Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics
Department of Telecommunication and Media Informatics

Targeted network protection solutions against earthquakes

Scientific Students' Association Report

Author:

Márton Molnár

Advisor:

Dr. Alija Pašić
Ferenc Mogyorósi

2021

Contents

Kivonat

Az Internet, mint a világ legnagyobb mesterséges hálózata, megkerülhetetlen része lett életünknek és napjaink információs társadalmában az egyik legfontosabb kritikus infrastruktúrának számít. Az utóbbi évtized technológiai forradalma miatt egyre több alkalmazás igényli a kis késleltetésű, nagy adatsebességű kommunikációt. Az olyan alkalmazások, mint például a valós idejű irányítórendszerek, nagyon érzékenyek bármilyen kiesésre, súlyos következményekkel járhatnak, ezért rendkívül fontos ezen kapcsolatok védelme.

A hálózati eszközök kiesését gyakran emberi mulasztás okozza (például link átvágások), de az átviteli és telekommunikációs cégeknek olyan kihívásokkal is szembe kell nézniük, mint a nagy hatósugarú katasztrófák. Katasztrófa sokféle okból következhet be, beleértve a természeti eseményeket (például földrengések, hurrikánok stb.), az emberi hibákat, vagy akár a rosszindulatú támadásokat. A természeti katasztrófák gyakran súlyosan érintik a kommunikációs hálózatokat, olykor országszintű kieséseket okozva, akár hosszabb időre.

A hálózatok megbízhatóságának növeléséhez 3 fő területet hívhatunk segítségül: a hibamodellezést, a hálózattervezést és a megbízható útvonalválasztást. A kutatásom során egy olyan keretrendszert fejlesztettem tovább, az úgynevezett FRADIR-t (FRAmework for DIsaster Resiliance), amely e három területet egyesítve garantálja a megszakítatlan adatforgalmat regionális hibák esetén is. Kutatásomban kifejezetten a földrengések elleni védekezésre fókuszáltam, mivel ezekről a dokumentált múltbéli események alapján pontos valószínűségi modelleket lehet létrehozni és a hálózatra gyakorolt hatásuk is jól meghatározható.

A pontos hibamodellezésnek köszönhetően a hálózat irányított fejlesztése nagyban hozzájárul a magas megbízhatóság eléréséhez, ezért a hálózat szétesésének valószínűségét elhanyagolható szintre szükséges csökkenteni. Ez a hálózatfejlesztés egy helyesen megválasztott megbízható útvonalválasztási megoldással kombinálva már képes garantálni a megszakítatlan kommunikációt. A hálózattervezésnél ezért azon közös kiesési kockázatú linkcsoportokra (SRLG) kell fókuszálni, amelyek kiesése a hálózat szétesését okozzák (vagyis amelyek minimális vágást alkotnak). Dolgozatomban új hálózatfejlesztési algoritmust is javaslok, az optimális megoldást biztosító ILP-hez képest tö-

redék idő alatt képesek eredményt adni.

Továbbá a dolgozatomban a megbízható útvonalválasztás kérdésével is foglalkozom. Vagyis bemutatom a hálózati kódolás (Network Coding) alapú útvonalválasztás előnyeit a hagyományos GDP-R útvonalválasztáshoz képest. Emellett a hibamodellezés, a hálózattervezés és a megbízható útvonalválasztás egymásra hatását is vizsgálom.

Abstract

The Internet - the largest artificial network in the world - plays a key part in our lives and has become the most important critical infrastructure of telecommunication. Thanks to the technical innovations of the past decade, low latency and high data speed are required by many services around the world. It is inevitable to protect the telecommunication network connections with increased awareness.

The reasons for network failures are often human errors (e.g. cutting a link during construction works), but the telecommunication networks need to be prepared for extensive disasters that may lead to multiple failures. These might be caused by natural disasters (e.g. earthquakes, tsunamis, floods), but also malicious attacks (hacking, electromagnetic-impulse attacks, weapons of mass destruction). Disasters like these often lead to extensive errors in the networks and cause service outages for longer periods. My study focuses on improving the resilience of networks in all aspects against future earthquakes with the lowest possible cost.

To increase the reliability and accessibility of telecommunication networks, we can approach the problem from three different aspects: failure modeling, network planning, and survivable routing. During my experiment, I continued the development of FRADIR (FRAmework for DIsaster Resilience) that aims to guarantee low disconnection probabilities even during large-scale natural disasters. In my paper, I focused on earthquakes using probabilistic models to determine their impact on the network with adequate accuracy.

With the help of a correct failure modeling phase, the targeted upgrade of network links increases the availability of the network. The targeted network planning and a correctly chosen routing algorithm can guarantee communication without interruptions if no disaster disconnects the network. That is why the goal is to minimize the network's probability of falling apart. During network planning, the main focus should be on the shared risk link groups (SRLG) disconnecting the network (they form a minimal cut in the network). In my experiment, I propose a novel network planning algorithm with a negligible runtime but fairly reasonable results.

Furthermore, in my paper, I deal with the question of survivable routing. I present the benefits of network coding compared to the traditional GDP-R routing of FRADIR.

Chapter 1

Introduction

The various impacts of the current pandemic have highlighted the importance of reliable communication networks and services. Changing user behaviour (e.g., online education and home office) increased network traffic and the required Quality of Service (QoS). In addtion, the spread of mission-critical services such as telesurgery and the stock market is steadily increasing. Their availability is highly dependent on the performance of the underlying networks. The availability and reliability of the communication infrastructure are usually quantified as Quality of Resilience (QoR) [55, 14, 56], which should be very high for mission-critical services. These properties are determined not only by the underlying network infrastructure, but also by the proper use of resources and technologies, and by the scientific knowledge to establish communication paths for such services in a reliable way.

Although network connectivity disruptions during construction are often the leading cause of service outages on the Internet, operators of large transport networks may also face additional challenges, such as natural disasters due to the national or continental extent of their networks [46]. Nonetheless, today's communication networks are still designed to account for the failure of only a single link [26] or link-pairs [25], and are not prepared for disaster scenarios. Such a traditional approach is clearly not sufficient to meet current requirements and challenges [46]. Therefore, proper failure modeling, network planning, and routing schemes and processes (i.e., protection mechanisms) can help us create truly reliable networks and services that our society can rely on even in catastrophic circumstances [36, 46].

Disasters refer to significant network outages in which telecommunication equipment in a particular area becomes inoperable. Disaster may can occur for a variety of reasons, including natural events (such as earthquakes, floods, fires, hurricanes, tsunamis, tornadoes, etc.), human error (i.e., technical failures that can lead to cascading outages), or even malicious attacks (hack-

ing, electromagnetic pulse attacks (EMP), or the use of weapons of mass destruction (WMD)) [19, 46]. In particular, natural disasters often affect the performance of communication networks by causing multiple node/link failures in disaster areas.

The increasing frequency of disaster-related massive outages seen over the past two decades magnifies the importance of the problem [46]. In order to ensure the high availability required by many network services (a common availability requirement is "five-nines", i.e., 0.99999), it is crucial to apply resilience mechanisms that can ensure adequate protection and fast recovery in disaster scenarios. Therefore, it is not surprising that disaster resilience of communication transport networks is of great interest [45, 19, 28].

Natural disasters are often modeled by regional outages, which can have different sizes and shapes. To cope with multiple link failures, the concept of Shared Risk Link Groups (SRLGs) was introduced. An SRLG consists of a set of links that are assumed to have a high probability of failing simultaneously. Regional failures by definition, correspond to a joint failure of nodes/links located in the affected geographic area [30, 29, 53], which form different sets of SRLGs. Most of these failure modeling approaches try to find the right tradeoff between the accuracy and the state space explosion (i.e., the number of SRLGs). Note that the number of SRLGs in these models can be reduced if the topology provides some basic connectivity even after regional failures, while maintaining accuracy. Therefore, jointly considering independent single link failures for reliable topology design and SRLGs to find disaster-resilient paths for the connections would further improve the end-user's perceived availability.

FRAmework for DIsaster Resilience (FRADIR) is the first framework to jointly leverage failure modeling, network planning, and survivable routing to ensure disaster resilience. It was originally introduced in [41] and showed that it is not sufficient to plan the network only for the steady-state, since the network is very frequently disconnected by disasters. Therefore, the framework was further refined in [42] by introducing novel components for failure modeling and network planning.

In the refined FRADIR-II framework [42], independent random failures and regional failures were jointly considered to model the impact of disasters. First, an infrastructure against random failures called *the spine* was designed to guarantee some availability to the working paths (WPs). In a second step, building on the SRLG approach to model disaster-related outages, a probabilistic regional failure model [57] was applied using a modified Euclidean distance of an edge to the epicenter of a disaster to generate a failure list that is considered more realistic than previous approaches. Based on the generated list, a link upgrade strategy was proposed that attempts to reduce the probability that the regional failures in the list will disconnect

the network. These frameworks used a special family of survivable routing algorithms: General Dedicated Protection (GDP [8, 5]), which ensures instant recovery from any protectable failure pattern (given for example as an SRLG list).

Although FRADIR/FRADIR-II demonstrated the benefits of jointly considering network planning, failure modeling, and survivable routing against disasters, there was still room for further improvements in all dimensions of the framework (e.g., rigid, predefined link upgrade steps depending on the topology). Most issues were addressed by eFRADIR introduced in [37]. It improved the FRADIR-II framework in several aspects (e.g., network upgrade and routing costs or algorithm runtime) to obtain more accurate disaster models and algorithms that help meet the requirements of mission-critical communication services. It utilized a novel a earthquake model built on historical seismic data for more realistic failure scenarios. Nevertheless, many questions remained unanswered:

- Can a heuristic algorithm find an optimal solution for the disaster-resilient network planning problem?
- Can the runtime of the heuristics be further reduced?
- Are network-coding-based routing methods applicable in the framework?

In this work, I focus on these questions and present several possible improvements in the eFRADIR framework:

- A minimization algorithm that can continuously monitor the necessity of the link upgrades performed by the heuristic algorithms and discards any unnecessary upgrade step.
- A novel disaster-resilient network planning method which uses a spanning tree to reduce the problem space of the network upgrade problem.
- The applicability of routing methods based on network coding in the context of eFRADIR.

In Chapter 2 I present the related works and the evolution of FRADIR schemes. In Chapter 3 the details of the state-of-the-art eFRADIR framework are presented, which are necessary to understand my contribution. In Chapter 4 after presenting the already existing heuristics that are used are baselines, I present the essence of my work, I introduce two novel approaches, the so-called minimization algorithm, which improves the performance of the existing heuristic, and in addition, I present my own new tree-based heuristic. In Chapter 5 the experimental results are presented, and a novel routing

aspect is introduced to the framework of FRADIR. In particular, I investigate the possibility and the performance of a network coding-based routing approach.

Chapter 2

Motivation and Background

In this chapter, I present some of the historical events which had a significant impact on telecommunication networks to highlight the importance of disaster resilience. Furthermore, I present the related work regarding survivable routing and network resilience in general. Section 2.1 discusses a few significant network outages caused by natural disasters or human errors. In Section 2.2 , I introduce the availability of a network, initialize the SRLG concept, and the Mercalli scale for the links' intensity tolerance. Section 2.3 shows some of the existing solutions for planning and managing a survivable network, including different routing algorithms. Finally, in Section 2.4 I present the concept of network coding, which is a possible option in networks to guarantee a better availability or a better bandwidth utilization, compared to any other routing algorithms.

2.1 Lessons Learned from Disasters

When a natural disaster occurs, the time required to restore the network can be measurably long, and the consequences of the outage can significantly affect the lives of people in the affected region. For example, earthquakes, tsunamis, floods or forest fires can cause the network to be down for several days (i.e. an internet blackout).

Some natural disasters have caused major network outages: Hurricane Katrina hurricane in 2005 crippled the power supply system and caused a ten-day outage of some network nodes, resulting in an only 85 percent availability [24]. In 2011, the so-called "The Greatest Japan Earthquake" not only damaged underwater links but also caused the failure of 1,500 telecommunication switches [21]. In the past century, fires have been recorded all over the world, some of which even burned wires and disrupted (or completely destroyed) communication between the nodes [64] (e.g., the fire around Greece

Year	Type	Area of impact	Consequences for communication networks
2005	hurricane Katrina	USA	long-lasting massive failures of nodes due to power supply faults
2006	earthquake (magnitude of 7.1)	Taiwan	failures of seven submarine optical cables connectivity between North America and Asia disrupted for several weeks
2011	earthquake (magnitude of 9.0)	Japan	failures of undersea optical links about 1500 telecom switching offices affected
2017	hurricane Maria	Latin America Mexican Gulf	no cellular communications in the affected area no Internet in Dominicana
2018	Attica fires	Greece	communications in the affected areas hardly possible
2020	cyclone Amphan	Eastern India	cuts of about 100 fiber links by falling trees reduction of the available network capacity down to 65-70% in the affected areas

Table 2.1: Examples of massive failures due to natural disasters [37]

in 2018). There was also a famous outage recorded in eastern India caused by Cyclone Amphan, which severely affected a forested area, destroying trees and resulting in torn cables - leading to 65% network availability. See Table 2.1 for further details.

Human errors can pose a serious threat, whether they are intentional or unintentional [27], such as the "Black Day of Facebook" from October 2021. The outage was - of course - unintentional, but since it lasted more than 5 hours worldwide, it is one of the largest network outage recorded in the modern Internet era. Although the failure Google experienced in 2013 lasted only 5 minutes, it reduced the Internet traffic by 40 percent during that time period [54]. Intentional failures (attacks) are another interesting topic. For example, in 2018 GitHub received a DDos attack with traffic of 1.35 Tbps (which is relatively high), it caused GitHub to have difficulty maintaining the quality of its service for about 20 minutes [31]. Physical attacks, such as bombs or other types of weapons of mass destruction can cause a whole new level of network outages that we may not have even seen yet.

2.2 The Fundamentals of Network Resilience

With a well planned network topology supplemented with a survivable routing mechanism it is possible to reduce / minimize the chance of any users experiencing outages and to improve the quality of the network. In this specific approach, the quality is measured with the metric called QoR (Quality of Resilience) [55]. This metric focuses on the availability of the network and the metric is designed to objectively rate the networks in terms of availability. Natural disasters, malicious attacks or even human errors often generate

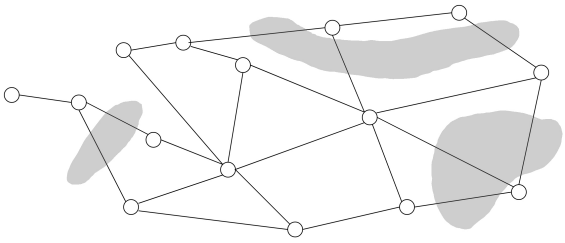


Figure 2.1: Example for Shared Risk Link Groups (SRLGs)

large outages in telecommunication networks, where a fairly big area of the network is unable to serve the requests for a long time. The time period that is required to recover the network's stable state depends on the size of the outage.

In order to guarantee the required availability (by standards), it is important to apply targeted methods to improve the resilience of the network. For telecom networks, the desired availability is referred to as 'five-nines'. It means that the network is available and functioning for 0.99999×365 days out of 365 days, thus the allowed unavailability time is less than 5 and a half minutes.

One of the most important things to keep in mind about natural disasters is that the range of the affected area can be relatively large, and there are not just single link outages on the network, but multiple link outages or regional outages [15]. The types of past events with accurate statistics can be modeled.

A probabilistic model can be created that indicates which coordinate on Earth (Longitude and Latitude) is at risk from an earthquake of a given magnitude. This modeling system can be used in the network planning phase - if we know the links that are at greater risk, we can focus more on their resilience in a targeted network planning. In my experiment, I used the FRADIR framework [35], which combines failure modeling, network planning, and survivable routing to simulate a real network and measure its resilience.

In real networks, there are usually many groups of links that together form what is called a shared risk link group (SRLG) with a higher probability of the network falling apart. Falling apart in this context refers to the notion of connectivity from graph theory, since networks can be represented by weighted graphs, and leads to a new definition called Shared Risk Link Groups (SRLGs). An SRLG is a group of links in the network that are located in an area that is physically at risk of possible failure of multiple links.

It is important to focus on disaster resilient network planning and survivable routing so that the network will still function after a natural disaster. Recently, a magnitude 6.5 earthquake hit Greece and surrounding countries, but several stronger earthquakes have also been recorded with greater impact on telecom networks. To measure the degree of resistance of an object to earthquakes, we can use the Mercalli scale [62]. The Mercalli scale has 12 values and each value describes how buildings and structures (even natural objects like rocks or the structure of the earth) will respond to a particular earthquake with that Mercalli level. For example, level 6 means that objects in a house may fall out of place and poorly structured or weaker buildings may crack, but level 10 means that well-structured buildings will be destroyed, rails will bend, and roads will collapse. Using this analogy, an initial intensity tolerance level was described for each link in the measured networks. This initial intensity tolerance for the network is level 6 of this Mercalli scale, which, as described above, seems most appropriate for a link in a telecommunications network in an advanced country.

So basically for each connection I assign this number called intensity tolerance with a value of 6 and create a list of these intensity tolerances. Of course, this value can be improved, which has a positive effect on the resilience of the network. If we increase the intensity tolerance of each link to a value of 7, the probability of the network collapsing in the event of an earthquake in its area decreases. In order to know which links have a higher risk in terms of the impact of an earthquake, the SRLGs have been described previously.

2.3 Survivable Network Design

Resilience of already deployed topologies against independent failures can be achieved by improving network availability and reliability through the use of network topology design tools [33, 18, 47, 43]. Establishing a high availability sub-graph at the physical layer can also play a significant role in network resilience [58]. To support mission-critical services, network operators must provide high availability services (in some cases with other protection mechanisms) and more sophisticated QoR classes [2]. Another approach that can be considered for improving the robustness of the network is to shield some links, as in [66], however, without explicitly considering availability.

Modeling network failures does not directly contribute to disaster resilience. Nevertheless, it is an important aspect as it is crucial to model the environment and the network properly, and therefore it is a widely studied topic [30, 22, 17, 29, 53]. Many works investigate the impact of natural disasters on terrestrial [30, 50, 17, 49] on underwater links [12, 63]. In [52], a greenfield (i.e., planning from scratch rather than extending the existing net-

work) network design approach was presented based on a new metric called multiple region-based connectivity, which describes multiple massive localized faults (i.e., multiple regional failures). In [4], the concept of emergency optical networks and hierarchical addressing was explored as a strategy to improve the resilience of optical networks to disasters.

In addition to the improved topology, the end-user's perceived availability can also be improved by careful connection design. Survivable routing schemes are used to improve connection resilience [44], often categorized by time scale and (bandwidth) cost in protecting against link failures [23, 7] and disasters [59]. General Dedicated Protection (GDP [8, 5]) is a family of survivable routing algorithms which ensures instant recovery from any protectable failure pattern (given for example as an SRLG list). Using the GDP approach, an acyclic graph with minimal cost can be constructed for a source–destination pair that ensures connectivity in all considered SRLG failure scenarios, often resulting in better bandwidth efficiency than a disjoint path-pair [65] for sparse SRLG lists. The concept was later extended with algebraic operations to support network coding for resilience in single link failure scenarios [48, 6, 40]. Geo-diverse routing can be used to increase network survivability to disasters by spatially separating disjoint paths according to predefined failure regions [13, 16, 3]. However, GDP can provide continuity of service even in the presence of regional failures and complex SRLG lists (where there may not be a failure-disjoint path pair), as long as the network remains connected upon a failure (which is not always the case during large-scale disasters).

If instantaneous recovery is part of the QoS requirement, i.e., after-failure signaling is completely eliminated from the recovery process, then no rerouting of data flow or retransmission of packets is possible in the case of a single link failure (which is common in transport networks). In [10], the bandwidth efficiency of dedicated protection approaches with instantaneous recovery was studied, and it was shown that user data must be split into arbitrary many parts to achieve this. From a practical point of view (e.g., network equipment and management complexity), this is not feasible. Therefore, Survivable Routing with Diversity Coding (SRDC) was introduced in [34], where the user data is split into at most two parts to ensure instantaneous recovery while approaching the theoretical lower bound in bandwidth efficiency in case of single-link failures.

2.4 Network Coding

In the event of a regional (or single-link) failure, it is critical to recover the network as quickly as possible, and it is not trivial to have such a short recovery time. An interesting approach is to modify the user data within

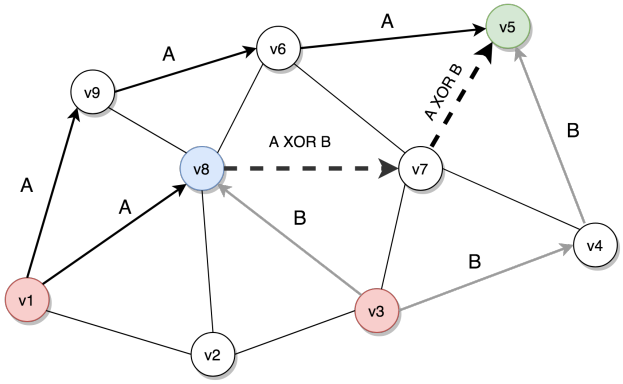


Figure 2.2: Network coding example, where sources $v1$ and $v3$ (red) are sending data to the destination $v5$ (green) and sending their data to the coding node $v8$ (blue) which sends A $\oplus$ B to destination $v5$.

the network which became more realistic in recent years. This method, called network coding, was first introduced by Ahlswede in 2000 [1]. The advantage of network coding is capacity efficiency, which comes from the fact that the source node sends divided data over the network links. For example, in the (1+N) solution, the source node creates a linear combination of the N input symbols and then uses a single protection path to send this combined symbol so that the data can be recovered over N paths.

A simpler solution is XOR coding (called Diversity Coding), where the data is split into two parts and two disjoint paths are used to send these two parts. In this case, the encoded data ($A \oplus B$) is sent over a third disjoint path, and the end node can recover the data from two of the three data parts. Instead of sending the entire data from the source over two disjoint paths, this method uses less of the bandwidth capacity by sending certain pieces of data over the disjoint paths. Of course, the network must have 2, 3, or as many disjoint paths as the coding scheme requires. Indeed, this results in a requirement for the network design to physically construct the network topology to meet these requirements. However, the use of other routing algorithms from the GDP family also forces the network to have certain properties. An example of network coding can be found in 2.2, and diversity coding (A $\oplus$ B coding) can be seen in 2.3.

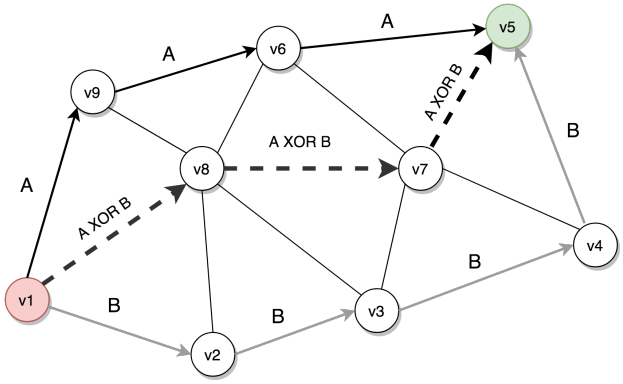


Figure 2.3: A $\oplus$ B coding example with source node $v1$ (red) sending A, B, and A $\oplus$ B through three disjoint paths to destination node $v5$ (green).

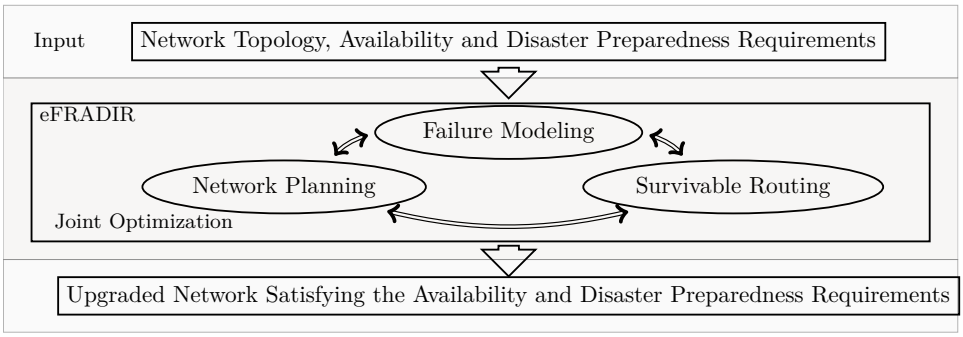


Figure 2.4: The high level concept of eFRADIR [37] – the joint utilization of failure modeling, network planning and survivable routing is the key for proper disaster preparedness.

2.5 The Evolution of FRADIR

The original FRADIR [35] framework, which is a combination of network planning, failure modeling, and survivable routing, was the first step toward a new strategy for improving the disaster resilience of networks. An innovative step in FRADIR was to combine single-link failures (e.g., cutting a cable) with multi-link failures (e.g., disasters). A new concept called spine was developed and used in FRADIR to guarantee maximal availability for all working paths. The baseline of the eFRADIR framework can be seen in Figure 2.4. The spine is a subgraph of the network with elements used by working paths serving traffic that requires a higher level of availability. In other words, spine means the links with the highest level of availability in the network. In this early version of the framework, a regional failure

modeling method was developed. A list of SRLG sets representing multi-link failures with a certain probability (the probability that a failure will occur and the links will fail) was created. Using the spine approach, the improved network contained fewer SRLGs and the resilience of a network was increased. Finally, the third step, survivable routing, was tested in terms of blocking probability. Two routing algorithms were compared: GDP [9] with routing (GDP-R) and SRLG disjoint path pair (1+1 routing). The initial results showed that GDP-R outperformed 1+1 routing. This approach still resulted in unprotectable outage scenarios when regional failures occured and the network became disconnected.

In FRADIR-II [36], a new method and approach against network interruptions was presented. In this way, the network could be stabilized against interruptions by (theoretically) increasing the link availability the tolerance level against earthquakes. Moreover, in FRADIR-II the spine concept was improved with minimal cost, and availability was guaranteed for all working paths. However, the modeling of the effects of an earthquake on the region was still not precise enough. FRADIR-II introduced the aforementioned link upgrade method, which was predefined for the network (after running the algorithms, it showed which links should be physically reinforced to improve the connectivity of the network). In this version, 1+1 routing was changed to SRLG diverse routing. This means that if all the links in the SRLG list are not present, diverse routing cannot guarantee the two disjoint paths on which 1+1 routing is based. Nevertheless, GDP-R has outperformed this modified version.

The latest version of the framework, which I also used in my experiment is called eFRADIR [37] (Enhanced FRADIR). Amongst the differences, first the changed failure modeling should be mentioned. From a a ground-shaking hazard model, it was improved to a mathematically and geographically more precise method with an earthquake activity and magnitude calculation model. In eFRADIR, two heuristic algorithms and an Integer Linear Program are presented to the steady state upgrade of the links against the disconnection.

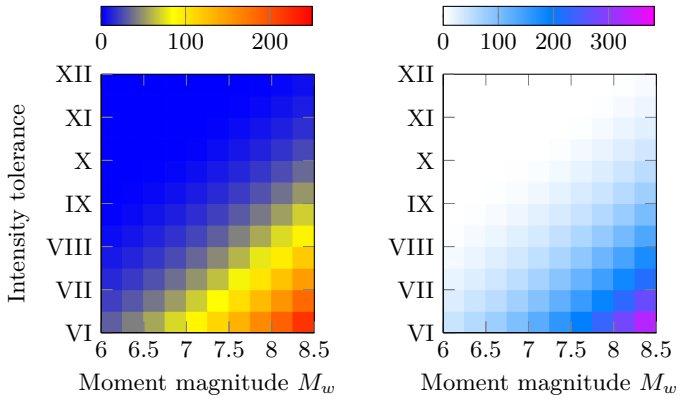
Chapter 3

The eFRADIR Framework

In this chapter, I present the relevant components of the eFRADIR framework: the network model, the failure modelling process, the network upgrade process, and the routing solutions. Note that the eFRADIR framework considers the disasters to be earthquakes because of the available data, but the failure modelling can handle any types of failures provided in a proper format. This chapter focuses on the latest version of the framework with the current technologies and models applied. While in Section 2.5, the evolution of FRADIR was studied, this chapter highlights the fundamentals of eFRADIR including the detailed description of failure moding, network modeling and the network upgrade modeling.

3.1 Network Model

The network is represented by a graph $G(V, E)$ embedded on the Earth surface. V is the set of nodes (e.g. Optical Cross-Connects (OXCs)) and E is the set of undirected edges (bidirectional fiber connections between the OXCs). Each edge e has a positive routing cost $c(e)$ and an availability $a(e) \in [0, 1]$ value. The position of each node is given by longitude and latitude coordinates. The availability value of each edge $e \in E$ is calculated as: $a(e) = 1 - \frac{MTTR}{MTBF(e)}$. The Mean Time To Repair ($MTTR$) a failure is considered as $MTTR = 24$ h and the mean time between steady state random failures of e is $MTBF(e) = \frac{CC*365*24}{\ell(e)}$ [h]. The parameter CC denotes the cable cut metric, which is assumed to be 450 km [2]. The unavailability of an edge e is calculated as $U(e) = 1 - a(e)$, with $a(e)$ being the availability of the edge. Note that the availability of an edge e is a function of its length, $\ell(e)$ [km], with the set $\mathcal{L} = \{\ell(e), e \in E\}$. Note that the cost of the upgrade methods is discussed in details in Section 3.3.



(a) Italy/Europe (b) USA

Figure 3.1: Disaster radius (in km) in function of moment magnitude and intensity tolerance. The values are calculated according to Eqs. (3.1) and (3.2), for Italy and the USA, respectively.

3.2 Failure Modeling

The task of failure modeling is to transform complex real-world data (network specifications, disaster predictions, etc.) into a simple form to ensure inputs for survivable routing, network planning, and so on. The failure modeling module answers the following question: What are the links that have a strictly positive probability of failing during the next disaster, and what are their probabilities? The answer can be given in the form of a list of Probabilistic Shared Risk Link Groups (PSRLGs), that is, by definition a list of link sets, each with a corresponding (failure) probability.

The eFRADIR framework uses the PSRLG definition proposed by [61]: For a link set $S \subseteq E$, the **Cumulative Failure Probability** of S (denoted by $\mathrm{CFP}(S)$) is the probability that at least S (and possibly other links) will fail. The link sets S with $\mathrm{CFP}(S) > 0$ are called PSRLGs, or, if their exact cumulative failure probability is not important, simply SRLGs.

The earthquake is identified by its epicenter and moment magnitude: **epicenter** $c_{i,j}$, which represents a latitude-longitude cell on the Earth's surface taken from a grid of cells over the network area; **moment magnitude** $M_w \in \{4.6, 4.7, \dots\} =: \mathcal{M}$. Let $\mathcal{E}_{i,j,M_w}$ denote the set of earthquakes with center in $c_{i,j}$ and magnitude in $(M_w - 0.1, M_w]$. Let the probability that the next earthquake is in $\mathcal{E}_{i,j,M_w}$ be p_{i,j,M_w}.

Any network link $e \in E$ can withstand seismic shocks of a certain intensity $H(e)$, i.e., if e somewhere is hit by an earthquake with an intensity higher than $H(e)$, e will fail; otherwise, it will remain intact. I will call $H(e)$ the

intensity tolerance of link e. I apply the intensity prediction equation of [39] and [11] for Europe and the USA, respectively. The expected intensity I at a site located at epicentral distance R is:

$$I_{\mathrm{It,EU}} = 1.621M_w - 1.343 - 0.0086(D-h) - 1.037(\ln D - \ln h) \tag{3.1}$$

$$I_{\mathrm{US}} = 0.44 + 1.70M_w - 0.0048D - 2.73\log_{10} D \tag{3.2}$$

where $D = \sqrt{R^2+h^2}$ is a hypocentral distance, and h represents the hypocentral depth, which may be viewed as the average depth of the source [39], h equals 3.91 km and 10 km for Italy/Europe and the USA, respectively. These two particular regions are considered, since the networks used in this study are backbone topology networks from Europe and the USA.

After each earthquake $\mathcal{E}_{i,j,M_w}$, the physical infrastructure with an intensity tolerance H is destroyed in an area $\mathit{disk}(c_{i,j}, R(M_w, H))$ of a circular disk. The radius $R(M_w, H)$ increases monotonically with magnitude M_w and decreases with H. With an intensity tolerance $H =$ VI , the catastrophe radius $R(M_w, H)$ for earthquakes with magnitude $M_w = 4.5$ for Italy/Europe and $M_w = 4.9$ for the USA and reaches a maximum of ~ 200 km for the strongest earthquake scenario considered in Italy with $M_w = 8.1$ and ~ 360 km in the worst scenario of the USA with a magnitude of $M_w = 8.4$.

The set of failed links is denoted as F_{i,j,M_w}. Let $I_{i,j,M_w}(S)$ be the indicator variable of earthquake $\mathcal{E}_{i,j,M_w}$ hitting at least link set S. This way:

$$I_{i,j,M_w}(S) = \begin{cases} 1 & \text{if } F_{i,j,M_w} \supseteq S \\ 0 & \text{otherwise} \end{cases} \tag{3.3}$$

Note that $I_{i,j,M_w}(S)$ also depends on the intensity tolerances $H(e)$ of the links of set S. For a link set S, $\mathrm{CFP}(S)$ can be calculated as:

$$\mathrm{CFP}(S) = \sum_{i,j \in \mathcal{I}_i \times \mathcal{I}_j} \sum_{M_w \in \mathcal{M}} p_{i,j,M_w} I_{i,j,M_w}(S) \tag{3.4}$$

3.3 Network Upgrade Model

Thanks to the failure modeling of eFRADIR [37], the PSRLGs show a realistic picture of the potential outages of the network in case of a disaster. Some of these potential failures disconnect the network and disrupt the communication. If the network remains connected after the given disasters, i.e., after each failure in the SRLG list, then the GDP-R can protect the connection against all these failures. This problem can be addressed by introducing an disconnection probability threshold (T_D), which is the target probability of

the upgrade methods.

The cost of the intensity tolerance upgrade used by the disaster resilience upgrade methods is directly proportional to the length of the link and the size of the update. Note that the disaster resilience upgrade cost is independent from the initial intensity tolerance of the link. For example, upgrading a one-level upgrade of a link (from level VI to level VII) costs half as much as a two-level upgrade (upgrading from level VI to level VIII).

It is assumed that every network link $e \in E$ has an initial intensity tolerance $H_0(e)$, which can be increased by $\Delta H(e)$ to a higher level ($H(e) = H_0(e) + \Delta H(e)$) at cost $\Delta H(e) * \ell(e)$, where $\ell(e)$ is the length of the link. The total intensity tolerance upgrade cost as the sum of the upgrade cost of all links:

$$\sum_{e \in E} \ell(e) \cdot \Delta H(e) \tag{3.5}$$

$\mathbf{H_0}$ denotes the vector of the initial intensity tolerances ($H_0(e)$) for every network link $e \in E$. Similarly $\mathbf{\Delta H}$ and $\mathbf{H}$ represent the vector of the upgrade levels and the final intensity tolerances, such that $\mathbf{H} = \mathbf{H_0} + \mathbf{\Delta H}$.

To determine if link $e \in E$ with intensity tolerance $H(e)$ fails in the case of an earthquake at $p \in \mathcal{P}$ with magnitude $M_w \in \mathcal{M}$, the earthquake's intensity has to be known at the link. It is denoted by $I(e, p, M_w)$ and calculated according to Eq. (3.1) in the case of Italy and according to Eq. (3.2) in the case of the USA. The matrix of the $I(e, p, M_w)$ values is denoted with $\mathbf{I}$. The probability of the given earthquake is denoted as $Pr(p, M_w)$, while the matrix of the probability values is denoted as $\mathbf{Pr}$.

3.4 GDP routing

By the term GDP, we mean General Dedicated Protection, a family of routing algorithms that are designed to recover from failures in no time. This GDP framework was designed to find optimal solutions for regional failures in networks [9], and a few of these routing algorithms were examined and compared in [38]. The algorithms from this study of the GDP [38] (forced spine routing, length minimization, hop count minimization and hybrid cost function) was compared with the 1+1 routing (the two disjoint paths between the source and the destination node) and the results showed that all of them outperformed 1+1 routing in terms of blocking probability (the data could not be sent to the destination). These routing algorithms are implemented with forced attention to the most popular failure scenarios, and the scenarios are modeled with an SRLG in the FRADIR framework. GDP-R focuses on creating a failure resilient network which provides instantaneous recovery against all possible failures that are listed with the SRLGs. Finding

an optimal solution in terms of bandwidth cost for GDP-R is NP-complete [10]. In contrast with GDP-R, GDP, the general protection scheme can be applied with network coding , instead of routing algorithms. It is proved that network coding has a better bandwidth capacity allocation, as it is shown in Section 5.7 later.

Chapter 4

Disaster Resilient Network Upgrade

In this chapter, I present the existing heuristic algorithms for the disaster resilient upgrade problem from the eFRADIR framework, introduce an additional algorithm that improves their efficiency (called MA, described in Section 4.2), and introduce my novel solution (called ST, described in Section 4.3) that uses spanning trees (obtained by Kruskal's algorithm [20]) which aims to reduce the problem space.

4.1 Heuristic Methods from eFRADIR

For upgrading the links in the network (which will improve the network's resilience level against a possible earthquake), two heuristic algorithms and a MILP (Mixed Integer Linear Program [51]) was introduced in eFRADIR. The heuristic methods iteratively upgrade one link with one level at every step until the disconnection probability of the network (P_D) is lower than the predefined threshold T_D. The MILP from eFRADIR describes the upgrade problem with a set of constraints and the optimal network upgrade solution can be obtained by solving the integer linear program. The heuristic methods are iterative upgrade methods that select one link for upgrade at each step according to some metric until the disconnection probability decreases to a predefined level. At the end of the algorithms the set of upgraded links are returned with the corresponding upgrade levels. In the following, I briefly describe the two heuristic network upgrade methods from eFRADIR and suggest an addition to them.

Notation	Description
$G(V, E)$	Input graph, its node set and edge set, respectively
$\mathcal{N}$	Set of minimum cut SRLGs
S	Set of links in a minimum cut
$\mathcal{P}$	Set of grid points
$\mathcal{M}$	Set of earthquake magnitudes
$Pr(p, M_w)$	Probability of an earthquake at point $p \in \mathcal{P}$ with magnitude $M_w \in \mathcal{M}$
P_D	Probability that the network will fall apart because of the next earthquake
T_D	Probability threshold, which specifies the scope of the defense. The goal is to decrease the probability of falling apart below this threshold.
$I(e, p, M_w)$	Intensity of an earthquake with epicenter p and magnitude M_w at link e
$H(e)$	Intensity tolerance of link e: $H(e) = H_0(e) + \Delta H(e)$
$H_0(e)$	Initial intensity tolerance of link e, integer
$\Delta H(e)$	Intensity tolerance upgrade for link e, integer
$\ell(e)$	Length of link e
L	List of previously upgraded links
α	Threshold parameter for ST algorithm

Table 4.1: The notations used in the heuristic algorithms to improve the network's resilience

Heuristic 1

This method serves as a baseline and shows that a more complex method is required to approach the optimal solution. At each step, the links of G are ordered based on their occurrences in the minimal-cut SRLGs in $\mathcal{N}$. The link with the highest occurrence count is selected for the upgrade. If multiple links have the same (highest) occurrence count then the one with the lowest intensity tolerance upgrade cost (i.e., the shortest length) is selected for an upgrade. After the selected link's intensity tolerance is increased by one level, the disconnection probability is recalculated using the `calcDP` function and the upgrade continues until $P_D < T_D$.

Heuristic 2

In this method, the decision to upgrade is based on the reduction in probability P_D (the network's probability to fall apart) that upgrading the link would entail, and the intensity tolerance upgrade cost of the link, summed.

At each step, we examine by how much the disconnection probability decreases in case of a link upgrade. The disconnection probability in the case of the upgrade of link e is $P'_{D,e}$. Since we are only interested in decreasing the probability below T_D, the probability decrease for link e is $P_D - \max\left(P'_{D,e}, T_D\right)$. To find the highest probability decrease for a unit cost, the total probability decrease of a link is divided by the cost of increasing the intensity tolerance of the link by one. At each step, the link with the highest probability decrease for a unit cost is selected for upgrade. After each upgrade step, the disconnection probability (P_D) is recalculated using the `calcDP` function. The upgrade process ends when the probability of the network falling apart reaches the probability threshold (T_D).

4.2 The Minimization Algorithm (MA)

This section describes an improvement possibility for the disaster-resilient network planning heuristic algorithms of eFRADIR framework which may improve the efficiency of those methods. This minimization method can continuously monitor the necessity of the link upgrades performed by the heuristic algorithms, discards any unnecessary upgrade steps, and reduces the runtime.

It is possible that there are links among the upgraded links that could be downgraded without increasing the disconnection probability P_D (or with increasing P_D but still remaining under the predefined threshold T_D). This is caused by the iterative manner of the upgrade process. The minimization algorithm (MA) can be used after each upgrade step or only at the end of the heuristic algorithm - when the disconnection probability is already below the predefined threshold ($P_D \leq T_D$). Therefore this algorithm allows us to monitor the necessity of the previous upgrade steps. the psudocode of MA is described in Algorithm 1.

First, the minimization algorithm iterates through all the links that have been added to the upgrade queue (L_1) and sees if any of them can be reverted/discarded (Alg. 1 from line 3 to line 10). It is done for each link by a disconnection probability recalculation after virtually discarding the link upgrade. If discarding the upgrade would not cause a disconnection probability increase or it would but the disconnection probability would still be below the predefined threshold then the it can be reverted. Then the links that can be reverted are saved in a separate list (L_{saved}).

Next, it creates the possible link pair from L_{saved} and saves them to L_2. It checks all the link pairs in L_2 to see whether their joint downgrade would still be possible (Alg. 1 from line 12 to line 21). After that, the link pairs that can be reverted are saved to L_{saved}. In the end, the result is $Lsaved$ containing

the links and link pairs that can be reverted. The function `choosemax` finds the link of link-pair with the largest cost reduction in L_{saved}. For example if link l_1 results in a cost reduction of 252 and link l_2 results in a cost reduction of 231, then l_1 will be reverted, even though both link upgrade can be reverted either without increasing the disconnection probability or going above the probability threshold. Similarly, if link l_1 results in a cost reduction of 252 and discarding the upgrade of link-pair (l_2, l_3) results in a cost reduction of 245, then l_1 will be reverted.

Algorithm 1 Minimization algorithm to revert unnecessary link upgrades

Input: $G(V, E)$, $\mathcal{L}$, $\mathbf{H}$, $\mathbf{I}$, $\mathbf{Pr}$, $\mathcal{N}$, P_D, T_D, r, L
Output: $maxRev$ {set of links which could be downgraded}

$L_1 \leftarrow L$
$L_{saved} \leftarrow \emptyset$
for all l in L_1 **do**
  $H(l) \leftarrow H(l) - 1$
  $P'_D \leftarrow$ `calcDP`$(S, \mathcal{N}, \mathbf{I}, \mathbf{Pr}, \mathbf{H})$
  if $P'_D = P_D$ or $P'_D \leq T_D$ **then**
    $L_{saved} \leftarrow L_{saved} \cup \{l\}$ {Adding l to saved}
  end if
  $H(l) \leftarrow H(l) + 1$
end for
$L_2 \leftarrow \{(l_1, l_2) : \forall (l_1, l_2) \in L^2_{saved}\}$
for all $(l_1, l_2) \in L_2$ **do**
  $H(l_1) \leftarrow H(l_1) - 1$
  $H(l_2) \leftarrow H(l_2) - 1$
  $P'_D \leftarrow$ `calcDP`$(S, \mathcal{N}, \mathbf{I}, \mathbf{Pr}, \mathbf{H})$
  if $P'_D = P_D$ **then**
    $L_{saved} \leftarrow L_{saved} \cup (l_1, l_2)$ {Adding (l_1, l_2) to saved}
    $H(l_1) \leftarrow H(l_1) + 1$
    $H(l_2) \leftarrow H(l_2) + 1$
  end if
end for
$maxRev \leftarrow$ `choosemax`(L_{saved}) {Choosing best revert}
return $maxRev$

The minimization algorithm is an additional optimization step for the heuristic algorithms that could not provide the optimal solution. Also, it serves as a test (also for my heuristic algorithm) to see how often the minimization algorithm produces a downgrade. Of course, if the original algorithm finds the optimal links to upgrade then the minimization algorithm cannot produce any improvement (no upgrade steps are unnecessary). Nevertheless the minimization algorithm can still produce valuable feedback, since it confirms our theory that a solution is close to the optimum.

4.3 A Spanning Tree Based Heuristics (ST)

I propose a novel heuristic algorithm for upgrading links in the network to improve the performance of previous heuristic algorithms and/or reduce the runtime. The algorithm is based on a spanning tree generation to reduce the problem space, however it is not trivial whether to construct a minimum or a maximum spanning tree from the network, and will be discussed later.

To obtain a spanning tree Kruskal's algorithm is used. An important step is to consider whether the desired probability threshold can be achieved if only links from the spanning tree are upgraded, or whether the algorithm must also select links that are not part of the spanning tree. In the optimal case (when only links from the spanning tree are selected), the number of edges that the algorithm has to iterate through is significantly less than the number of edges in the graph.

A real-life network often consists of multiple disjoint paths between two nodes (1+1 routing is based on multiple disjoint paths), so the number of edges (E) can be much larger than the number of nodes (N). However, a spanning tree can always be constructed with n-1 edges, which means a smaller input size. Apart from knowing the complexity reduction, I would still like to prove that the links used in a minimal spanning tree give a result close to the optimal solution. Otherwise, the algorithm proposed by a fellow researcher of mine earlier based on the probability reduction values could not be improved and the spanning tree approach might not perform well.

The weighting of edges is described in the next section. Theoretically, both the minimum and maximum spanning tree could be a solution, and I had to test both cases. The key move of the algorithm is to base the weighting of the edges on a value that gives us valuable information about whether upgrading a link is beneficial/optimal (the cost is calculated using the initial state of the links and are not changed during the algorithm).

The weighting I use is based on the approaches of the previous two heuristic algorithms. I calculate the number of SRLGs in which the given link (e) is present, and also the probability that the network will fall apart if every link from one of the SRLGs fails simultaneously (i.e., the entire SRLG is affected by the earthquake that leads to the failure of the entire link group) that contains the given link (e). This means that the links in the spanning tree contains information about the vulnerable links, but still reduce the number of links that the algorithm has to iterate through by throwing out the links that would not have much impact on the stable state of the network in case of a failure. The weight function can be changed as a parameter in the algorithm between (a) SRLG event (b) SRLG probability (c) weighted sum of these two. The weighting is denoted by w, and the pseudocode for the algorithm is described in Alg. 2.

Algorithm 2 Spanning tree heuristics

Input: $G(V, E)$, $\mathcal{L}$, $\mathbf{H_0}$, $\mathbf{I}$, $\mathbf{Pr}$, $\mathcal{N}$, P_D, T_D, w, α
Output: $G(V, E)$, $\mathbf{H}$: graph with improved earthquake resilience

$\mathbf{H} \leftarrow \mathbf{H_0}$ {Initial intensity tolerance}
$S \leftarrow \texttt{spantree}(G(V, E), w)$ {Create spanning tree}
for all $e \in S$ **do**
  $H(e) \leftarrow H(e)_{max}$
end for
$P'_D \leftarrow \texttt{calcDP}(G, \mathcal{N}, \mathbf{I}, \mathbf{Pr}, \mathbf{H})$
if $P'_D > T_D$ **then**
  {The links in the tree are not enough}
  $\mathbf{H} \leftarrow \mathbf{H_0}$ {Reset intensity tolerance}
  while $P_D > T_D$ **do**
    $D \leftarrow \texttt{calculateDowngradeImpact}(G, \mathcal{N}, \mathbf{I}, \mathbf{Pr}, \mathbf{H})$
    $l \leftarrow \texttt{selectlink}(D)$ {Best upgradeable link in the graph}
    $l_{st} \leftarrow \texttt{selectSTlink}(D, S)$ {Best upgradeable link in the spanning tree}
    if $l = l_{st}$ **then**
      $H[l] \leftarrow H[l] + 1$
    else
      if $D[l] - D[l_{st}] < \alpha$ **then**
        $H[l_{st}] \leftarrow H[l_{st}] + 1$
      else
        $H[l] \leftarrow H[l] + 1$
      end if
    end if
    $P_D \leftarrow \texttt{calcDP}(S, \mathcal{N}, \mathbf{I}, \mathbf{Pr}, \mathbf{H})$
  end while
else
  $\mathbf{H} \leftarrow \mathbf{H_0}$ {Reset intensity tolerance}
  while $P_D > T_D$ **do**
    $D \leftarrow \texttt{calculateDowngradeImpact}(S, \mathcal{N}, \mathbf{I}, \mathbf{Pr}, \mathbf{H})$
    $l \leftarrow \texttt{selectlink}(D)$ {Best upgradeable link in the graph}
    $H[l] \leftarrow H[l] + 1$
    $P_D \leftarrow \texttt{calcDP}(S, \mathcal{N}, \mathbf{I}, \mathbf{Pr}, \mathbf{H})$
  end while
end if

This algorithm first creates a spanning tree using the chosen weight calculation method for each edge. Then, for each link in the spanning tree, it upgrades the link's intensity tolerance to the maximum level denoted by $H(e)_{max}$ (which is referring to the maximum level of physical resilience for a link, described in Section 3.3). This shows whether the spanning tree is sufficient to (theoretically) improve the network's resilience, or the algorithm needs to pick other edges which are not included in the spanning tree. If the tree edges are not enough to perform a probability disconnection decrease big enough, for each link, the benefit of upgrading it is calculated with the function `calculateDowngradeImpact`. Then, the link which causes the biggest decrease in the probability of falling apart T_D link is selected from the tree edges and from the non-tree edges, and they are compared. it is possible that represent are the same edge, however it is not necessary. If not, their impact is measured as it was calculated earlier with `calculateDowngradeImpact`. Here, the α parameter means if the difference between these two links' impact is below this α, then the link from the tree is upgraded (its intensity tolerance level) denoted with l_st. If the α is large, this means that upgrading even the best link from the spanning tree is not a great choice in terms of the expected decrease in the probability of disconnection. In this case, the non-tree edge's intensity tolerance is upgraded by one.

The other case in which choosing links from the spanning tree is enough to reach the probability threshold T_D, the values of the links' probability decrease is calculated with `calculateDowngradeImpact` and each time, the link with the largest value is selected, until the threshold T_D is reached.

A few important and not trivial questions had to be decided before running the algorithm: 1. whether to use the minimum or the maximum spanning tree in the graph, and 2. how to calculate the weight on the edge. I experimented with different weight calculation methods and also tested the algorithm with both minimum and maximum spanning tree. A maximum spanning tree is logical, if the weight in the graph is the number of SRLGs the link is part of, or the probability of the network falling apart if the given link goes down. However, the minimum spanning tree can be optimal if the edge weight calculation is simply the length of the link.

Chapter 5

The Experimental Results

In this chapter I present the comprehensive experimental results. First in Section 5.1 we present the examined networks and their properties. In Section 5.4 the different heuristics approaches' performance is analyzed. In Section 5.5 the link upgrade is analyzed, meanwhile in Section 5.6 the runtime analysis is presented. Last but not least in Section 5.7 the performance of a network coding based routing approach is investigated. Note that until now the possibility of introducing a network coding based approach to the FRADIR framework was not analyzed.

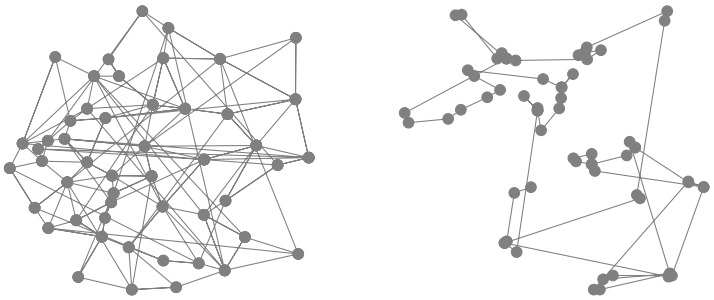
5.1 Analysis of the Networks

I conducted simulation on four networks obtained from [32] and [60]. These networks are real-life backbone network models from the USA, Germany, Italy and Europe. From this point in my paper, I refer to them as 'USA/Germany/Italy/Europe networks'. In Table 5.1 the basic characteristics of the networks are given.

One can observe that these networks have a wide variety of node count, edge count, average node degree, physical location, and physical extent. The node and edge count affects the runtime of the network upgrade methods, while the physical parameters affect the earthquake probability model. Earth-

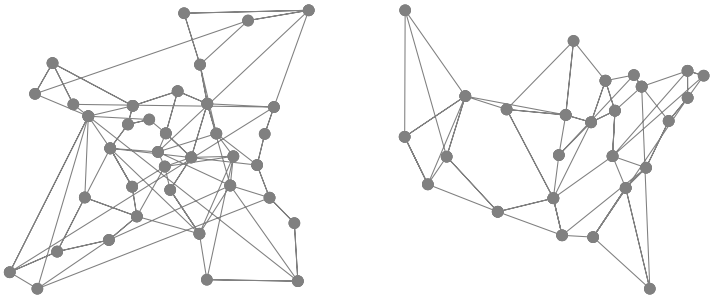
Network name	**No. of nodes**	**No. of edges**	**Avg. node degree (γ)**
USA [32]	26	42	3.23
Italy [60]	25	35	2.72
Europe [32]	37	57	3.08
Germany [32]	50	89	3.52

Table 5.1: Basic characteristics of the networks used in the simulations



(a) Germany network (b) Italy network

Figure 5.1: The graph representation of the Germany and Italy networks



(a) EU network (b) USA network

Figure 5.2: The graph representation of the Europe and USA networks

quakes are much more likely in the area of Italy network than in the area of the Germany network. The average distance between nodes in the USA network is significantly larger than in the Italy or Germany network. However, the network of Germany is the most complex with its 50 nodes and 89 edges, although its physical size is comparable to the Italy network. In Figure 5.1 the Germany and the Italy network can be observed. The difference of the two networks is quiet significant, the Germany network has two times more nodes (50) than the Italy network (25) on a comparable area. Additionally, the average node degree is higher in the Germany network ($\gamma = 3.52$) than in the Italy network ($\gamma = 2.72$). In Figure 5.2 the topology of the Europe and USA network can be seen. The Europe network has less nodes than the Germany network (37 vs 50) but greater physical extent, and has more nodes and smaller physical extent then the USA network (37 vs 26). Regarding the average node degree (γ), for the Italy network ($\gamma = 2.72$), the difference is significant compared to the other networks (above 3). Also, it can be seen in comparison with the Germany network in Figure 5.1.

5.2 The Effect of MA

In this section, I present the simulation results of the Minimization Algorithm. To see how MA performs in terms of cost reduction, I applied the algorithm on the heuristic methods of eFRADIR in two settings (after each upgrade step denoted as MA_{step}, and only after the upgrade process denoted as MA_{end}). I considered four scenarios to gain insights about the performance of MA:

1. Heuristic 1 + MA_{step}
2. Heuristic 1 + MA_{end}
3. Heuristic 2 + MA_{step}
4. Heuristic 2 + MA_{end}

The effect of the minimization algorithm was tested on the USA network for the four scenarios. The results can be seen in Figure 5.4. It indicates that the performance of Heuristic 2 cannot be improved with MA, no upgrade step was discarded. It was expected, since Heuristic 2 is proven to perform within 5% from the optimal solution, thus MA could not improve its performance. However, the results show small improvements on Heuristic 1 on the USA network. At high T_D values, when only a few links are upgraded, no upgrade step is unnecessary, but at lower T_D values MA discards several upgrade steps. According to these results, there seems to be any difference between MA_{step} and MA_{end}. Both methods produce the same solution. Note that the MA algorithm is still a valuable addition to Heuristic 2, too, since the MA is possibly still able to improve the algorithm's performance depending on the network topology.

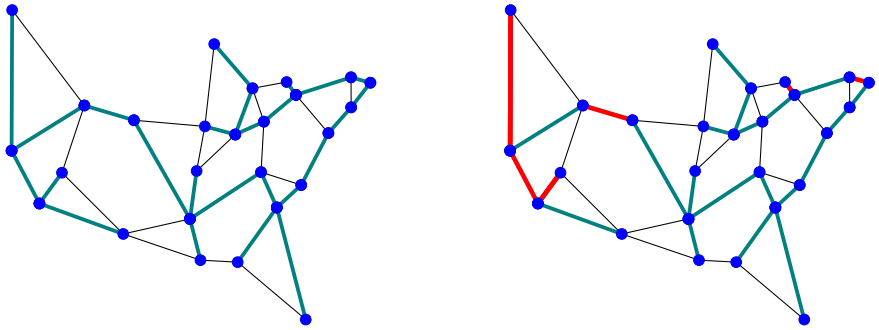
5.3 Results of the Spanning Tree Algorithm

The performance of my ST algorithm was analyzed in several different scenarios. I examined the algorithm performance depending on the spanning tree calculation method. In particular minimum and maximum spanning tree were generated, and several weight calculation methods were utilized, to find the best possible one. The following weight calculation methods are used in the simulations:

PROB the summed probability of the SRLGs that contain the link

OCCUR the number of SRLGs that contain the link

Spanning Tree in the USA network Spanning Tree in the USA network with upgraded links



(a) Spanning tree in the USA network

(b) Spanning tree in the USA network with upgraded links

Figure 5.3: Spanning tree on USA network with and without upgraded links

T_D	**PROB**	WEIGHT	OCCUR	LEN-MAX	LEN-MIN
0.0005	**5257**	8198	8198	10122	5234
0.0006	**4630**	7876	7942	9183	4607
0.0007	**4098**	6986	7051	8270	4097
0.0008	**4083**	6753	6753	8036	4060
0.0009	**3550**	6958	6551	7123	3550
0.001	**3603**	5661	5661	6508	3520
0.002	**1682**	2830	2830	3330	1682
0.003	**758**	2200	1982	2005	758
0.004	**380**	591	592	614	380

Table 5.2: Upgrade cost comparison of the ST methods on the USA network

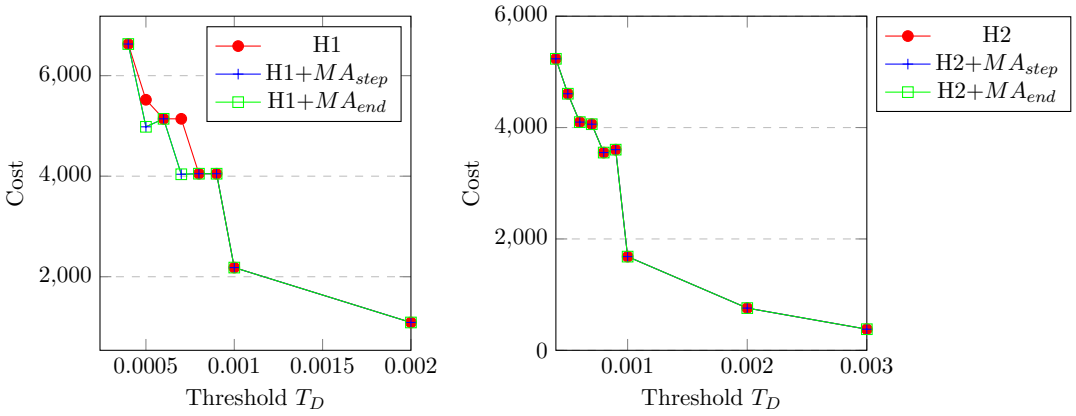
WEIGHT the weighted average of PROB and OCCUR

LEN the length of the link (= one-level upgrade cost)

In case of PROB, the weight is the summed probability of the SRLGs that contain the link. OCCUR means that the weight is set the number of SRLGs containing the link. WEIGHT stands for the weighted average of the previous two. The parameter α determines the ratio of the two:

$$\text{WEIGHT} = \alpha * \text{PROB} + (1 - \alpha) * \text{OCCUR} \tag{5.1}$$

LEN means that the weight equals the length of the link (which is the upgrade cost of a one-level intensity tolerance upgrade). In this case, two



(a) Minimized Heuristic 1 (USA)

(b) Minimized Heuristic 2 (USA)

Figure 5.4: The effect of MA on Heuristic 1 and Heuristic 2, in the USA network

spanning tree generation objectives were evaluated: minimum and maximum spanning tree, denoted as LEN-MIN and LEN-MAX. In the other cases (PROB, OCCUR, and WEIGHT), the maximum spanning tree was generated.

Table 5.2 presents the results of the 5 spanning tree generation setting on the USA network. In term of upgrade cost, the PROB and LEN-MIN spanning tree generation methods give the best solutions. In some cases the upgrade cost is almost 50% lower than in case of the other three methods. It makes sense that the LEN-MAX returns the highest upgrade cost, since in this case the spanning tree contains mostly the expensive links of the network (the upgrade cost is proportionate to the length). The OCCUR method solves the upgrade similar to Heuristic 1 since the endangered links are determined based on their occurrence count in the SRLGs. This is reflected in the results too, barely beating the LEN-MAX method. The poor performance of the OCCUR method comes out in the WEIGHT method too, resulting in high upgrade cost solutions. Because the probabilistic values carry a lot information about the endangered state of the link therefore the good performance of the PROB method was expected. Similarly, good performance of LEN-MIN was expected, since it uses the spanning tree containing mostly cheap links to upgrade.

I concluded an additional comparison with the most promising weight calculation method (PROB). Previously, the PROB weight calculation was paired with a maximum spanning tree generation. In this comparison, the minimum and maximum spanning tree version of the PROB weight calculation is examined on the USA network. Figure 5.5 presents the upgrade costs at

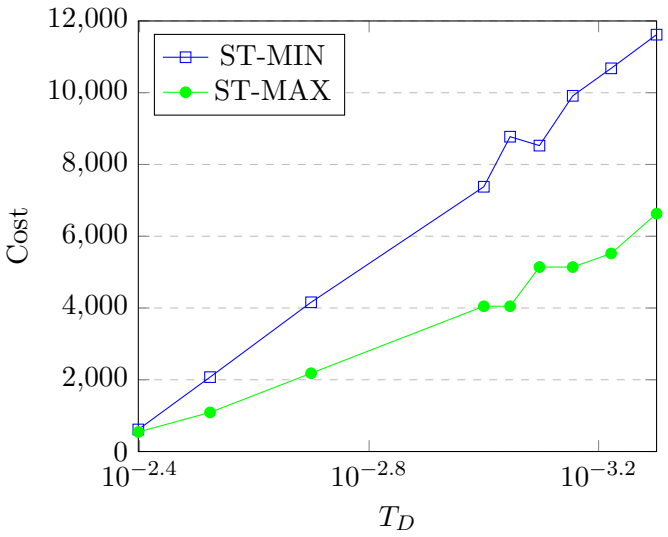


Figure 5.5: Comparison of the upgrade cost of the two types of ST (minimum and maximum tree) for several probability thresholds (T_D), for the USA network.

various probability threshold levels. It is clear that the maximum spanning tree generation is superior to the minimum spanning tree generation when the PROB weight calculation is used. In case of the WEIGHT and OCCUR weight calculation methods, the results were the same, i.e. the maximum spanning tree is significantly better than the minimum spanning tree.

5.4 The Heuristic Algorithms Comparison

In this section, my novel ST algorithm is compared to the network upgrade methods from eFRADIR (ILP, Heuristic 1, and Heuristic 2). The minimum and maximum spanning tree version of ST are used in these comparisons with the weight calculation method PROB. Figure 5.6 presents the upgrade cost comparison of eFRADIR's upgrade methods and the PROB-MIN and PROB-MAX ST methods on the Italy network. The results show that the Heuristic 1 and the PROB-MIN version of the ST have the highest upgrade cost. As expected, the ILP solves the upgrade at the lowest cost but Heuristic 2 is not far behind. The PROB-MAX version of the ST outperforms Heuristic 1 and ST-MIN but cannot beat Heuristic 2.

Another simulation was performed on the Europe network using the two heuristics from eFRADIR and the ST method with PROB-MAX spanning tree generation. As it can be seen in Figure 5.7, the ST algorithm and Heuristic 2 produces the exact same results at every probability threshold.

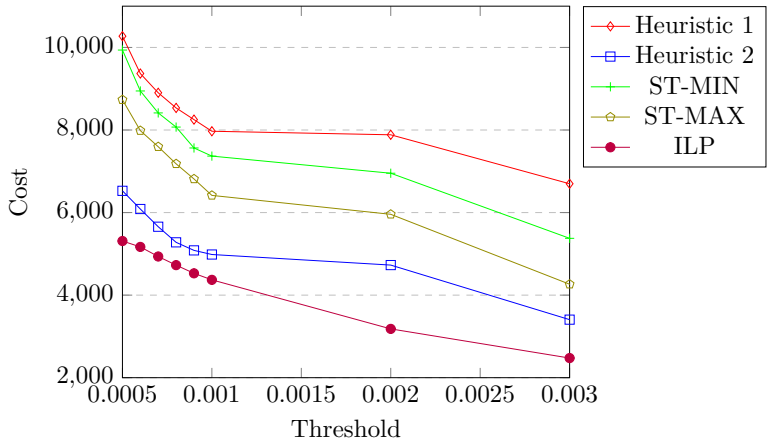


Figure 5.6: Comparison of the upgrade cost of the upgrade methods from eFRADIR and two types of ST (minimum and maximum tree) for several probability thresholds (T_D), for the Italy network.

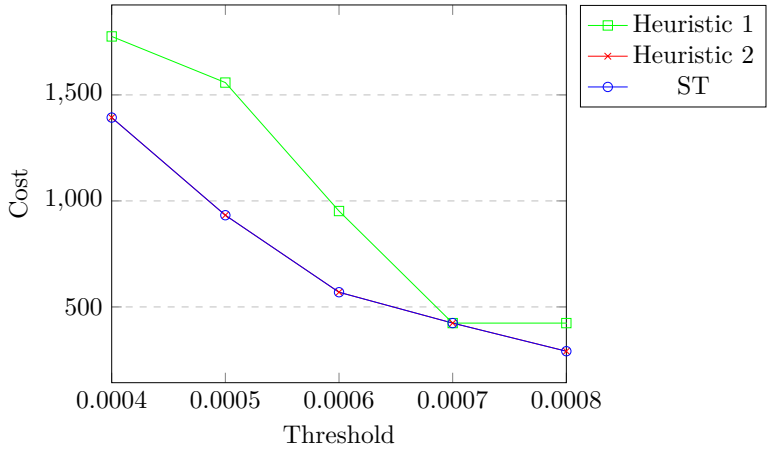
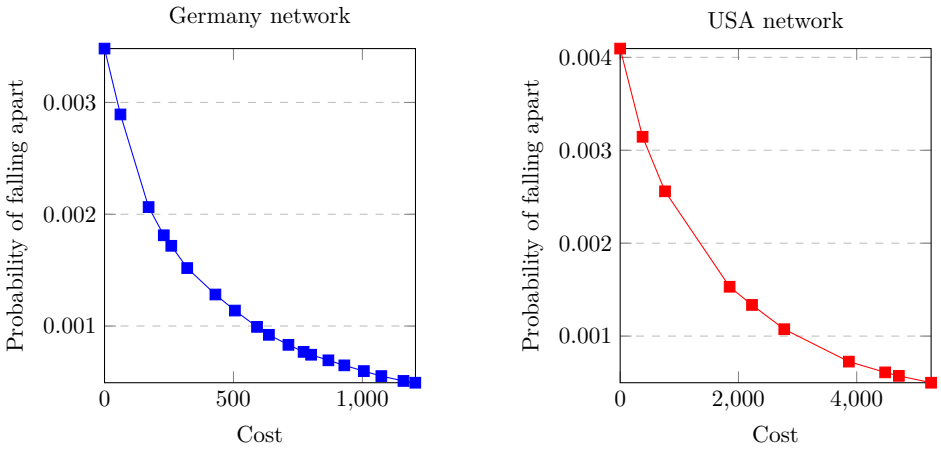


Figure 5.7: Comparison of the upgrade cost of the heuristic upgrade methods from eFRADIR and the ST method with PROB-MAX for several probability thresholds (T_D), for the Europe network.

The performance of Heuristic 1 is much worse than the other two. This shows that depending on the characteristics of a given network, the ST algorithm is able to match the Heuristic 2 algorithm in terms of upgrade cost.



(a) Probability/Cost function for the upgraded links (Germany)

(b) Probability/Cost function for the upgraded links (USA)

Figure 5.8: Cost analysis for the upgraded links with their probability decrease using ST algorithm

5.5 Link Upgrade Analysis

Upgrading the links will decrease the probability of the network falling apart. This means that if the algorithm chooses a link in the beginning and modifies its intensity tolerance, recalculating the network's probability of disconnection will give a different, decreased value. The amount which every link gives as a benefit is not linear during the upgrading process. The first links that the algorithm upgrades will cause the disconnection probability to decrease by a lot. Then, with every upgraded link this value decreases, so that choosing the e.g. 10th link will have less impact on the disconnection probability and so on. With getting closer to the given threshold value, this value slowly approaches zero as every upgraded link is less and less beneficial regarding the cost used.

Knowing this fact, an interesting question to bring up is whether it is beneficial to upgrade links with a small positive effect on the disconnection probability, or to stop before the steepness of the function seen in Figure 5.8 flattens. This however opens up another topic which will not be discussed in this paper, but the trends show this for every network, even though the number of links that were upgraded have large differences in the Germany and the USA networks.

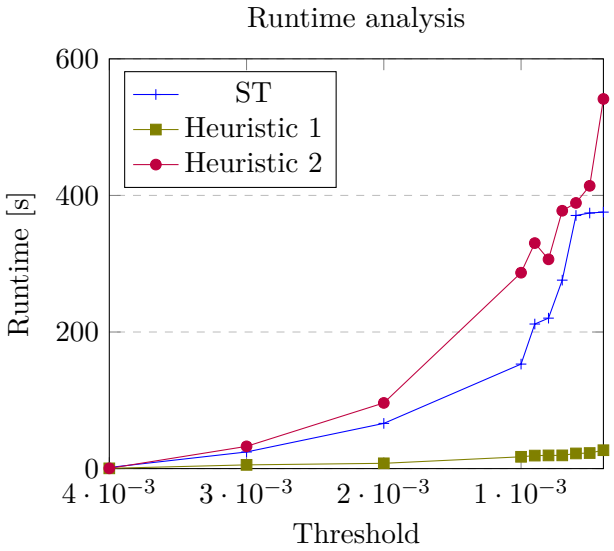


Figure 5.9: Runtime comparison for the heuristic algorithms on Germany network

5.6 Runtime Analysis

In this section, I compare the algorithms based on the runtime. When analyzing the runtime of the algorithms (see Figure 5.9), one thing is worth noting: ST is faster than its 'predecessor', the algorithm Heuristic 2, due to the high number of edges it inspects when computing the probability of failure. The main advantage of ST is the problem space reduction: ET performs $N - 1$ iterations at every step (because it has $N - 1$ edges), rather than $|E|$ iterations as Heuristic 2. Of course, these differences are not significant, and a well-performing algorithm is more desired than an algorithm that runs in milliseconds. As we showed in the previous section, in some cases ST is able to match Heuristic 2 in terms of upgrade cost, and now it is clear that ST has lower runtime than Heuristic 2.

Thresholds		ST					H2				
T_D	T_S	Int.Tol. Upg. Cost	Average availability NC	Average availability GDP-R	Average capacity NC	Average capacity GDP-R	Int.Tol. Upg. Cost	Average availability NC	Average availability GDP-R	Average capacity NC	Average capacity GDP-R
0.01	0.01	789	0.996591	0.996573	4.82	4.82	719	0.996591	0.996573	4.82	4.82
	0.005		0.997275	0.997220	5.13	5.16		0.996708	0.996620	4.97	5.00
0.005	0.01	1,978	0.996626	0.996608	4.79	4.79	1,745	0.996591	0.996573	4.82	4.82
	0.005		0.997110	0.997067	5.08	5.09		0.996708	0.996620	4.97	5.00
	0.001		0.998808	0.998645	8.27	8.42		0.997478	0.996876	5.70	5.78
0.001	0.01	5,958	0.996307	0.996307	4.35	4.35	4,728	0.996591	0.996573	4.82	4.82
	0.005		0.996622	0.996556	4.82	4.84		0.996708	0.996620	4.97	5.00
	0.001		0.996087	0.995939	6.25	6.25		0.997478	0.996876	5.70	5.78
	0.0005		0.999483	0.999388	9.08	9.20		0.999496	0.999468	9.50	9.60
0.0005	0.01	7,985	0.995641	0.995641	3.98	3.98	6,087	0.996591	0.996573	4.82	4.82
	0.005		0.996876	0.996432	4.74	4.77		0.996708	0.996620	4.97	5.00
	0.001		0.996087	0.995939	6.25	6.25		0.997478	0.996876	5.70	5.78
	0.0005		0.998671	0.998562	8.60	8.63		0.999437	0.999326	8.96	9.09

Table 5.3: Comparison of the routing results in the case of different intensity tolerance upgrade methods for the Italy network to guarantee a minimal target availability $\widehat{a_{WP}} = 0.995$).

5.7 The Performance Analysis of a Network Coding based Routing Approach

The results in this section include various aspects (e.g., availability and capacity allocation). Most importantly, a network coding (NC) based approach was introduced in contrast to GDP with Routing (GDP-R). Analyzing the results show that a general improvement can be measured in the availability when using network coding instead of GDP-R , as it can be seen in Table 5.3. A new variable was introduced called T_S which stands for the SRLG probability. In this context, T_S denotes the set of regional failures which have a greater probability for the network's disconnection if they all fail than e.g. 0.01, 0.005, or 0.001, as it can be seen in Table 5.3. ST and Heuristic 2 has slight differences in both availability and average capacity allocation results but looked very similar. A key point is that network coding produces a better capacity allocation value for all experiments, this comes from the fact that coding has a better bandwidth utilization since sending out the divided packets save bandwidth.

Comparing the Heuristics, no obvious trend can be measured, however for the largest threshold values (T_D) , ST performed better, and for smaller thresholds, Heuristic 2 did. As previously analyzed, upgrade costs are lower for Heuristic 2. About capacity allocation, an interesting peak value is for $T_s = 0.001$ and $T_D = 0.005$ which is significantly larger than the Heuristic 2's value. Also, for $T_s = 0.001$ and $T_D = 0.001$ the results are measurably higher. For the other threshold values, ST has a lower capacity allocation value.

In summary, the NC slightly outperforms the GDP-R algorithms in terms of bandwidth utilization and availability. Note that in our experimental

setups, no capacity constraints were introduced; hence the NC algorithm could not show its full potential in terms of robustness and flexibility. In addition, it is worth mentioning that the NC routing can be calculated in polynomial time, while the GDP-R is an NP-complete problem. Of course, the 'cost' of these benefits of NC is the rise of in-network complexity, i.e., that NC compatible switches are necessary.

Chapter 6

Summary

During my experiment, I studied the evolution of the FRADIR framework, the history of earthquake-based network outages from all over the world. I analyzed the previous results of the link upgrade methods implemented beforehand and examined how survivable routing algorithms work. Then I proposed a new heuristic algorithm (denoted as ST) to find the proper links in a network, which could positively impact the network's connectivity if we physically upgrade its intensity tolerance. This algorithm (ST) is based on the construction of a spanning tree with a maximum weight where the weight on the edges is calculated by their impact on the network's vulnerability. I also created a minimizing algorithm (MA) for this purpose that is designed to increase their performance and get a closer result to the optimal solution for this problem (provided by the ILP). Finally, I tested how a network coding-based routing (denoted with NC) performs in terms of availability and capacity allocation compared to the GDP with Routing (GDP-R) in two already enhanced (i.e., upgraded with our heuristics) networks.

The results show that the ST approach might not work well in terms of minimizing the upgrade cost since the possible shorter links could be left out from the spanning tree; nonetheless, it provided a good performance compared to Heuristic 2's approach regarding availability and capacity allocation. This can be regarded as a significant finding. The minimization algorithm (MA) delivered significant improvements for the existing heuristic algorithm Heuristic 1 as expected and minor improvements for Heuristic 2 and ST. In addition, I showed that the NC routing outperforms the current choice of the FRADIR framework, both in terms of availability and capacity consumption.

Bibliography

[1] Rudolf Ahlswede, Ning Cai, S-YR Li, and Raymond W Yeung. Network information flow. *IEEE Transactions on information theory*, 46(4): 1204–1216, 2000.

[2] Abdulaziz Alashaikh, Teresa Gomes, and David Tipper. The spine concept for improving network availability. *Computer Networks*, 82: 4–19, 2015.

[3] M. Waqar Ashraf, Sevia M. Idrus, Farabi Iqbal, and Rizwan Aslam Butt. On spatially disjoint lightpaths in optical networks. *Photonic Network Communications*, 36(1):11–25, Aug 2018. ISSN 1572-8188.

[4] Yoshinari Awaji, Hideaki Furukawa, Sugang Xu, Masaki Shiraiwa, Naoya Wada, and Takehiro Tsuritani. Resilient optical network technologies for catastrophic disasters. *Journal of Optical Communications and Networking*, 9(6):A280–A289, 2017.

[5] P. Babarczi, A Pasic, J. Tapolcai, F. Németh, and B. Ladóczki. Instantaneous recovery of unicast connections in transport networks: Routing versus coding. *Computer Networks*, 82:68–80, 2015. ISSN 1389-1286. doi: http://dx.doi.org/10.1016/j.comnet.2015.02.010.

[6] P. Babarczi, J. Tapolcai, A. Pašić, L. Rónyai, E. R. Bérczi-Kovács, and M. Médard. Diversity coding in two-connected networks. *IEEE/ACM Transactions on Networking*, 25(4):2308–2319, Aug 2017. ISSN 1063-6692. doi: 10.1109/TNET.2017.2684909.

[7] P. Babarczi, M. Klügel, A. M. Alba, M. He, J. Zerwas, P. Kalmbach, A. Blenk, and W. Kellerer. A mathematical framework for measuring network flexibility. *Computer Communications*, 164:13–24, 2020. ISSN 0140-3664. doi: 10.1016/j.comcom.2020.09.014. Special Issue on IFIP Networking 2019 Conference.

[8] Péter Babarczi, Gergely Biczók, Harald Øverby, János Tapolcai, and Péter Soproni. Realization strategies of dedicated path protection: A bandwidth cost perspective. *Computer Networks*, 57(9):1974 – 1990, 2013. ISSN 1389-1286.

[9] Peter Babarczi, Gergely Biczok, Harald Øverby, János Tapolcai, and Peter Soproni. Realization strategies of dedicated path protection: A bandwidth cost perspective. *Computer Networks*, 57(9):1974–1990, 2013.

[10] Péter Babarczi, Alija Pašić, János Tapolcai, Felicián Németh, and Bence Ladóczki. Instantaneous recovery of unicast connections in transport networks: Routing versus coding. *Computer Networks*, 82:68–80, 2015.

[11] William H Bakun. Mmi attenuation and historical earthquakes in the basin and range province of western north america. *Bulletin of the Seismological Society of America*, 96(6):2206–2220, 2006.

[12] Cong Cao, Moshe Zukerman, Weiwei Wu, Jonathan H Manton, and Bill Moran. Survivable topology design of submarine networks. *Journal of Lightwave Technology*, 31(5):715–730, 2013.

[13] Yufei Cheng, Deep Medhi, and James P. G. Sterbenz. Geodiverse routing with path delay and skew requirement under area-based challenges. *Networks*, 66(4):335–346, 2015. ISSN 1097-0037.

[14] Piotr Cholda, János Tapolcai, Tibor Cinkler, Krzysztof Wajda, and Andrzej Jajszczyk. Quality of resilience as a network reliability characterization tool. *IEEE network*, 23(2):11–19, 2009.

[15] Rodrigo de Souza Couto, Stefano Secci, Miguel Elias Mitre Campista, and Luís Henrique Maciel Kosmalski Costa. Network design requirements for disaster resilience in iaas clouds. *IEEE Communications Magazine*, 52(10):52–58, 2014.

[16] A. de Sousa, D. Santos, and P. Monteiro. Determination of the minimum cost pair of D-geodiverse paths. In *The 2017 International Conference on Design of Reliable Communication Networks (DRCN 2017)*, Munich, March 8-10 2017.

[17] Ferhat Dikbiyik, Massimo Tornatore, and Biswanath Mukherjee. Minimizing the risk from disaster failures in optical backbone networks. *Journal of Lightwave Technology*, 32(18):3175–3183, 2014.

[18] B. Elshqeirat, S. Soh, S. Rai, and M. Lazarescu. Topology design with minimal cost subject to network reliability constraint. *IEEE Transactions on Reliability*, 64(1):118–131, March 2015. ISSN 0018-9529. doi: 10.1109/TR.2014.2338253.

[19] Teresa Gomes, János Tapolcai, Christian Esposito, David Hutchison, Fernando Kuipers, Jacek Rak, Amaro De Sousa, Athanasios Iossifides,

Rui Travanca, Joao André, et al. A survey of strategies for communication networks to protect against large-scale natural disasters. In *2016 8th international workshop on resilient networks design and modeling (RNDM)*, pages 11–22. IEEE, 2016.

[20] Harvey J Greenberg. Greedy algorithms for minimum spanning tree. *University of Colorado at Denver*, 1998.

[21] M. Farhan Habib, Massimo Tornatore, Ferhat Dikbiyik, and Biswanath Mukherjee. Disaster survivability in optical communication networks. *Comput. Commun.*, 36:630–644, 2013.

[22] John Heidemann, Lin Quan, and Yuri Pradkin. *A preliminary analysis of network outages during hurricane sandy.* University of Southern California, Information Sciences Institute, 2012.

[23] W. Kellerer, A. Basta, P. Babarczi, A. Blenk, M. He, M. Klügel, and A. M. Alba. How to measure network flexibility? - A proposal for evaluating softwarized networks. *IEEE Communications Magazine*, 56(10): 186–192, 2018. ISSN 0163-6804. doi: 10.1109/MCOM.2018.1700601.

[24] Alexis Kwasinski, Wayne W. Weaver, Patrick L. Chapman, and Philip T. Krein. Telecommunications power plant damage assessment for hurricane katrina-site survey and follow-up results. *IEEE Systems Journal*, 3(3):277–287, 2009. ISSN 1932-8184. doi: 10.1109/JSYST.2009.2026783. Funding Information: Manuscript received October 25, 2008; revised February 28, 2009. First published August 25, 2009; current version published September 16, 2009. This work was supported in part by the National Science Foundation (NSF) under Award ECS-0554090 and by the Grainger Center for Electric Machinery and Electromechanics at the University of Illinois Urbana-Champaign.

[25] Victor Yu Liu and David Tipper. Spare capacity allocation using shared backup path protection for dual link failures. *Computer Communications*, 36(6):666–677, 2013.

[26] Yu Liu, David Tipper, and Peerapon Siripongwutikorn. Approximating optimal spare capacity allocation by successive survivable routing. In *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213)*, volume 2, pages 699–708. IEEE, 2001.

[27] Carmen Mas Machuca, Stefano Secci, Petra Vizarreta, Fernando Kuipers, Antonios Gouglidis, David Hutchison, Simon Jouet, Dimitrios Pezaros, Ahmed Elmokashfi, Poul Heegaard, and Sasko Ristov.

Technology-related disasters: A survey towards disaster-resilient software defined networks. 09 2016. doi: 10.1109/RNDM.2016.7608265.

[28] Andreas Mauthe, David Hutchison, Egemen K Cetinkaya, Ivan Ganchev, Jacek Rak, James PG Sterbenz, Matthias Gunkelk, Paul Smith, and Teresa Gomes. Disaster-resilient communication networks: Principles and best practices. In *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pages 1–10. IEEE, 2016.

[29] Biswanath Mukherjee, M Farhan Habib, and Ferhat Dikbiyik. Network adaptability from disaster disruptions and cascading failures. *IEEE Communications Magazine*, 52(5):230–238, 2014.

[30] Sebastian Neumayer, Gil Zussman, Reuven Cohen, and Eytan Modiano. Assessing the vulnerability of the fiber infrastructure to disasters. *IEEE/ACM Transactions on Networking*, 19(6):1610–1623, 2011.

[31] P Nicholson. Five most famous ddos attacks and then some, 2020.

[32] Sebastian Orlowski, Roland Wessäly, Michal Pióro, and Artur Tomaszewski. SNDlib 1.0–Survivable Network Design library. *Networks*, 55(3):276–286, 2010. http://sndlib.zib.de.

[33] D. Papadimitriou and B. Fortz. Reliability-dependent combined network design and routing optimization. In *2014 6th International Workshop on Reliable Networks Design and Modeling*, pages 31–38, Nov 2014. doi: 10.1109/RNDM.2014.7014928.

[34] Alija Pašić, János Tapolcai, Péter Babarczi, Erika R Bérczi-Kovács, Zoltán Király, and Lajos Rónyai. Survivable routing meets diversity coding. In *2015 IFIP Networking Conference (IFIP Networking)*, pages 1–9. IEEE, 2015.

[35] Alija Pašić, Rita Girão-Silva, Balázs Vass, Teresa Gomes, and Péter Babarczi. Fradir: A novel framework for disaster resilience. In *2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pages 1–7. IEEE, 2018.

[36] Alija Pašić, Rita Girão-Silva, Balázs Vass, Teresa Gomes, Ferenc Mogyorósi, Péter Babarczi, and János Tapolcai. Fradir-ii: An improved framework for disaster resilience. In *2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pages 1–7. IEEE, 2019.

[37] Alija Pašić, Rita Girão-Silva, Ferenc Mogyorósi, Balázs Vass, Teresa Gomes, Péter Babarczi, Péter Revisnyei, Janos Tapolcai, and Jacek

Rak. efradir: An enhanced framework for disaster resilience. *IEEE Access*, 9:13125–13148, 2021.

[38] Lejla Pasic, Azra Pašić, Ferenc Mogyorósi, and Alija Pašić. Fradir meets availability. pages 1–6, 03 2020. doi: 10.1109/DRCN48652.2020.1570603965.

[39] C. Pasolini, D. Albarello, P. Gasperini, V. D'Amico, and B. Lolli. The attenuation of seismic intensity in Italy, Part II: modeling and validation. *Bulletin of the Seismological Society of America*, 98(2):692–708, 2008.

[40] A. Pašić, P. Babarczi, J. Tapolcai, E. R. Bérczi-Koávcs, Z. Király, and L. Rónyai. Minimum cost survivable routing algorithms for generalized diversity coding. *IEEE/ACM Transactions on Networking*, 28(1):289–300, Feb 2020. ISSN 1558-2566. doi: 10.1109/TNET.2019.2963574.

[41] Alija Pašić, Rita Girão-Silva, Balázs Vass, Teresa Gomes, and Péter Babarczi. FRADIR: A novel framework for disaster resilience. In *10th International Workshop on Resilient Networks Design and Modeling (RNDM 2018)*, Longyearbyen, Svalbard (Spitsbergen), Norway, Aug. 27-29 2018.

[42] Alija Pašić, Rita Girão-Silva, Balázs Vass, Teresa Gomes, Ferenc Mogyorósi, Péter Babarczi, and János Tapolcai. FRADIR-II: An improved framework for disaster resilience. In *11th International Workshop on Resilient Networks Design and Modeling (RNDM 2019)*, Nicosia, Cyprus, October 2019.

[43] Y. Prieto, J. E. Pezoa, N. Boettcher, and S. K. Sobarzo. Increasing network reliability to correlated failures through optimal multiculture design. In *CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies*, pages 1–6, Oct 2017. doi: 10.1109/CHILECON.2017.8229516.

[44] Jacek Rak. *Resilient routing in communication networks*, volume 118. Springer, 2015.

[45] Jacek Rak, David Hutchison, Eusebi Calle, Teresa Gomes, Matthias Gunkel, Paul Smith, Janos Tapolcai, Sofie Verbrugge, and Lena Wosinska. Recodis: Resilient communication services protecting end-user applications from disaster-based failures. In *2016 18th International Conference on Transparent Optical Networks (ICTON)*, pages 1–4. IEEE, 2016.

[46] Jacek Rak, David Hutchison, Janos Tapolcai, Rasa Bruzgiene, Massimo Tornatore, Carmen Mas-Machuca, Marija Furdek, and Paul Smith.

Fundamentals of communication networks resilience to disasters and massive disruptions. In *Guide to Disaster-Resilient Communication Networks*, pages 1–43. Springer, 2020.

[47] F. Robledo, P. Romero, and M. Saravia. On the interplay between topological network design and diameter constrained reliability. In *2016 12th International Conference on the Design of Reliable Communication Networks (DRCN)*, pages 106–108, March 2016. doi: 10.1109/DRCN.2016.7470842.

[48] S. Rouayheb, A. Sprintson, and C. Georghiades. Robust network codes for unicast connections: A case study. *IEEE/ACM Transactions on Networking*, 19(3):644–656, 2011.

[49] Hiroshi Saito. Analysis of geometric disaster evaluation model for physical networks. *IEEE/ACM Transactions on Networking*, 23(6):1777–1789, 2014.

[50] Hiroshi Saito. Spatial design of physical network robust against earthquakes. *Journal of Lightwave Technology*, 33(2):443–458, 2015.

[51] Alexander Schrijver. *Theory of linear and integer programming*. John Wiley & Sons, 1998.

[52] Arunabha Sen, Sudheendra Murthy, and Sujogya Banerjee. Region-based connectivity – a new paradigm for design of fault-tolerant networks. In *International Conference on High Performance Switching and Routing*, pages 1–7. IEEE, 2009.

[53] Rodrigo Souza Couto, Stefano Secci, Miguel Mitre Campista, Kosmalski Costa, and Luis Maciel. Network design requirements for disaster resilience in IaaS clouds. *IEEE Communications Magazine*, 52(10):52–58, 2014.

[54] J Svetlik. Google goes down for 5 minutes, internet traffic drops 40%. *URL https://www. cnet. com/news/googlegoes-down-for-5-minutes-internet-traffic-drops-40*, 2013.

[55] János Tapolcai, P Cholda, Tibor Cinkler, Krzysztof Wajda, Andrzej Jajszczyk, Achim Autenrieth, Stefan Bodamer, Didier Colle, Giuseppe Ferraris, H Lonsethagen, et al. Quality of resilience (qor): Nobel approach to the multi-service resilience characterization. In *2nd International Conference on Broadband Networks, 2005.*, pages 1328–1337. IEEE, 2005.

[56] János Tapolcai, Piotr Cholda, Tibor Cinkler, Krzyszt of Wajda, Andrzej Jajszczyk, and Dominique Verchere. Joint quantification of re-

silience and quality of service. In *2006 IEEE International Conference on Communications*, volume 2, pages 477–482. IEEE, 2006.

[57] János Tapolcai, Balázs Vass, Zalán Heszberger, József Biró, David Hay, Fernando A. Kuipers, and Lajos Rónyai. A tractable stochastic model of correlated link failures caused by disasters. In *Proc. IEEE INFOCOM*, Honolulu, USA, April 2018.

[58] David Tipper. Resilient network design: challenges and future directions. *Telecommunication Systems*, 56(1):5–16, 2014. ISSN 1018-4864. doi: 10.1007/s11235-013-9815-x.

[59] M. Tornatore, P. Babarczi, O. Ayoub, S. Ferdousi, R. Lourenco, J. Zerwas, A. Blenk, M. Klügel, and W. Kellerer. Alert-based network reconfiguration and data evacuation. In J. Rak and D. Hutchison, editors, *Guide to Disaster-resilient Communication Networks*, chapter 14, pages 353–377. Springer, 2020. ISBN 978-3-030-44685-7. doi: 10.1007/978-3-030-44685-7_14.

[60] Alessandro Valentini, Balázs Vass, Jorik Oostenbrink, Levente Csák, Fernando A. Kuipers, Bruno Pace, David Hay, and János Tapolcai. Network resiliency against earthquakes. In *11th International Workshop on Resilient Networks Design and Modeling (RNDM 2019)*, Nicosia, Cyprus, October 2019.

[61] Balázs Vass, János Tapolcai, David Hay, Jorik Oostenbrink, and Fernando Kuipers. How to model and enumerate geographically correlated failure events in communication networks. In *Guide to Disaster-Resilient Communication Networks*, pages 87–115. Springer, 2020.

[62] Harry O Wood and Frank Neumann. Modified mercalli intensity scale of 1931. *Bulletin of the Seismological Society of America*, 21(4):277–283, 1931.

[63] W. Wu, B. Moran, J. H. Manton, and M. Zukerman. Topology design of undersea cables considering survivability under major disasters. In *2009 International Conference on Advanced Information Networking and Applications Workshops*, pages 1154–1159, 2009.

[64] G Xanthopoulos and M Athanasiou. 'attica region, greece july 2018: A tale of two fires and a seaside tragedy. *Wildfire*, 28(2):18–21, 2019.

[65] J. Yallouz and A. Orda. Tunable QoS-aware network survivability. *IEEE/ACM Transactions on Networking*, 25(1):139–149, 2017.

[66] J. Zhang, E. Modiano, and D. Hay. Enhancing network robustness via shielding. In *11th International Conference on the Design of Reliable*

Communication Networks (DRCN 2015), pages 17–24, March 2015. doi: 10.1109/DRCN.2015.7148980.