed to calculate the associated energy at the specific location in the impact area.

By expanding the impact area, the destructive energy of the disaster decreases and as a result, we assume that the probability of failure is reduced with distance. Based on energy loss behaviour, the failure probability for each component (link or node) is modeled as:

$$Pf(x,v) = e^{-\varphi(x/v)} \quad (5)$$

where φ is defined as *decay rate* and can be considered as a decrement parameter based on energy reduction behaviour and *v* is the wave velocity. Each failure event $P_f \in Q$ may occur at distance *x,* from the epicentre by traveling wave with assumed constant velocity *v*. Once a failure event, P_f happens, node $N_i \in V$ may fail with the probability failure in (5).

According to the given explanations of the travelling wave properties and considering

that the released energy in a destructive natural phenomenon decreases exponentially with increasing distance, we assume an exponential decay model to calculate failure probabilities of network components in this research rather than using normal (or Gaussian) distribution or a predefined list of values.

3.4 Restoration Mechanism and disruption time

We use an MPLS-like model for implementation of the restoration mechanism here, because of its relevance and applicability to backbone networks. MPLS provides a set of protocols for managing and controlling the core network that has been considered as a suitable solution for QoS management in IP network. MPLS improves traffic engineering by integrating layer 2 and 3 of Open System Interconnection (OSI) model. Label switching, the main part of MPLS design, is able to execute fast packet forwarding. Label Switching Router (LSR) by employing Label Distribution Protocol establishes Label Switching Path (LSP).On the edge of the network, Ingress LSR (I-LSR) picks up unlabeled packets adds labels to them and forwards them through LSP [68].

Restoration time in MPLS-based networks has been studied in [69]. The authors discussed recovery time in MPLS networks in both protection and restoration methods. In this thesis, we consider a dynamic restoration scheme in MPLS-based network, where the backup path is setting up after failure detection.

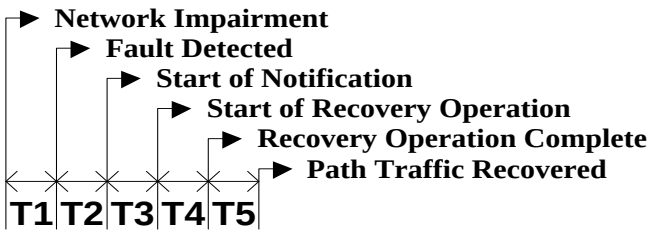


Figure 7. MPLS recovery cycle model[70].

The recovery scheme can be accomplished by adjacent nodes to the failure, or by the source node of the flow. Authors in [70] have provided an MPLS recovery cycle model (Figure 7). The recovery cycle model is composed of five separate time slots.

Fault Detection time (T1) is the amount of the time needed by adjacent nodes for failure detection. Hold-off time (T2) is a pre-determined time assigned to the lower layer protection to wait prior to MPLS-based recovery action and can be set to zero. During notification time (T3), the source node of each flow receives the failure notification message and I-LSR starts recovery operation in (T4). Traffic will be rerouted during traffic recovery time (T5). Once the recovery operation is finished, the destination nodes receive the traffic again. The total restoration time is $T_1+T_2+T_3+T_4+T_5$.

In this research, without loss of generality, we assume that the notification delay can be negligible for the adjacent nodes to the failed link. When the source node receives the failure notification message, it calculates a new path and sets up a new Label Switching Path (LSP) by the signaling protocol. Two types of messages employed in the signaling are Path messages and Reserve (Resv) messages. We consider the network disruption time as:

Notification time $(\sum_{i=1}^{n} PG_i + PS_i) +$ *Path messages delay* $(\sum_{i=1}^{m} PG_i + PS_i) +$ *Reserve messages* $(\sum_{i=1}^{m} PG_i + PS_i)$. (6)

Here, PG_i is propagation delay on link $L_i \in E$ and PS_i is processing delay on node $Ni \in V$, n is the number of nodes on the path between the nodes that detects the failure and the source node and m is the number of nodes between the source node of the flow and the destination node. In a large-scale failure scenario, we need to restore several failures at the same time. In this case, restoration time can be computed as an average or

maximum required time to recover the network.

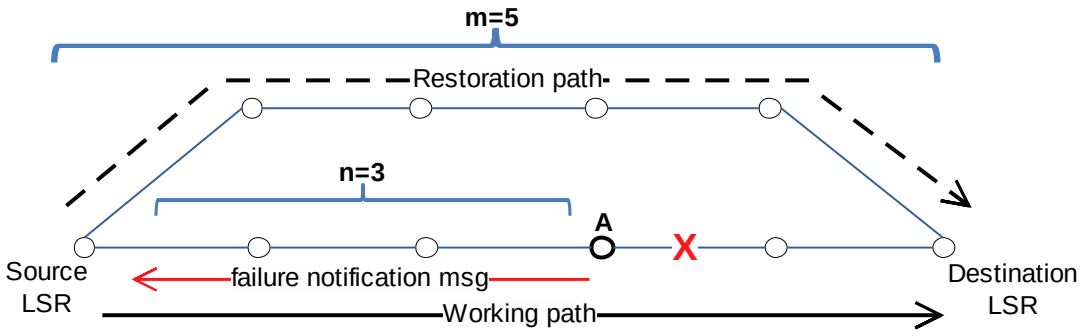


Figure 8. Global restoration mechanism in an MPLS network [69].

Figure 8 shows an example of a dynamic restoration scheme in an MPLS network. In this example, node A detects a failure on the adjacent link and sends a failure notification message to the source LSR.

3.5 Performance evaluation: probabilistic vs. deterministic failures

We evaluated the efficiency of the proposed model in large-scale failure scenarios under several different scenarios, in order to provide a meaningful comparison between deterministic versus probabilistic as well as static versus dynamic methods.

We first provide a comparison between deterministic and probabilistic large-scale failures with an assumption that failure probability is constant throughout the disaster expansion. We later show how the change from this constant probability model to our dynamic probabilistic model affects the performance. This model evaluates network performance between these different approaches. The model is simulated using MATLAB and applied to the European network COST-239 (Figure 9). The network consists of 11 nodes with an average nodal 7 and 26 links. Using a coordinate vector as in [9] the geographical location is determined and an adjacency matrix indicates the

connection between nodes.

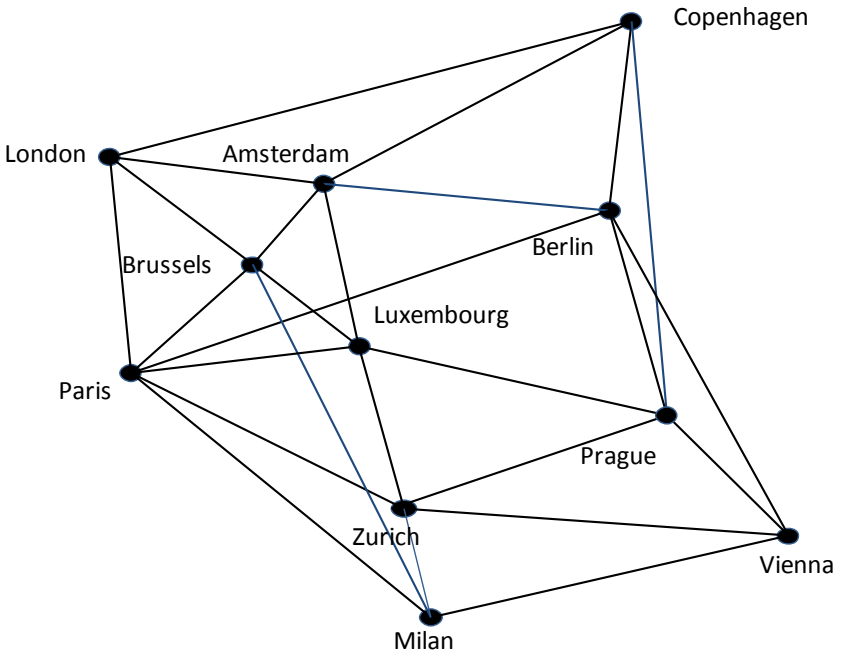


Figure 9. COST-239 network topology.

A unit end-to-end demand matrix is considered for each pair of nodes. A weighted shortest path algorithm is used to route each demand. The working capacity of a link is defined as the sum of all demands routed through that link [9]. To simplify our analysis and without loss of generality, we assume that the epicentre is always one of the network nodes and we compute the average result for all the nodes. The maximum impact range studied in this model is 500 km.

We studied large-scale failure models with constant failure probability in two different scenarios. In the first scenario, we assumed a constant failure probability for the entire disaster duration and each involved node and link in the impact area face a certain probability of failure. The model is simulated in four different failure probabilities: 20%, 40%, 60% and 80%. The simulation models parameters are summarized in Table 1.

Table 1. Disaster model with constant failure probability in entire disaster region

		Distance from the epicentre (km)					
Simulation Model		**Epicentre**	Under 100 km	100 to 200 Km	200 to 300 km	300 to 400 km	400 to 500 km
Case 1	Failure probability	100%	80%	80%	80%	80%	80%
Case 2		100%	60%	60%	60%	60%	60%
Case 3		100%	40%	40%	40%	40%	40%
Case 4		100%	20%	20%	20%	20%	20%

If the network is partitioned, the traffic flows from one partition to another cannot be restored. By expanding the impact range in each interval, the algorithm determines nodes and links within the impact area.

In the second scenario, we assumed a constant failure probability limited to a geographical area with a fixed reduction in failure probability between the regions. We considered a decrement rate in the range of 15%, 20%, 25% and 30% and employed it to reduce the failure probability for each 100 km of disaster expansion. This model aims to simulate a situation where the failure probability decreases with distance by expanding through the regions. Table 2 summarizes the failure probability parameters. All the other parameters in this model are the same as the parameters in the simulation model when the failure probability is constant across the entire impacted region.

Table 2. Disaster model with the limited geographical constant failure probability and fixed reduction rate

Simulation Model	Reduction rate		Distance from the epicentre (km)					
			Epicentre	Under 100 km	100 to 200 km	200 to 300 km	300 to 400 km	400 to 500 km
Case 1	15%	Failure probability	100%	85%	70%	55%	40%	25%
Case 2	20%		100%	80%	60%	40%	20%	0
Case 3	25%		100%	75%	50%	25%	0	0
Case 4	30%		100%	70%	40%	10%	0	0

3.5.1 Performance results

In this section, we present the results obtained from modeling large-scale failure scenarios with deterministic and probabilistic damage patterns and provide a comparison between them. In order to evaluate network performance in each failure scenario, we studied several important metrics such as the number of failed network components and the percentage of the lost demands.

We also computed the required network restoration time in each failure scenario. Figure 10 illustrated the studied performance metric when the failure probability is constant throughout the failure model.

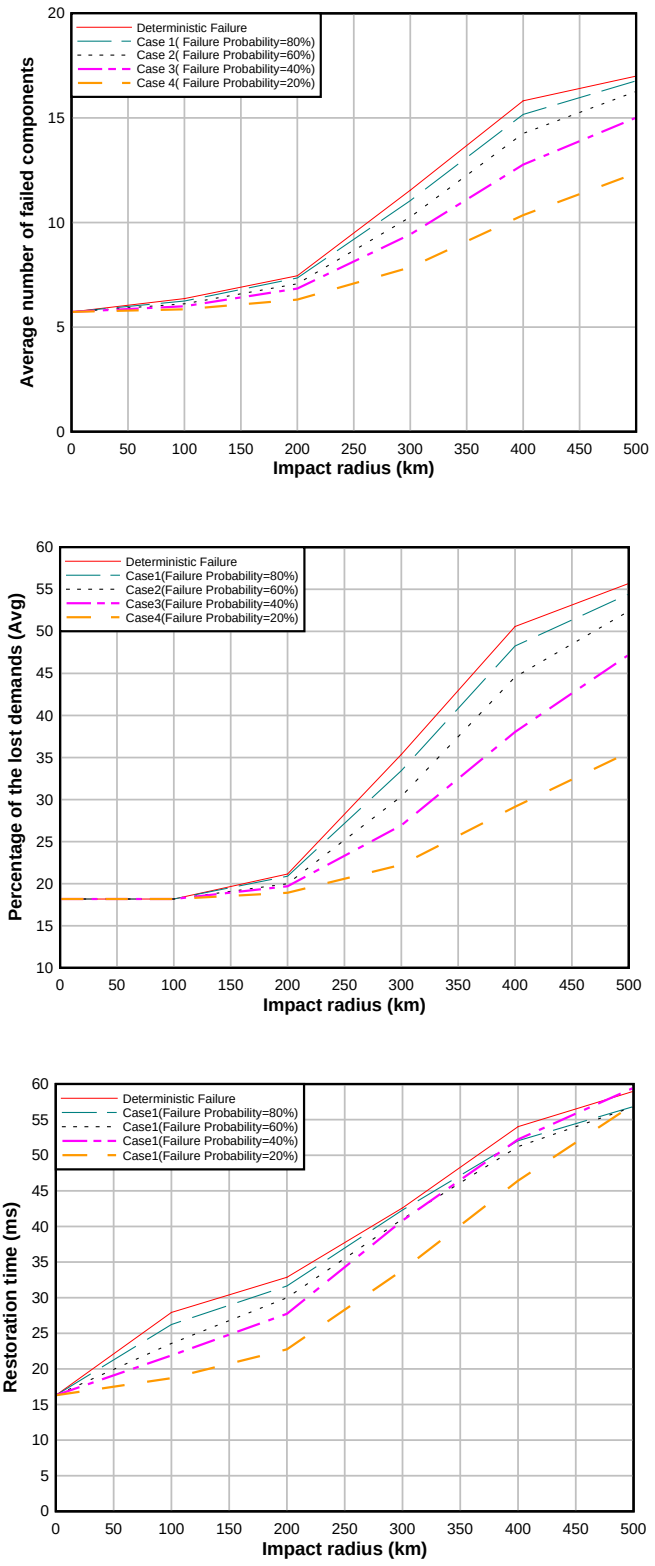
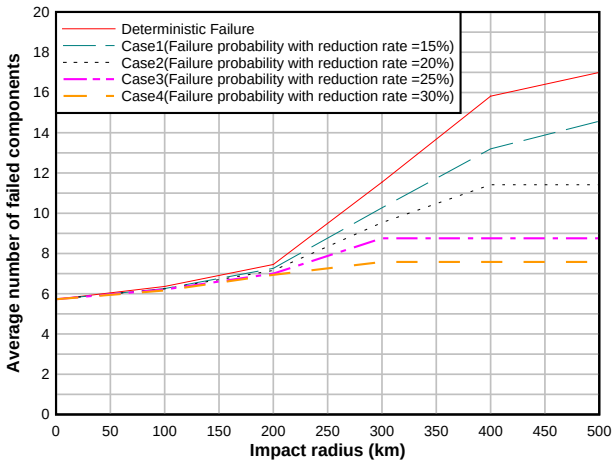
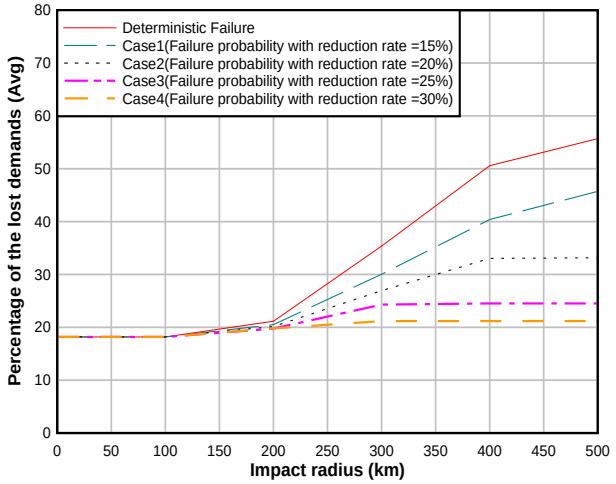


Figure 10. Simulation results with constant failure probability in the entire impacted area.

Figure 11 shows the results for a fixed reduction in failure probability for each

distance.





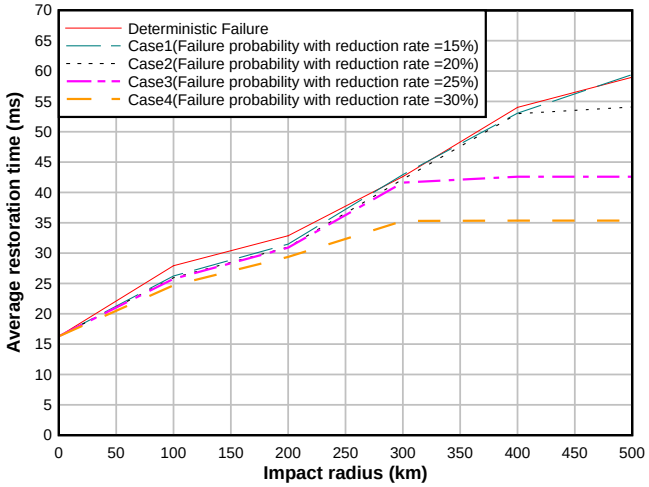


Figure 11. Simulation results with constant failure probability with fixed distance reduction.

Next we analyze the results obtained for each of the above simulation models and explain network performance.

3.5.2 Performance analysis and discussion

Figure 10 shows the results obtained for a simulation model with a constant failure probability across the entire impacted area. As can be seen, the average number of damaged network components in the deterministic failure scheme is significantly different from the probabilistic failure approaches especially when the failure probability decreases. The simulation results show that there can be a difference of 25% in the lost demands with the probabilistic failure model compared to the deterministic failure model. This difference in the lost demands indicates how considering a failure probability with different values can affect the obtained results. The results also show the difference in the required restoration time between the deterministic and probabilistic failure models with different failure probability values. In all cases, deterministic failure model needs more restoration time.

In Figure 11, we present the results obtained by simulating disaster models with a constant probability of failure in a limited geographical area with a fixed reduction between regions. As can be seen, the average number of damaged network components and also the average percentage of the lost demands are directly affected by changing the probability of failure. In a failure model, a greater reduction in the probability of the failure leads to a fewer number of network components being damaged. This difference also can be seen clearly in the amount of the lost demands, when the failure probability reduces faster through the impact area.

By looking at the required restoration time, the deterministic failure model and the

probabilistic failure model with less reduction value almost show the same average restoration time. With an increasing reduction rate in the failure probability, the difference between deterministic and probabilistic failure models shows significant changes.

3.6 Performance evaluation: wave-like probability failure models

We improved the proposed model by computing the failure probability of each impact expansion based on energy reduction behaviour. Decay rate is the employed parameter to compute failure probability. We assume a disaster's wave travels with a constant velocity *v* and the probability of the failure will be reduced with *decay rate* φ.

We applied our model to the European network COST-239. Dijkstra's algorithm is employed to route the demand for each link through the shortest path. We simulate the proposed model for each node as the epicentre and a constant failure expansion velocity of 10 km/s. We assumed the impact radius would expand at the rate of about 10 km/s, up to maximum 500 km at a constant speed.

We assumed an earthquake-like model for disasters. The propagation velocity of the waves in an earthquake depends on geographical characteristics and earth materials which can be up to 8.5 km/s [71]. We used the propagation velocity of 10 km/s as the worst-case scenario. This range of impact is assumed to be a circle which the radius R, at $time = t(s)$ is $R = r(km)$ and at $time = t + T(s)$ is $R = r + 10T(km)$.

In order to implement a proactive approach, we assume a natural disaster early warning system is in place, or that the first failure is detected by the network itself. We assume full disruption/failure at the epicentre. As the disaster typically spreads in seconds to minutes while our rerouting algorithm can operate within tens to a couple of hundreds

of milliseconds, there is enough time to prevent paths from upcoming damages.

Three different scenarios have been studied: fast, medium, and slow decay. We assumed failure probability in the fast decay model is 40%, 60% in the medium decay model, and 80% in the slow decay model when 100 km away from the epicentre. As we explained earlier the selected values of decay rates aim to model the failure probability in such a way that the model is built like an earthquake. Using exponential decay, the energy reduction is faster compared to a linear approach through the region. The proposed model is not limited to the selected values for the decay rate and can be examined with any other values. The decay rate in each failure probability scenario is calculated and shown in Table 3.

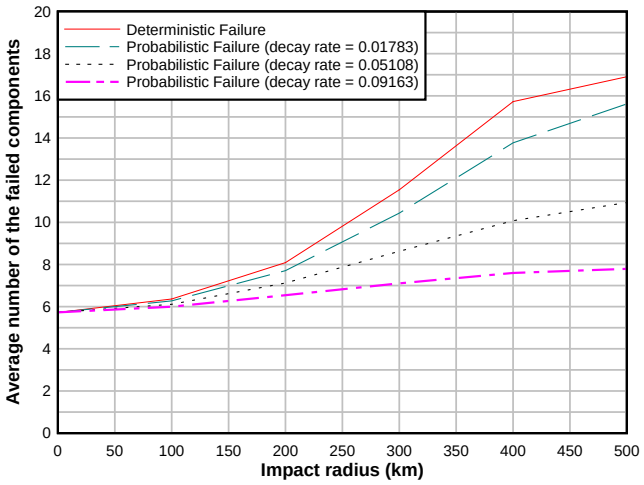
Table 3. Decay rates for probability of failures

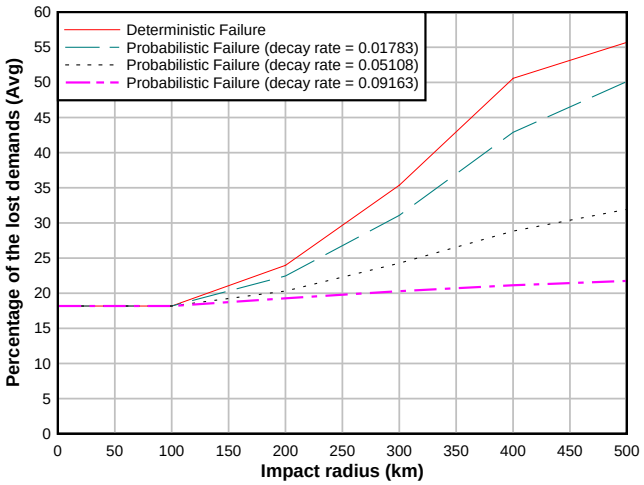
Decay rate	Failure probability in 100 km far away from the epicentre
0.01783 (slow decay)	80%
0.05108 (medium decay)	60%
0.09163 (fast decay)	40%

The average number of failed network components, required restoration time and the percentage of the lost demands are the metrics that are studied in this simulation model.

3.6.1 Performance results

Here, we present results of modeling failure probability using wave-like attributes (Figure 12). The studied metrics are the number of failed network components, the average of lost demands and also the delay time required for network restoration. The results include three different decay rates compared with a disaster scenario using a deterministic failure approach.





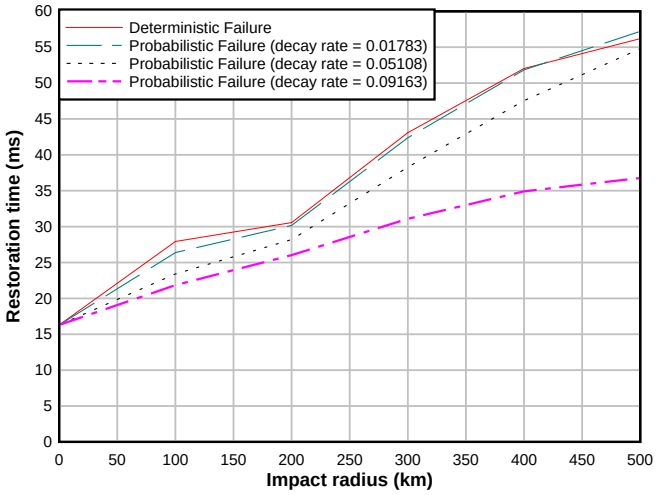


Figure 12. Simulation results in large-scale failure model with wave-like failure probability.

3.6.2 Performance analysis and discussion

Figure 12 shows the results obtained by simulating a large-scale damage model with wave-like failure probability. The three different scenarios show that in the case with a higher probability of failure, the number of affected network components and the average percentage of the lost demands caused by the damage are higher. The lost demands in the probabilistic approaches may be significantly less than deterministic failure models and are highly dependent on the speed at which wave energy decays.

In the fast decay model, the probability of failure reduces significantly as the disaster's wave spreads through the region. It means network components at a distance from the epicentre have a greater chance of survival. The fewer number of damaged network devices leads to time savings and less delays in the restoration mechanism.

3.7 Concluding remarks

In this chapter, we studied network performance using two different views of failure; deterministic and probabilistic. For each failure approach, we examined several different scenarios through simulation models. A deterministic failure model is compared to two probabilistic failure models, where the failure probability is considered fixed throughout all the disaster scenarios for all components. We then studied another model where the failure probability is considered to be fixed only for a specific region and the value changes for the next understudy region with a fixed value reduction. Our main goal was to study several different models to give a comprehensive view of the difference between deterministic and probabilistic failure models and their outcomes in network performance for disaster scenarios.

We have extended the view of probabilistic failure by considering a wave-like model.

In the proposed model, failure probabilities follow a time-varying model and change as the disaster spreads. The proposed model is inspired by earthquake behaviour, which starts from an epicentre and expands through the region where it loses its energy and destructive power as it is expanding. The studied model would give a more realistic failure possibility in a network when it is treated with disasters.

Chapter 4: Preventive protection model

Natural disasters are among the main destructive factors in large-scale failure scenarios. While each proposed protection model (chapter 2) using dynamic or pre-planned protection mechanisms deals with some aspects of large-scale failure management in communication networks, there is still no comprehensive solution that takes the unique features of major disaster scenarios into account; namely the facts that these events are dynamic and the situation on the ground changes rapidly. The impact range of a disaster event expands with time and simultaneous probabilistic failures occur during the impact. Most solutions take static post-event approaches in which either the network must be significantly overdesigned to be able to cope with the immediate impact of a disaster, or use restoration efforts that take too long to respond to changes in network conditions as the disaster impact spreads. The dynamic behaviour of natural disasters and their probabilistic failure pattern indicates a need for a dynamic probabilistic protection approach to address the issue and reduce the number of disrupted connections in the network.

Our objective here is to propose a proactive approach that would allow network operators to salvage as much backbone traffic as possible while the disaster event is still in effect. Our technique is predictive, dynamic and probabilistic at the same time. As opposed to previous studies, which used static failure probabilities, our technique builds a dynamic probabilistic model and updates it as the impact of failure (e.g., earthquake) spreads. Our technique is also proactive, for example it evaluates the reliability of paths in real time during the disaster impact period and makes preventive rerouting decisions based on the risk level.

4.1 Proactive time-varying protection concept

Here, we present a novel preventive protection method, which would be appropriate for dynamic disaster scenarios such as earthquakes, nuclear explosions or hurricanes. The proposed method can be used to increase the resilience level of the network by employing preventive rerouting.

We recall from the study of previous works that most of the developed models in large-scale failure events focused on indicating the vulnerable parts of the network for further improvement and not developing a real-time solution in case of disasters. To keep network functionality at an accepted level, it seems necessary to mitigate disaster effects in the current working network. The core concept of the preventive protection model is to reroute high-risk connections prior to failure to reduce the number of disrupted connections in disasters scenarios.

4.1.1 Compute end-to-end path failure probability

The preventive protection method is probabilistic and dynamic. In order to implement a proactive approach, we assume a natural disaster early warning system or that first failure detection by the network is in place and the network management system is able to receive notification of the occurrence of a disaster, as well as continuing reports about how it expands. For the purpose of this work we use an earthquake disaster model; i.e., a disaster impact area that starts from an epicentre and expands with time.

Once a network failure is detected, an exponential decaying rate for failure probability is computed based on the level of intensity of the disaster and the available background knowledge of the geographical characteristics of the area. This factor can be employed to calculate failure probability for each component in the network. This model has been

presented in [72] and has been discussed in Chapter 3.

Although we employed an exponential decay model to compute the failure probability for each network component in this study, any other approach capable of estimating failure probability can be used in this model. It makes the proposed model applicable in any large-scale failure scenario such as nuclear explosion or natural disasters whenever the failure probability for the network components can be estimated (theoretical or empirical).

We assume that a single link can survive the impact with a probability of $1 - P_f^{ij}(R_t)$. Each path in the network may consist of several links. The regional dependence between the failures of links and nodes in an area is included in calculating individual probabilities of failure, as we explained in Chapter 3. Once the probabilities are determined, we can assume that failure events happen independently. With the above knowledge, end-to-end path failure probability is computed as:

$$P_f\left(path_{(i,j)}\right) = 1 - \prod_{e_{ij} \in E} \left(1 - P_f^{ij}(R_t)\right) \tag{7}$$

For example in Figure 13, failure probability for a link between node A and B is shown as $P_{f(A,B)}$ and the probability that this link survives the failure is $\left(1 - P_{f(A,B)}\right)$.

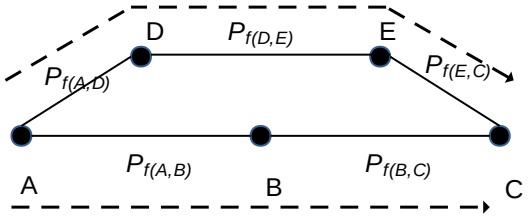


Figure 13. Failure probabilities for links.

The end-to-end path failure probability in Figure 13 for the source node A to destination node C can be illustrated as follows if the path passes through node B:

$P^{B}_{f(A,C)} = [1 - ((1 - (P_{f(A,B)})) \times (1 - (P_{f(B,C)})))]$.

Or if data is sent through nodes D and E:

$P^{D,E}_{f(A,C)} = [1 - ((1 - (P_{f(A,D)})) \times (1 - (P_{f(D,E)})) \times (1 - (P_{f(E,C)})))]$.

4.1.2 k-shortest paths failure probabilities computation

Depending on the network topology and epicentre of the disaster, several alternative paths from the source to the destination may be available for each affected connection. In this step, the existing k-shortest paths are computed and the outputs are sorted with the shortest path first. For each source node *i* and destination node *j* we may have a group of shortest paths as:

$$path(i, j)_1, path(i, j)_2, ..., path(i, j)_k$$

Using equation (7), we can calculate the end-to-end probability of failure for each path as: $P_f\left(path_{(i,j)}\right)_1, P_f\left(path_{(i,j)}\right)_2, ..., P_f\left(path_{(i,j)}\right)_k$

The calculated failure probability for each shortest path from source node *i* to destination node *j* will be further employed in preventive rerouting strategy.

Figure 14 is an illustrative example of an expandable disaster model. There are several paths available between nodes *A* and *B*, two of which are highlighted. Failure probabilities are illustrated in different colours for each impact radius and decrease as the impact expands. The path k_1 utilizes links 1 and 2 and the alternative path k_2 consists of links 3 and 4.

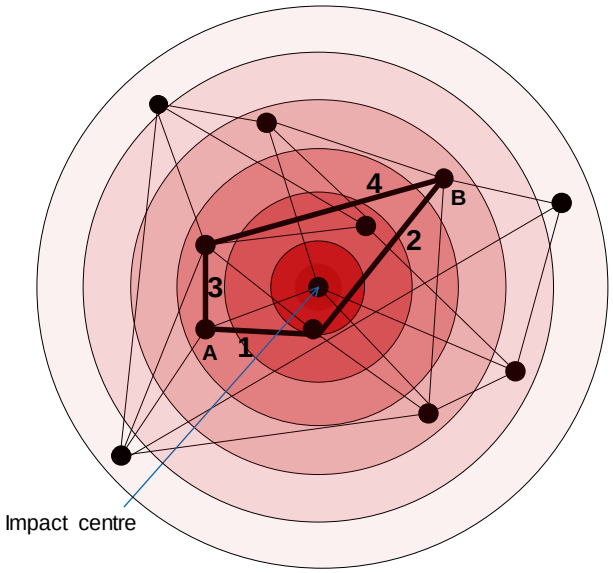


Figure 14. Network with expandable failure and k-shortest paths.

4.2 Preventive rerouting strategy

The main strategy for data flow protection in the preventive protection model is to reroute traffic of endangered paths before failure and as a result reducing the number of disrupted connections. The paths that are close to the epicentre are considered high risk and their traffic should be rerouted through the other paths with further distance to the epicentre. As the destructive power of natural disaster waves decreases with distance from the centre of the incident, the proposed preventive rerouting strategy and switching traffic to an alternative path between source and destination nodes may reduce traffic damage probability.

A group of shortest paths may be available for each source and destination nodes with different end-to-end failure probabilities for this purpose. To reroute traffic through more reliable paths, preventive protection models employ risk threshold parameters to decide how to reroute traffic through more reliable routes. For example, in Figure 12, links 1 and 2 in path k_1 pass through the area nearest to the impact centre, which results in a higher

end-to-end path failure probability. In the proposed method, based on the defined thresholds, we assume the appropriate action is to switch demands from *A* to *B* through path k_2 (links 3 and 4), which has a lower end-to-end failure probability.

4.2.1 Preventive decision parameters

Having different paths with different failure probabilities gives us a holistic view of the intensity of the approaching failure in the network. We may anticipate that a path with a higher failure probability would be more fragile in the face of expanding disaster and traffic through this path is in danger. To address this issue, the proposed model should be able to distinguish at-risk paths and make an appropriate decision to switch traffic through more reliable paths.

Here we define two decision making parameters; *upper threshold* (T_{Up}) and *lower threshold* (T_{Lo}). We denote the lower threshold as $T_{Lo} \in [0,1]$ and the upper threshold as $T_{Up} \in [0,1]$. Paths with an end-to-end failure probability higher than T_{Up} are considered endangered paths with data flows that need to be protected. We apply T_{Lo} to define a 'safe zone' for the paths with a lower end-to-end probability of failure, therefore having more chances to survive.

4.2.2 Pre-failure protection

Figure 15 illustrates an example of the preventive rerouting mechanism and protecting traffic passing through an endangered link prior the failure.

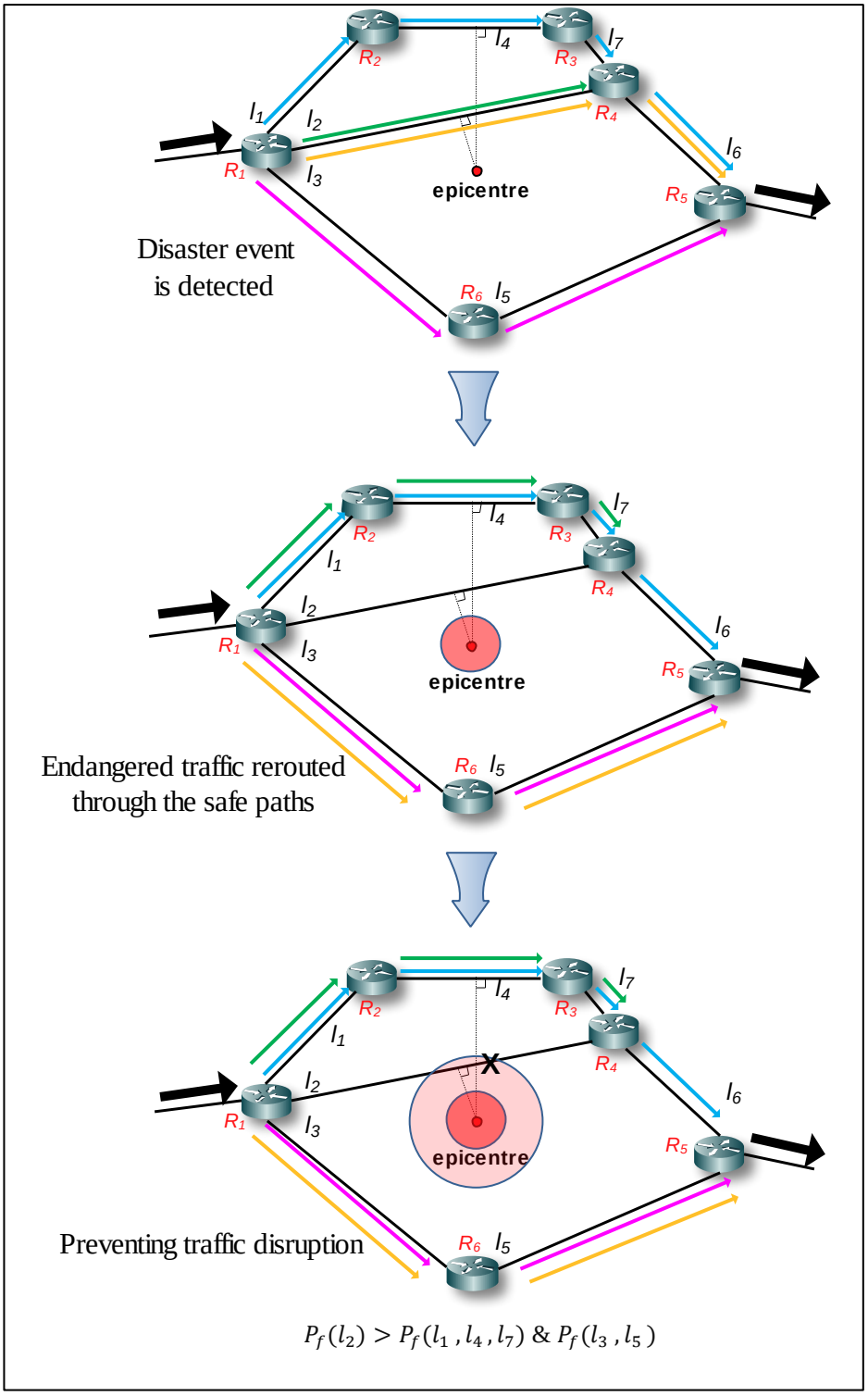


Figure 15. Preventive rerouting prior to failure.

To reroute traffic we consider three possible scenarios based on assigned threshold parameters and describe the decision making procedure based on the end-to-end path

failure probability:

a) $P_f\left(path_{(i,j)}\right)_1 \leq T_{Lo}$

In this situation, the first computed shortest path has a lower failure probability than the lower threshold. We assume this path falls in the safe zone and has a good chance of surviving the approaching damage. This path can therefore be considered reliable for passing traffic flows and no rerouting is required. This path can also be selected as a reliable backup path for preventive rerouting.

b) $P_f\left(path_{(i,j)}\right)_1 \geq T_{Up}$

The end-to-end probability of failure is higher than the upper threshold, which means that the path is more likely to fail in the future (i.e., a path in the 'danger zone') and an upcoming damage can disrupt this connection. The proper action is to find another shortest path in the lower threshold zone and reroute traffic flows through it prior to failure so that they will not be disrupted once the disaster impact area reaches this path. If the preventive method could not find a path in the lower threshold zone, any path with a lower failure probability than the current path will be selected to reroute the traffic.

c) $T_{Up} \leq P_f\left(path_{(i,j)}\right)_1 \leq T_{Lo}$

In this scenario, the first found shortest path remains as the working path. We keep this path as a working path but will not use it as a safe backup route for others. If this path fails, the preventive protection model tries to reroute its traffic through the path in the safe zone. The process of the preventive protection model is summarized in Figure 16.

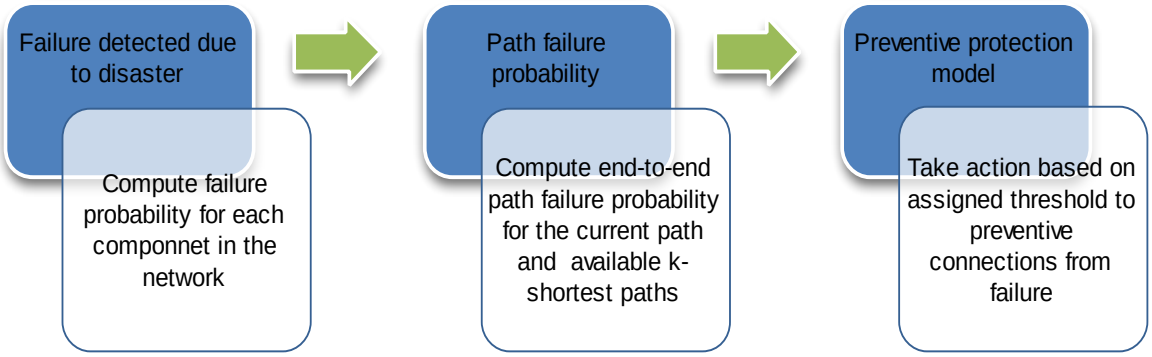


Figure 16. Preventive protection model.

The difference between upper threshold and lower threshold can be chosen by the network designer based on the desired level of survivability and the available resources in the network.

In all of the above scenarios, if the number of available k-shortest paths is one, it is considered to be the best candidate path. Having several shortest paths is directly related to the network topology and the failure intensity. In highly damaged networks, more links and nodes will fail and as a result, less network resources will be available to reroute traffic.

4.3 Performance evaluation

To evaluate the performance of the preventive protection model, we adopt the following metrics:

a) *The Number of Disrupted connections*: Any disruption in network operation can lead to loss of data and impact network performance. To ensure continued system operation in the case of a disaster, a dynamic path restoration mechanism tries to reroute demand of the disrupted connection through a backup path. The proposed model aims to decrease the number of disrupted connections to improve network survivability.

b) *Network Disruption time*: Disrupted connections need time to be recovered. We use

the Multiprotocol Label Switching (MPLS) service time model for our computation, as it provides a good model for connection-oriented backbone services.

c) *Number of preventive rerouted connections*: In the proposed method, we apply the upper and lower threshold to compute substitute paths with a desired level of the end-to-end failure probability.

An implementation of our preventive protection scheme can be summarized as following:

Preventive protection scheme

While Impact radius < maximum radius

Compute impact area

For all components within impact area:

Determine failure probability

Fail/not fail each network component *(using a loaded coin-toss probability model)*

Remove failed nodes and links from the network

Compute end-to-end path failure for each demand

Based on upper and lower threshold:

Reroute failed demands to the preventive paths

Reroute likely to fail demands to the preventive paths

Calculate number of disrupted connections

Calculate network disruption time

Calculate number of preventive rerouted connections

End For;

Wait for notification about expansion of impact radius

End while;

The computed worst case time complexity of the proposed algorithm for the number of links |E| and nodes |V| is $O(|V^3|)$ which is polynomial and feasible to achieve.

The process to calculate alternative paths and reroute traffic prior to failure works in the background and does not interfere with the current traffic flow in the network. However, it will increase the network processing overhead during the computing process. The above metric is directly related to how the values of the upper and lower thresholds are adjusted. It can be utilized to improve network performance based on the available resources and the expected resilience level.

In preventive rerouting procedures, when the substitute path with the acceptable level of end-to-end failure probability is computed and established, the traffic of the current working path is switched. We assume that the switching time is negligible, therefore this operation allows the traffic between the two nodes to flow continuously.

To evaluate network performance and validate the observed results, four real-world network topologies; Cost239, TeliaSonera, Sprint and Level 3 (Figure 9 and Figures 17, 18, 19) with different nodal degrees are employed to simulate the proposed model.

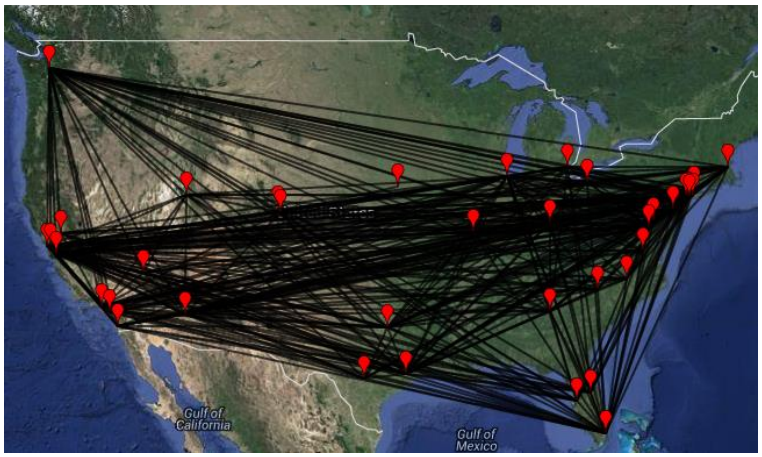


Figure 17. Level3 network.

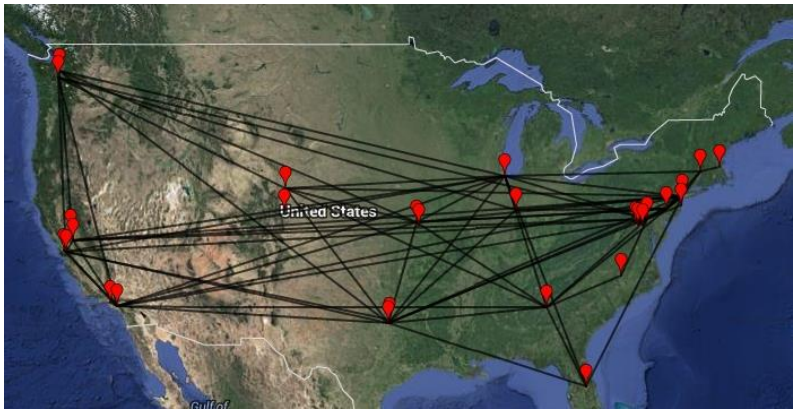


Figure 18. Sprint network

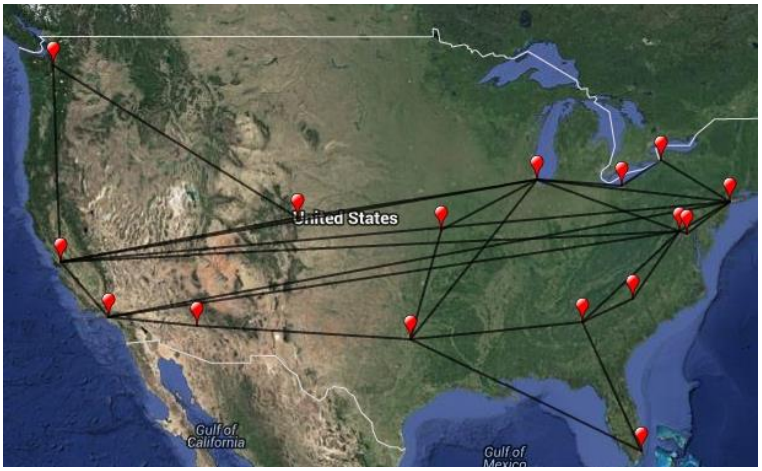


Figure 19. TeliaSonera network

We study the network performance for each network topology in four different scenarios. In each scenario we simulate the proposed model with different threshold ranges to illustrate how the selected upper and lower threshold can affect network performance.

In our simulations, we compared our results with the deterministic failure scenario, which is the scenario used in prior large-scale failure analysis, e.g. in [9] in order to provide a view into the impact of considering probabilistic failures and probabilistic countermeasures on the overall robustness of the network. Table 4 shows the selected topologies to simulate the proposed model.

Table 4. Real world topologies specifications

Network	Coverage	Nodes	Links	Avg. Node Degree
Cost239	Europe	11	26	4.7
TeliaSonera	U.S.	16	29	3.6
Sprint	U.S.	28	76	5.4
Level 3	U.S.	38	376	19.7

In each simulation scenario, we chose one node of the network as the epicentre, and then we simulated each scenario 50 times in order to collect sufficient sample data for statistical analysis. Each case was run in four different scenarios as shown in Table 5 and shows the selected thresholds ranges in each scenario.

Table 5. Selected threshold ranges for simulation model.

Scenario1	Upper threshold = 50% Lower threshold = 25%
Scenario2	Upper threshold = 75% Lower threshold = 25%
Scenario3	Upper threshold = 75% Lower threshold = 50%
Scenario4	Upper threshold = 80% Lower threshold = 40%

The network performance for each topology was studied for 40 seconds as assumed disaster duration. The probability failure in this study is computed with the *Decay rate (φ)= 0.01783.*

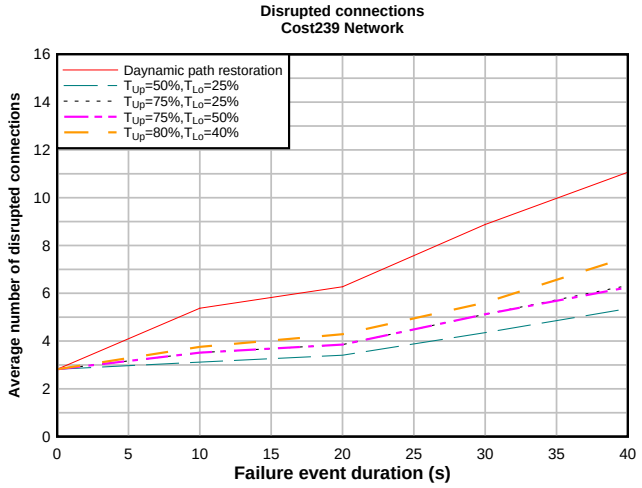
4.3.1 Performance results

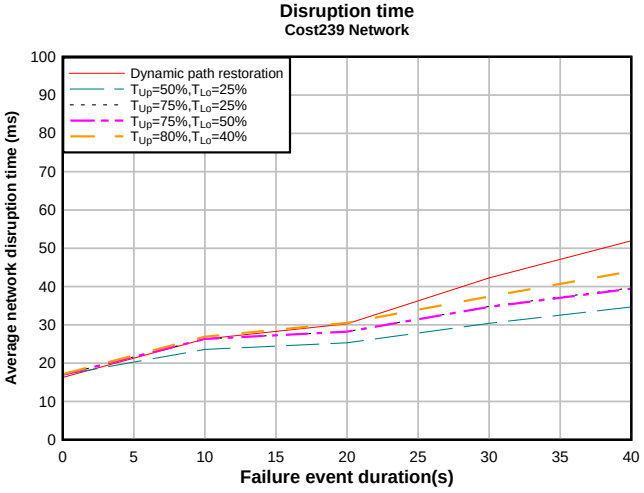
Each figure in this part includes the results obtained from the dynamic path restoration mechanism as well as our proactive protection approach to show the effectiveness of the preventive protection model. The results have been computed as an average value among all the nodes and illustrated with the corresponding time of the disaster duration. For each

simulated topology, we illustrate the following parameters:

- *average number of disrupted connections*
- *average network disruption time (ms)*
- *number of preventive rerouted connections.*

We assumed that the disaster duration is about 40s and the proposed model is simulated in four different threshold ranges.





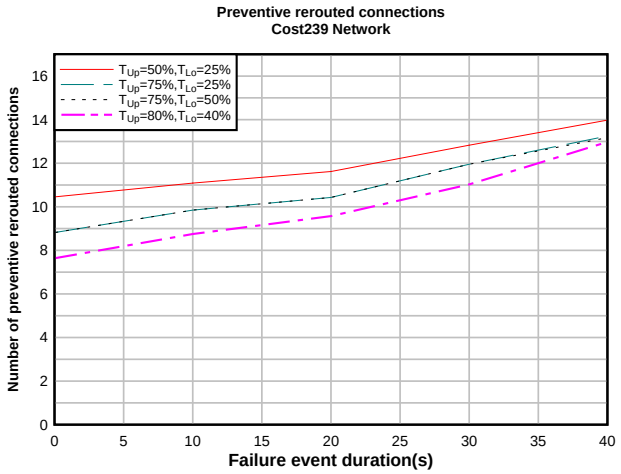
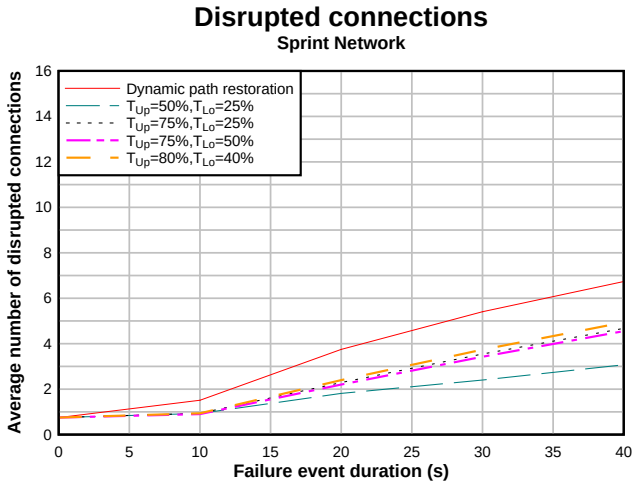
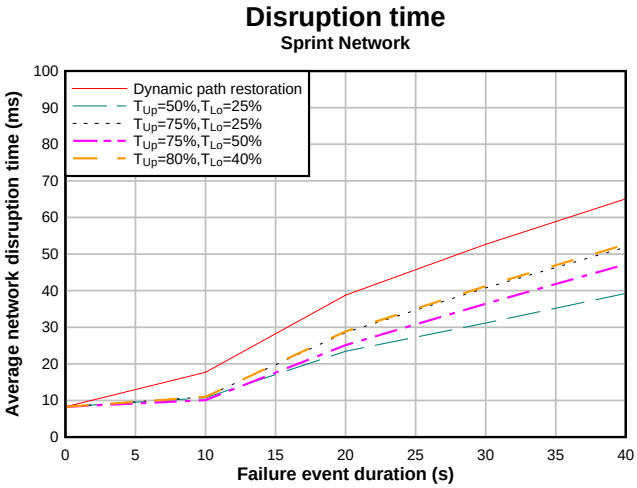


Figure 20. COST-239 network performance.

Figure 20 shows the obtained results in European network COST-239.





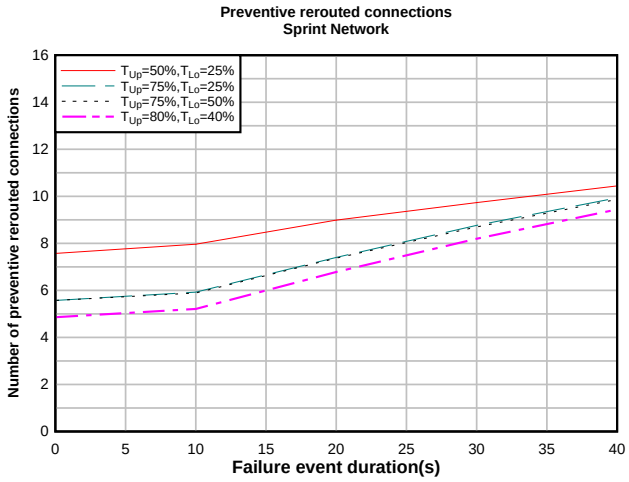
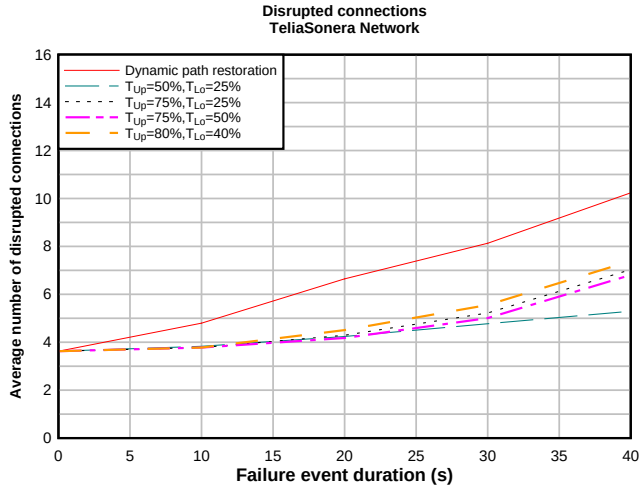
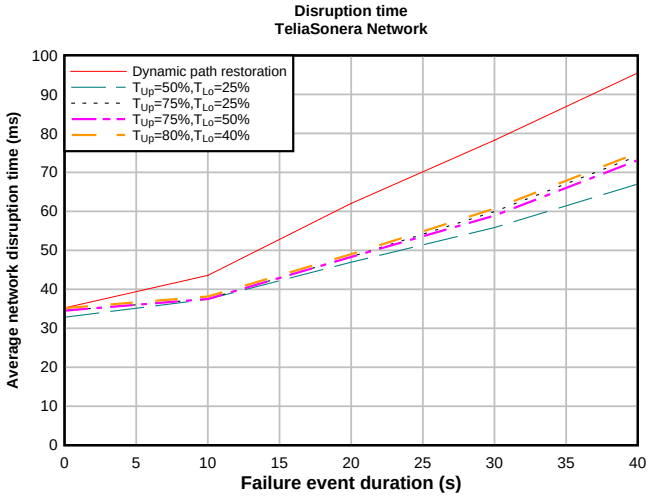


Figure 21. Sprint network performance.

Figure 21 illustrates performance network for the Sprint network.





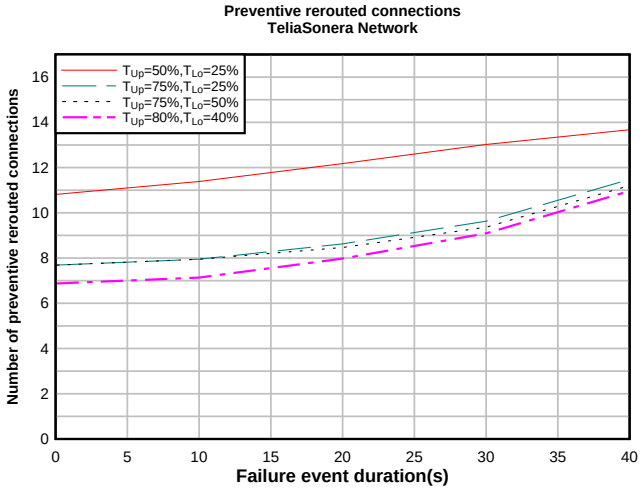
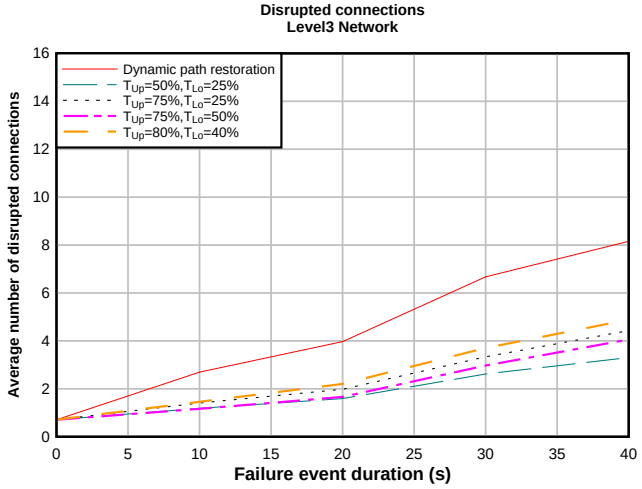
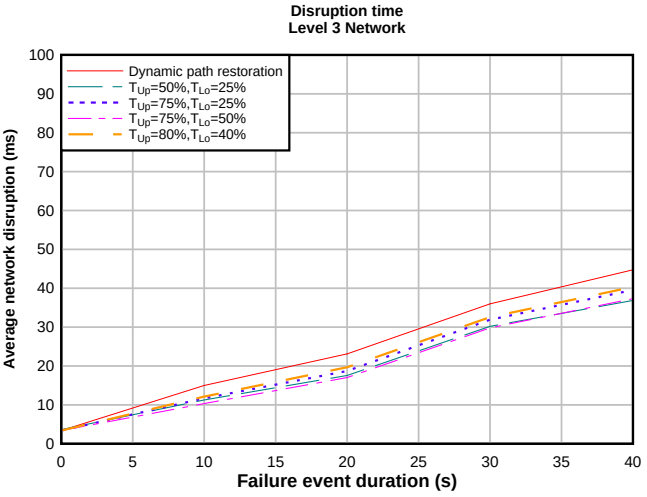


Figure 22. TeliaSonera network performance.

In Figure 22 we show the obtained results in TeliaSonera network.





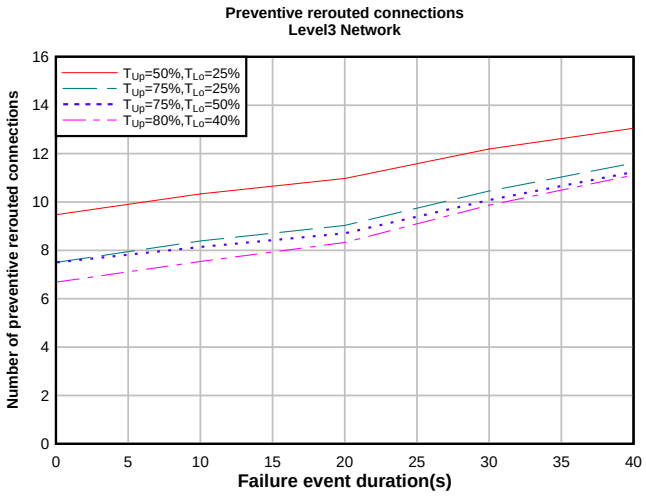


Figure 23. Level3 network performance.

And finally we show the results for the Level3 network in Figure 23.

4.3.2 Performance analysis and discussion

We assume the duration of a natural disaster is about 40 seconds, at which point its destructive energy reaches zero and the disaster ends. As we considered that the disaster propagates with a constant speed of 10 km/s, it covers an area with a radius of 400 kilometers, which is a considerable geographical area. In our simulation model, the network performance of the affected area in different discrete time intervals is investigated.

The proposed preventive protection model was successful in reducing the average number of disrupted connections in all of the studied topologies regardless of how the threshold ranges are selected. The results among different threshold ranges indicate that the selected range has a direct effect on the network performance. In this case, a preventive protection model with a lower value for the upper threshold (Upper threshold = 50%) saved more connections compared to the other scenarios because the proposed model identified more endangered connections and protected them prior to the failure.

The selected threshold range in the proposed model determines the required rerouted connections to increase the network protection level. The results revealed that to provide better protection more connections need to be routed (Upper threshold = 50%), which means more overload on the network. Based on the available network resources and the desired protection level, an appropriate threshold range can be considered

The other performance metric studied in this research was the network disruption time. The results show the preventive protection model could significantly decrease the average network disruption time in all simulated topologies. The selected threshold range in each scenario provides a different level of improvement, which can be employed by network designers to acquire the desired level of resilience.

4.4 Concluding remarks

The proposed preventive protection approach is a novel mechanism to improve network protection and demonstrates the ability to enhance network resiliency in large-scale disaster events. Determination of endangered flow paths can be used to switch their traffic through reliable paths prior to failure. This approach can save connections against upcoming damage and reduce the number of disrupted connections in the network. To indicate endangered and safe paths two parameters (upper threshold and lower threshold) are employed in traffic rerouting and risk determination. A proper adjustment in threshold parameters can lead to enhanced network protection in failure events. The network performance as a result of applying the proposed preventive approach was studied for different failure scenarios among a variety of real-world network topologies. The results showed that the proposed model was able to reduce network disruption and improve network performance significantly under large-scale failure scenarios.

Chapter 5: Risk parameters adjustment

The preventive protection scheme essentially implements some important components of a risk management system for backbone networks. The general framework of risk management in communication networks has been described in detail in [73]. It identifies four aspects of risk management: risk framing, risk assessment, risk response and risk monitoring. The preventive protection algorithm mainly deals with risk assessment and response. For risk monitoring, we assume some kind of a natural disaster early warning system, such as alarms from a network of sensors or first failure detection by the network nodes, is in place. We further assume that the network management system is able to receive notification of the occurrence of failures and continuing reports about how they expand.

For risk assessment in this work we use an earthquake disaster model; i.e. a disaster impact area that starts from an epicentre and expands with time. The idea in preventive protection is to assess the failure probability for each network component such as a link or node using mathematical models in each decision interval[60]. The current risk model is limited to using the relative power of the earthquake wave to evaluate the probability of failure. Our review indicates that more comprehensive models for the impact of such disasters on telecommunication equipment do not yet exist. Also, while the focus of our work is on regional and geographically-contained disasters, the proposed response methods can also be employed in other types of large-scale failures, such as cyber-attacks, provided that proper risk assessment models are developed for such cases.

To mitigate risk failures in a communication network, we should consider the relationship between risk and vulnerability. Applying protection to vulnerable flows

against upcoming threats may reduce the size of damage. In this case high risk flows that are vulnerable to damage should be transferred to a safe area based on the selected risk thresholds. The essential factors influencing the preventive protection model are decision rerouting parameters that specify high-risk and safe zones in the impacted network. Once the end-to-end failure probabilities for the *k*- shortest paths between each pair of nodes are calculated, the preventive protection scheme reroutes the endangered traffic. This decision is based on the chosen upper threshold that indicates the high risk zone.

Although one may expect that selecting a low value for upper threshold would give better protection, it also requires more rerouting, which means more bandwidth overhead and higher restoration delays.

The importance of adjusting decision parameters, their impact on network performance, and the provided level of protection motivated us to conduct a comprehensive study on this matter.

In this section, we develop a procedure to parameterize rerouting decision factors in a preventive protection model to study the effect of different risk threshold values on network performance.

5.1 Initialization risk parameters procedure

The assigned value to the upper risk threshold indicates the endangered zone and based on this parameter, the preventive protection model will predict upcoming failure for the traffic passing through this area as the disaster expands. By changing the upper risk threshold factor, the extent of the high risk area will be changed. We recall that the lower risk threshold represents the safe area and traffic through this area has a higher chance to survive.

In order to study the effect of the risk threshold parameters on network performance, we initialize the upper risk threshold parameter to the highest acceptable value (predefined). This initial value implies the minimum number of preventive rerouting, because by decreasing the upper risk threshold, more and more traffic flows will have to be rerouted. By reducing a predefined fixed value of upper risk threshold, the lower risk threshold will be computed and assigned. By increasing the difference between the upper and lower threshold values, we expect that the endangered traffic will be transferred through a safer area and therefore protect against failure. Obviously, a more secure area should be further away from the epicentre, which means a longer path for the data flow.

The proposed procedure will start with the highest assigned upper risk threshold value and the computed lower risk threshold. At each decision interval (determined by changes in network conditions, predefined intervals, or based on expected expansion of failure impact range), the probabilistic failures for network paths are calculated and a simulation analysis of the number of preventive rerouted and disrupted connections is conducted. Results for each decision interval are recorded and depicted as a trend for all studied steps to give a comprehensive view of the impact of adjusted risk thresholds parameters on traffic protection and network performance.

After examining all the possibilities for the upper risk threshold parameter and recording the obtained results for each decision interval, the proposed procedure increases the difference value between the thresholds and repeats all of the previous steps to obtain new results that depict a new trend for further study. We increase the distance between the thresholds to assess how these differences may affect network efficiency when the preventive model tries to reroute traffic through safer areas.

Here we recall that to reroute traffic through the safe zone it is necessary that a

preventive protection model is able to find a path in this area, otherwise the endangered data will be rerouted through any available path with a probability of failure lower than the current path or leave the flow untouched. Given this circumstance, even with an increasing difference between the thresholds, the proposed model may not be able to pass information through better routes. We show the steps of the proposed procedure for threshold adjustment operation in Figure 24.

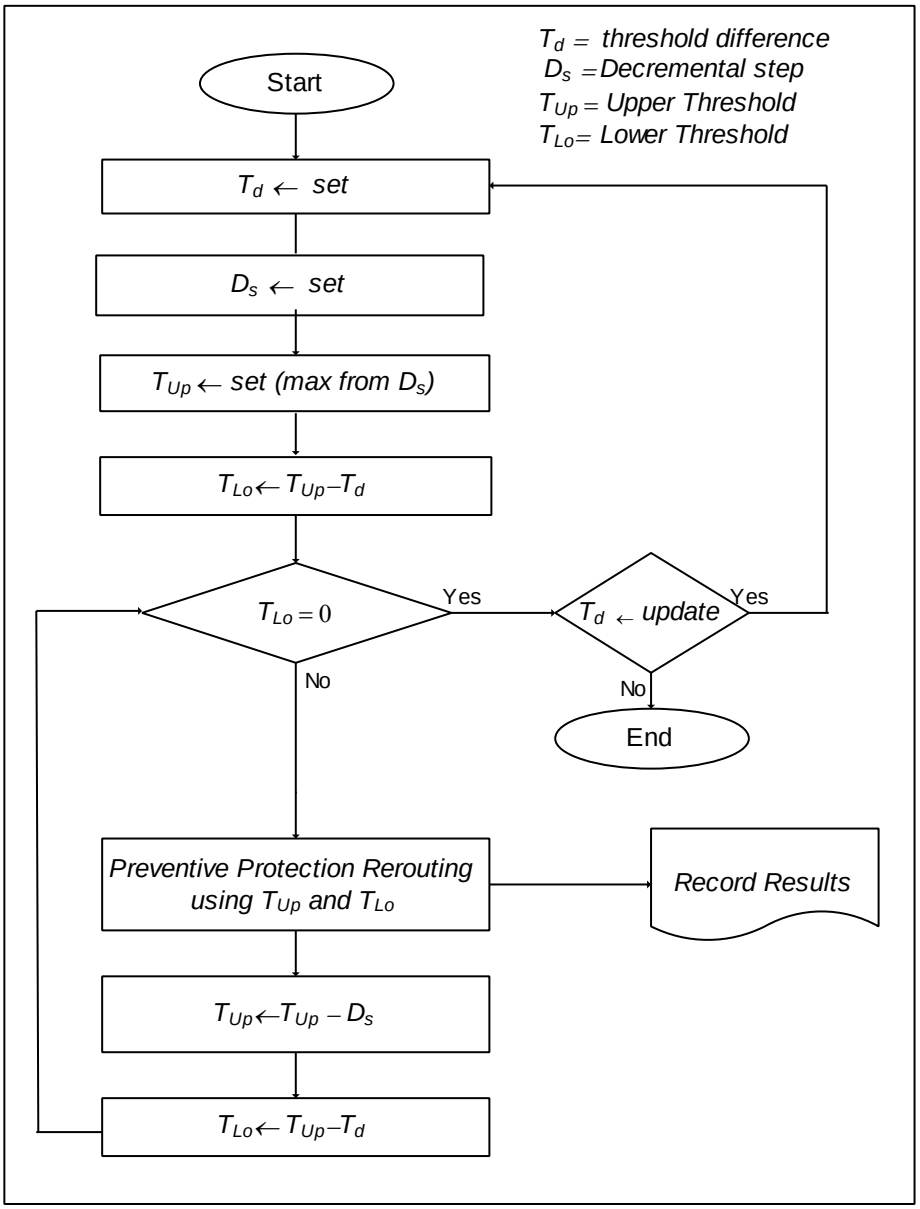


Figure 24. Thresholds adjustment flowchart.

In the illustrated flowchart, T_d is the assigned difference between upper and lower risk thresholds. Different protection scenarios can be modeled by assuming a fixed upper threshold and increasing T_d to compute and assign a lower threshold. D_s is a decremental factor to initialize the upper threshold in each successive step by reducing the upper threshold to a new value in each simulation scenario. This parameter can be adjusted based on the number of required failure scenarios and the expected data results for further process.

5.2 Risk mitigation effectiveness

Rerouting traffic prior to failure is a fundamental aspect of increasing the protection level in the preventive model. Using this approach, the number of disrupted connections decrease and the provided resiliency level improves. Upon failure detection, the proposed model is triggered to transfer information while the disaster expands. Since the preventive rerouting process occurs in the background, it does not interfere with network operation; however it may increase the network overload with the rerouting procedure.

Given that failures in a natural disaster scenario follow a probabilistic pattern, it is important to decide which paths are in danger and require immediate protection and also how to determine more reliable paths to reroute the endangered traffic. It should be noted that routing traffic through longer paths will increase delays and may lead to increased costs. The selected backup routes should provide the required protection level while adding the least cost to the network. It is also important to mention that rerouting connections with a low failure probability and have a higher chance to survive the disaster only increases unnecessary overhead on the network. To address these issues, the proper values must be assigned to the upper and lower thresholds, which can affect network

performance significantly.

In summary, the objective of the adjustment threshold procedure is to achieve the minimum number of required rerouting that would provide an acceptable disruption ratio. If the expected disruption ratio is still too high, the upper threshold is lowered in steps until the desired disruption levels are achieved.

It should be noted that as the failure model in our research follows a probabilistic pattern, the results of each failure scenario may be different. To address this issue, each failure scenario will be studied under several simulation runs.

5.3 Performance evaluation

In this section, we evaluate the performance of the thresholds adjustment procedure by modeling different large-scale failure scenarios. The disaster failure in our work has been modeled as a circular region whose radius expands with a constant velocity (rough model for an earthquake). The network components in an impact area can be nodes and their connected links or part of links. We assume that the failure probability of a node is the same as its connected link. The closest part of each impacted link by the disaster has been used to calculate the failure probability of the link.

At any time, all network components outside the impacted area will be considered in an operational status, while those in the impacted area may fail with a dynamically calculated probability using a travelling wave model as in [60, 74]. The closest part of each impacted link by the disaster has been used to calculate the failure probability of the link. We assume that the failure probability of a node is the same as its connected link. We assume that if a node fails, all its connected links are failed and cannot transfer data. Obviously, full restoration of all flows in a large-scale failure scenario is infeasible. The

reason is that if the source/destination nodes of a flow fail, that flow cannot be rerouted. We assume sufficient capacity for rerouting exists in the network. Capacity optimization in large-scale scenarios is still under research.

We chose *TeliaSonera US L3 Network* with 16 nodes and 29 links for our simulations [75]. We consider end-to-end unit demand between each pair nodes to generate traffic flows. To model the disasters, we assume that the epicentre is always at one of the network nodes.

We simulate disaster scenarios for each node (16 nodes) and compute the average result for 100 simulation runs to allow accurate statistical analysis. The simulation scenarios are presented in Table 6.

Table 6. Threshold differences range and upper and lower thresholds value in each scenario

	T_{Up}:upper threshold, T_{Lo}:lower threshold										
			Initialization steps								
Threshold Difference Range	10%	T_{Up}	95%	90%	85%	80%	...	25%	20%	15%	10%
		T_{Lo}	85%	80%	75%	70%	...	15%	10%	5%	0
	20%	T_{Up}	95%	90%	85%	80%	...	35%	30%	25%	20%
		T_{Lo}	75%	70%	65%	60%	...	15%	10%	5%	0
	30%	T_{Up}	95%	90%	85%	80%	...	45%	40%	35%	30%
		T_{Lo}	65%	60%	55%	50%	...	15%	10%	5%	0
	40%	T_{Up}	95%	90%	85%	80%	...	55%	50%	45%	40%
		T_{Lo}	55%	50%	45%	40%	...	15%	10%	5%	0

To simulate the proposed model we use predefined values for initializing the risk thresholds by considering a fixed difference between them. In each step, we deduct 5%

from the upper threshold to simulate a new failure scenario with updated threshold values. The simulation steps are terminated when the lower threshold value reaches zero. After simulating all steps in the predefined range, we expand the difference between the thresholds to simulate a new failure scenario. By expanding the distance between the thresholds, we evaluate the efficiency of the proposed model in four different rerouting decision models. By increasing the difference between thresholds in each failure scenario, the preventive model tries to find a backup path further away from the epicentre with a lower end-to-end path failure probability.

The predefined assigned values in our model will cover a vast range of upper and lower thresholds with slightly different thresholds in each simulation step. Eventually, the obtained results for all steps are illustrated as a trend for further processing and analysis.

5.3.1 Performance results

Here we present the performance results of the proposed threshold adjustment procedure. We study the number of disrupted connections in the impacted network as an important metric to indicate the provided level of resiliency. The average number of disrupted connections for all nodes in different thresholds ranges (starting with the highest upper threshold) are computed and illustrated as a graph. In each simulation model, we assigned a fixed value to the threshold difference (i.e., 10%) and decrease the upper threshold slightly in each successive step to model different failure scenarios. The obtained results in each step have been depicted with a specific symbol on the graph. After simulating all steps in the selected range, the gap between the thresholds will be expanded to model a new failure scenario.

Figure 25 illustrates the results of the adjustment algorithm on the average number of

disrupted connections. The graph shows four different failure scenarios with different distance values between upper and lower thresholds. The yellow line in the graph illustrates the average result for all the curves.

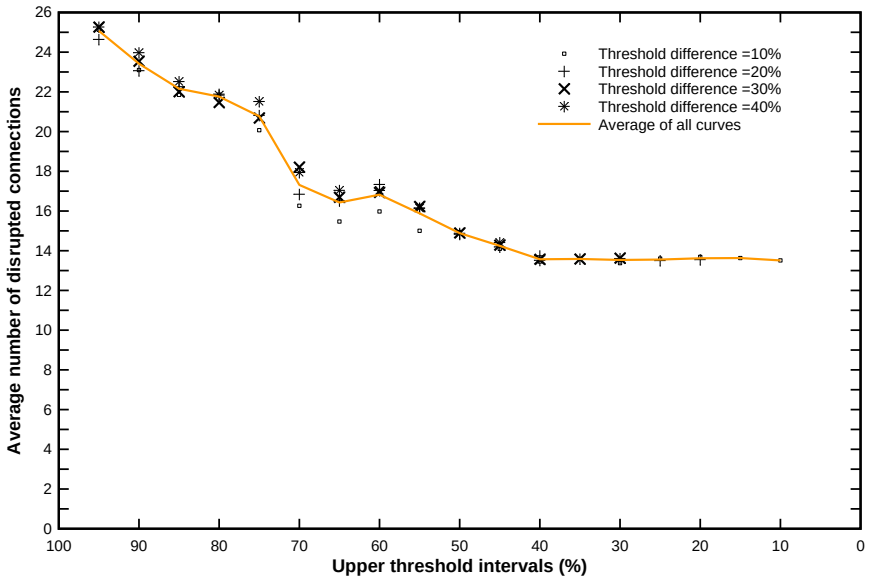


Figure 25. Threshold adjustment results

The rerouted traffic may increase network overload due to damaged links for preventive purposes. We therefore consider preventive rerouting as a metric for each failure scenario. To study this metric in each failure scenario, we assigned a fixed value to the threshold gaps and simulated failures through successive steps of a predefined range of upper thresholds. The studied upper thresholds in each scenario start with the highest value and decreases gradually to cover all the upper thresholds in the range. The average number of preventive rerouting for all nodes in each failure scenario is computed and illustrated as a graph.

By increasing the distance value between risk thresholds, a new failure scenario has been modeled and the results recorded. In this study, we simulated the proposed procedure in four different failure scenarios. The assigned fixed value to the distance

between the upper and lower risk thresholds are based on Table 6 (10%, 20%, 30% and 40%).

The results in Figure 26 show the average number of preventive rerouting connections in four different threshold adjustment scenarios.

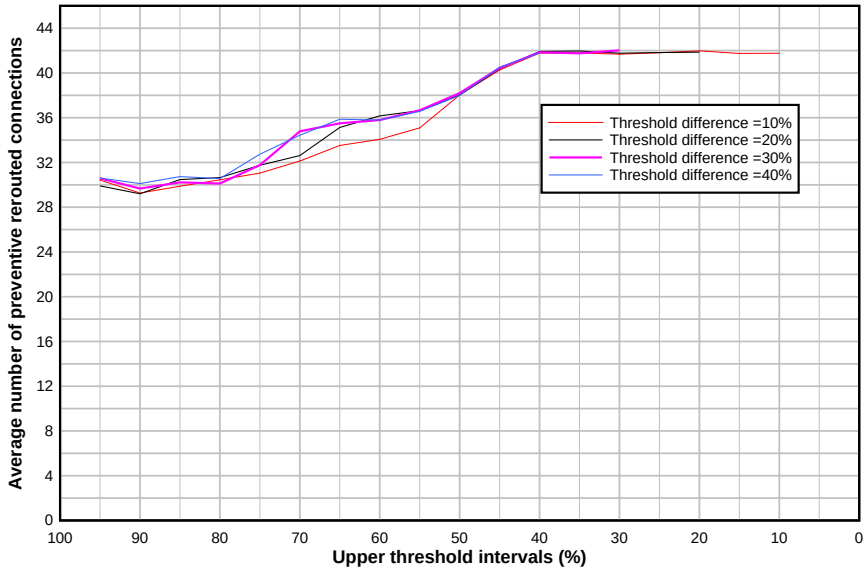


Figure 26. Preventive rerouting in different threshold ranges.

The studied network topology (*TeliaSonera US L3 Network)* contains 16 nodes (cities). Considering the assumption that the epicentre can be located in each city, we examined different failure scenarios and network performance was studied in each scenario (Figure 27). The results obtained for each node (epicentre) indicate the efficiency of applying a preventive model and the improved performance compared to the dynamic restoration approach.

The studied metrics in each node are the average number of disrupted connections (preventive and dynamic restoration) and the average number of preventive rerouting. The average results have been calculated by performing 50 simulation model runs with the upper risk threshold of 70% and lower threshold of 60%. For each city (node) in the

network, three metrics were calculated and the performance results are illustrated in Figure 27.

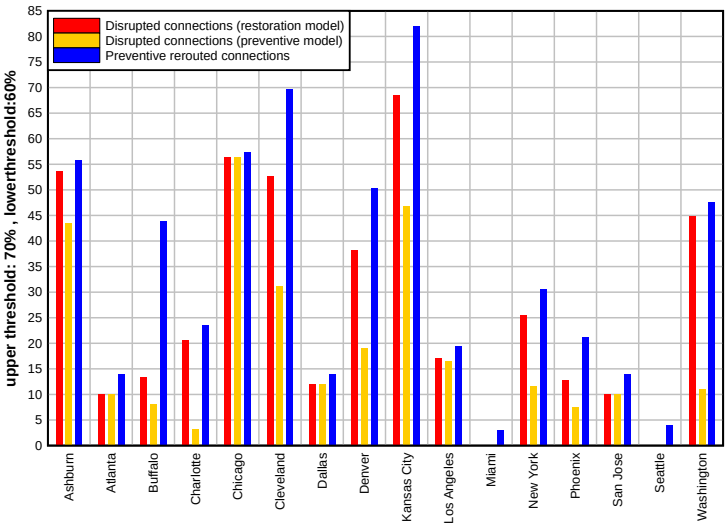


Figure 27. Network performance for upper threshold= 70%.

5.3.2 Result analysis and discussion

As can be seen in Figure 25, there is a sharp reduction at around 70% of the upper threshold value, after which the graph decreases gradually. We can conclude that in general there is a trade-off point after which further reduction in the upper threshold increases the number of reroutings without significantly contributing to network robustness. The results in Figure 26 show the average number of preventive rerouting connections in four different threshold adjustment scenarios.

The results show that different scenarios converge when the upper threshold is equal to 50%. It shows that preventive rerouting can reach a point where the lower threshold at any value gives the same results. The reason can be the lack of available paths with a lower failure probability less than the lower threshold. In this situation, the preventive protection model reroutes the endangered or disrupted connections to any path with a lower failure probability, which is not necessarily in the safe zone.

Figure 26 reveals that the upper threshold in the preventive protection model is the main contributing factor in determining the number of preventive rerouted connections and future disruptions. It is the main decision parameter for network operators. Once they choose an acceptable level of robustness (disruptions under large-scale failure scenarios), they can adjust the upper threshold to achieve that level with minimal rerouting operations.

In Figure 27 we show network performance when the upper threshold is assigned to 70% with lower threshold equal to 60%. As can be seen, the preventive protection model was successful in reducing the number of disrupted connections based on the selected thresholds. In the proposed model, disrupted connections are connections that are able to re-establish after failure. In this example, if an epicentre is located in Miami or Seattle, both the classical restoration method and preventive protection model are not able to restore the damaged connections, which implies that all demands have been lost. The results in Figure 27 also show that the performance of the preventive protection model in some nodes within the selected range of thresholds is significant. The geographical location of these nodes and the available path in the vicinity of the epicentre can affect preventive protection performance.

5.4 Concluding remarks

In this chapter, we provided a method to refine the parameters of a preventive protection scheme in a dynamic and proactive manner with the goal of reducing the number of disrupted connections in large-scale scenarios. We showed why adjusting threshold parameters in this model have an important effect on protecting data flows prior to failure. We developed an algorithm to regulate decision-making probabilistic

parameters employed in preventive rerouting. The proposed algorithm analyzes network performance in different threshold ranges and records the results for each threshold value. The results obtained for different threshold scenarios can be processed by network operators to make decisions on how to adjust threshold parameters. The proposed approach showed that selecting the upper threshold plays the most important role in the protection decision making process.

Chapter 6: Self-adaptive failure mitigation

Here we recall, from the previous discussions that appropriate traffic protection against a time-varying destructive phenomenon serves to prevent damage before it occurs. In this case, the level of risk for traffic routes should be evaluated and the flow should be rerouted to more reliable paths prior to failure. The high-risk paths can be identified based on appropriate decision parameters in a preventive protection scheme as an effective dynamic probabilistic solution to address large-scale failure scenarios.

In this section we develop a self-adapting preventive approach to improve the re-tuning decision parameters. The proposed approach dynamically adjusts decision parameters to provide an appropriate level of protection while the impact domain of the natural disaster expands through the region and increases the risk of failure for network components.

To develop the proposed model we consider topological properties in disaster domain such as network components centrality. In this regard, node and link betweenness are among the parameters that are of concern to network researchers to evaluate network performance or estimate network vulnerability. We determine the impact of such decision factors on the performance of risk-based proactive rerouting.

A disaster event usually occurs for a limited time in a specific region and damages network components in a manner that can be considered probabilistic [72]. Proper protective actions must consider network topology and traffic flow characteristics in the disaster zone as well as the impact of failure on network performance. Protective actions must also be able to adapt dynamically with the damage spreading through the region as the disaster range and impact zone expands. The topological properties of the network

may be different in each interval decision time based on how many links or nodes fail. Therefore, a careful examination of the relationship between the topology of the network and the impact of the disaster on network operation could provide us with insights into how to adjust decision parameters according to dynamic conditions of the network.

By improving the employed approach to initialize rerouting threshold parameters from a fixed and predefined manner to a dynamic and adaptive way, we could enhance the proposed preventive model to act as a perfect protection model in large-scale failure scenarios. Adding adaptation features to the protection model makes it appropriate for protecting data flows in an efficient way that facilitates network management.

In the following we examine a few important topological parameters that play a role in the network protection decision-making process.

6.1 Network components centrality

The strategic importance of some nodes or links in a network can be more than other network components. A node is important in this context if its removal affects the efficiency of the preventive protection. The importance of a node or link may increase the criticality of the paths that are using those components. One way to study the importance of nodes or links in a network is to evaluate its betweenness centrality. With the assumption that data between the source and destination takes the shortest path, our interest is to evaluate the importance of the network components using betweenness centrality. Freeman [76] discussed the importance of node betweenness, which counts the fraction of shortest paths passing a given node. The node betweenness for node $v \in V$ can be shown as:

$$bc(v) = \sum_{s,d \in V s \neq d} \frac{\xi_{sd}(v)}{\xi_{sd}} \tag{8}$$

where s and d are the source and destination nodes of the flow, ξ_{sd} is the total number of available shortest paths between s and d and $\xi_{sd}(v)$ is the number of shortest paths between s and d that pass through node v.

Betweenness can also be applied to links by defining edge betweenness, which is the fraction of the shortest paths between two nodes that run along that link [77]. Edge betweenness for a link in a path between the source s and destination d can be illustrated by,

$$bc(l) = \sum_{s,d \in V s \neq d, l \in G} \frac{\xi_{sd}(l)}{\xi_{sd}} \tag{9}$$

where $\xi_{sd(l)}$ is the number of shortest paths through link l for the data flow between the node s and d.

A failure event may change the relative importance of network components. A low betweenness centrality indicates a link that is not carrying much traffic flow. However it is possible that, due to changes in the network topology because of link or node failures, the shortest paths between pair nodes change as the disaster impact area expands. In this case a link that was previously determined to have low betweenness in the former topology may become part of the shortest paths in the post-failure topology and as a result receives a higher betweenness centrality. In this case, adaptive protection should consider paths using this link as risky paths for further action. Considering the dynamic changes in the network topology and the importance of adjusting the preventive threshold, we propose a new risk threshold parameter in the next section.

6.2 Preserving strategic importance links

The destruction produced by a natural disaster expands dynamically, and over time the destructive energy gradually decreases to zero. The damage caused by natural disasters can therefore be depicted through a time-varying probabilistic failure model, which is more realistic compared to deterministic failure approaches. The seismic gap method may be employed for long-term earthquake forecasting. The assumption is that large earthquakes happen more or less regularly in the region and time because of the gradual accumulation stress and sudden release by failure [78]. However, they are not capable of identifying the exact location, severity of the disaster and the possible size of the vulnerable area.

It should also be noted that the characteristic of the impacted area by the disaster has a significant effect on the damage rate. For example, the rate of damage of an earthquake in a crowded city may be higher than the same disaster in an uninhabited place such as the middle of a desert due to the existence of facilities such as residential communication networks, power grids and similar infrastructure.

The above facts highlight the need for network disaster-protection approaches that are proactive and able to respond dynamically to changes on the ground as the impact range of the disaster spreads or moves. Such schemes should be able to predict the future risk posed to network traffic flows in real time and to take precautionary action, in e.g., rerouting high risk flows to low risk regions to minimize the chance of service disruptions. The most important question in designing proactive risk-based schemes is to develop decision factors for calculating the risk in real time and determining appropriate action based on the perceived risk.

6.2.1 Preventive Rerouting Threshold

To improve the efficiency of preventive protection methods and to make them adaptable with network conditions, we merge upper and lower risk thresholds to one decision parameter called Preventive Rerouting Threshold (PRT). Any path with a failure probability higher than PRT is considered to be an endangered path and its traffic is rerouted through any available path with a failure probability less than PRT. If the model is unable to find a path under PRT, the best available path with the least failure probability is then selected to reroute the data.

By determining the failed nodes and links in each inspecting interval as the disaster impact area expands, we obtain an updated topological status of the network. This information is used to recompute the PRT and adjust the decision parameters adaptive to network conditions. The main contributions of the adaptive model are as follow:

- Decision parameters in preventive protection models will be initialized by network operators [60], however assigning value to PRT in an automated way can improve network management. PRT is computed based on the strength of the disaster, regional characteristics and network topology properties in the impacted area. The computed PRT based on the above knowledge is used in the protection approach.
- PRT is updated as a disaster expands through the region and considering the network status in each interval. Adjusting PRT in each decision interval leads to an updated PRT in tune with the needs of network protection.
- Adapting the protection model with network conditions helps to dynamically determine high-risk paths in each decision interval. It is possible that some

routes, which are considered to be safe paths in the previous interval, are detected as endangered paths with the updated PRT in the new interval and have to be rerouted prior to failure. This property eliminates the need for the lower threshold to determine the safe zone.

The proposed model protects endangered paths by rerouting them through the safe zone that is dynamically determined in each decision interval. The process to compute and assign PRT parameter in the protection model is explained next.

6.2.2 Self-adapting rerouting parameters

A disaster may affect a limited geographical area. Rerouting traffic through paths outside the hazard zone is a static protection approach. The drawback of such static approaches is that rerouting all connections out of the disaster area is costly. In particular, considering that the impact range of the disaster is dynamically expanding, a static rerouting approach would have to be very conservative; i.e. predict the maximum possible range of the impact area and reroute all paths to the farthest regions outside this range, which would result in extremely long backup paths that would consume far more resources than the shortest paths.

On the other hand, failures in large-scale scenarios follow a probabilistic pattern and each network device has a chance to survive the disaster. In this case, there is no need to transfer data from links with low failure probabilities with the intention of safeguarding their information. Additionally, traffic flow priorities can also be considered; i.e. high priority flows can be rerouted while flows with low priority or low probability of failure can be left for the next interval decision.

An appropriate solution to calculate PRT is to consider failure probability and the

strategic importance of links. Figure 28 shows a disaster zone and the affected links and nodes. Each link in the disaster area contains a failure probability and an edge betweenness centrality. The end-to-end path failure probability in a network is greater than or equal to the minimum failure probability of the associated links[60]. If a link has a high failure probability we might argue that any path using that link is at risk. In this case, the failure probability of a link in the disaster zone can be used to assess upcoming path failure probability.

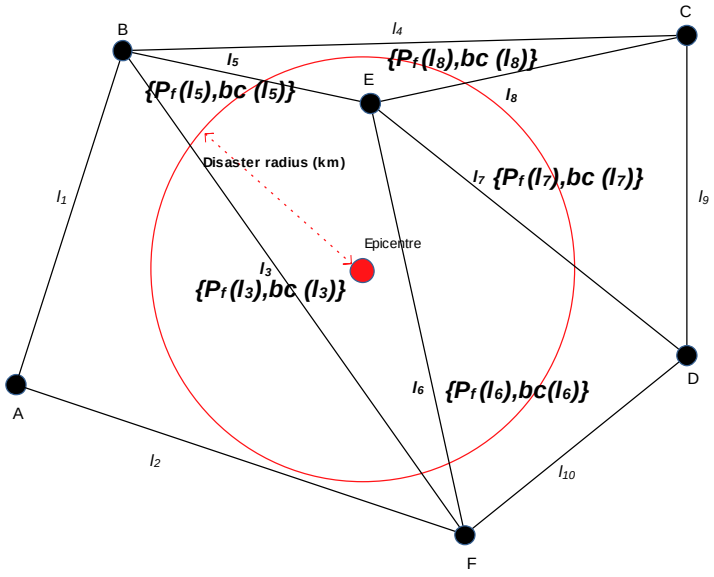


Figure 28. Disaster zone and network topological properties.

To evaluate the strategic importance of a link, we compute the value of link betweenness for each link in the disaster zone. Link betweenness centrality and link failure probability are used to assign a damage risk rate to a link for further protection action as follows:

$$\delta_l = P_f(l) \times bc(l) \tag{10}$$

Here, δ_l is the damage risk rate of link l with betweenness centrality $bc(l)$ and failure probability $P_f(l)$. δ_l can be used to decide whether data passing the link in the disaster

zone needs protection or not. To apply path protection, $P_f(l)$ of the chosen δ_l can be a candidate value for the threshold parameters to indicate the endangered zone. Paths with an end-to-end failure probability more than the determined $P_f(l)$ should be rerouted prior to failure.

The most endangered link in the disaster zone indicates with $max(\delta_l)$. This value may be obtained from a high rate of $P_f(l)$ or $bc(l)$ or both (equation 4). In this case, a high $P_f(l)$ value is not a good candidate for the risk threshold parameter because a high threshold value forces the preventive rerouting scheme to leave more paths intact as they are below the protection threshold. The lack of inadequate protection to overlooked high-risk paths may lead to increase disrupted connections in the network.

$min(\delta_l)$ made of a low failure probability indicates a link in the disaster zone with a good chance of surviving the disaster and connections using this link may remain undisrupted. Assigning low $P_f(l)$ value of $min(\delta_l)$ as a threshold parameter may cause unnecessary preventive rerouting and impose extra unnecessary protection for paths with a high chance of surviving the damage.

To adjust an appropriate rerouting threshold capable of protecting endangered paths with less extra overhead on the network, we employ the average failure probability adapted from the highest and lowest link damage risk rate in the disaster zone. To compute the risk threshold parameter in each interval decision, we consider the maximum and minimum calculated link damage risk rate and determine the associated failure probability. The average of the determined failure probabilities is employed by the proposed model to adjust the rerouting decision factor, PRT:

$$PRT = Avg(P_f(\max(\delta_l)) + P_f(\min(\delta_l))) \tag{11}$$

Changes in topology, resulting from failures due to the impact of the disaster, may alter betweenness centrality for the remaining links, which needs to be recomputed for the post-failure topology in each interval decision. The new betweenness value is used to update the PRT and keep the decision parameter adaptive with the network status. We show the procedure of calculating PRT in the following algorithm:

PRT adjustment algorithm

BEGIN
1: **for all** $l \in E'$
2:$P_{f(l)} \leftarrow$ *Calculate failure probability*
3:$b_{c(l)} \leftarrow$ *Calculate edge betweenness centrality*
4:$\delta_{(l)} \leftarrow P_{f(l)} \times b_{(c)}$
5: **end for**
6: **while** *impact radius < max disaster zone*
7: $P_f\ (max\ \delta_{(l)})$ = *failure probability of* $max\ \delta_{(l)}$
8: $P_f\ (min\ \ \delta_{(l)}\ )$ = *failure probability of* $min\ \delta_{(l)}$
9: $PRT \leftarrow Avg\ (P_f\ (max\ \delta_{(l)})\ , P_f\ (min\ \ \delta_{(l)}))$
10: **if** *impacted components= failed*
11: *remove failed links and nodes*
12: $b_{c(l)} \leftarrow recompute$
13: $\delta_{(l)} \leftarrow recompute$
14: $PRT \leftarrow update$
15: **end if**
16: *expand impact radius*
17: **end while**
END

The computed worst case time complexity for the self-adaptive protection algorithm in a network consists of |E| links and |V| nodes is O(|V^3|) which is polynomial and feasible. In the next section, we evaluate the performance of the proposed model and present our numerical results and analysis.

6.3 Performance evaluation

We evaluate the efficiency of the proposed approach by conducting a simulation of various failure scenarios. The selected network topologies are the European Reference Network (ERnet) with 37 nodes, 57 links and a mean nodal degree of 3.08 and North-American Reference Network (NARNet) with 39 nodes, 60 links and a mean nodal degree of 3.07, which are used in [79] to study dynamic survivable routing in a Multiprotocol Label Switching (MPLS) network. The other applied simulation parameters are the same.

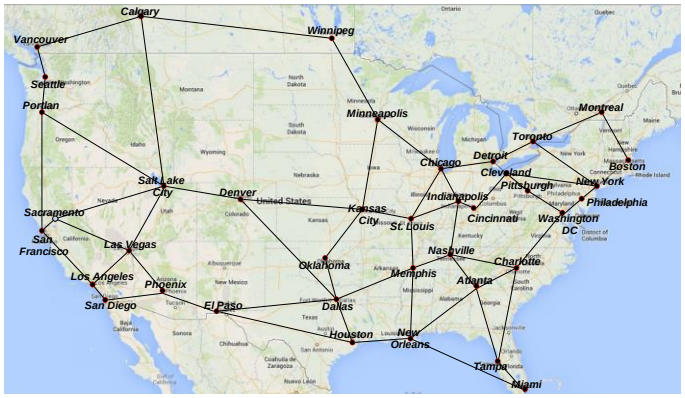


Figure 29. Real-world network topologies: North-American Reference Network (NARNet) [79].

Figure 30. Real-world network topologies: European Reference Network (ERNet) [79].

Figures 29 and 30 show the network topologies employed to study self-adaptive protection. The topologies in our study are undirected graphs. The disaster is modeled in a circular shape with a radius that expands with time. We simulate the disaster duration for 50 seconds.

We model end-to-end unit demand for each pair of nodes to simulate traffic in the network. The possibility of a disaster can be located in any part of the network. To evaluate the efficiency of the proposed model, we simulate the disaster events in several random places in two real-world network topologies.

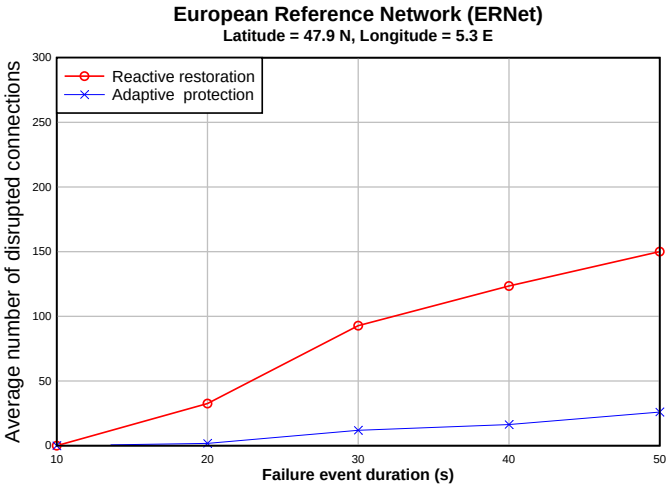
Here the obtained results of two random locations of each network are illustrated with the information provided in Table 7.

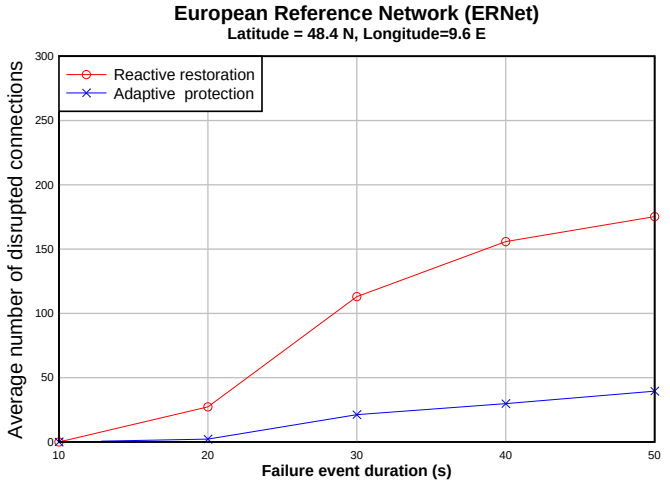
Table 7. Disaster geographical locations

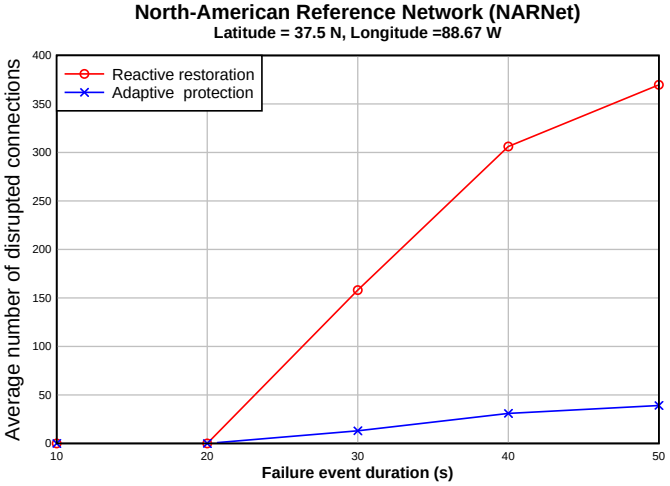
Network	***Geographical coordinates***
ERNET	latitude = 47.9 N, longitude =5.3 E latitude = 48.4 N, longitude =9.6 E
NARNET	latitude = 37.5N, longitude = 88.6W latitude = 40.82N, longitude =80.9 W

6.3.1 Performance results

Figure 31 presents the results of adaptive protection for disaster events in these four locations. The studied parameter is the average number of disrupted connections, which is computed during the disaster scenario (50s). The results illustrate a comparison between adaptive and reactive protection methods for the studied metric.


European Reference Network (ERNet)
Latitude = 47.9 N, Longitude = 5.3 E
Reactive restoration
Adaptive protection
Average number of disrupted connections
Failure event duration (s)
0
50
100
150
200
250
300
10
20
30
40
50


European Reference Network (ERNet)
Latitude = 48.4 N, Longitude=9.6 E
Reactive restoration
Adaptive protection
Average number of disrupted connections
Failure event duration (s)
0
50
100
150
200
250
300
10
20
30
40
50


North-American Reference Network (NARNet)
Latitude = 37.5 N, Longitude =88.67 W
Reactive restoration
Adaptive protection
Average number of disrupted connections
Failure event duration (s)
0
50
100
150
200
250
300
350
400
10
20
30
40
50

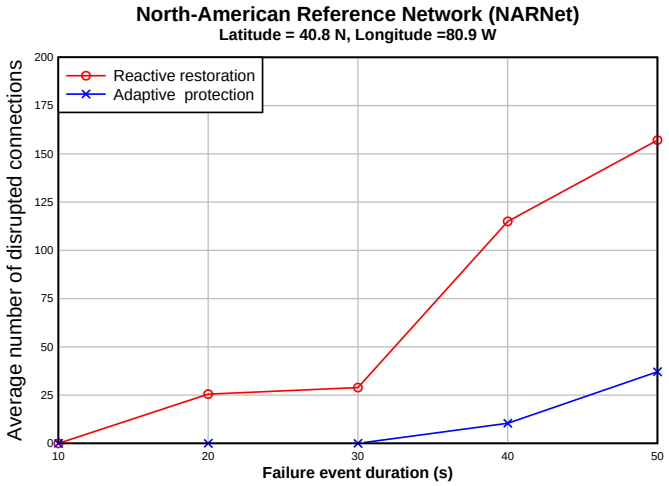
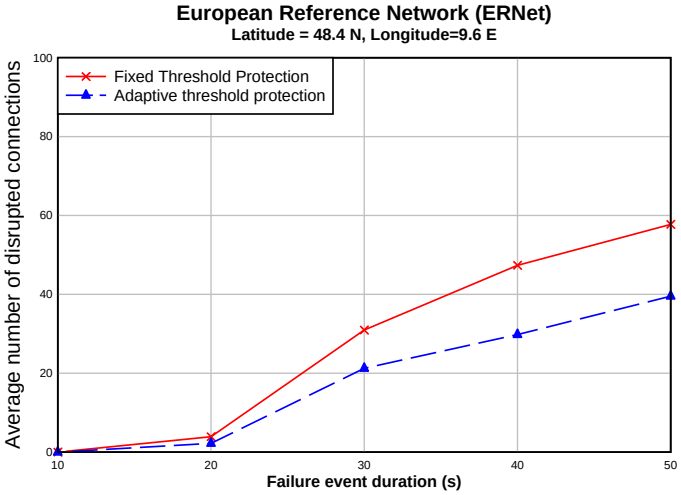
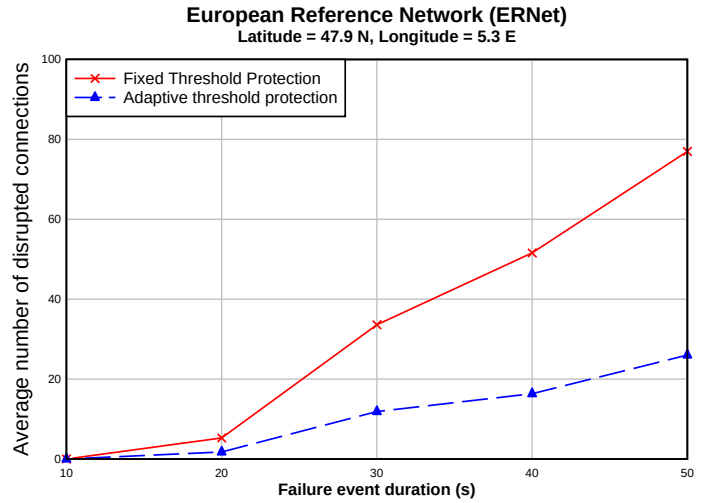
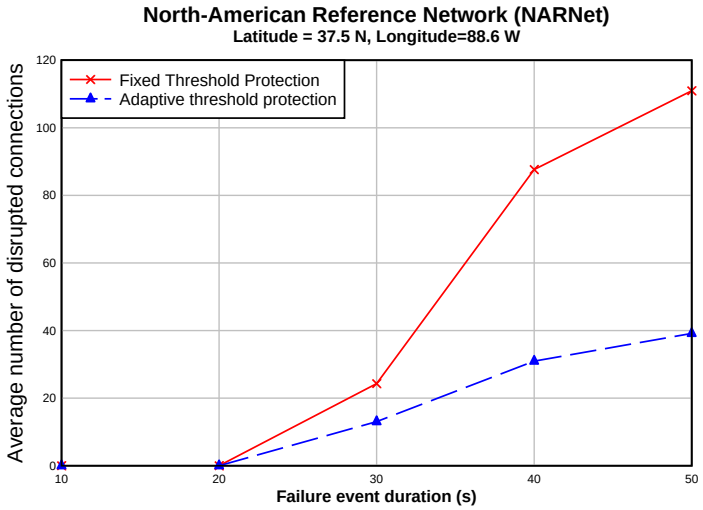


Figure 31. Number of disrupted connections in large-scale failure scenarios.

Figure 32 is a comparison between fixed thresholds protection (upper threshold 75%, lower threshold 50%) and the adaptive protection model.







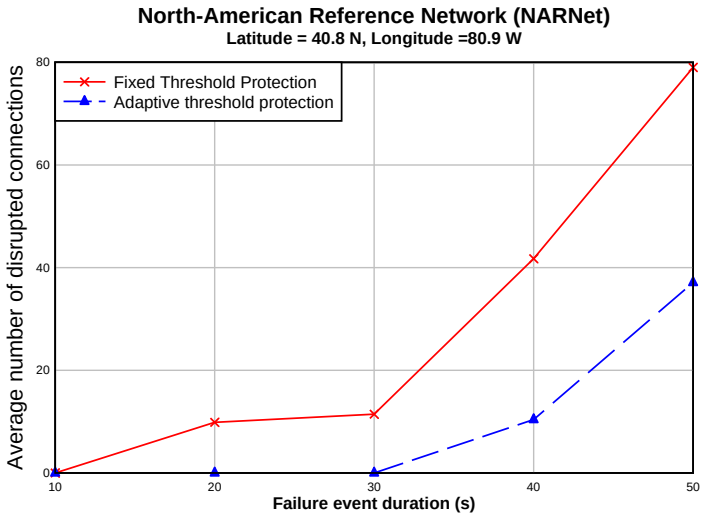


Figure 32. Network performance with fixed and adaptive threshold assignment.

The assigned thresholds in the above performance study are chosen as examples and

can be changed to any other values for further examination. The selected parameter to investigate network performance for reactive and proactive protection approach is the average number of disrupted connections during the disaster event (50s). The results are provided for two random locations in the European reference network and two random locations in the North-American reference network. Each graph represents reactive protection with pre-assigned thresholds and a self-adaptive approach where thresholds change dynamically. Figure 33 demonstrates changes in PRT value in the adaptive protection approach while the disaster expands through the region.

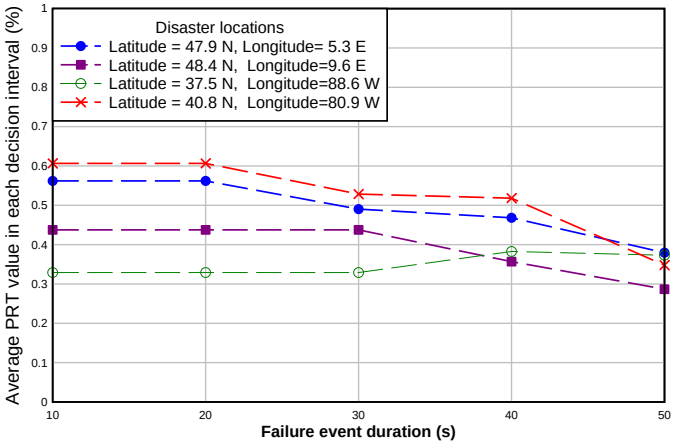


Figure 33. Threshold adjustment with disasters expansion.

The studied parameters are the average PRT values in percentage, for each decision interval (each 10 second). Four random locations in two real-world topologies have been studied with this metric and results are obtained for disaster duration that is assumed to be about 50s.

The results for preventive protection rerouting for the disaster locations in ERNet and NARNet networks are depicted in Figure 34.

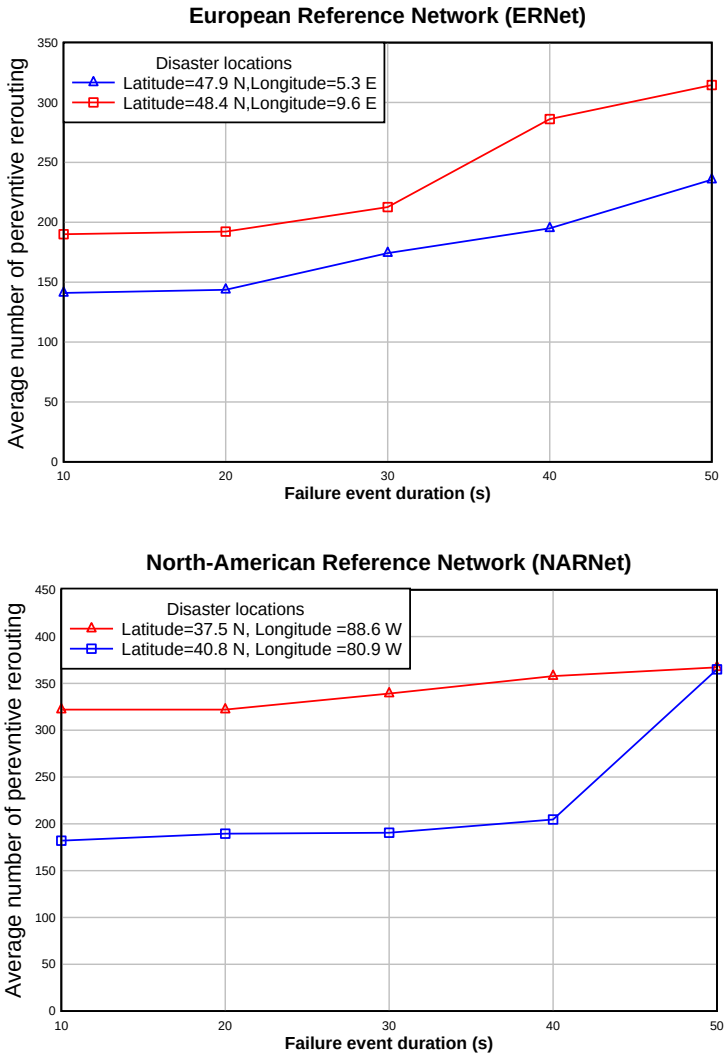


Figure 34. Preventive protection rerouting.

The metric in this study is the average number of preventive rerouting during the disaster scenario (50s). Selected random locations are the same as previous studies as we mentioned earlier.

The obtained results with 95% confidence interval for the interval of $\left(\bar{X} \pm 1.96 \frac{\sigma}{\sqrt{n}}\right)$ are presented in Table 8. Here, $\bar{X}$is the sample mean value, σ is the standard deviation and n is the sample size. The interval value less than 10^{-6} is shown as zero in the table.

Table 8. Obtained results with Confidence Level of 95.0%.

Network			Confidence Level(95.0%) in each inspection interval in second				
			10s	***20s***	***30s***	***40s***	***50s***
ERNet *Adaptive*	lat = 47.9 N lon =5.3 E	Avg. Number of disrupted connections	No Failure	1.76 ± 0.186	11.88 ± 2.018	16.34± 3.278	26.02 ± 7.061
	lat = 48.4N lon =9.6 E		No Failure	2.22 ± 0.377	21.24 ± 3.294	29.8 ± 4.470	39.54 ± 7.087
ERNet *Fixed thresholds*	lat = 47.9 N lon =5.3 E		No Failure	5.28 ± 0.559	33.6 ± 6.008	51.58 ± 8.268	76.98 ± 10.664
	lat = 48.4N lon =9.6 E		No Failure	3.90 ± 0.594	30.96± 4.433	47.36± 5.294	57.74 ± 6.043
NARNet *Adaptive*	lat = 37.5N lon =88.6W		No Failure	No Failure	13.05± 4.909	30.95± 8.990	39.15± 9.789
	lat = 40.82N lon =80.9 W		No Failure	No Failure	No Failure	10.4± 2.362	37.1± 3.511
NARNet *Fixed thresholds*	lat = 37.5N lon =88.6W		No Failure	No Failure	24.3 ± 6.098	87.65± 14.106	110.95 ± 18.306
	lat = 40.82N lon =80.9 W		No Failure	9.86± 1.964	11.45 ± 1.660	41.75 ± 3.719	79 ± 15.844
ERNet *Adaptive*	lat = 47.9 N lon =5.3 E	Avg. valve of PRT	0.56± 0	0.56± 0	0.49 ± 0.00759	0.46 ± 0.01691	0.37± 0.01730
	lat = 48.4N lon =9.6 E		0.43 ± 0	0.43 ± 0	0.43 ± 0	0.35 ± 0.02274	0.28 ±0.02075
NARNet *Adaptive*	lat = 37.5N lon =88.6W		0.32 ± 0	0.32 ± 0	0.32 ± 0	0.38 ± 0.01080	0.37 ± 0.03133
	lat = 40.82N lon =80.9 W		0.60 ± 0	0.60 ± 0	0.53 ± 0.01460	0.52 ± 0.01234	0.31 ± 0.01897
ERNet *Adaptive*	lat = 47.9 N lon =5.3 E	Avg. number of preventive rerouting	141± 0	143.64 ± 0.279	174.24 ± 2.907	194.94 ± 6.589	235.58 ± 8.000
	lat = 48.4N lon =9.6 E		190 ± 0	192.22 ± 0.377	212.66 ± 3.617	286.14 ± 11.223	314.54 ± 8.0399
NARNet *Adaptive*	lat = 37.5N lon =88.6W		322 ± 0	322 ± 0	339.15 ± 5.984	357.75 ± 10.801	367.2 ± 12.837
	lat = 40.82N lon =80.9 W		182 ± 0	189.5± 2.079	190.5 ± 1.714	204.65 ± 6.339	365 ± 40.940

6.3.2 Result analysis and discussion

As can be seen in Figure 31, the number of disrupted connections in the adaptive protection model for all failure scenarios is reduced significantly compared to the reactive restoration approach. The fewer number of disrupted connections translates to more

reliability in the network. Because of the long distances among nodes and links in the North-American Reference Network topology compared to the European Reference Network, it may take time for the disaster to impact network components. During this gap, the impacted network may not experience a disruption in connections.

We have provided a comparison for self-adaptive protection approach, where the threshold parameter can adjust itself based on network requirements and topology properties with a reactive protection model with pre-assigned threshold ranges (Figure 32). The selected parameters in the fixed threshold approach are upper threshold (75%), lower threshold (50%). The results indicate that the adaptive protection model improves network efficiency by reducing the number of disrupted connections compared to the fixed thresholds approach. As the self-adaptive protection model is able to adjust itself with network conditions, the ultimate protection would be applied against failure scenarios. As can be seen, disruption in the network could be significantly reduced during disaster events in the self-adaptive protection approach.

In Figure 33, the behaviour of PRT in different inspection intervals is depicted. PRT can adjust itself in combination with the network status in each decision interval time based on an updated network topology in each interval decision and by considering the disaster area to provide better protection. This can explain why PRT in each failure scenario follows a different pattern. The results indicate that if the network requires more protection and the self-adaptive approach determines that more paths are in danger and should be rerouted through more reliable paths, the threshold parameters change reactively to accomplish this requirement. On the other hand, the proposed protection approach is also able to increase the PRT value to reduce the number of required rerouting when it is determined that network protection can be enhanced with less

preventive rerouting. The results for preventive protection rerouting for the disaster locations are depicted in Figure 33. Based on the rerouting decision parameter's value and topological properties in the disaster area, the number of preventive rerouting paths to improve network protection may be different. The results presented in Figure 34 are directly related to the assigned PRT value and also the number of failed paths that need traffic transferred through more reliable paths.

6.4 Concluding remarks

In this chapter we improved the preventive protection model and made decision rerouting parameters adaptable with network conditions. We considered the strategic importance of the link in the network or link betweenness centrality and failure probability for endangered links to indicate the potential damage risk to each link involved in the impact area. Using the average failure probability of the maximum and minimum computed link damage risks, the proposed protection model calculated and assigned the rerouting decision parameters to reroute data prior to failure. As the disaster may change the network topology, the decision parameter has to be updated in each interval decision according to network conditions.

Chapter 7: Design preventive protection in SDN network

Distinctive features in SDN provide flexibility for network developers to improve new experiments in a much more efficient way. In this chapter we design a protection model in SDN technology and explain the implementation steps in detail. We also study the required time to reroute the considerable number of data flows in SDN Openflow switches and examine the impact of a large topology on the controller when it needs to interact with extensive required data flow updates.

7.1 SDN architecture overview

Separating control plane and data plane in communication networks motivated network developers to introduce Software Defined Networking (SDN). Control plane handles the logic of traffic transmission such as data routing decisions or desired access policies. Data plane is involved in traffic forwarding based on the defined logic in the control plane. Decoupling of these two important cores in an operational network can lead to enhance flexibility for network developers to experiment new ideas independent of the implemented hardware. Controlling the entire network from a central point, using developed software in tune with network requirements, may improve network performance efficiently and reduce debugging or reconfiguration efforts.

Flow tables in switches and routers can be programmed using OpenFlow protocol. The defined configurations and desired policies in the controller are transferred to the OpenFlow switches through a secure channel [80]. Figure 35 shows the connection between controller and switches through OpenFlow protocol. Using OpenFlow protocol, OpenFlow controller instructs OpenFlow switches to update their flow table entries to accomplish appropriate actions [80].

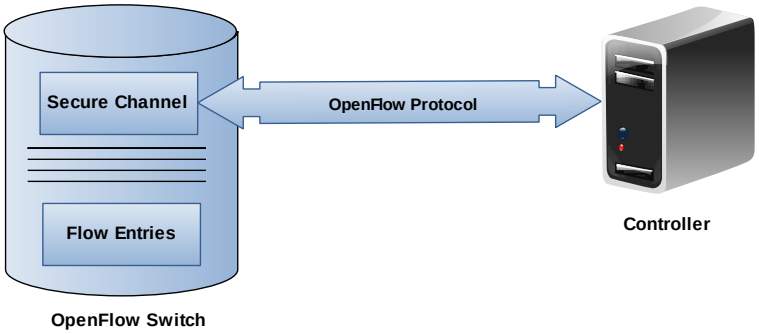


Figure 35. OpenFlow interaction

Along with developments in communication technology, providing a reliable connection is always important for service providers and subscribers. In this regard, network reliability is one of the main concerns for network designers and SDN developers. Network resiliency In SDN technology has been studied in several aspects such as improvement in fast notification to the controller or development in dynamic restoration or pre-planned protection mechanisms which have been discussed in chapter 2 (literature review).

In the literature, the main effort is to respond to failure events through a reactive approach and is mainly focused on single link failure scenarios. Here, our objective is to examine a proactive protection approach in SDN technology using pre-knowledge of potential failures that may affect a part of the network. The proposed model is not limited to a single failure problem and can improve network resiliency in large-scale failure scenarios such as natural disasters or power outages. Considering SDN technology and its features, our previous study of a preventive protection model is [60] fully appropriate and consistent with this concept. In the next section we explain our proposed model to mitigate disaster effects using SDN technology. We apply a preventive protection mechanism to SDN technology to design a new model that is able to address failure issues caused by disasters.

7.2 Disaster protection in SDN paradigm

The available capabilities in SDN technology such as centralized controller, programmability and separation of data and control planes are the features that make this technology appropriate to develop a proactive protection mechanism in natural disaster scenarios. To improve network protection, the proposed model programs and manages data plane using OpenFlow protocol based on flow patterns in the controller. An application on top of the controller defines flow paths for each source and destination and decides how data should be routed in a disaster event. The controller inserts flow entries instructed by the disaster protection application and updates the routing table in each OpenFlow switches. Without SDN features, managing preventive rerouting and applying it proactively would be difficult or even infeasible in disaster scenarios.

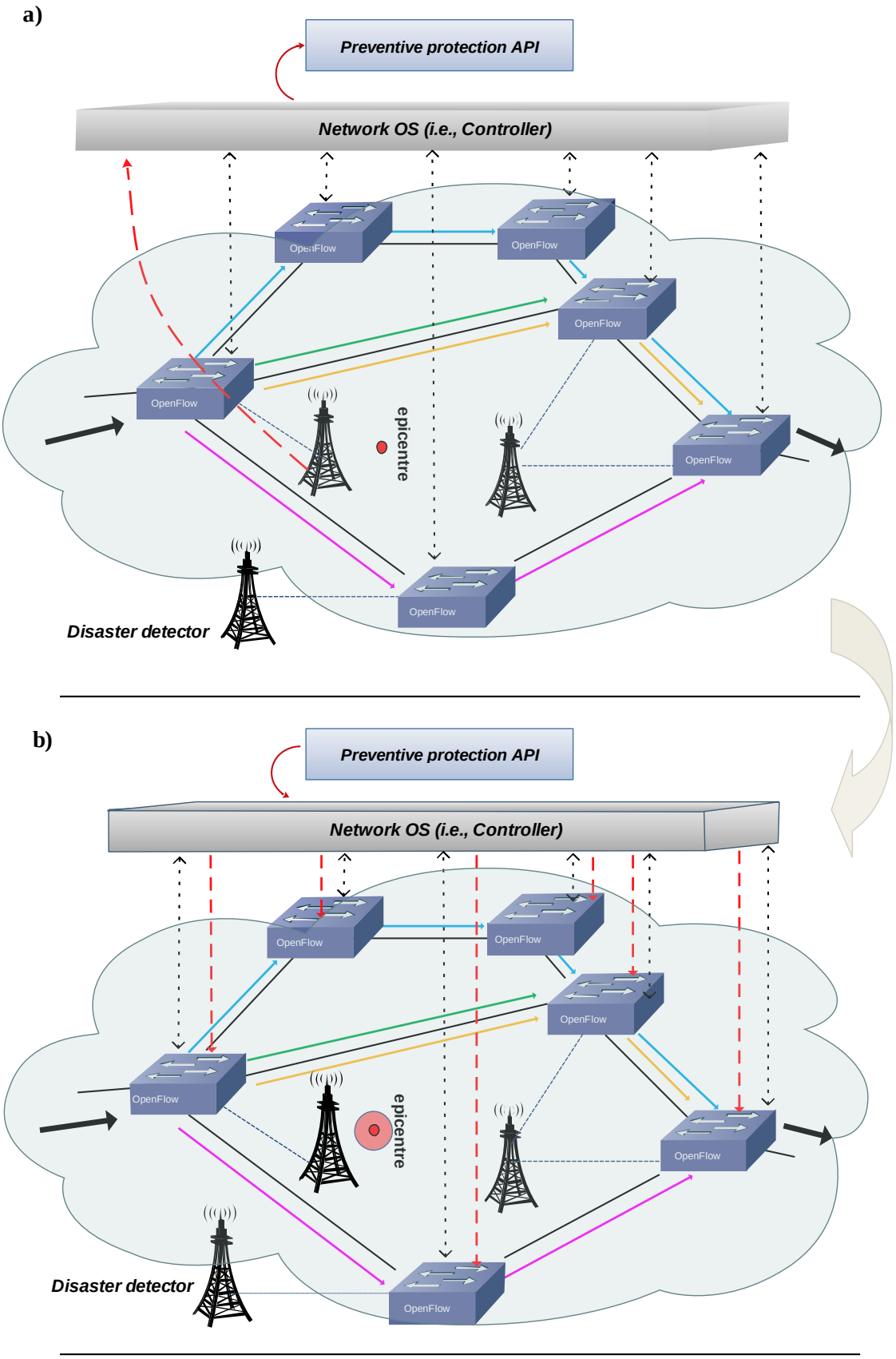
To improve network resiliency in case of natural disasters, the corresponding disaster protection application processes the received disaster's information and sends necessary protection decisions to the controller before a disaster can destroy the entire network. We assume an earthquake-like model in our study, where the velocity propagation can be up to 8.5 km/s depending on geographical characteristics and earth materials [71]. This indicates that the disaster mitigation application and the SDN controller have a sufficient time to decide and apply desired protection policies, prior to damage of substantial parts of the communication infrastructure.

The proposed protection model acts in a proactive way, which makes it distinctive from reactive protection mechanisms in failure scenarios. In a proactive protection mechanism, rerouting decisions are undertaken before a connection is disrupted. In contrast, reactive protection in current SDN technology responses to failures after fault

detection and during a time consuming process reroutes traffic through computed backup paths. Consequently, the delay between failure detection and traffic restoration results in packet loss. Although in preventive protection mechanism some expected reliable backup paths may fail as the applied method is probabilistic, the proposed model is able to save a significant number of connections against upcoming damage.

7.2.1 Disaster mitigation application

The disaster mitigation application is responsible for processing the received data regarding the disaster event. This information can be obtained by sensors designed to detect the occurrence or possible occurrence of natural disasters. The obtained information may include the area and severity of the disaster. Disaster detection or early warning and OpenFlow improvements to generate and send appropriate packets with disaster information are not considered in this thesis and need further research. In this chapter, we assume a disaster mitigation application is able to receive this information. The proposed application listens to the controller and, once a disaster event is detected, the application starts to process the received disaster data. Based on the provided information which is included structural conditions of the disaster area and its severity, the mitigation application computes the failure probability for each of the network components. According to the distance of the network components (node or link) to the epicentre, we may have different failure probabilities for each network component. This information will be used to calculate end-to-end path failure probability between each source and destination nodes. Considering this information, the proposed application is able to determine more reliable paths with less failure probability and send instructions regarding the new paths to the controller. Accordingly, the controller updates flow tables


a)
Preventive protection API
Network OS (i.e., Controller)
OpenFlow
OpenFlow
OpenFlow
OpenFlow
OpenFlow
OpenFlow
epicentre
Disaster detector
b)
Preventive protection API
Network OS (i.e., Controller)
OpenFlow
OpenFlow
OpenFlow
OpenFlow
OpenFlow
OpenFlow
epicentre
Disaster detector

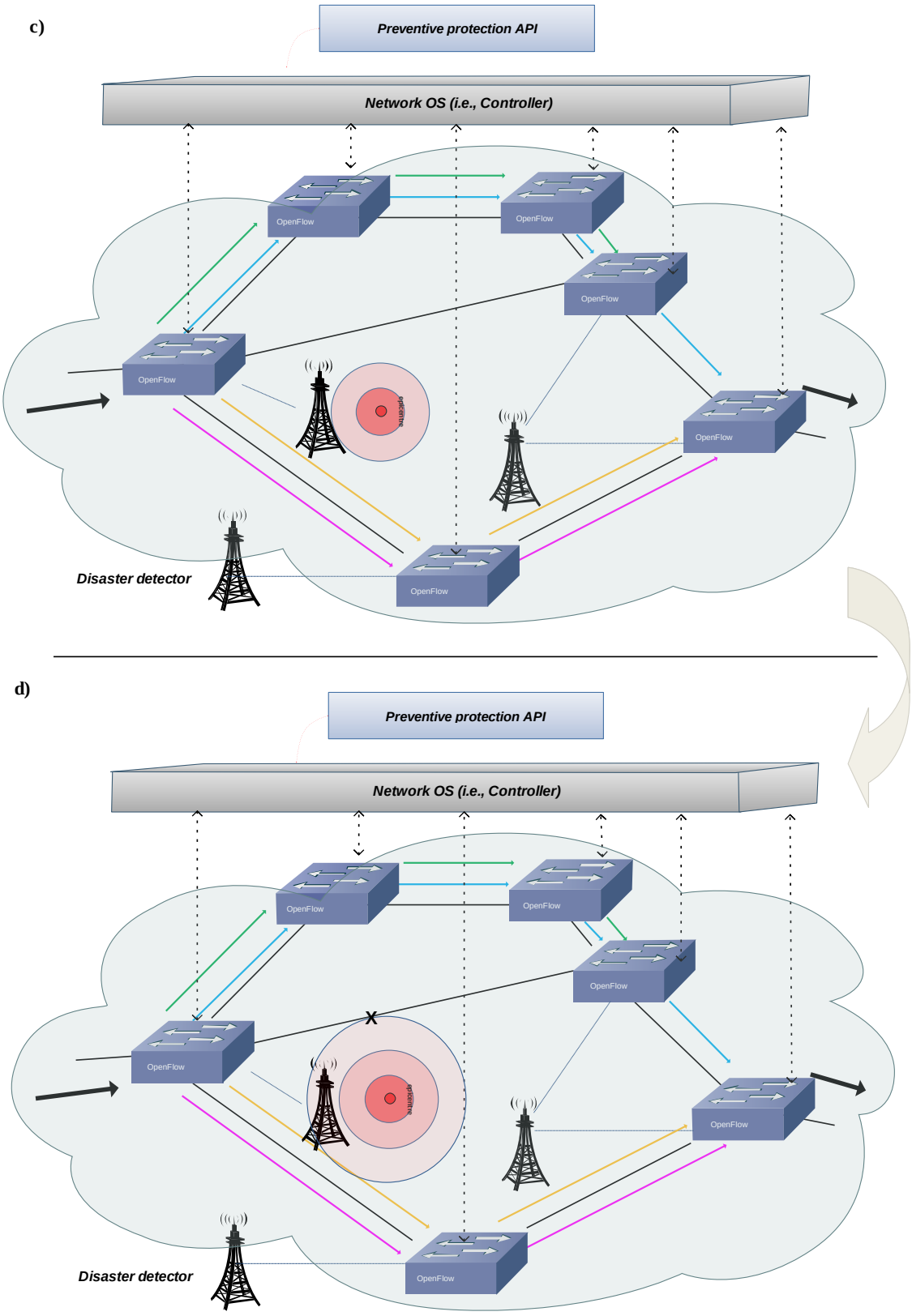


Figure 36. SDN preventive protection steps

for selected OpenFlow switches with new paths and endangered traffic is rerouted through more reliable paths.

In Figure 36 we show the process of the preventive protection in SDN. Figure 36-a illustrates that a disaster sensor detects a possibility of a disaster and sends messages to the controller, which then triggers an event and notifies the preventive protection application. In Figure 36-b, the corresponding application processes the received data and computes reliable paths and sends the policy back to the controller. Afterward, the controller injects new paths and updates OpenFlow switches based on the indicated policy. Figure 36-c shows that while the disaster expands, the traffic of the endangered path is rerouted through more reliable paths determined by the preventive protection application. At a moment of the endangered link failure (Figure 36-d), its traffic has been already moved through new paths and the endangered traffic is therefore protected against failure. By expanding the disaster, if any link or node is damaged, the preventive mitigation application is notified and the traffic of the lost link is rerouted through a reliable path. The contributions of the proposed approach in a natural disaster conditions are:

- Proactive protection approach reroutes traffic of the endangered path prior to failure. In this way, the amount of lost information will be reduced. In contrast, current reactive restoration mechanisms in SDN restore traffic once the controller has been informed and backup paths are determined along with updating routing tables in OpenFlow switches. This process comes with delay which may cause packet loss.
- In the reactive restoration approach, backup paths are calculated by the controller, usually using shortest path algorithm. Since the controller has no knowledge of the

disaster spreading, the assigned backup path may also be damaged by the disaster expansion. In the proactive protection model, traffic is rerouted through more reliable paths with a lower failure probability thus giving them a chance of survival, even with disaster expansion.

- The proactive protection model is able to improve network resiliency in multi-failure events as it follows a probabilistic pattern and the provided protection is based on the available network infrastructure (post-failure topology). This feature perceives the proposed preventive model from a predefined backup path protection method. There is a possibility that in the predefined protection approach, working and backup paths are both damaged with disaster expansion. On the other hand, pre-determining a backup path for a failure situation of a probabilistic nature is very hard or infeasible.

7.2.2 Performance study

We evaluate the efficiency of SDN controller by study failures in European Reference Network (ERnet) with 37 nodes and 57 links and a mean nodal degree of 3.08. Each city in the topology represents a node in our study, which is considered as an OpenFlow switch. We simulate the disaster duration for 50 seconds for a random place, around the east of France (longitude = 47.9 N, latitude=5.3 E). To study the performance of protection in SDN network, we consider an off-line running of the preventive model and instruct the controller using the obtained results. Table 9 shows the required preventive rerouting from the time that the disaster is detected and then for each 10s interval.

Table 9. Instructed number of preventive rerouting to the controller

Interval	Detecting disaster	10s	20s	30s	40s
Number of rerouted paths	141	3	14	11	79

The details of the implementation for the experimental test-bed are provided in Appendix section. Figure 37 shows an overview of SDN test-bed implementation.

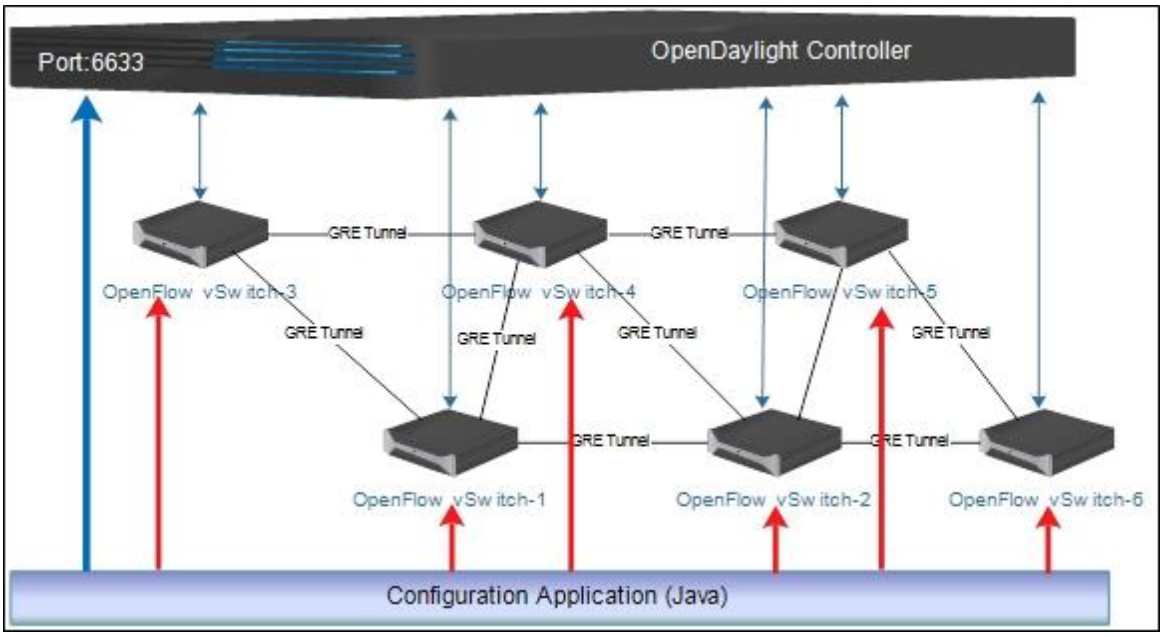
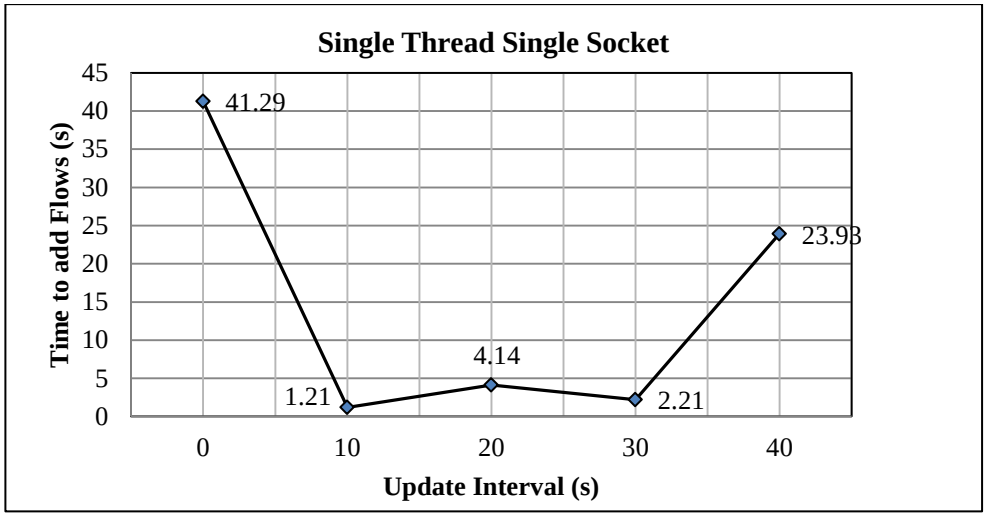
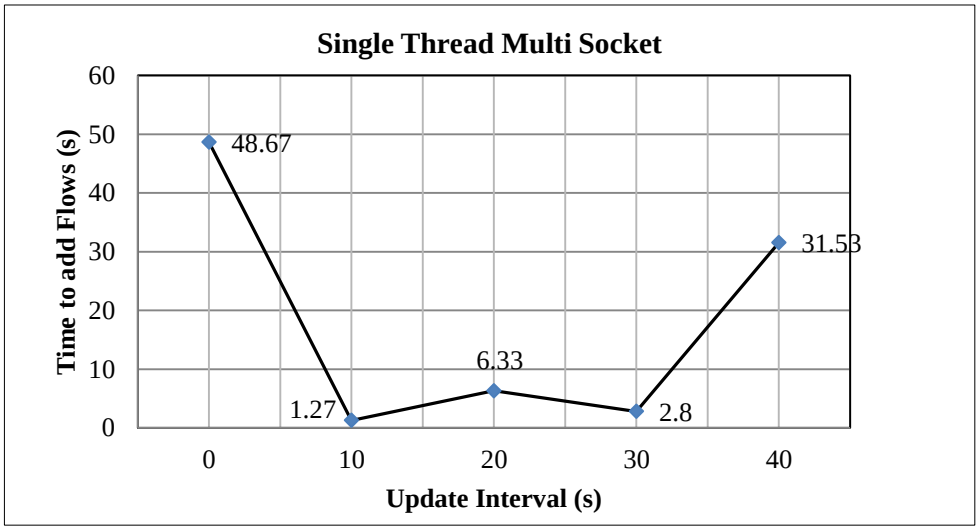


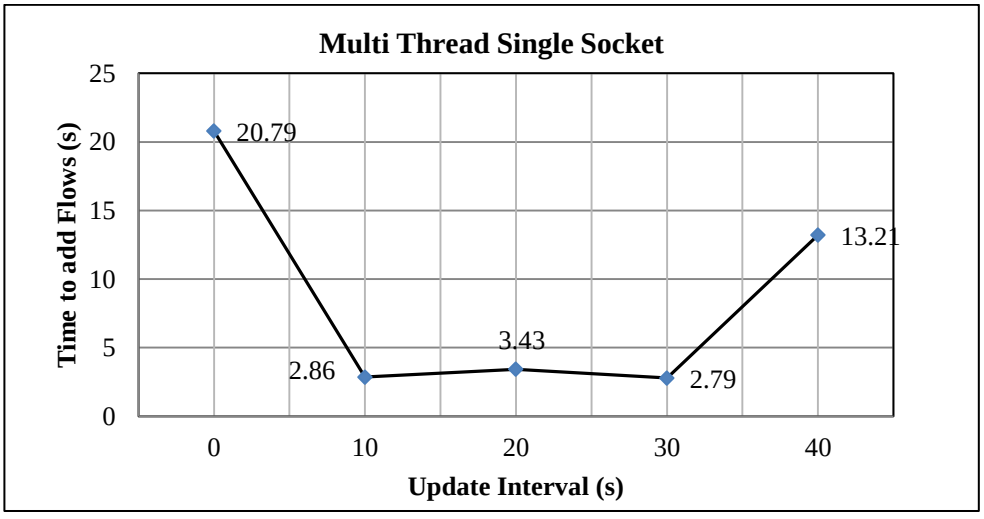
Figure 37. SDN Controller and OpenFlow vSwitches

At the time that a disaster is detected or the possibility of a disaster is predicted, an extensive amount of rerouting is required until the end of the disaster event. In this case, the controller should update a considerable number of paths. As the common way to interact between API and the controller is through http connection, we examine different ways to instruct the controller. To evaluate performance, the required time to add data flow updates is computed. Following approaches are studied to interact with the controller:

- Single thread, single socket, Single thread, multi socket
- Multi thread, single socket, Multi thread, multi socket







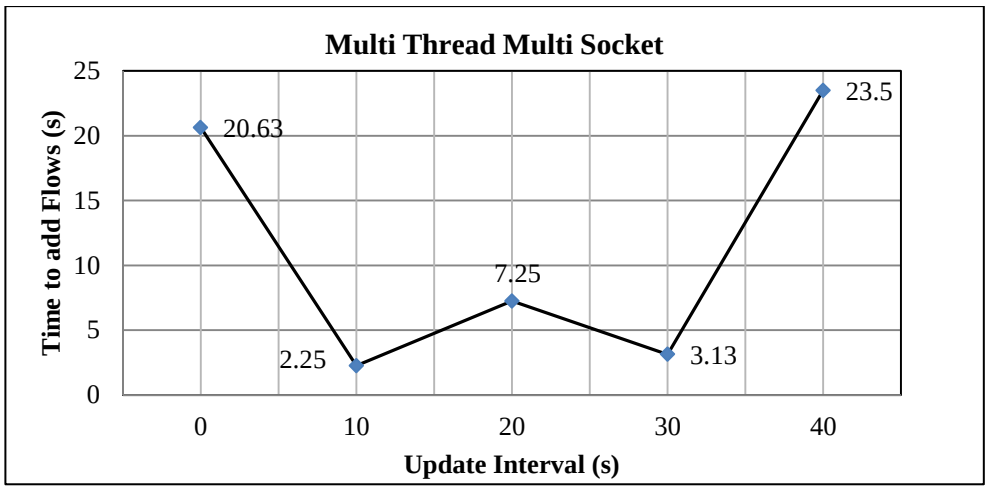


Figure 38. Controller response time in different interaction ways

Figure 38 shows the required time to update the OpenFlow switches flow table using different approaches. In the first approach, single thread single socket, each required update is sent to the controller sequentially. A considerable number of requested data flow updates in the first interval are processed through a time consuming process. By decreasing the number of data flow updates, we can see that the consumed time to update OpenFlow virtual switches flow tables decreases. To improve the controller response time and accelerate the process, we implemented the request in the form of single thread multi socket. The results are the same as the previous approach and indicate that the controller only listens to one port for web connections and the process of applying data flow updates is the same as the single thread and single socket approach. By using multi thread to instruct the controller to apply data flow updates, we can see that the response time decreases considerably (i.e., almost half of the previous approaches). Using a multi thread and multi socket approach shows the same results as explained earlier as the OpenFlow controller interacts with web request through only one port.

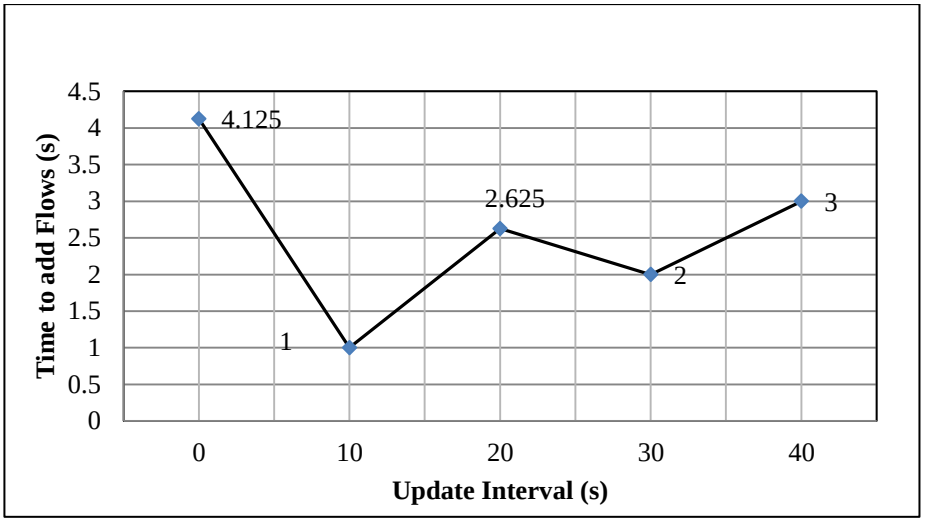


Figure 39. OVS direct interaction.

To reduce the required time to add new paths, we extend our experience to install flows directly to the OpenFlow switches. This extension can be improved as embedded part in the OpenFlow controller as a separate module, specified for disaster recovery.

The results presented in Figure 39 shows that direct interaction with OpenFlow switches can improve the required time considerably. This improvement can be considered for further OpenFlow protocol development to instruct OpenFlow virtual switches without involving controllers and quickly updates data flow tables.

Chapter 8: Conclusion and future works

Network survivability as an important factor to provide reliable communication in large-scale failure scenarios was the main focus of this research. Through this thesis, we provided an extensive study of network survivability in large-scale failure scenarios in both deterministic and probabilistic approaches. We developed an approach considering destructive wave energy behaviour in a time-varying, large-scale failure scenario to compute probability of failures for network components in disaster area. We extended the time-varying probabilistic model and introduced a novel preventive protection approach to enhance network resiliency in large-scale failure scenarios. The developed scheme applied end-to-end path failure probabilities and used switching parameters, called upper and lower thresholds, to reroute endangered traffic through more reliable paths. The results indicate that the proposed model was able to decrease the average network disruption time as well as the average number of disrupted connections. Both improved parameters are important to enhance the level of resilience and ensure undisrupted data delivery in the network. We provided a method to refine the parameters of a preventive protection scheme in a dynamic and proactive manner with the goal of reducing the number of disrupted connections in large-scale scenarios. We showed why adjusting threshold parameters have an important effect to protect data flows prior to failure and studied the influence of them on network performance. We proposed an algorithm to analyze network performance in different threshold ranges and discussed how parameter value assignments can affect network performance and the provided protection level. To improve the preventive protection model and make decision rerouting parameters adaptable with network conditions, we considered the strategic importance of the link in

the network or link betweenness centrality in addition to failure probability for endangered links. These two parameters employed to indicate the potential damage risk to each link involved in the impact area. Using the average failure probability of the maximum and minimum computed link damage risks, the proposed protection model calculated and assigned the rerouting decision parameters in an automated way. As the disaster may change the network topology, the proposed approach was to be able to update decision parameters in each interval inspection according to network conditions. Considering software defined networking as an emerging technology, we designed an approach to improve network protection in large-scale failure scenarios in SDN network. The performance of the SDN controller to apply an extensive number of data flow updates through different http interaction ways was studied.

At this point, our proposed model can successfully increase the required level of network resiliency and apply protection in large-scale failure scenarios. The proposed model can be improved considering several aspects for further studies.

Future research in large-scale failure scenarios includes developing an optimization model to reduce the number of preventive rerouting paths while providing the maximum network resiliency. By optimizing the decision parameters, network resiliency in large-scale failure scenarios can be improved while decreasing the added overhead on the network caused by extra required preventive rerouting.

Although the preventive protection model is distinct from the failure probability estimation process and capable of improving network protection as long as the failure probability of network components are provided, an enhanced process to determine failure probability for each specific disaster scenario such as earthquakes, hurricanes, etc., can be considered as a significant improvement in future studies. This improvement can

be considered as a collaborative effort between IT developers and experts in the study of the disruptive behaviour of natural disasters to estimate the possible failure probability for network components with enhanced accuracy.

Taking into account the SDN technology, develop a disaster mitigation application specified to address failures in large-scale disaster scenarios can be an important development in future. Embedding the preventive protection model in OpenFlow protocol to reduce external application interaction with the controller can be a solution to provide carrier-grade network reliability.

Security features also can be considered as a further development in different parts of the proposed preventive model such as receiving secure messages regarding the disaster information and securely applying threshold parameters.

References

[1] G. Wellbrock and T. J. Xia, "The road to 100g deployment [Commentary]," *Communications Magazine, IEEE,* vol. 48, pp. S14-S18, 2010.

[2] Y. Kitamura, Y. Lee, R. Sakiyama, and K. Okamura, "Experience with Restoration of Asia Pacific Network Failures from Taiwan Earthquake," *IEICE Transactions on Communications* vol. 90, pp. 3095-3103, 2007.

[3] S. Erjongmanee, C. Ji, J. Stokely, and N. Hightower, "Large-Scale inference of network-service disruption upon natural disasters," presented at the Proceedings of the Second international conference on Knowledge Discovery from Sensor Data, Las Vegas, NV, 2010.

[4] Z. Hui, C. Ou, and B. Mukherjee, "Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints," *Networking, IEEE/ACM Transactions on,* vol. 11, pp. 248-258, 2003.

[5] J. P. Rohrer, A. Jabbar, and J. P. G. Sterbenz, "Path diversification for future Internet end-to-end resilience and survivability," *Springer Telecommunication Systems,* pp. 1-18, 2012.

[6] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *Lightwave Technology, Journal of,* vol. 21, pp. 870-883, 2003.

[7] S. Lei, Z. Jing, and B. Mukherjee, "Dynamic provisioning with availability guarantee for differentiated services in survivable mesh networks," *Selected Areas in Communications, IEEE Journal on,* vol. 25, pp. 35-43, 2007.

[8] I. Towhata, "Geotechnical Earthquake Engineering," 2008, p. 75.

[9] B. Bassiri and S. S. Heydari, "Network survivability in large-scale regional failure scenarios," presented at the Proceedings of the 2nd Canadian Conference on Computer Science and Software Engineering, Montreal, Quebec, Canada, 2009.

[10] T. Gomes, C. Simões, and L. Fernandes, "Resilient routing in optical networks using SRLG-disjoint path pairs of min-sum cost," *Telecommunication Systems,* pp. 1-13, 2011.

[11] T. Gomes and L. Fernandes, "Obtaining a SRLG-disjoint path pair of min-sum cost," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, 2010, pp. 582-588.

[12] M. Kiese, V. Marcheva, J. Eberspacher, and D. Schupke, "Diverse routing based on shared risk link groups," in *Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on*, 2009, pp. 153-159.

[13] J. Sterbenz, E. Çetinkaya, M. Hameed, A. Jabbar, S. Qian, and J. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," *Telecommunication Systems,* pp. 1-32, 2011.

[14] *The ns-3 Network Simulator.* http://www.nsnam.org/.

[15] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano, "Assessing the Vulnerability of the Fiber Infrastructure to Disasters," *Networking, IEEE/ACM Transactions on,* vol. 19, pp. 1610-1623, 2011.

[16] M. Menth, A. Reifert, and J. Milbrandt, "Self-Protecting Multipaths – A Simple and Resource-Efficient Protection Switching Mechanism for MPLS Networks," in *NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*. vol. 3042, N. Mitrou, K. Kontovasilis, G. Rouskas, I. Iliadis, and L. Merakos, Eds., ed: Springer Berlin Heidelberg, 2004, pp. 526-537.

[17] M. Menth, R. Martin, and U. Sporlein, "Optimization of the Self-Protecting Multipath for Deployment in Legacy Networks," in *Communications, 2007. ICC '07. IEEE International Conference on*, 2007, pp. 421-427.

[18] L. Ran, W. Xiaoliang, and J. Xiaohong, "Network survivability against region failure," in *Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on*, 2011, pp. 1-6.

[19] A. Sen, S. Murthy, and S. Banerjee, "Region-based connectivity - a new paradigm for design of fault-tolerant networks," in *High Performance Switching and Routing, 2009. HPSR 2009. International Conference on*, 2009, pp. 1-7.

[20] A. Sen, S. Bao Hong, Z. Ling, and H. Bin, "Fault-Tolerance in Sensor Networks: A New Evaluation Metric," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006, pp. 1-12.

[21] M. Vasconcelos and R. Salles, "Resilience in Computer Network Management," in *NETWORKING 2012*. vol. 7289, R. Bestak, L. Kencl, L. Li, J. Widmer, and H. Yin, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 109-120.

[22] W. Chung-Yu and M. Naraghi-Pour, "Path restoration with QoS and label constraints in MPLS networks," in *Communications, 2004 IEEE International Conference on*, 2004, pp. 1278-1282 Vol.2.

[23] J. L. Marzo, E. Calle, C. Scoglio, and T. Anjali, "Adding QoS protection in order to enhance MPLS QoS routing," in *Communications, 2003. ICC '03. IEEE International Conference on*, 2003, pp. 1973-1977 vol.3.

[24] J. Rohrer, A. Jabbar, and J. G. Sterbenz, "Path diversification for future internet end-to-end resilience and survivability," *Telecommunication Systems,* vol. 56, pp. 49-67, 2,2014.

[25] C. Yufei, L. Junyan, and J. P. G. Sterbenz, "Path geo-diversification: Design and analysis," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2013 5th International Congress on*, 2013, pp. 46-53.

[26] Y. Cheng, M. T. Gardner, J. Li, R. May, D. Medhi, and J. P. G. Sterbenz, "Optimised heuristics for a geodiverse routing protocol," in *Design of Reliable Communication Networks (DRCN), 2014 10th International Conference on the*, 2014, pp. 1-9.

[27] M. T. Gardner, R. May, C. Beard, and D. Medhi, "Using Multi-Topology Routing to improve routing during geographically correlated failures," in *Design of Reliable Communication Networks (DRCN), 2014 10th International Conference on the*, 2014, pp. 1-8.

[28] K. Walkowiak, M. Klinkowski, B. Rabiega, and R. Goścień, "Routing and spectrum allocation algorithms for elastic optical networks with dedicated path protection," *Optical Switching and Networking,* vol. 13, pp. 63-75,2014.

[29] S. Sahhaf, W. Tavernier, D. Colle, M. Pickavet, and P. Demeester, "Availability analysis of resilient geometric routing on Internet topology," in *Design of Reliable Communication Networks (DRCN), 2014 10th International Conference on the*, 2014, pp. 1-8.

[30] R. K. Sinha, F. Ergun, K. N. Oikonomou, and K. K. Ramakrishnan, "Network design for tolerating multiple link failures using Fast Re-route (FRR)," in *Design of Reliable Communication Networks (DRCN), 2014 10th International Conference on the*, 2014, pp. 1-8.

[31] L. Hyang-Won, E. Modiano, and L. Kayi, "Diverse Routing in Networks With Probabilistic Failures," *Networking, IEEE/ACM Transactions on,* vol. 18, pp. 1895-1907, 2010.

[32] C. Weidong, I. Stoica, and R. H. Katz, "Backup path allocation based on a correlated link failure probability model in overlay networks," in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, 2002, pp. 236-245.

[33] W. Xiaoliang, J. Xiaohong, and A. Pattavina, "Assessing network vulnerability under probabilistic region failure model," in *High Performance Switching and Routing (HPSR), 2011 IEEE 12th International Conference on*, 2011, pp. 164-170.

[34] W. Xiaoliang, J. Xiaohong, A. Pattavina, and L. Sanglu, "Assessing physical network vulnerability under random line-segment failure model," in *High Performance Switching and Routing (HPSR), 2012 IEEE 13th International Conference on*, 2012, pp. 121-126.

[35] L. Kayi, L. Hyang-Won, and E. Modiano, "Reliability in Layered Networks With Random Link Failures," *Networking, IEEE/ACM Transactions on,* vol. 19, pp. 1835-1848, 2011.

[36] M. Rahnamay-Naeini, J. E. Pezoa, G. Azar, N. Ghani, and M. M. Hayat, "Modeling Stochastic Correlated Failures and their Effects on Network Reliability," in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, 2011, pp. 1-6.

[37] P. K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "The resilience of WDM networks to probabilistic geographical failures," in *INFOCOM, 2011 Proceedings IEEE*, 2011, pp. 1521-1529.

[38] E. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. G. Sterbenz, "Modelling communication network challenges for Future Internet resilience, survivability, and disruption tolerance: a simulation-based approach," *Telecommunication Systems,* pp. 1-16,2011.

[39] J. P. Rohrer and J. P. G. Sterbenz, "Predicting topology survivability using path diversity," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, 2011, pp. 1-7.

[40] K. Vajanapoom, D. Tipper, and S. Akavipat, "Risk based resilient network design," *Telecommunication Systems,* pp. 1-13, 2011.

[41] C. S. Ho and C. Woei, "Differentiated service survivability in WDM backbone networks," in *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*, 2010, pp. 1170-1173.

[42] O. Diaz, F. Xu, N. Min-Allah, M. Khodeir, M. Peng, S. Khan*, et al.*, "Network Survivability for Multiple Probabilistic Failures," *Communications Letters, IEEE,* vol. 16, pp. 1320-1323, 2012.

[43] D. Pereira Junior and M. Camillo Penna, "A new algorithm for dimensioning resilient optical networks for shared-mesh protection against multiple link failures," *Optical Switching and Networking,* vol. 13, pp. 158-172, 7// 2014.

[44] A. Tizghadam and A. Leon-Garcia, "Betweenness centrality and resistance distance in communication networks," *Network, IEEE,* vol. 24, pp. 10-16, 2010.

[45] P. K. Agarwal, A. Efrat, S. K. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "Network vulnerability to single, multiple, and probabilistic physical attacks," in *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, 2010, pp. 1824-1829.

[46] I. Mishkovski, M. Biey, and L. Kocarev, "Vulnerability of complex networks," *Communications in Nonlinear Science and Numerical Simulation,* vol. 16, pp. 341-349, 2011.

[47] S. Boccaletti, J. Buldú, R. Criado, J. Flores, V. Latora, J. Pello*, et al.*, "Multiscale vulnerability of complex networks," *Chaos: An Interdisciplinary Journal of Nonlinear Science,* vol. 17, pp. 1-4, 2007.

[48] E. K. Cetinkaya, A. M. Peck, and J. P. G. Sterbenz, "Flow robustness of multilevel networks," in *Design of Reliable Communication Networks (DRCN), 2013 9th International Conference on the*, 2013, pp. 274-281.

[49] E. Jahanpour and X. Chen, "Analysis of complex network performance and heuristic node removal strategies," *Communications in Nonlinear Science and Numerical Simulation,* vol. 18, pp. 3458-3468, 2013.

[50] Y. Jun, H. Haibo, and S. Yan, "Integrated Security Analysis on Cascading Failure in Complex Networks," *Information Forensics and Security, IEEE Transactions on,* vol. 9, pp. 451-463, 2014.

[51] X. Yongxiang and D. J. Hill, "Attack Vulnerability of Complex Communication Networks," *Circuits and Systems II: Express Briefs, IEEE Transactions on,* vol. 55, pp. 65-69, 2008.

[52] L. Qingjie, F. Jilin, and G. Huanzhi, "Research on a New Network Model for Fault Location Based on Betweenness," in *Advanced Technology in Teaching - Proceedings of the 2009 3rd International Conference on Teaching and Computational Science (WTCS 2009)*. vol. 117, Y. Wu, Ed., ed: Springer Berlin Heidelberg, 2012, pp. 417-424.

[53] A. Bigdeli, A. Tizghadam, and A. Leon-Garcia, "Survivable routing using path criticality," in *Computing, Networking and Communications (ICNC), 2012 International Conference on*, 2012, pp. 793-797.

[54] M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle, "Endurance: A new robustness measure for complex networks under multiple failure scenarios," *Computer Networks,* vol. 57, pp. 3641-3653, 12/9/ 2013.

[55] POX Controller Source Code [Online]. Available: https://github.com/noxrepo/pox , 2014

[56] R. Vaghani and C.-H. Lung, "A Comparison of Data Forwarding Schemes for Network Resiliency in Software Defined Networking," *Procedia Computer Science,* vol. 34, pp. 680-685, 2014.

[57] J. Kempf, E. Bellagamba, A. Kern, D. Jocha, A. Takacs, and P. Skoldstrom, "Scalable fault management for OpenFlow," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 6606-6610.

[58] A. Sgambelluri, A. Giorgetti, F. Cugini, F. Paolucci, and P. Castoldi, "OpenFlow-based segment protection in Ethernet networks," *Optical Communications and Networking, IEEE/OSA Journal of,* vol. 5, pp. 1066-1075, 2013.

[59] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, "OpenFlow: Meeting carrier-grade recovery requirements," *Computer Communications,* vol. 36, pp. 656-665, 2013.

[60] A. Izaddoost and S. S. Heydari, "Enhancing network service survivability in large-scale failure scenarios," *Communications and Networks, Journal of,* vol. 16, pp. 534-547, 2014.

[61] A. Al-Rumaih, D. Tipper, Y. Liu, and B. A. Norman, "Spare Capacity Planning for Survivable Mesh Networks," presented at the Proceedings of the IFIP-TC6 / European Commission International Conference on Broadband Communications, High Performance Networking, and Performance of Communication Networks, 2000.

[62] C. Hongsik, S. Subramaniam, and C. Hyeong-Ah, "Loopback recovery from double-link failures in optical mesh networks," *Networking, IEEE/ACM Transactions on,* vol. 12, pp. 1119-1130, 2004.

[63] Z. Jing, Z. Keyao, and B. Mukherjee, "A comprehensive study on backup reprovisioning to remedy the effect of multiple-link failures in WDM mesh networks," in *Communications, 2004 IEEE International Conference on*, 2004, pp. 1654-1658 Vol.3.

[64] C. Hongsik, S. Subramaniam, and C. Hyeong-Ah, "On double-link failure recovery in WDM optical networks," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 2002, pp. 808-816 vol.2.

[65] S. Shah-Heydari and O. Yang, "Performance study of multiple link failure restorability of shared protection trees," in *Broadband Communications, Networks and Systems, 2007. BROADNETS 2007. Fourth International Conference on*, 2007, pp. 594-600.
[66] M. Mansfield, "Understanding Physics " pp. 281-282, 2005.
[67] R. D. Woods and L. P. Jedele, "Energy-Attenuation Relationships from Construction Vibrations," *Vibration Problems in Geotechnical Engineering* pp. 187-202, 1985.
[68] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture,," *RFC3031 IETF,* 2001.
[69] A. Autenrieth, "Recovery time analysis of differentiated resilience in MPLS," in *Design of Reliable Communication Networks, 2003. (DRCN 2003). Proceedings. Fourth International Workshop on*, 2003, pp. 333-340.
[70] V. Sharma and F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery," *RFC 3469,* 2003.
[71] S. Siegesmund and R. Snethlage, *Stone in Architecture: Properties, Durability*, 4th ed., 2011.
[72] A. Izaddoost and S. S. Heydari, "Analyzing network failures in disaster scenarios using a travelling wave probabilistic model," in *Communications (QBSC), 2012 26th Biennial Symposium on*, 2012, pp. 138-141.
[73] P. Chołda, E. L. Følstad, B. E. Helvik, P. Kuusela, M. Naldi, and I. Norros, "Towards risk-aware communications networking," *Reliability Engineering & System Safety,* vol. 109, pp. 160-174,2013.
[74] A. Izaddoost and S. S. Heydari, "Preventive network protection in probabilistic large-scale failure scenarios," in *Globecom Workshops (GC Wkshps), 2012 IEEE*, 2012, pp. 858-862.
[75] (2014). *http://www.ittc.ku.edu/resilinets/maps/*.
[76] L. C. Freeman, "A set of measures of centrality based on betweenness.," *Sociometry* vol. 40, 1977.
[77] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proceedings of the National Academy of Sciences,* vol. 99, pp. 7821-7826, June 11, 2002 2002.
[78] H. Kanamori, "Earthquake prediction:An overview," *in International Handbook of Earthquake & Engineering Seismology, Volume 81B, edited by W. H. K. Lee, H. Kanamori, P. C. Jennings, and C. Kisslinger,* vol. Academic Press, London, pp. 1205-1216, 2003.
[79] J. Tapolcai, H. Pin-Han, and A. Haque, "TROP: A Novel Approximate Link-State Dissemination Framework For Dynamic Survivable Routing in MPLS Networks," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 19, pp. 311-322, 2008.
[80] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford*, et al.*, "OpenFlow: enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.,* vol. 38, pp. 69-74, 2008.

Appendix

Experimental test-bed and implementation details

We discuss several ways to deploy interaction between API and the controller as following:

a) Single thread, single socket

The first approach is to add the requested flows through REST API and sends requests one at a time. In this situation, we have same socket (IP address + port) for all requests. For the experimental model in this study we use a web access to the controller.

b) Single thread, multiple sockets

The selected controller in this experiment (OpenDaylight) does not allow us to use different ports to establish http connections. To create multiple sockets one solution is to use same port with different IP addresses. To have several IP addresses in the controller, we are allowed to increase the number of ethernet cards in the virtual machine (VM) up to 10. Since one of these connections will be dedicated to the Internet for any required update, the rest can be used for adding several IP addresses and create load balancing in the controller. For this purpose, we assign different IP address to each ethernet card. By running the API, at each time one IP address will be selected and the request will be sent to the controller.

c) Multiple Threads, Single Socket

Rather than running each request sequentially, the other solution is create new thread for each HTTP request and let that request run in its own thread until it has completed.

d) Multiple Threads, Multiple Socket

This solution is a combination of the previous scenarios, trying a mix of multi-

threading and multiple sockets.

To simulate the disaster event we implemented this model in virtual test-bed which we explain in following.

Experimental evaluation has been implemented on a Dell CS24-T4 server with 32GB memory, 12 Intel Xeon CPUs with 2.133 GHZ frequency on 925 GB hard drive capacity. The test-bed is implemented in virtual platform. Hypervisor in the platform is VMware ESX-i. To distribute the physical server and create more virtual machines with load balancing among them, we added another ESX-i server to the cluster in the VMware vCenter. Each virtual machine has been configured with CentOS 6.5 and OpenVSwitch (OVS) 2.1.2. acts as a node of the chosen topology.

Each OVS VM has 2GB memory with 11 GB allocated hard disk. To be able to test ping between source and destination, each OVS VM needs to have a host connected to it. In order to configure a host for each OVS VM, we created another VM and assigned a bridge port (i.e., br10) of OVS to have connection to the host. Tiny Core Linux is the best option to have a light operation system in this extra layer of virtualization. Tiny Core Linux operating system can run well on only 17 MB hard space and 128 MB RAM. In our experimental test-bed, we configure Tiny Core Linux OS on top of the CentOS using VirtualBox with 128 MB memory and 256 MB disk space. This extra configuration adds another layer of virtualization and complexity to the system. The controller in the experimental model is configured with OpenDaylight software running on one of the CentOS VMs. The selected IP address scheme for this experiment is 10.10.0.0/16. Table 8 shows the IP addresses distribution among VMs.

Table10. IP addresses scheme in experimental test bed.

Device Name	IP Address(s)	Description
OpenDaylight Controller	10.10.0.100	
OpenVSwitches (nodes)	10.10.X.0	"X" refers to the switch number
Hosts	10.10.X.10	"X" refers to the switch number
Physical server	10.10.0.1	
Desktop PC	10.10.0.2	

As the OVS is a software switch, it should be installed on top of the existing system. It also should be able to tie to physical port using bridge. The bridge acts as a middle interface between the OVS software and the physical ethernet port. For example in each OVS we create a bridge called br0 and attached its port to the physical ethernet port. The associated IP address will be assigned to br0 and not to the ethernet port. To make possible that two OVSs interact to each other and keep configuration persistence, we need an overlay link between them such as generic routing encapsulation (GRE) tunnel. The GRE tunnel will be configured in another bridge (i.e., br0) and makes up link between two switches.

By adding IP addresses to the OVSs and configure GRE tunnels among them, upon loading OpenDaylight, the graphical interface of the controller shows the nodes and links via a http connection.

By looking at the topology, we can see some adjacent nodes are located far away from each other. In this case, sending a packet from a source to the destination with considerable distance will cause propagation delay. To apply this delay, we have

calculated the actual distance between adjacent nodes (cities) in ERnet topology using google map distance tool with an acceptable approximation.

To simulate propagation delay for each link we use traffic control (TC) module in Linux, however this module is not awareness of software bridges (i.e., br0, br1, etc.) employed by OVSs. TC properties should be applied to the physical port (i.e., eth0) directly. The problem with this is that if we configure our entire overlay GRE tunnels that connect to various switches on top of this port, then any delay configuration on the physical port will be applied to all GRE tunnels, resulting in each tunnel having the same delay value which is in contrast with our goal.

To address this issue, TC should be applied directly to each physical port. In Linux VM we are able to extend ethernet ports to maximum 10, means that we can connect each OVS to maximum 10 other switches. Here we recall that, based on the selected topology, maximum OVS connections are 6 and this feature can fulfill our requirements by adding extra physical ports to each Linux VM. For each added physical port, we create an individual bridge and then configure tunnels among switches with different source and destination IP addresses. In this way, we are able to apply delay to each physical port and simulate propagation delay.