Universidade de Aveiro
2022

Fábio Daniel
Moreira Barbosa

Projeto e Gestão de Recursos de Redes Óticas Elásticas Resilientes a Desastres

Disaster-resilient Network Design and Resource Management of Elastic Optical Networks

Universidade de Aveiro
2022

Fábio Daniel
Moreira Barbosa

Projeto e Gestão de Recursos de Redes Óticas Elásticas Resilientes a Desastres

Disaster-resilient Network Design and Resource Management of Elastic Optical Networks

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Engenharia Eletrotécnica, realizada sob a orientação científica do Doutor Amaro Fernandes de Sousa, Professor auxiliar do Departamento de Eletrónica, Telecomunicações e Informática e do Doutor Agostinho Miguel Mendes Agra, Professor associado c/ agregação do Departamento de Matemática da Universidade de Aveiro.

Este trabalho foi financiado pela FCT – Fundação para a Ciência e a Tecnologia, I.P., através da bolsa de doutoramento SFRH/BD/132650/2017. Esta investigação foi apoiada por Fundos FEDER através do Programa Operacional Regional do Centro e por Fundos Nacionais através da FCT no âmbito do projeto ResNeD (CENTRO-01-0145-FEDER-029312). Esta investigação foi também apoiada pelo programa europeu COST (*European Cooperation in Science & Technology*) no âmbito da ação CA15127 RECODIS. Este trabalho teve como instituição de acolhimento o Instituto de Telecomunicações, pólo de Aveiro.

o júri / the jury

presidente / president

Doutor Vasco Afonso da Silva Branco
Professor Catedrático, Universidade de Aveiro.

vogais / examiners committee

Doutor Rui Jorge Morais Tomaz Valadas
Professor Catedrático, Universidade de Lisboa - Instituto Superior Técnico;

Doutor Paulo Miguel Nepomuceno Pereira Monteiro,
Professor Associado, Universidade de Aveiro;

Doutora Teresa Martinez dos Santos Gomes
Professora Auxiliar, Universidade de Coimbra;

Doutor Pedro Mendes Ferrão Simões Patrício,
Professor Auxiliar, Universidade da Beira Interior;

Doutor Amaro Fernandes de Sousa (Orientador),
Professor Auxiliar, Universidade de Aveiro.

agradecimentos / acknowledgements

Aos meus orientadores, Doutor Amaro Fernandes de Sousa e Doutor Agostinho Miguel Mendes Agra, agradeço a total disponibilidade, dedicação e entusiasmo demonstrados, a amizade e por acreditarem sempre nas minhas capacidades para a realização deste doutoramento.

Ao diretor do programa doutoral, Doutor Armando Nolasco Pinto, agradeço por facultar a minha integração neste doutoramento. Ao Departamento do Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, agradeço as condições de aprendizagem e crescimento científico providenciadas. À secretaria do DETI, em particular à Ana Sofia Ribeiro, agradeço a disponibilidade para o esclarecimento de todos os assuntos relacionados ao programa doutoral.

Ao pólo de Aveiro do Instituto de Telecomunicações, agradeço a facultação de condições de excelência para realização do meu trabalho de investigação científica. Ao pessoal técnico e administrativo do Instituto de Telecomunicações, em particular, à Sandra Corujo e à Suzana Condesso, agradeço a total disponibilidade e suporte demonstrados.

À Fundação para a Ciência e a Tecnologia, agradeço o apoio financeiro para a realização do meu doutoramento. Aos projetos ResNeD e RECODIS, agradeço o apoio financeiro para apresentar o meu trabalho de investigação científica em diversas conferências e revistas científicas internacionais.

Agradeço ainda a todas as pessoas com que tive a oportunidade de trabalhar ao longo deste doutoramento. Em particular, Doutor Krzysztof Walkowiak e Doutora Róża Goścień, agradeço a forma cordial com que me receberam em Wrocław, na Polónia, para a realização da nossa colaboração científica.

À minha namorada, Luisa, agradeço o companheirismo, confiança e todo o apoio incondicional demonstrado ao longo destes anos. Aos meus pais e irmão, agradeço o incentivo e os sacrifícios que ajudaram a tornar este percurso possível.

E a todos aqueles que direta ou indiretamente contribuíram para o sucesso do meu percurso académico, o meu muito obrigado!

Palavras Chave

Resiliência a Desastres; Redes Óticas Elásticas; Projeto de Redes Robustas; Deteção de Nós Críticos; Encaminhamento, Modulação e Atribuição de Espectro; Programação Linear Inteira; Telecomunicações.

Resumo

Falhas provocadas por desastres, devido a causas naturais, tecnológicas ou humanas, tornaram-se mais frequentes e abrangentes, causando uma degradação drástica nos serviços de comunicação providenciados por redes de telecomunicações. Este facto tem uma importância extrema, uma vez que estes serviços de comunicação constituem uma parte com importância crítica na nossa sociedade.

Este problema é ainda mais crítico em redes óticas pois uma única fibra ótica pode transportar informação de uma grande quantidade de serviços da rede. É importante não só recuperar rapidamente os elementos da rede afetados por um desastre (problema pós-desastre) mas também avaliar e minimizar, antes do desastre ocorrer, o impacto deste nos serviços entre nós fora da área afetada (problema pré-desastre).

Esta tese está centrada no problema pré-desastre e visa investigar como as redes óticas elásticas (EONs) podem ser usadas de forma eficiente, em termos de custo, para que o impacto de falhas provocadas por desastres seja minimizado. Esta tese considera os desastres resultantes de ataques humanos maliciosos a alguns elementos da rede.

Primeiramente, avalia-se a vulnerabilidade de rede óticas existentes a essas falhas, recorrendo principalmente a variantes do problema de Deteção de Nós Críticos (CND), um problema de otimização que procura o conjunto de nós cuja falha simultânea interrompe o maior número de serviços da rede. Um algoritmo exato de geração de linhas é proposto para o problema CND no contexto de redes óticas transparentes.

Em seguida, fornece-se aos operadores de telecomunicações ferramentas para aumentar a robustez das topologias de redes óticas contra falhas provocadas por desastres. Por um lado, investiga-se como expandir as redes óticas existentes, recorrendo à adição de ligações, com o objetivo de aumentar a robustez a múltiplas falhas de nós. Numa abordagem heurística, dado um limite para o comprimento de fibra adicional, é apresentado um algoritmo *greedy* aleatório e um algoritmo *greedy* determinístico. Numa abordagem exata, desenvolvem-se métodos para calcular a fronteira de Pareto do problema de otimização biobjetivo que considera a maximização da robustez e a minimização do custo de expansão da rede. Por outro lado, fornece-se uma seleção de custo mínimo de nós *gateway* para redes de outros operadores com resiliência máxima contra multiplas falhas. O problema de Seleção de Nós *Gateway* (GNS) é definido, propondo uma metodologia exata para a obtenção de todos os ótimos de Pareto.

Resumo (cont.)

Finalmente, explora-se as vantagens do planeamento e da operação de redes óticas com flexibilidade espectral (proporcionada por redes óticas elásticas). Considerando tráfego estático e dinâmico, com uma mistura de pedidos *unicast* e *anycast* servidos pela rede, propõem-se algoritmos de Encaminhamento, Modulação e Atribuição de Espectro (RMSA) resilientes a múltiplas falhas de nós. Esses algoritmos RMSA baseiam-se numa métrica introduzida, chamada disponibilidade do caminho em desastres, que mede a probabilidade de um caminho não ser afetado por um ataque a vários nós.

Keywords

Disaster Resilience; Elastic Optical Networks; Robust Network Design; Critical Node Detection; Routing, Modulation and Spectrum Assignment; Integer Linear Programming, Telecommunications.

Abstract

Disaster-based failures, due to either natural, technological or human causes, became more frequent in time and wider in scope, degrading drastically the communication services supported by telecommunication networks. This is of utmost importance since communication services are an important part of our society critical infrastructure.

This issue is even more critical in optical networks where a single optical fiber can carry a very large amount of service demands. It is important not only to quickly recover the failed network elements disrupted by a disaster (post-disaster problem) but also to evaluate and minimize, before the disaster occurs, its impact on services between nodes outside the disaster area (pre-disaster problem).

This thesis focuses on the pre-disaster problem and aims to investigate how Elastic Optical Networks (EONs) can be used in a cost-effective manner so that the impact of disaster-based failures is minimized. This thesis considers the disasters due to malicious humans attacks against some network elements.

First, the vulnerability of existing optical networks to these failures is assessed, mainly resorting to variants of the Critical Node Detection (CND) problem, an optimization problem that seeks the set of nodes whose simultaneous failure mostly disrupt the network services. An exact row generation algorithm is proposed for the CND problem in the context of transparent optical networks.

Then, we provide telecommunication operators with tools to enhance the robustness of optical network topologies against disaster-based failures. On one hand, we investigate how to upgrade existing optical networks, through link addition, aiming to enhance their robustness to multiple node failures. In a heuristic approach, within a given fiber length budget, a multi-start greedy randomized algorithm and a greedy deterministic algorithm are presented. In an exact approach, methods to compute the Pareto frontier of the bi-objective optimization problem that considers both the robustness maximization and the minimization of the cost of upgrading the network are proposed. On the other hand, a minimum cost gateway nodes selection to third-party networks with maximum disaster resilience against multiple failures is provided. The Gateway Node Selection (GNS) problem is defined, proposing an exact methodology to obtain all Pareto-optimal solutions.

Abstract (cont.)

Finally, we exploit the advantages of spectrally (provided by elastic optical networking) flexible optical network planning and operations. Considering static and dynamic traffic, with a mix of unicast and anycast service demands, Routing, Modulation and Spectrum Assignment (RMSA) algorithms resilient to multiple node failures are proposed. These RMSA algorithms are based on an introduced metric, called path disaster availability, that measures the probability of a routing path not being disrupted by a multiple node attack.

Contents

List of acronyms

A2TR	Average 2-Terminal Reliability
CLD	Critical Link Detection
CND	Critical Node Detection
DAT	Distance-Adaptive Transmission
DC	Data Center
EON	Elastic Optical Network
ESP	Edge Selection Problem
GNS	Gateway Node Selection
FF	First-Fit
FS	Frequency Slot
ILP	Integer Linear Programming
LFS	Lowest Frequency Slot
MF	Modulation Format
MILP	Mixed Integer Linear Programming
NDC	Node Demand Centrality
PDA	Path Disaster Availability
RNG	Relative Neighbourhood Graph
RSA	Routing and Spectrum Assignment
RMSA	Routing, Modulation and Spectrum Assignment
RNUP	Robust Network Upgrade Problem
SDM	Space Division Multiplexing
SLA	Service Level Agreement

Chapter 1

Introduction

Large-scale failure events are becoming a concern to telecommunications network operators as such events are becoming more frequent in time and wider in scope [RH20]. Disaster-based multiple failures, due to either natural, technological or human causes, can seriously disrupt any telecommunication network [RHC$^+$16]. A key component when dealing with these disaster-based multiple failures consists in taking into account the network design aiming the robustness to those failures [GTE$^+$16]. Following the work of COST Action RECODIS [RHC$^+$16], disaster resilience of networks involves the following three main components: network vulnerability assessment, disaster-resilience network enhancements, and disaster-resilient resource management.

On one hand, a natural disaster typically affects a specific area. A problem of interest is the identification of the network areas that, upon failure, maximally degrade the network performance: in [NZCM11, TKI$^+$15], it is studied how to compute the most vulnerable network parts, subject to geographically-correlated failures and, in [AEG$^+$13], probabilistic failure models are considered where nodes closer to a disaster central point have higher failure probabilities. On the other hand, human attacks can involve the simultaneous failure of network components without geographical correlation and such attacks can be even more destructive [FWG$^+$16].

Current networks have intrinsic design vulnerabilities affecting their resilience to disasters. One approach to improve their disaster resilience is to design the networks so that backup links exist when primary links become unavailable [GBHC15]. Other alternatives have been proposed: [SVCM12] exploiting immunization strategies (i.e. fortifying certain links) by identifying links to be immunized that minimize the impact of failures; [ZMH17] considering shielding critical links (e.g. strengthening cables) under general and geographical failures; [MHD14] exploiting the rearrangement of the network resources and services on a partially damaged network; and [dSMS17] selecting some nodes that, if made robust, improve the network resilience against multiple node failures.

Disaster-resilient resource management can be provided by path diversification [RJS14]. An example is GeoDivRP [CGL$^+$15], a protocol able to provide multiple geographically diverse paths to end nodes. Other examples are [dSSM17] using the concept of D-geodiverse paths (i.e. a pair of paths with a minimum geographical distance D between them from a source to a destination node), [TKI$^+$15] addressing the determination of pairs of region-disjoint paths and

[KO14, NEM15] modeling disaster failures as a generalization of the min-cut and max-flow problems.

In [RCM17], an interesting way to classify any multiple failure scenario on a telecommunication network is proposed. It considers the following three components:

- Element: node and/or link;
- Temporal dimension: static or dynamic (epidemic-like or cascading);
- Strategy: random or targeted (sequential or simultaneous).

In this thesis, the main focus is to consider multiple failures caused by malicious human attacks. On one hand, node shutdowns are harder to realize than link cuts. On the other hand, in the attacker's perspective, node shutdowns are the most rewarding as the shutdown of a single node also shuts down all its incident links. Here, we consider mainly the scenario of node failures since they are the most harmful cases of malicious human activities. Therefore, in the classification proposed in [RCM17], we focus on static targeted simultaneous multiple node failures.

Given a telecommunication network topology, in some of the addressed challenges, we are considering a worst-case scenario approach. In such cases, we seek the set of nodes whose simultaneous failure mostly disrupt the network services. This can be computed with the optimal solution of an optimization problem, commonly named Critical Node Detection (CND) problem. For a given number c, this optimization problem consists of computing a set of c nodes (named critical nodes) such that their elimination maximally reduces the network connectivity according to a given connectivity metric. In the preparedness of telecommunication networks against large-scale failures, the optimal value of the CND problem has been recently considered as a metric to evaluate the network resilience to multiple node failures, as in [dSMS17], where some network nodes are selected, resorting to the CND optimal solution, to be made robust such that they never fail.

The CND problem has been extensively addressed in different network contexts and different connectivity metrics have been considered: minimizing the pairwise connectivity, maximizing the number of connected components, and minimizing the number of nodes of the largest connected component size [LTK18], among others. Moreover, alternative CND formulations have been proposed with different objective functions and/or constraints, e.g. the beta-vertex disruptor [DXT$^+$10] and the component-cardinality-constrained variant [LTK16]. In this thesis, the focus is on the CND variant whose objective is to compute a set of c nodes whose removal minimizes the pairwise connectivity of the network [ACEP09, SGL12, Ven12], a variant that has been used in the vulnerability evaluation of telecommunication networks to multiple node failures [dSS20, SdSM18].

By comparing several real telecommunication networks, in [RCM17], it is concluded that the most robust networks under targeted attacks have high values of average nodal degree, low values of average shortest path length, and low diameter. In order to implement a flexible optical network, a new kind of ROADM (Reconfigurable Optical Add-Drop Multiplexer) is required that allows flexible spectrum to be switched from the input to the output ports. This approach is called Elastic Optical Networking (EON) and it has the following two key properties: the optical spectrum can be flexibly divided and the Bandwidth Variable Transceivers (BVT) can generate optical paths with different bit rates [GJLY12].

In EONs, the optical spectrum of each fiber link is organized in *frequency slots* (FSs).

Assuming a transparent optical network (i.e. optical network without intermediate electrical regeneration required), each demand between a pair of nodes is routed over an end-to-end *lightpath*. In the source node, data is converted from electrical to optical domain resorting to a modulation format (MF) and emitting on a set of contiguous FSs, transmitted through a routing path over the network and, in the target node, data is converted back to the electrical domain. Multiple lightpaths can be set up in a way such that their FSs do not overlap on any network fiber link.

Due to many factors that affect light transmission over fibers, in a transparent optical network, there is the need to impose a maximum length for the routing path of each lightpath, named *transparent reach*. For example, comparing the modulation formats QPSK and 16-QAM, in a single carrier lightpath, the 16-QAM carries twice the number of bits/symbol but imposes a shorter transparent reach. Then, in a shorter routing path, the same line rate (in bits/second) can be transmitted by 16-QAM instead of QPSK with a half symbol rate, occupying less FSs [JKT$^+$10]. This is the main principle behind the distance-adaptive spectrum allocation strategies [JKT$^+$10, TR17].

On one hand, when the MF is fixed (i.e. all lightpaths are modeled with the same MF), the decision on the routing path and FSs of each lightpath is known as the Routing and Spectrum Assignment (RSA) problem. On the other hand, when multiple MFs are available, this assignment problem has to include the MF configuration selection to each lightpath, which is widely known as the Routing, Modulation and Spectrum Assignment (RMSA) problem [CTV11]. The support of different service demands in EONs is ruled by the RMSA algorithm, which decides how the optical network resources are assigned to each network service demand.

Frequently, the main goal of the RMSA algorithm is to use the EON resources in an efficient way by keeping the spectrum resources usage as low as possible, aiming to increase the probability of future demands being accommodated [AR17, GZLZ12, KW11, WK13]. Nevertheless, due to the continuous advances of EONs in terms of node architectures and transceiver characteristics (e.g. higher bit rates), other goals are also important. For example, the minimization of transceiver costs and the minimization of the network power consumption [CSO15, GWK15, PAK$^+$12]. In this research, a novel objective to the RMSA algorithm is introduced, which is the minimization of the impact of disaster-based failures.

Further flexibility of EONs is provided by the novel sliceable-bandwidth variable transponders (S-BVTs). These devices can generate multiple optical carriers to support different lightpaths towards different destinations or to be merged into a single higher-rate super-channel. This flexibility can be used to optimally set up EONs, such as in [dSTP16] where ILP formulations for the minimum cost configuration of S-BVTs are presented or in [DGS$^+$15] where a dynamic routing, spectrum and transponder assignment scheme for dynamic EONs is proposed or also in [ZZY$^+$15] where ILP formulations for the energy-efficient traffic grooming with S-BVTs are presented.

Figure 1.1 illustrate the spectrum savings of using the flexible spectrum provided by EON for three examples of demands with different bit rates and transmission distances.

In the first spectrum configuration, each FS has a fixed grid of 50 GHz and operates with the QPSK format (which carries 100 Gbps on each lightpath). On one hand, “A” represents a demand that perfectly fits this configuration; on the other hand, both “B” and “C” require multiple lightpaths to fit within this configuration, wasting network resources due to the use

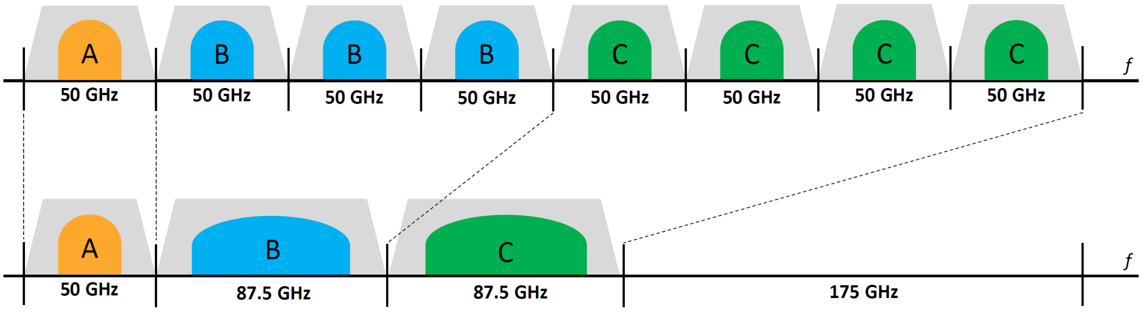


Figure 1.1: EON flexibility illustration for three demands: A (100 Gbps, 1000 km), B (300 Gbps, 1000 km), and C (400 Gbps, 200 km). On the top spectrum, representation of the spectrum needs of each demand on a 50 GHz fixed grid, assuming QPSK modulation (i.e. 100 Gbps per frequency slot). On the bottom spectrum, the same demands with adaptive modulation optimized for required bit rate and flexible spectrum (transceiver model based on [RBMT17] and transmission reaches based on [KRS$^+$16]).

of an inefficient MF and the use of multiple channels that require multiple guard-bands.

In the second spectrum configuration, demand “B” has been merged into a higher-rate super-channel with the MF 8-QAM, reducing the spectrum usage from 150 GHz to 87.5 GHz. Moreover, demand “C” has also been merged into a higher-rate super-channel with the MF 16-QAM (since it requires a shorter reach when compared to “B”), reducing the spectrum usage from 200 GHz to 87.5 GHz. Therefore, the global spectrum saving is 175 GHz, which allows more client demands to be served by the EON with this spectrum flexibility.

Besides the introduction, this initial chapter is organized into five sections. Section 1.1 presents the main research objectives addressed in this thesis. The thesis structure of the remaining chapters is given in Section 1.2. The main contributions of this thesis are summarized in Section 1.3, both in terms of scientific novelty and the interest of the work to the telecommunication network operators. Section 1.4 presents the author’s contributions, and finally, Section 1.5 presents the final considerations and possible future research directions.

1.1 Research general objectives

The main goal of this thesis is to investigate how EONs can be used in a cost-effective manner so that the impact of disaster-based failures, mainly caused by malicious attacks against network nodes, is minimized. This goal is composed by the following four interrelated issues.

The first issue is on how to assess the vulnerability of existing optical networks to disaster-based failures. Given an existing telecommunications network, one must identify the network elements (nodes and/or links) whose simultaneous failure minimizes the network connectivity (measure in terms of a given connectivity metric, e.g. pairwise connectivity). This issue involves the definition of appropriate network vulnerability metrics and the development of efficient techniques for computing the set of network critical elements that maximize these vulnerability metrics.

Next, the second issue is on how to upgrade existing optical networks to enhance their robustness to multiple failures. Given an existing optical network, one must identify a set of new fiber cables, connecting pairs of nodes that are not connected in the current network. The goal is to develop appropriate techniques able to compute the additional network links that maximally contribute to the network robustness to disasters, i.e. minimizing the vulnerability metrics of the resulting upgraded network.

Contrasting with upgrading existing networks through link addition, the third issue is on how to enhance the network disaster resilience by resorting to third-party networks for temporary connectivity in a failure scenario. Given an existing optical network and considering that there also exists, at least, one third-party network that operates in the same geographical region, one must identify a set of gateway nodes, in order to connect both networks (temporarily in a failure scenario), such that the network resilience against disaster-based failures is maximized.

Finally, the fourth issue is on how to implement disaster-resilient resource management. Given an EON (either an existing or an upgraded one), one must derive a resource management strategy minimizing the number of service demands that are disrupted by the simultaneous failures of the critical elements. This issue involves the RMSA mechanism used to groom all service demands on a set of lightpaths such that the impact of multiple failures is minimized.

To summarize, each one of these interrelated issues corresponds to one of the following main research objectives of this thesis:

1. Assessment of the network vulnerability to disaster-based failures.
2. Disaster-resilient network design through link addition.
3. Disaster-resilient network design resorting to third-party networks.
4. Disaster-resilient resource management of elastic optical networks.

In the following subsections, these four objectives are further detailed, providing insights on the approaches and methodologies used to address each objective.

1.1.1 Assessment of the network vulnerability to disaster-based failures

The aim is to provide telecommunications network operators with tools for the vulnerability assessment of their optical networks to disaster-based failures. The envisaged vulnerability metric is the total demand supported when all critical elements fail. The network vulnerability score and the set of critical network elements are the outcomes of the tool.

This task is addressed in the context of transparent optical networks (i.e. optical networks without intermediate electrical regeneration of lightpaths required). This assessment problem takes into account the transparent reach of each type of lightpath and exploits the EON feature that allows the dynamical change of optical modulation formats enabling longer transparent reaches at the cost of larger spectrum widths.

The vulnerability metrics are mainly based on optimization problems that will be approached firstly by Integer Linear Programming (ILP) methods that are potentially able to compute optimal solutions. Starting from known ILP models for the CND problem (e.g. [SdSM18]), we include new variables and/or constraints aiming to correctly define new CND problem variants that model optical networks.

To handle those large-size instances for which the ILP approach becomes computationally expensive, appropriate heuristic techniques based on techniques such as local branching (successfully used in [BdSA18a] and [AdSD16] for optical network design problems) are investigated. Moreover, since elements (nodes and/or links) in the center of the network topology are potentially more critical, centrality metrics (for example, closeness and betweenness centrality) are also exploited as a means to obtain fast efficient heuristic algorithms.

All methods are extensively tested on publicly available optical network topologies that can be found, for example, in [KNF$^+$11, OWPT10, Sim14].

1.1.2 Disaster-resilient network design through link addition

The aim is to provide telecommunication network operators with tools to upgrade their optical network topologies on the next investment period and for a given available CAPEX (*Capital Expenditure*) investment budget.

For a given transparent optical network, the goal is to identify a set of new fiber cables, within the investment budget, that maximally increase the network disaster robustness to multiple failures. It can be defined as a bi-level optimization problem: the objective of the master problem is to select the new fiber cables maximizing the total connectivity, considering the simultaneous failure of a set of critical elements (nodes and/or links); and, the objective of the subproblem is to identify a set of critical elements minimizing the total network connectivity (this subproblem is addressed on the previous research objective).

Firstly, this problem is addressed using heuristic methodology (resorting to stochastic and deterministic algorithms). These methods are extensively tested on publicly available optical network topologies. The results obtained by each heuristic are used to analyze the trade-off between investment budget and disaster robustness gains and to understand how this trade-off is influenced by the network topology characteristics (e.g. average node degree and average fiber length).

Then, the proposed problem is addressed using exact approaches. Here, the main goal is to provide to the telecommunication network operators optimal trade-offs between investment budget and robustness gains. It consists in solving a bi-objective optimization problem: minimizing the investment budget while maximizing the network robustness against disaster-based failures. Resorting to robust optimization, to achieve those optimal trade-offs, we aim to compute the Pareto frontier (either partial or complete) to this bi-objective problem.

1.1.3 Disaster-resilient network design resorting to third-party networks

In the previous objective, by upgrading the network robustness through link addition, the focus is on the design of all working links of the network. In contrast, here the focus is on the network design with backup links (i.e. links that are only available when a multiple failure occurs). To achieve this objective, we consider that temporary connectivity between some nodes (called gateway nodes) can be provided by third-party network operators that might exist in the same geographical region.

The aim is to provide telecommunications network operators with tools to minimize the cost of the gateway nodes to third-party telecommunication networks white maximizing the network disaster resilience against multiple failures. This aim is an optimization problem that can be also formulated as a bi-level problem: here, the objective of the master problem is to select the gateway nodes that maximize the temporary connectivity provided by third-party operators, considering the simultaneous failure of a set of critical elements; and, once again, the objective of the subproblem is to identify a set of critical elements that minimize the network connectivity. To solve this kind of bi-level problem, robust optimization techniques are required (e.g. [ACF$^+$13, ASNP16]).

The goal is to provide to the telecommunication network operators optimal trade-offs between the cost of the gateway nodes, connecting the network to the third-party operators, and the network resilience gains. Resorting to robust optimization, we aim to compute the complete Pareto frontier of the bi-objective optimization problem that considers the conflicting objectives of minimizing the investment budget (i.e. gateway node selection cost) and maximizing the network robustness to multiple failures.

1.1.4 Disaster-resilient resource management of elastic optical networks

Currently, optical networks use mechanisms to guarantee full demand protection for single link or single node failures. In a disaster failure scenario, multiple network elements may fail simultaneously and full demand protection is not viable. So, the aim is to provide telecommunication network operators with appropriate extensions to the current resource management strategies to make their networks as resilient as possible to disaster-based failures.

The resource management task involves the RMSA of a set of lightpaths that can groom all service demands. To implement the disaster-resilience feature, we aim to develop RMSA algorithms, on both regular and failure states, that assign the network demands to lightpath such that a disaster-based failure disrupts, on average, a minimum amount of service demands.

We address this task resorting to heuristic algorithms, extensively testing them on publicly available optical network topologies. The results obtained with these algorithms can be used to compare all different disaster resilience algorithmic approaches, to analyze the trade-off between the total network capacity and the robustness gains of each approach, and to understand how this trade-off is influenced by the topology and optical networking characteristics of the networks (e.g. network traffic load).

1.2 Thesis structure

The structure of this thesis is based on a collection of scientific publications, namely four papers (three already published and one recently submitted) in international journals. Each one of the four next chapters (from Chapter 2 to Chapter 5) corresponds to each one of these journal papers. Chapters 2, 3 and 5 present the corresponding published papers correcting a few identified typos. Additionally, in the appendices of this thesis, the four published conference proceedings produced within this research are presented, complementing the content of the journal papers.

All these eight works address the research objectives defined in Section 1.1. In Table 1.1, we present a summary of the research objectives addressed in each chapter (and appendix) of the thesis. In this table, the reference associated with each chapter is also presented.

Table 1.1: Research objectives addressed in each chapter (and appendix) of this thesis.

		Research objectives			
Chapter	Reference	Vulnerability Assessment	Netw. Design (link addition)	Netw. Design (third-parties)	Resource Management
2	[BdSA20]	✗	✗		
3	[BAdS21]	✗	✗		
4	(submitted)	✗		✗	
5	[BdSA$^+$21]				✗
A	[BAdS18]	✗			
B	[BdSA18b]	✗	✗		
C	[BdSA19a]	✗	✗		✗
D	[BdSA$^+$19b]				✗

Notice that, in general, the conference proceedings publications address identical issues to the international journal works. However, as we will show in the following sections, the algorithmic approach is quite different in the majority of the cases.

1.2.1 Network vulnerability assessment

Firstly, we approach the vulnerability assessment in the context of transparent optical networks resorting to a variant of the Critical Node Detection (CND) problem. In such networks, data is converted into light in the source node, routed through an exclusive optical path (i.e. without any electrical regenerators), and converted back to the electric domain at the destination node. Moreover, this routing path must be bounded by the transparent reach, a maximum optical length value which is imposed by the optical degradation suffered by the lightpath both on fiber links and on intermediate optical nodes.

For a given graph representing a transparent optical network, a given weight associated to each node pair and a given positive integer c, the CND problem variant addressed in Appendix A (i.e. [BAdS18]) is the determination of the set of c nodes that, if removed from the graph, minimize the total weight of the node pairs that remain connected. In the context of these networks, a node pair is considered connected only if the surviving network (i.e. network without the critical nodes) provides it with a shortest path within the transparent reach of the network. To solve this variant of the CND problem, we present a path-based Integer Linear Programming model together with an exact row generation algorithm to solve it.

Although heuristics based on node centrality metrics are commonly used to quickly identify a set of critical nodes, in the computational results presented in Appendix A, we illustrate that these heuristics are not able to identify, in general, the optical set of critical nodes. In the results, we also show that real backbone network topologies are not resilient to multiple node failures.

This work was presented on the nineteenth edition of the *Congresso da Associação Portuguesa de Investigação Operacional*, on September 2018, in Aveiro, Portugal.

The exact row generation algorithm proposed to solve the CND problem is further used on Appendix B (i.e. [BdSA18b]) and on Chapter 2 (i.e. [BdSA20]) to evaluate the network robustness of transparent optical network topologies to multiple node failure. In the latter case, we observed that, in most cases, the optimal solution of the classical CND variant (i.e. without the transparent reach restriction imposed by our study case) is also the optimal solution of our CND variant, since disconnecting the network into disjoint components has the higher impact on the objective function. Moreover, the classical CND variant can be modeled with a compact ILP model, which is solved, using a commercial solver, much faster than using our exact row generation algorithm.

Therefore, in Chapter 2, we have considered the compact CND model to quickly find a feasible set of critical nodes. Moreover, in Appendix C and in Chapter 3, we have only considered the compact CND model to evaluate the network robustness to multiple failures because it is time-efficient and due to the fact that optical networks technological evolution in the past years (e.g. elastic optical networking) tends to increase the transparent reach to a point where it is no longer an important feature to be considered in the study.

Finally, we also evaluate the network resilience with the Average 2-Terminal Reliability (A2TR) against a simultaneous failure of a critical node set. The A2TR metric is defined as the number of node pairs that remain connected if all critical nodes fail, i.e., the optimal value of a weightless version of the CND problem.

1.2.2 Network upgrade problem

One of the main problems addressed in this thesis is the network upgrade problem. It aims to identify a set of new fiber links, within a given budget, to be added to an existing network in order to obtain an upgraded topology that maximizes the network robustness against multiple node failures.

Firstly, in Appendix B (i.e. [BdSA18b]), within the context of transparent optical networks, a multi-start greedy randomized algorithm is proposed to generate, with a given fiber length budget, network topologies resilient to critical node failures. After fine-tuning the probabilities of each candidate link being selected in a way that the method efficiently generates good network topologies, the best results are obtained by guaranteeing that at least one end-node of each added link is a node with the lowest node degree and considering probabilities inversely proportional to the square of the link length (i.e. giving a higher probability to shorter links).

Using this multi-start algorithm, we first assess the resiliency gap of existing networks, i.e. the relative difference between the resilience of an existing network topology and of a new network topology design to maximize its resilience with the same fiber budget. Then, we assess how much this resiliency gap can be reduced by upgrading an existing network topology through link addition. Testing the proposed methodology on network topologies with publicly available information, the computational results show that the resiliency gap of existing topologies is significantly large; however, network upgrades with only 10% additional fiber length (that aim to maximize the network resilience against multiple node failures) can significantly reduce the resiliency gaps.

This work was presented on the tenth edition of the *International Workshop on Resilient Network Design and Modeling*, in August 2018, in Longyearbyen, Norway. Moreover, this work has been awarded the *Best Paper Award* of the conference.

In Chapter 2 (i.e. [BdSA20]), the network upgrade problem is addressed with an alternative method based on a greedy deterministic algorithm where the computational results show that the new deterministic methodology obtains better solutions when compared with the previous method (proposed in [BdSA18b]). The proposed algorithm selects iteratively a new link among the candidate links whose end-nodes belong to two distinct components of the surviving network topology (i.e. graph resulting by removing the optimal critical nodes from the given topology). Each link is selected in a deterministic manner selecting either the shortest candidate link or the candidate link with the minimum value of its length times the sum of its end-nodes degrees. This selection stops when there is no longer a candidate link with its length within the available budget.

Besides the publication in an international scientific journal, the content of Chapter 2 was also presented, as an extended abstract, on the ninth edition of the *International Network Optimization Conference*, in June 2019, in Avignon, France.

In both these works, we approach the problem of upgrading an existing network using heuristic methodologies (stochastic in [BdSA18b] and deterministic in [BdSA20]). Contrarily, in Chapter 3 (i.e. [BAdS21]), we aim to optimally enhance the robustness of networks against multiple node failures. Here, instead of considering a given budget to upgrade a given network, we develop methods to compute the Pareto frontier where the cost of upgrading the network is one of the objectives. The other objective is the maximization of the network robustness metric. Although this approach does not directly solve the problem for a given budget, we can obtain from the Pareto frontier the optimal solution for any budget value.

In Chapter 3, the problem in modeled as a bi-objective formulation, minimizing the cost of the added edges and maximizing the robustness of the resulting upgraded network against multiple node failures. A general iterative framework is first presented to obtain the complete Pareto frontier. Then, two different algorithms are proposed based on a cover model for the edge selection problem that, when compared with a classic path formulation, proved to be much more efficient. The computational results conducted show that the proposed methodology based on the cover model is effective in computing Pareto solutions for graphs with up to 100 nodes, including four telecommunication networks topologies.

1.2.3 Third-party networks approach

In telecommunication networks, full connectivity resilience against multiple failures is too expensive. As the Pareto frontier results presented in Chapter 3 illustrate, full connectivity resilience requires a network topology with too many redundant links. Alternatively, the connectivity resilience of a given telecommunications network can be improved by resorting to available third-party networks for temporary additional connectivity until the failing elements are restored. In such an approach, some network nodes must be selected to act as gateway nodes to available third-party telecommunication networks when a multiple failure event occurs.

In Chapter 4, for a given network topology and considering a cost associated to each node (i.e. cost of turning it into a gateway node), our goal with this approach is to select the optimal set of gateway nodes, providing simultaneously maximum connectivity resilience and minimum total cost. Since these are conflicting objectives, this Gateway Node Selection (GNS) problem is defined as a bi-objective optimization problem such that its Pareto-optimal solutions represent all optimal trade-offs between the cost of selecting the gateway nodes and connectivity resilience improvement.

Here, since we resort to the network nodes to improve its resilience to failures, the connectivity resilience of a given GNS solution is evaluated by a standard variant of the Critical Link Detection (CLD) optimization problem. An exact optimization algorithm is proposed, based on a row generation algorithm and on set cover cuts, similar to the one presented in Chapter 3. The computational results demonstrate the effectiveness of the proposed algorithm on four well-known telecommunication network topologies. Moreover, the computational results show that the highest resilience gains are obtained with the lowest cost values, which indicates that smaller investments allow to obtain the highest connectivity resilience gains.

1.2.4 Resource management of elastic optical networks

The last issue addressed in this thesis is the resource management of EONs, namely defining a RMSA policy to be adopted by the telecommunication operator such that the impact of multiple failures is minimized.

First, in Appendix C (i.e. [BdSA19a]), this topic is addressed where an estimated set of demands to be supported by a given EON is considered and a RMSA policy is defined to be adopted by the operator on both the regular state and any failure state.

Here, a worst-case scenario approach is adopted to evaluate the network resilience against multiple node failures by identifying the set of nodes whose simultaneous failure maximally reduce the demand percentage that is supported by the network. This problem is solved heuristically by computing two sets of failure nodes. The first set is obtained by solving a weighted version of the CND problem, where the weight associated to each node pair is given by the total demand between those two nodes. The second set is computed resorting to the introduced Node Demand Centrality (NDC) metric, which measures the impact of each node failure on the demands between all other node pairs.

Then, for the same estimated demands, the same RMSA policy, and a fiber budget equal to the total fiber length of the existing network, we also address the design problem aiming to determine a new EON topology maximizing the resilience metric (i.e. demand percentage supported in the failure state imposed by its critical nodes). This optimization problem is heuristically solved by resorting to the multi-start algorithm presented in Appendix B.

The computational results show that new network topology solutions are much more resilient than real EON topologies against multiple node failures. The improvements provided by these alternative topologies (with an identical total fiber length of the original topologies) are obtained with topologies with more homogeneous node degrees, which are very different from the node degrees distribution of the real network topologies.

This work was presented on the fifteenth edition of the *International Conference on the Design of Reliable Communication Network*, in March 2019, in Coimbra, Portugal.

Next, in Appendix D (i.e. [BdSA$^+$19b]), a RMSA policy resilient to multiple node failures is proposed. This RMSA algorithm considers a new metric on the decision of each demand routing path, named path disaster availability metric, which measures the probability of each path of the network not being affected by a multiple node failure. In this work, a static set of demands is considered for each well-known tested topology. Each demand can represent either a unicast service (i.e. connection peer-to-peer) or anycast service (i.e. connection between a client and a data center).

In Appendix D, we consider a different node attack model, where an attacker “discovers” (with some probability) a set of nodes and plans to attack them simultaneously. We assume that the number of attacked nodes has lower and upper bounds and that the probability of s nodes being attacked is inversely proportional to the number of attacked nodes. Then, by generating multiple random attacks based on those probabilities, the resiliency of each RMSA algorithm to multiple node attacks is evaluated by two parameters: the average non-disrupted demand (i.e. demand that is not disrupted after a failure) and the average surviving demand (i.e. demand that is still supported after a failure).

The computational results show that the RMSA decision is always better when the disaster path availability metric is used. Moreover, the best way to use the path disaster availability metric in the RMSA decision depends on the traffic load of the EON. For lightly loaded networks, the best RMSA policy is the one that gives higher priority to the proposed metric in the assignment, while for heavily loaded networks, the best RMSA policy is the one that gives higher priority to spectrum usage efficiency. For medium loaded networks, a mix criterion proved to be the most efficient in the RMSA assignment.

This work was presented on the eleventh edition of the *International Workshop on Resilient Network Design and Modeling*, in October 2019, in Nicosia, Cyprus.

Finally, in Chapter 5 (i.e. [BdSA$^+$21]), we address the resource management of a dynamic EON, where demand requests arrive randomly one at a time and the accepted demands last in the network for a random time duration. Then, an additional goal of the RMSA policy is to efficiently use the spectrum resources available in order to maximize the acceptance probability of future demand requests. To obtain RMSA algorithms resilient to multiple node failure events, we resource to the path disaster availability metric, previously used in the offline variant of the RMSA problem (where all demands are assumed to be known at the beginning).

Here, we exploit the use of this metric in the RMSA of dynamic EONs by combining it with spectrum usage metrics in a dynamic way based on the network load level. The aim is that the efficient use of the resources is relaxed for improved resilience to multiple node failures when the EON is lightly loaded, while it becomes the most important goal when the EON becomes heavily loaded.

Considering the attack model proposed in [BdSA$^+$19b] and a mix of unicast and anycast services for each simulation, the computational results show that the RMSA algorithms combining the path disaster availability metric with spectrum usage metrics are the best trade-off between spectrum usage efficiency and resilience to multiple node failures.

1.3 Research contributions

This section describes the main contributions provided by this research. These contributions are divided into two interrelated categories: scientific novelty, where one summarizes the models and methods developed within this research; and telecommunication network operators applicability, where one explains the techniques that telecommunication operators can exploit in their real-world optical networks operation.

1.3.1 Scientific novelty

Here, we highlight the original contributions of this research to the scientific community, namely models, optimal methods and heuristic algorithms proposed.

- We present an ILP model, combined with an exact row generation algorithm, to optimal solve the variant of the CND problem that minimizes the weighted pairwise connectivity, in the context of transparent optical networks.
- We propose a greedy randomized generation algorithm that, for a given maximum length budget, generates network topologies with high connectivity.
- Alternatively, we propose a greedy deterministic algorithm, that also generates topologies with high connectivity. We combine this algorithm with a local search algorithm that aims to improve the generated topology.
- We model the robust network upgrade problem (RNUP) as a bi-objective optimization problem and propose an upgrade algorithm that computes its complete Pareto frontier. We also prove that this approach optimally solves the RNUP (i.e., it finds all Pareto-optimal solutions).
- We propose two efficient algorithms (based on row generation and components separation, respectively) to solve the RNUP problem, resorting to a cover formulation of the edge selection subproblem.
- We present and model the Gateway Node Selection (GNS) problem as a bi-objective optimization problem, proposing a general GNS algorithm that computes its complete Pareto frontier.
- We propose an efficient row generation algorithm, based on a set cover model, that computes all Pareto-optimal solutions of the GNS problem.
- We introduce the Node Demand Centrality (NDC) metric that, for each node of an EON topology, measures the impact of the node failure on the demands between all other node pairs.
- We introduce the path disaster availability metric that, for each routing path, measures the probability of that path being available in the surviving network (i.e. reduced graph without the failure nodes and its links). Additionally, we present a recursive algorithm to compute this metric.
- We present multiple RMSA algorithms, with both static or dynamic traffic, aiming to increase the disaster resilience of EONs against multiple node failures.
- Finally, all methods developed within this research are implemented in suitable software and extensively tested resorting to publicly available optical network topologies from [KNF$^+$11, OWPT10, Sim14], showing the full applicability of the proposed methodologies.

1.3.2 Telecommunication network operators applicability

Recall that the main objective of this thesis is to develop tools that allow telecommunication network operators to use their EONs in a cost-effective manner so that the impact of disaster-based failures is minimized.

Firstly, we provide the operators with a method to assess the vulnerability of transparent optical networks to multiple node failures. It consists of an exact algorithm for a variant of the CND problem that takes into account the transparent reach restrictions imposed by these optical networks.

Then, we present appropriate techniques to enhance the disaster-resilience of telecommunications networks. We approach this enhancement on two alternative ways: on the design of all working links, through link addition; and on the design with backup links, resorting to gateway nodes connecting the network to other third-party networks.

For a given available investment budget, we propose algorithms, both stochastic and deterministic, to upgrade transparent optical networks, enhancing their resilience to disaster-based failures. Moreover, we propose methodologies that enable the telecommunication operator to analyze the trade-off between the investment cost of upgrading the network and the gains in terms of robustness against multiple node failures.

Finally, we provide operators with appropriate resource management strategies to make their networks more resilient to disaster-based failures. Namely, we present RMSA algorithms (firstly considering static traffic and then adapting those for dynamic traffic), based on realistic EON features (unicast and anycast demands, modulation formats, transmission reach, grouping multiple optical channels into a single spectral super-channel, etc.), that proved to be much more disaster-resilient than commonly used RMSA strategies.

1.4 Author's contributions

All the works presented in this collection of scientific papers resulted from the research of the thesis author with both supervisors. We work together on the conceptualization of each proposed problem, the methodology used to approach each one, the selection of suitable software to implement it, the formal and computational results analysis, the writing, reviewing, and editing of each paper.

Exceptionally, the conference proceeding [BdSA$^+$19b] and the international journal paper [BdSA$^+$21] had the contribution of two external members to this research: Dr. Krzysztof Walkowiak and Dr. Róża Goścień, from the Wrocław University of Science and Technology, in Poland. The external members introduced testing parameters that represent more realistic instances to test our disaster-resilient RMSA algorithms. Namely, the introduction of rules to calculate, for a given network demand, the most efficient MF and the number of required contiguous FS of the lightpath. Moreover, they also proposed the distinction between unicast and anycast traffic (i.e. traffic between clients and traffic between a client and a data center, respectively).

On all works produced within the context of this thesis, including the ones that resulted from an international scientific collaboration, the thesis author had exclusive responsibility in the implementation of all methods on adequate software and elaboration of suitable illustrations (tables and figures) that summarize the computational results obtained. Moreover, specifically in the work presented in Chapter 5, the thesis author also introduced the three mixed RMSA variants (to the regular state), from which one proved to be the best overall RMSA algorithm.

1.5 Final considerations and future research

As humans increasingly rely on telecommunication networks in their everyday life, operators need to have reliable networks. In this research, we provide the operators with tools to increase the resilience of EONs against disaster-based failures. These tools are divided into two different categories: network design and resource management.

This research has made contributions both in terms of scientific novelty and applicability to real-world telecommunication networks. We resort to different kinds of techniques, both optimal and heuristic, to achieve the main objectives of this thesis.

The main focus of this research was on disaster-based failures caused by malicious human attacks and, since that in the attacker's perspective, node shutdowns are the most rewarding than link cuts, the network resilience was mainly measured in terms of multiple node failures. Nevertheless, in the network design approach that considers temporary connectivity provided by third-party networks, since one resorted to gateway nodes to increase the disaster resilience, the latter was measured in terms of multiple link failures. One research direction is to adapt the proposed algorithms considering now multiple node failures. Additionally, since link cuts are easier to realize than node shutdowns, another research direction is to adapt the network design and resource management of EONs methodology to disasters based on multiple link failures, or even a combination of failure elements (i.e. both nodes and links).

Regarding additional research directions, in general, spatial flexibility in optical networks, also named space division multiplexing (SDM), is a novel approach that uses a space domain, provided by cores in multi-core fibers, in which the spatial resources are flexibly assigned to lightpaths. The fiber space dimension increases the overall transmission capacity in a cost-effective manner [SAZS15] but the additional flexibility increases the networking complexity requiring new optimization methods [KCG$^+$15]. However, there are few papers concerning EON optimization with spatial flexibility. Some examples either propose simple heuristics for the Routing, Spectrum and Core Assignment (RSCA) problem [SPK$^+$15, TH14] or ILP formulations for basic versions of it [LHZ15, MZSF14].

A future research direction is to consider this spatial flexibility in the resource management of EONs, by introducing in our disaster-resilient RMSA algorithms the core assignment component. It would result in the RMCSA (routing, modulation, core and spectrum assignment) problem, which is quickly becoming arguably the most important problem of EONs.

Another research direction can also be to consider a path geo-diversification approach, similarly to [dSSM17]: for each working lightpath, a backup lightpath will be considered such that the geographical distance between the two lightpaths has to be higher than a given minimum distance. Then, the idea is to consider a robust approach where the set of most disruptive disaster scenarios is firstly computed and, then, the pairs of working and backup lightpaths must be as much disjoint as possible over all critical elements of each disaster scenario. In this way, the solutions would enhance the reliability also multiple failures causes by natural disasters.

As a final remark, at the initial stage of this research, there were plans to develop methods addressing the case of translucent optical networks (i.e. optical networks whose geographical dimension require the use of intermediate electrical regeneration). This aim is more challenging as it increases the complexity of the studied problems when compared to transparent optical networks since it includes the regenerator location problem (e.g. the number of additional regenerators and the network nodes to install them). However, with the technological evolution of optical networks, the transmission reach is increasing to a point where, in many real-world EONs, all client demands can be served exclusively on the optical level (avoiding the high costs of intermediate regenerators), and therefore, it is no longer essential for EON operators to use electrical regenerators.

Bibliography

[ACEP09] A. Arulselvan, C. Commander, L. Elefteriadou, and P. Pardalos. *Detecting critical nodes in sparse graphs.* Computers & Operations Research, 36(7):2193–2200, 2009.

[ACF$^+$13] A. Agra, M. Christiansen, R. Figueiredo, L. Hvattum, M. Poss, and C. Requejo. *The robust vehicle routing problem with time windows.* Computers & Operations Research, 40(3):856–866, 2013.

[AdSD16] A. Agra, A. de Sousa, and M. Doostmohammadi. *The minimum cost design of transparent optical networks combining grooming, routing, and wavelength assignment.* IEEE/ACM Transactions on Networking, 24(6):3702–3713, 2016.

[AEG$^+$13] P. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman. *The resilience of WDM networks to probabilistic geographical failures.* IEEE/ACM Transactions on Networking, 21(5):1525–1538, 2013.

[AR17] F. Abkenar and A. Rahbar. *Study and analysis of routing and spectrum allocation (RSA) and routing, modulation and spectrum allocation (RMSA) algorithms in elastic optical networks (EONs).* Optical Switching and Networking, 23:5–39, 2017.

[ASNP16] A. Agra, M. Santos, D. Nace, and M. Poss. *A dynamic programming approach for a class of robust optimization problems.* SIAM Journal on Optimization, 26(3):1799–1823, 2016.

[BAdS18] F. Barbosa, A. Agra, and A. de Sousa. *Critical node detection with connectivity based on bounded path lengths.* In XIX Congresso da Associação Portuguesa de Investigação Operacional, Aveiro, Portugal, 2018.

[BAdS21] F. Barbosa, A. Agra, and A. de Sousa. *The minimum cost network upgrade problem with maximum robustness to multiple node failures.* Computers & Operations Research, 136:105453, 2021.

[BdSA18a] F. Barbosa, A. de Sousa, and A. Agra. *The design of transparent optical networks minimizing the impact of critical nodes.* Electronic Notes in Discrete Mathematics, 64:165–174, 2018.

[BdSA18b] F. Barbosa, A. de Sousa, and A. Agra. *Topology design of transparent optical networks resilient to multiple node failures.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

[BdSA19a] F. Barbosa, A. de Sousa, and A. Agra. *Evaluation and design of elastic optical networks resilient to multiple node failures.* In 15th International Conference on the Design of Reliable Communication Networks (DRCN), pages 154–161, 2019.

[BdSA$^+$19b] F. Barbosa, A. de Sousa, A. Agra, K. Walkowiak, and R. Goścień. *A RMSA algorithm resilient to multiple node failures on elastic optical networks.* In 11th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2019.

[BdSA20] F. Barbosa, A. de Sousa, and A. Agra. *Design/upgrade of a transparent optical network topology resilient to the simultaneous failure of its critical nodes.* Networks, 75(4):356–373, 2020.

[BdSA$^+$21] F. Barbosa, A. de Sousa, A. Agra, K. Walkowiak, and R. Goścień. *RMSA algorithms resilient to multiple node failures in dynamic EONs.* Optical Switching and Networking, 42:100633, 2021.

[CGL$^+$15] Y. Cheng, M. Gardner, J. Li, R. May, D. Medhi, and J. Sterbenz. *Analysing geopath diversity and improving routing performance in optical networks.* Computer Networks, 82:50–67, 2015.

[CSO15] B. Chatterjee, N. Sarma, and E. Oki. *Routing and spectrum allocation in elastic optical networks: a tutorial.* IEEE Communications Surveys Tutorials, 17(3):1776–1800, 2015.

[CTV11] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos. *Elastic bandwidth allocation in flexible OFDM-based optical networks.* Journal of Lightwave Technology, 29(9):1354–1366, 2011.

[DGS$^+$15] M. Dallaglio, A. Giorgetti, N. Sambo, L. Velasco, and P. Castoldi. *Routing, spectrum, and transponder assignment in elastic optical networks.* Journal of Lightwave Technology, 33(22):4648–4658, 2015.

[dSMS17] A. de Sousa, D. Mehta, and D. Santos. *The robust node selection problem aiming to minimize the connectivity impact of any set of p node failures.* In 13th International Conference on Design of Reliable Communication Networks (DRCN), pages 138–145, 2017.

[dSS20] A. de Sousa and D. Santos. *Vulnerability evaluation of networks to multiple failures based on critical nodes and links.* In J. Rak and D. Hutchison, editors, Guide to Disaster-Resilient Communication Networks, pages 63–86. Springer International Publishing, Cham, 2020.

[dSSM17] A. de Sousa, D. Santos, and P. Monteiro. *Determination of the minimum cost pair of D-geodiverse paths.* In 13th International Conference on Design of Reliable Communication Networks (DRCN), pages 101–108, 2017.

[dSTP16] A. de Sousa, A. Tomaszewski, and M. Pioro. *Bin-packing based optimisation of EON networks with S-BVTs.* In International Conference on Optical Network Design and Modeling (ONDM). IEEE, 2016.

[DXT$^+$10] T. Dinh, Y. Xuan, M. Thai, E. Park, and T. Znati. *On aproximation of new optimization methods for assessing network vulnerability.* In Proceedings IEEE INFOCOM, pages 1–9, 2010.

[FWG$^+$16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GBHC15] S. Gilbert, D. Butry, J. Helgeson, and R. Chapman. *Community resilience economic decision guide for buildings and infrastructure systems.* National Institute of Standards and Technology (NIST) Special Publication 1197, 2015.

[GJLY12] O. Gerstel, M. Jinno, A. Lord, and S. Yoo. *Elastic optical networking: a new dawn for the optical layer?* IEEE Communications Magazine, 50(2):12–20, 2012.

[GTE$^+$16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[GWK15] R. Goścień, K. Walkowiak, and M. Klinkowski. *Tabu search algorithm for routing, modulation and spectrum allocation in elastic optical network with anycast and unicast traffic.* Computer Networks, 79:148–165, 2015.

[GZLZ12] L. Gong, X. Zhou, W. Lu, and Z. Zhu. *A two-population based evolutionary approach for optimizing routing, modulation and spectrum assignments (RMSA) in O-OFDM networks.* IEEE Communications Letters, 16(9):1520–1523, 2012.

[JKT$^+$10] M. Jinno, B. Kozicki, H. Takara, A. Watanabe, Y. Sone, T. Tanaka, and A. Hirano. *Distance-adaptive spectrum resource allocation in spectrum-sliced elastic optical path network* [topics in optical communications]. IEEE Communications Magazine, 48(8):138–145, 2010.

[KCG$^+$15] D. Klonidis, F. Cugini, O. Gerstel, M. Jinno, V. Lopez, E. Palkopoulou, M. Sekiya, D. Siracusa, G. Thouenon, and C. Betoule. *Spectrally and spatially flexible optical network planning and operations.* IEEE Communications Magazine, 53(2):69–78, 2015.

[KNF$^+$11] S. Knight, H. Nguyen, N. Falkner, R. Bowden, and M. Roughan. *The internet topology zoo.* IEEE Journal on Selected Areas in Communications, 29(9):1765–1775, 2011.

[KO14] Y. Kobayashi and K. Otsuki. *Max-flow min-cut theorem and faster algorithms in a circular disk failure model.* In IEEE Conference on Computer Communications (INFOCOM), pages 1635–1643. IEEE, 2014.

[KRS$^+$16] P. Khodashenas, J. Rivas-Moscoso, D. Siracusa, F. Pederzolli, B. Shariati, D. Klonidis, E. Salvadori, and I. Tomkos. *Comparison of spectral and spatial super-channel allocation shemes for SDM networks.* Journal of Lightwave Technology, 34(11):2710–2716, 2016.

[KW11] M. Klinkowski and K. Walkowiak. *Routing and Spectrum Assignment in Spectrum Sliced Elastic Optical Path Network.* IEEE Communications Letters, 15(8):884–886, 2011.

[LHZ15] Y. Li, N. Hua, and X. Zheng. *Routing, wavelength and core allocation planning for multi-core fiber networks with MIMO-based crosstalk suppression.* In Opto-Electronics and Communications Conference (OECC), 2015.

[LTK16] M. Lalou, M. Tahraoui, and H. Kheddouci. *Component-cardinality-constrained critical node problem in graphs.* Discrete Applied Mathematics, 210:150–163, 2016.

[LTK18] M. Lalou, M. Tahraoui, and H. Kheddouci. *The critical node detection problem in networks: a survey.* Computer Science Review, 28:92 – 117, 2018.

[MHD14] B. Mukherjee, M. Habib, and F. Dikbiyik. *Network adaptability from disaster disruptions and cascading failures.* IEEE Communications Magazine, 52(5):230–238, 2014.

[MZSF14] A. Muhammad, G. Zervas, D. Simeonidou, and R. Forchheimer. *Routing, spectrum and core allocation in flexgrid SDM networks with multi-core fibers.* In International Conference on Optical Network Design and Modeling (ONDM), pages 19–22, 2014.

[NEM15] S. Neumayer, A. Efrat, and E. Modiano. *Geographic max-flow and min-cut under a circular disk failure model.* Computer Networks, 77:117–127, 2015.

[NZCM11] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano. *Assessing the vulnerability of the fiber infrastructure to disasters.* IEEE/ACM Transactions on Networking, 19(6):1610–1623, 2011.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[PAK$^+$12] E. Palkopoulou, M. Angelou, D. Klonidis, K. Christodoulopoulos, A. Klekamp, F. Buchali, E. Varvarigos, and I. Tomkos. *Quantifying spectrum, cost, and energy efficiency in fixed-grid and flex-grid networks* [invited]. IEEE/OSA Journal of Optical Communications and Networking, 4(11):B42–B51, 2012.

[RBMT17] C. Rottondi, P. Boffi, P. Martelli, and M. Tornatore. *Routing, modulation format, baud rate and spectrum allocation in optical metro rings with flexible grid and few-mode transmission.* Journal of Lightwave Technology, 35(1):61–70, 2017.

[RCM17] D. Rueda, E. Calle, and J. Marzo. *Robustness comparison of 15 real telecommunication networks: structural and centrality measurements.* Journal of Network and Systems Management, 25(2):269–289, 2017.

[RH20] J. Rak and D. Hutchison. *Guide to disaster-resilient communication networks.* Computer Communications and Networks, Springer International Publishing, Cham, 2020.

[RHC+16] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska. *RECODIS: Resilient communication services protecting end-user applications from disaster-based failures.* In 18th International Conference on Transparent Optical Networks (ICTON). IEEE, 2016.

[RJS14] J. Rohrer, A. Jabbar, and J. Sterbenz. *Path diversification for future internet end-to-end resilience and survivability.* Telecommunication Systems, 56(1):49–67, 2014.

[SAZS15] G. Saridis, D. Alexandropoulos, G. Zervas, and D. Simeonidou. *Survey and evaluation of space division multiplexing: from technologies to optical networks.* IEEE Communications Surveys & Tutorials, 17(4):2136–2156, 2015.

[SdSM18] D. Santos, A. de Sousa, and P. Monteiro. *Compact models for critical node detection in telecommunication networks.* Electronic Notes in Discrete Mathematics, 64:325–334, 2018.

[SGL12] M. Di Summa, A. Grosso, and M. Locatelli. *Branch and cut algorithms for detecting critical nodes in undirected graphs.* Computational Optimization and Applications, 53(3):649–680, 2012.

[Sim14] J. Simmons. *Optical network design and planning*. Springer, Switzerland, 2nd edition, 2014.

[SPK+15] D. Siracusa, F. Pederzolli, D. Klonidisz, V. Lopezy, and E. Salvadori. *Resource allocation policies in SDM optical networks* (invited paper). In International Conference on Optical Network Design and Modeling (ONDM), pages 168–173. IEEE, 2015.

[SVCM12] J. Segovia, P. Vilà, E. Calle, and J. Marzo. *Improving the resilience of transport networks to large-scale failures.* Journal of Networks, 7(1):63–72, 2012.

[TH14] H. Tode and Y. Hirota. *Routing, spectrum and core assignment for space division multiplexing elastic optical networks.* In 6th International Telecommunications Network Strategy and Planning Symposium (Networks). IEEE, 2014.

[TKI+15] S. Trajanovski, F. Kuipers, A. Ilic, J. Crowcroft, and P. Van Mieghem. *Finding critical regions and region-disjoint paths in a network.* IEEE/ACM Transactions on Networking, 23(3):908–921, 2015.

[TR17] S. Talebi and G. Rouskas. *On distance-adaptive routing and spectrum assignment in mesh elastic optical networks.* IEEE/OSA Journal of Optical Communications and Networking, 9(5):456–465, 2017.

[Ven12] M. Ventresca. *Global search algorithms using a combinatorial unranking-based problem representation for the critical node detection problem.* Computers & Operations Research, 39(11):2763–2775, 2012.

[WK13] K. Walkowiak and M. Klinkowski. *Joint anycast and unicast routing for elastic optical networks: Modeling and optimization.* In IEEE International Conference on Communications (ICC), pages 3909–3914, 2013.

[ZMH17] J. Zhang, E. Modiano, and D. Hay. *Enhancing network robustness via shielding.* IEEE/ACM Transactions on Networking, 25(4):2209–2222, 2017.

[ZZY+15] J. Zhang, Y. Zhao, X. Yu, J. Zhang, M. Song, Y. Ji, and B. Mukherjee. *Energy-efficient traffic grooming in sliceable-transponder-equipped IP-over-elastic optical networks* [invited]. IEEE/OSA Journal of Optical Communications and Networking, 7(1):142–152, 2015.

Chapter 2

Design/Upgrade of a Transparent Optical Network Topology Resilient to the Simultaneous Failure of its Critical Nodes

Abstract: This paper addresses two related problems in the context of transparent optical networks. In the network design problem, the aim is to identify a set of fiber links to connect a given set of nodes. In the network upgrade problem, the aim is to identify a set of new fiber links to add to a given network topology. For a given fiber length budget, the aim in both problems is to maximize the network resilience to the simultaneous failure of its critical nodes. The resilience is evaluated by the Average 2-Terminal Reliability (A2TR) against a set of critical node failures and the critical nodes are the ones that minimize the A2TR of the network. So, the design/upgrade problem is a bi-level max-min optimization problem. Recently, a multi-start greedy randomized heuristic was proposed for both problems. Here, we propose an alternative method based on a greedy deterministic algorithm and we provide computational results showing that the new method obtains better solutions. The results show that the resiliency difference between existing network topologies and the best network design solutions is very high but this difference can be significantly reduced by network upgrades with small fiber length budgets.

Keywords: Transparent Optical Networks, Critical Node Detection, Resilient Network Design, Disasters, Optimization, Heuristics

F. Barbosa, A. de Sousa, and A. Agra. *Design/upgrade of a transparent optical network topology resilient to the simultaneous failure of its critical nodes.* Networks, 75(4):356–373, 2020.

2.1 Introduction

Large-scale failures can seriously disrupt a telecommunications network due to either natural, technological or malicious human activities [RHC$^+$16]. Two recent surveys conducted within COST Action RECODIS are [GTE$^+$16] on strategies to protect networks against large-scale natural disasters and [FWG$^+$16] on security challenges in communication networks. When dealing with large-scale failures, it is important not only to recover from failures as quick as possible (the post-disaster problem), but also to prepare the network to minimize the impact of such failures (the pre-disaster problem).

This work deals with the pre-disaster problem by addressing the design (and upgrade) of telecommunication networks aiming to enhance their resilience to large-scale failures. To reach this goal, we first adopt a proper network resiliency metric and, then, we propose design methods aiming to optimize the network resiliency metric. We address the design of resilient network topologies in the context of transparent optical networks. Note that, in general, multiple failures might involve only links or nodes and links (a node failure implies that its links also fail). For example, in malicious human attacks, node shutdowns are harder to realize but they are the most rewarding in the attackers' perspective since the shutdown of a single node also shuts down its incoming/outgoing fiber links. Moreover, power outages can only shut down nodes since fiber links do not require power supply. Here, we consider as large-scale failures the case of multiple node failures as they are the most harmful cases.

For a given network topology, if some nodes are considered critical due to some reason, the network design should take it into consideration, as in [BdSA18a] where the approach proposed in [AdSD16] is adapted to the design of a transparent optical network minimizing the failure impact of a given set of critical nodes. Here, we consider that the resilience of a network topology is evaluated by the Average 2-Terminal Reliability (A2TR) against a set of critical node failures. The A2TR metric is defined as the number of node pairs that remain connected if all critical nodes fail. The critical nodes of a network are the nodes that minimize the A2TR of the network, an optimization problem commonly named Critical Node Detection (CND) problem. So, the design problem is a bi-level max-min optimization problem.

CND problems have been considered in different contexts and are gaining special attention in the vulnerability evaluation of telecommunication networks to large-scale failures [GTE$^+$16]. In [ACEP09], the CND problem is defined as the detection of a given number c of critical nodes aiming to minimize the number of connected node pairs. Recently, this and other variants of CND have been addressed [SdSM18, SGL12, VBP14, VPP15], but none of these works addresses the CND problem in the context of transparent optical networks. Other metrics have been used to evaluate the vulnerability of networks in other contexts [RCM17] or assuming multiple geographically correlated failures [NZCM11]. There are also works on improving the preparedness of networks to multiple failures, some by changing the network topology [BGLR05, NYWF17, ZL12], while others by proposing strategies to recover from failures [DTM14, STD15]. None of these works, though, uses the optimal solution of the CND problem to assess the vulnerability of networks. On the other hand, CND was used in [dSMS17] but resiliency improvement is exploited by optimal robust node selection on a given network topology. The advantage of using CND is that it provides a worst case resiliency analysis, i.e., in any failure involving the same number of failing nodes, the resulting A2TR is never worse than the value provided by the CND optimal solution.

In transparent optical networks, data is converted into light in the source node and transmitted through an all optical path, named *lightpath*, towards the destination node. Due to many optical degradation factors, like attenuation, dispersion, crosstalk and other non-linear factors, there is a maximum length, named *transparent reach*, for each lightpath to work properly. If a lightpath is required on a path whose length is higher than the transparent reach, regenerators must be placed at intermediate nodes to convert the optical signal into the electrical domain, regenerate the signal and reconvert it back to the optical domain (when regenerators are used, the network is referred to as a translucent network). Nevertheless, the use of regenerators is expensive and puts an additional burden on the network management and, so, they are avoided when possible. The design of translucent networks must take into account the cost imposed by the required regenerators, which is out of the scope of this work. The methods proposed in this work are applicable to transparent optical networks, i.e., optical networks whose diameter (the highest optical length among the shortest paths of all node pairs) is not higher than the transparent reach. Note that the optical length of a path depends both on the length of its links and on its number of hops, i.e., number of intermediate nodes). We model the optical degradation suffered by a lightpath while traversing an intermediate node as a fiber length value Δ, i.e., by considering it equivalent to the degradation incurred due to the transmission over a fiber of length Δ. So, when accounting for the A2TR metric, the CND problem has to consider that two nodes are connected only if the surviving network provides them with at least one path whose optical length is within the required transparent reach.

In [BdSA18b], a multi-start greedy randomized method was proposed to generate network topologies, with a given fiber length budget, that are resilient to critical node failures. The method is also adapted in [BdSA18b] to the upgrade of an existing network topology. Here, we propose an alternative method for the same network design/upgrade problem based on a greedy deterministic algorithm and provide computational results showing that the new method obtains better solutions than the one proposed in [BdSA18b]. With the updated results, we review the conclusions taken in [BdSA18b] concerning the resiliency values obtained between the network design and the network upgrade solutions. The computational results will show that the resiliency difference between existing topologies and the best network design solutions is very high but this difference can be significantly reduced by network upgrades with small fiber length budgets.

The paper is organized as follows. Section 2.2 describes a path-based Mixed Integer Linear Programming (MILP) model defining the CND problem in the context of transparent optical networks and a row generation algorithm that is used to solve the problem. Section 2.3 proposes deterministic algorithms to generate network topologies resilient to the simultaneous failure of their critical nodes. The computational results are presented and discussed in Section 2.4. Finally, Section 2.5 presents the main conclusions of the work.

2.2 Critical node detection problem

Consider a transparent optical network represented by an undirected graph $G = (N, E)$ where $N = \{1, ..., n\}$ is the set of nodes and $E \subseteq \{(i, j) \in N \times N : \ i < j\}$ is the set of fiber links. For each link $(i, j) \in E$, parameter l_{ij} represents its length. The transparent reach of the network is denoted by parameter $T > 0$ and the fiber length equivalent to the degradation suffered by a lightpath while traversing an intermediate node is denoted by parameter $\Delta > 0$.

We assume that $l_{ij} \leq T$ for all $(i,j) \in E$; otherwise, such link is worthless and can be removed from G.

The set of all paths in G between $i \in N$ and $j \in N$ (with $i < j$ and $(i,j) \notin E$) with length not greater than T is denoted by P_{ij}. Each path $p \in P_{ij}$ is defined by the binary parameters β_k^p, indicating whether node $k \in N$ (which can be an end node) is in p or not, and α_{kt}^p indicating whether link $(k,t) \in E$ is in p or not. So, P_{ij} is composed by all paths p such that $\sum_{(k,t)\in E} \alpha_{kt}^p l_{kt} + \Delta\big(\sum_{k\in N} \beta_k^p - 2\big) \leq T$.

To model the CND problem, we consider for each node $i \in N$ a binary variable v_i indicating whether i is a critical node or not. We consider also for each node pair (i,j), with $i,j \in N :$ $i < j$, a binary variable u_{ij} which is 1 if nodes i and j can be connected through a path satisfying the transparent reach T, and 0 otherwise. Then, for a given number c of critical nodes, a path-based formulation for the CND problem is given by the following Integer Linear Programming (ILP) model:

$$\min \quad z := \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} u_{ij} \tag{2.1}$$

$$\text{s.t.} \quad \sum_{i=1}^{n} v_i \leq c, \tag{2.2}$$

$$u_{ij} + v_i + v_j \geq 1, \quad (i,j) \in E, \tag{2.3}$$

$$u_{ij} + \sum_{k=1}^{n} \beta_k^p v_k \geq 1, \quad (i,j) \notin E,\ p \in P_{ij}, \tag{2.4}$$

$$v_i \in \{0,1\}, \quad i \in N, \tag{2.5}$$

$$u_{ij} \in \{0,1\}, \quad i,j \in N:\ i < j. \tag{2.6}$$

The objective function (2.1) value z is the A2TR value defined as the total number of connected node pairs in the surviving graph (i.e., the graph given by removing all critical nodes from G). Constraint (2.2) ensures that at most c nodes are selected as critical nodes (in any optimal solution, c critical nodes are selected). Constraints (2.3) guarantee that a pair of adjacent nodes (i.e., with a direct link between them) is connected if none of the two nodes is a critical node. Constraints (2.4) are the generalization of constraints (2.3) for the node pairs that are not adjacent in G: node pair (i,j) is connected if there is one path $p \in P_{ij}$ such that none of its nodes is a critical node. Constraints (2.5)-(2.6) are the variable domain constraints. Note that, since variables v_i are binary, constrains (2.3) and (2.4) impose $u_{ij} \geq 1$ when nodes i and j are connected, which then, due to the objective function, forces $u_{ij} = 1$. Therefore, constraints (2.6) can be replaced by $u_{ij} \geq 0$. The resulting MILP model will be considered henceforward and is referred to as the *exact CND model.*

The total number of constraints (2.4) depends on the graph topology, the link lengths and the values of T and Δ. However, the exact CND model becomes too large (i.e., with too many constraints) for relatively small sized instances which does not allow solution by any available solver for reasonable sized instances. Instead, a row generation approach can be used to solve the exact CND model as described in Algorithm 2.1.

In line 1, a **MILP'** model given by the exact CND model without constraints (2.4) is

Algorithm 2.1 Exact algorithm for the CND problem

```
1: Input: $G = (N, E)$, $c$. Initialize and solve MILP' model (2.1)–(2.6) without constraints
   (2.4). Let $(u^*, v^*)$ be the optimal solution.
2: repeat
3:   Set NCuts $\leftarrow 0$ and $K \leftarrow \{i \in N : v_i^* = 1\}$
4:   Compute subgraph $G_K = (N \backslash K, E_K)$, where $E_K = \{(i,j) \in E : \; i,j \notin K\}$
5:   for all node pair $(i,j) \notin E_K$ do
6:     Compute shortest path $p \in P_{ij}$ and its optical length $d$
7:     if $d \leq T$ and $u_{ij}^* + \sum_{k=1}^{n} \beta_k^p v_k^* = 0$ then
8:       Add to MILP' constraint (2.4) corresponding to path $p$
9:       NCuts $\leftarrow$ NCuts $+1$
10:    end if
11:  end for
12:  if NCuts $> 0$ then
13:    Solve MILP' model with the added constraints. Update $(u^*, v^*)$ accordingly
14:  end if
15: until NCuts $= 0$
```

initialized and solved. Then, in the main cycle (lines 2–15), the separation problem associated with constraints (2.4) is solved (lines 3–11) where the identified violated constraints (whose number is accounted in NCuts) are added to **MILP'** (lines 7-10) and, finally, **MILP'** is solved again (lines 12–14). The algorithm ends when no violated constraint is found (line 15) and the optimal solution is the solution of the last solved **MILP'** model.

The separation problem associated with constraints (2.4) is solved as follows. In line 4, the subgraph $G_K = (N \backslash K, E_K)$ is computed by removing from G the critical nodes of set K (determined in line 3) and the corresponding incident edges and adding Δ to the length of each edge in E_K. Since the number of intermediate nodes of a path is equal to the number of edges minus one, the shortest path value in G_K is equal to the optical path length plus Δ. So, between each pair of nodes i and j in $N \backslash K$, such that $(i,j) \notin E_K$ (line 5), the shortest path p in G_K is determined (by Dijkstra algorithm) and its optical length d computed as the length of p minus Δ (line 6) and the violation of the constraint (2.4) associated to p is checked (line 7).

Note that if the imposition of the transparent reach T is relaxed (i.e., considering $T \to +\infty$), we get one of the classical CND problem variants for which there are known efficient compact MILP models. One such model, proposed in [SdSM18], is as follows. Consider for each pair of nodes (i,j) the set $N_{ij} \subset N$ which represents the set of adjacent nodes to i (on graph G) if the node degree of i is not higher than the node degree of j, or the set of adjacent nodes to j, otherwise. Then, the previous constraints (2.4) can be replaced by the following (polynomial sized) constraints:

$$u_{ij} \geq u_{\{ik\}} + u_{\{kj\}} - 1 + v_k, \;\; (i,j) \notin E, \;\; k \in N_{ij}. \tag{2.7}$$

In these constraints, $u_{\{ik\}}$ represents variable u_{ik} if $i < k$ or variable u_{ki} otherwise (the same meaning to $u_{\{kj\}}$). Constraints (2.7) guarantee that for each pair of nodes i and j not adjacent in G, they are connected if there is a non-critical node $k \in N_{ij}$ connected to both i and j. The resulting MILP model, i.e., replacing constraints (2.4) by constraints (2.7), is referred to as the *compact CND model.*

Note that the optimal solution value of the compact CND model is an upper bound on the optimal solution value of the exact CND model since all node pairs that are connected are accounted in the objective function of the compact CND model while the ones whose shortest path length over the surviving network is higher than the transparent reach T are not accounted in the exact problem. Nevertheless, in most cases, the optimal solution of the compact CND model is also the optimal solution of the exact problem and its resolution is much quicker when using a standard solver (it does not require the row generation method of Algorithm 2.1). As will be described in the next section, we use this fact to derive computationally efficient algorithms for the network design/upgrade problem.

2.3 Network design/upgrade problem

Consider an existing network $G = (N, E)$ with a total fiber length L and a fiber length budget $B = L + L'$, with $L' \geq 0$. The Network Design Problem aims to identify a new network topology connecting all nodes in N whose total fiber length is not higher than B. The Network Upgrade Problem aims to identify a set of fiber links within the budget L' to be added to the existing topology. In both cases, the aim is to obtain a network (design or upgrade) topology that maximizes the A2TR value of the simultaneous failure of its critical nodes.

In [BdSA18b], a multi-start greedy randomized algorithm was proposed for this network design/upgrade problem. The method randomly generates multiple network topologies, with a fiber length budget given by B. Each topology is generated by a greedy randomized algorithm that builds a network by randomly selecting one link at a time until no new link can be added within the fiber budget B. In that stochastic method, the evaluation of each network topology uses centrality based heuristics in a preliminary evaluation and, if necessary, Algorithm 2.1 to compute its exact A2TR value. At the end, the method outputs the best generated topology, i.e., the one with highest A2TR value. Here, we propose an alternative deterministic method based on a greedy approach. The main differences when compared with the previous approach are that a single greedy solution is generated and, on each greedy step, the selected link is based on the critical nodes of the current partial topology (resulting from all already selected links). As a consequence, the critical nodes must be computed at each step of the greedy algorithm.

The proposed method is composed by three tasks which are run in sequence. In the first task, a greedy deterministic algorithm is run so that a topology solution is computed. In the second task, a local search method is applied to the previous solution to try to find a better one. Both first and second tasks consider the network A2TR evaluation imposed by the critical nodes based on the compact CND model. Finally, the third task evaluates the previous solution in terms of optical transparency and using the exact CND model. If the previous solution is not optically transparent and/or the evaluation provided by the exact CND model is lower than the evaluation value provided by the compact CND model, the third task uses the unused budget to add new links so that the network topology becomes optically transparent and the exact A2TR value becomes as close as possible to the value provided by the compact CND. Next, we describe the tasks in three separate subsections and, then, describe the overall algorithms in the fourth subsection.

2.3.1 Greedy deterministic approach

In the first task, both network design and upgrade problems are conceptually modeled as the upgrade of a network topology represented by graph $G = (N, E)$ where $E = \{\}$ in the network design problem and E is the set of fiber links of an existing network in the network upgrade problem. In both cases, parameter l_{ij}, with $i < j$, represents the length of the fiber link between nodes i and j (either an existing link or a possible new link).

Consider the following notation. For a general graph $G = (N, \mathcal{E})$ and a given set of critical nodes $K \subset N$, consider the surviving graph given by $G_K = (N \backslash K, \mathcal{E}_K)$, with $\mathcal{E}_K = \{(i,j) \in \mathcal{E} : i, j \notin K\}$. The surviving graph G_K might be composed by different connected components where a node in one component has no connectivity to a node of any other component. So, for a given set of critical nodes $K \subset N$, parameter m_K indicates the number of connected components of the surviving graph G_K and the binary parameters $cp_K(i,j)$ indicate that nodes $i, j \in N \backslash K$ are in different components of G_K (if $cp_K(i,j) = 1$) or in the same component (if $cp_K(i,j) = 0$).

Algorithm 2.2 presents a greedy deterministic algorithm to upgrade a network represented by graph $G = (N, E)$ with a fiber budget B. This algorithm iteratively selects a candidate link among the ones whose end-nodes belong to two different components in the current surviving network topology, i.e., the topology resulting by removing its critical nodes from the current partial topology.

Algorithm 2.2 has four Input parameters (line 1): besides the graph G and the fiber budget B, the algorithm has a third integer parameter c representing the number of critical nodes of interest and a fourth parameter which is an Input set of links E' considered as follows. In the network upgrade problem, we consider the Input link set $E' = \{\}$. In the network design problem, we follow [BdSA18b] considering the Input link set E' given by the Relative Neighbourhood Graph (RNG) [Tou80], which is defined as follows: nodes $i, j \in N$ are connected by a link if and only if there is no other node $k \in N \backslash \{i, j\}$ such that $l_{ik} \leq l_{ij}$ and $l_{jk} \leq l_{ij}$. The preliminary tests have shown that this set of links provides a good initial balance between connectivity and amount of used fiber budget in the network design problem.

In line 2, some relevant variables are initialized: $\bar{z}$ which represents the CND optimal value of the current partial topology; B_R which represents the amount of fiber budget still available; and set $\mathcal{K}$ which includes all computed sets of critical nodes. Algorithm 2.2 is an iterative process (lines 3-18) where each iteration is composed of two phases: an **Adding Phase**, where links are added to set E' in order to improve the CND value of the resulting topology until the available budget is not enough to add more links; and a **Removing Phase**, where all links in E' are reevaluated and removed if their elimination does not decrease the CND optimal value of the resulting topology. In each iteration, set E'_{add} (and set E'_{rem}) represents the set of links added to (and removed from) the network in the current iteration. These sets are initialized empty at the beginning of each iteration (line 4).

In the Adding Phase (lines 5-14), the compact CND model is solved for the current partial topology $(N, E \cup E')$ (lines 6-7), its set of critical nodes is stored in set K (line 8) and the set of network components imposed by the critical node set K is determined (line 9). In line 10, if the number of components m_K is one (the network is fully connected to any c node failures) or if the shortest available link connecting two components is larger than the remaining budget, no new link is added and the Adding Phase ends. Otherwise, the link $(i, j) \notin E \cup E'$ with

Algorithm 2.2 Greedy deterministic algorithm

```
1: Input: $G = (N, E)$,  $B$, $c$,  $E'$
2: $\bar{z} \leftarrow 0$, $B_R \leftarrow B$ and $\mathcal{K} \leftarrow \{\}$
3: repeat
4:    $E'_{\text{add}} \leftarrow \{\}$ and $E'_{\text{rem}} \leftarrow \{\}$
5:    repeat
6:       Solve compact CND model for graph $G \leftarrow (N, E \cup E')$
7:       Let $z^*$ be the optimal value and $(u^*, v^*)$ be the optimal solution
8:       $\bar{z} \leftarrow z^*$, $K \leftarrow \{i \in N : v_i^* = 1\}$ and $\mathcal{K} \leftarrow \mathcal{K} \cup \{K\}$
9:       Compute the $m_K$ components of graph $\big(N \backslash K, (E \cup E')_K\big)$
10:      if $m_K \geq 2$ and $\min_{(i,j)}\{l_{ij} : cp_K(i,j) = 1\} \leq B_R$ then
11:         Compute new link $(i,j)$ corresponding to $\min_{(i,j)}\{f(i,j) : cp_K(i,j) = 1, l_{ij} \leq B_R\}$
12:         $E' \leftarrow E' \cup \{(i,j)\}$, $E'_{\text{add}} \leftarrow E'_{\text{add}} \cup \{(i,j)\}$ and $B_R \leftarrow B_R - l_{ij}$
13:      end if
14:   until no new link added to set $E'_{\text{add}}$
15:   if $E'_{\text{add}} \neq \{\}$ then
16:      [Removing Phase]
17:   end if
18: until $E'_{\text{add}} = \{\}$ or $E'_{\text{rem}} = \{\}$ or $E'_{\text{rem}} = \big\{\text{last } |E'_{\text{rem}}| \text{ links added to set } E'_{\text{add}}\big\}$
```

the smallest value of a given function $f(i,j)$ that connects two nodes belonging to different components is selected (line 11) and the selected link is added to the current partial topology (line 12). Function $f(i,j)$ can be one of the two following possibilities:

(i) $f_1(i,j) = l_{ij}$, i.e., the link length;

(ii) $f_2(i,j) = l_{ij} \times (\delta_i + \delta_j)$, where δ_i and δ_j are the degree of nodes i and j in the current partial topology $(N, E \cup E')$.

The Adding Phase is repeated until no new link is selected (line 14). In lines 15-17, if at least one link was added in the Adding Phase, the Removing Phase (described in Algorithm 2.3) is run. Algorithm 2.2 runs until no links are added in the Adding Phase, or no links are removed in the Removing Phase or the last links added in the Adding Phase are the links removed in the Removing Phase (line 18).

The Removing Phase (Algorithm 2.3) is an iterative process (lines 2-14) that evaluates each link $(i,j) \in E'$ in decreasing order of its length l_{ij}. For each $(i,j) \in E'$, first, the algorithm computes (in line 3) graph G' that represents the upgraded network without link (i,j). Then, the compact CND of G' is solved (line 8) and if its CND value z' is not lower than the current resiliency value $\bar{z}$ (line 10), the link (i,j) is removed from E' since it does not degrade the resilience of the current topology (line 11).

Our preliminary tests showed that most of the CND optimal solutions in this phase overlap with previous solutions (stored in set $\mathcal{K}$, line 8 of Algorithm 2.2). So, in order to improve the computational efficiency of the Removing Phase, in lines 4-6 of Algorithm 2.3, the resiliency value z'_K is computed for each critical node set $K \in \mathcal{K}$ in graph G' (i.e., the number of connected node pairs in graph G' without nodes K). Then, if the minimum of these values is not lower than the current resiliency value (line 7), the algorithm needs to solve the compact

Algorithm 2.3 Removing Phase of Algorithm 2.2

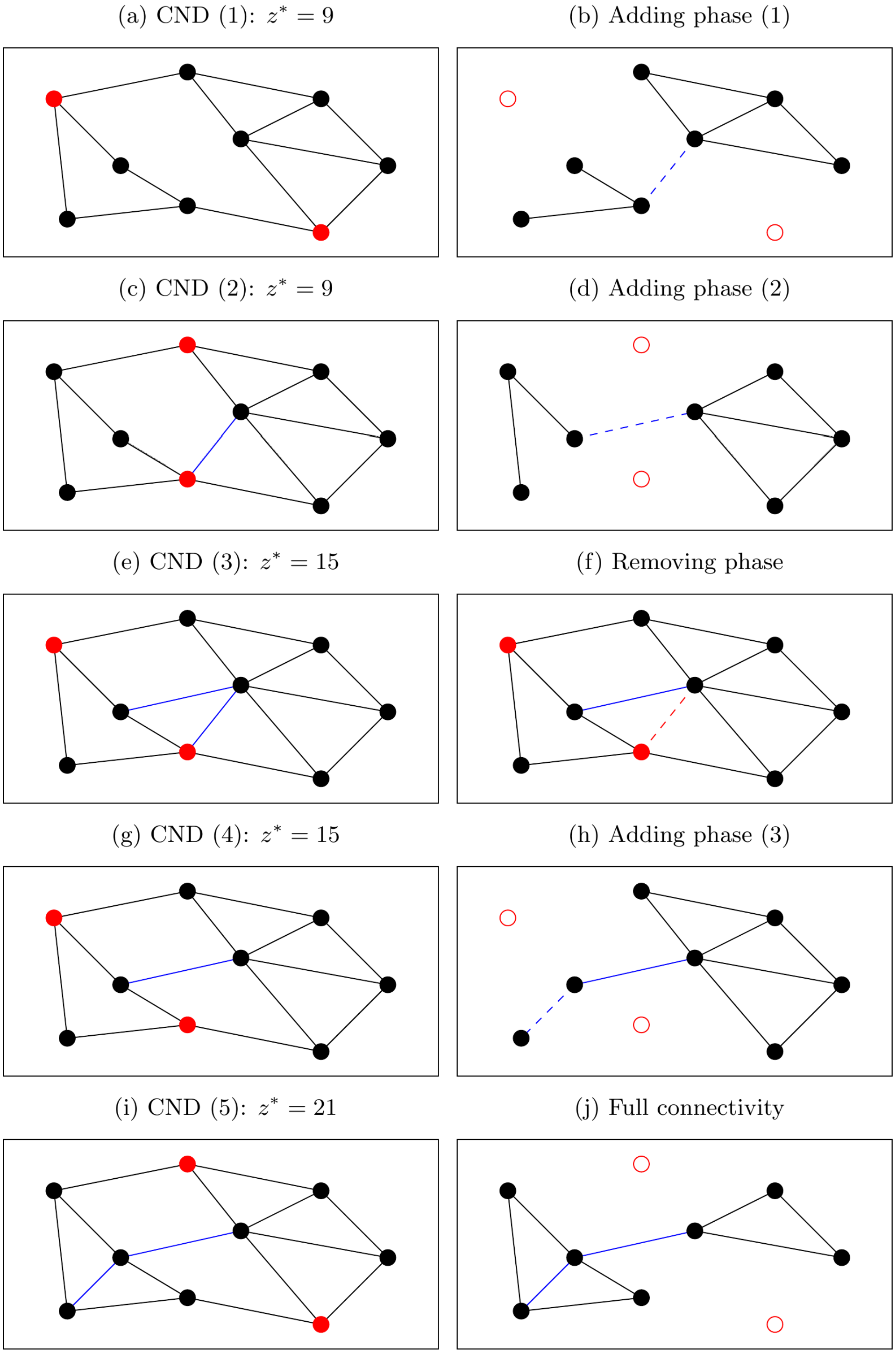
```
1: **Input**: $G = (N, E)$, $c$, $E'$ (in decreasing order of length)
2: **for all** $(i, j) \in E'$ **do**
3:     $G' \leftarrow \big(N, (E \cup E')\backslash\{(i, j)\}\big)$
4:     **for all** $K \in \mathcal{K}$ **do**
5:         $z'_K \leftarrow$ resiliency value given by set of critical nodes $K$ in graph $G'$
6:     **end for**
7:     **if** $\min_{K\in\mathcal{K}}\{z'_K\} \geq \bar{z}$ **then**
8:         Solve *compact* **CND** *model* for graph $G'$ and set $z'$ as the optimal value
9:         $K \leftarrow \{i \in N : v^*_i = 1\}$ and $\mathcal{K} \leftarrow \mathcal{K} \cup \{K\}$
10:        **if** $z' \geq \bar{z}$ **then**
11:            $E' \leftarrow E'\backslash\{(i, j)\}$, $E'_{\text{rem}} \leftarrow E'_{\text{rem}} \cup \{(i, j)\}$ and $B_R \leftarrow B_R + l_{ij}$
12:        **end if**
13:    **end if**
14: **end for**
```

CND model. Otherwise, we know that the current link (i, j) cannot be removed and, therefore, we do not need to solve the compact CND model for graph G' (line 8) which is the most time consuming part of the algorithm.

Figure 2.1 is an illustration of Algorithm 2.2 for a graph with 9 nodes shown in (a), a fiber budget $L' = 15\%L$, $f(i, j) = f_1(i, j)$ and $c = 2$ critical nodes. Initially, the compact CND model is solved for the initial graph to compute its critical nodes, highlighted in red in (a). By removing the critical nodes, it results in the surviving network in (b) with $m_K = 2$ network components (with 3 and 4 nodes, respectively) and the selected link is the shortest one (recall that $f_1(i, j) = l_{ij}$) that connects both components, highlighted in dashed blue in (b). This link is added to the topology, resulting in the upgraded graph in (c), and the optimal critical node set is recomputed. This process is repeated once more, obtaining the upgraded graph in (e). Then, by removing its critical nodes from the graph, there is no candidate link to be added within the remaining fiber budget. At this stage, the Removing Phase starts and the first added link, highlighted in dashed red in (f), is now removed because the resulting topology in (g) has the same resiliency value as the one in (e). This removal increases the available fiber budget B_R. The Adding Phase runs again which now adds a new link, highlighted in dashed blue in (h), obtaining the topology in (i). In this example, this last topology has maximal resiliency, i.e., by removing its critical set of 2 nodes, the surviving network in (j) is fully connected.

In Algorithm 2.2, each added link takes into account the set of critical nodes given by the optimal solution of the compact CND model. A potentially better algorithm is, for each partial topology, to consider the S best critical node sets, with $S > 1$, as in Algorithm 2.4. Algorithm 2.4 has many similarities with Algorithm 2.2: lines 2-10 are similar and lines 25-31 in Algorithm 2.4 are equal to lines 12-18 in Algorithm 2.2 (which means that the Removing Phase is also equal).

In line 11 of Algorithm 2.4, a set of variables c_{ij} are initialized to zero. These variables count, in a weighted manner, the number of times that each candidate link $(i, j) \notin E \cup E'$ connects two components in the S alternative surviving graphs, i.e., the surviving graphs of the S best CND solutions. Note that in line 7, $\bar{z}$ is set with the solution value of the first



(a) CND (1): $z^* = 9$

(b) Adding phase (1)

(c) CND (2): $z^* = 9$

(d) Adding phase (2)

(e) CND (3): $z^* = 15$

(f) Removing phase

(g) CND (4): $z^* = 15$

(h) Adding phase (3)

(i) CND (5): $z^* = 21$

(j) Full connectivity

Figure 2.1: Example of Algorithm 2.2, considering $c = 2$, $f(i,j) = f_1(i,j)$, $L' = 15\%L$, the initial graph in (a). On left, graph $(N, E \cup E')$ in each iteration, with the critical nodes in red, links of E in black and links of E' in blue. On right, the surviving graph in each iteration, added link in dashed blue and removed link in dashed red.

Algorithm 2.4 Greedy deterministic algorithm, considering S CND solutions

```
1: **Input:** $G = (N, E)$, $B$, $c$, $E'$, $S$
2: $\bar{z} \leftarrow 0$, $B_R \leftarrow B$ and $\mathcal{K} \leftarrow \{\}$
3: **repeat**
4:     $E'_{\text{add}} \leftarrow \{\}$ and $E'_{\text{rem}} \leftarrow \{\}$
5:     **repeat**
6:         Initialize and solve *compact* **CND** *model* for graph $G \leftarrow (N, E \cup E')$
7:         Let $z^*$ be the optimal value and $(u^*, v^*)$ be the optimal solution. Set $\bar{z} \leftarrow z^*$
8:         $K \leftarrow \{i \in N : v_i^* = 1\}$ and $\mathcal{K} \leftarrow \mathcal{K} \cup \{K\}$
9:         Compute the $m_K$ components of graph $\big(N \backslash K, (E \cup E')_K\big)$
10:        **if** $m_K \geq 2$ **and** $\min_{(i,j)}\{l_{ij} : cp_K(i,j) = 1\} \leq B_R$ **then**
11:            Initialize $s \leftarrow 1$ and $c_{ij} \leftarrow 0$, for all candidate links $(i,j) \notin E \cup E'$ such that
               $l_{ij} \leq B_R$
12:            **while** $s \leq S$ **and** $m_K \geq 2$ **do**
13:                **for all** $(i,j) \notin E \cup E' : cp_K(i,j) = 1, l_{ij} \leq B_R$ **do**
14:                    $c_{ij} \leftarrow c_{ij} + (\bar{z}/z^*)$
15:                **end for**
16:                **if** $s < S$ **then**
17:                    Add constraint $\sum_{i=1}^{n} v_i^* v_i \leq \sum_{i=1}^{n} v_i^* - 1$ to *compact* **CND** *model* of graph $G$
18:                    Solve *compact* **CND** *model*. Let $z^*$ be the optimal value and $(u^*, v^*)$ be the
                       optimal solution
19:                    $K \leftarrow \{i \in N : v_i^* = 1\}$ and $\mathcal{K} \leftarrow \mathcal{K} \cup \{K\}$
20:                    Compute the $m_K$ components of graph $\big(N \backslash K, (E \cup E')_K\big)$
21:                **end if**
22:                $s \leftarrow s + 1$
23:            **end while**
24:            Compute new link $(i,j) \notin E'$ corresponding to $\max_{(i,j)}\{c_{ij}/f(i,j) : l_{ij} \leq B_R\}$
25:            $E' \leftarrow E' \cup \{(i,j)\}$, $E'_{\text{add}} \leftarrow E'_{\text{add}} \cup \{(i,j)\}$ and $B_R \leftarrow B_R - l_{ij}$
26:        **end if**
27:    **until** no new link added to set $E'_{\text{add}}$
28:    **if** $E'_{\text{add}} \neq \{\}$ **then**
29:        [Removing Phase]
30:    **end if**
31: **until** $E'_{\text{add}} = \{\}$ **or** $E'_{\text{rem}} = \{\}$ **or** $E'_{\text{rem}} = \big\{$last $|E'_{\text{rem}}|$ links added to set $E'_{\text{add}}\big\}$
```

compact CND (the lowest value among all S surviving graphs). Then, for each candidate link (i,j) that connects two components of the current surviving graph (line 13), c_{ij} increases by $\bar{z}/z^*$ where z^* is the solution value of the current surviving graph. Note that the ratio $\bar{z}/z^*$ is always less than or equal to 1. So, the idea behind this weighted sum is to give a lower weight in the link selection to the links connecting two components of the surviving graphs whose CND solution values are worst. Finally, in line 24, the link $(i,j) \notin E \cup E'$ with the largest value of $c_{ij}/f(i,j)$ is selected (like before, $f(i,j)$ is set either with $f_1(i,j)$ or with $f_2(i,j)$).

While the best CND solution of each partial topology is computed in line 6 of Algorithm 2.4, the additional alternative CND solutions are computed in the loop 12-23. This loop ensures that the algorithm will continually compute a compact CND solution until either it loops S times or $m_k = 1$ (line 12), i.e., the current surviving graph does not have multiple components. The condition in line 16 ensures that the compact CND model is optimized at most S times. Finally, given a set of critical nodes K, the added constraint (line 17) excludes this set from the set of feasible solutions of the compact CND model so that, when it is solved again (line 18), it will result in the next best set of critical nodes.

Note that, while computing the S sets of critical nodes for each partial topology, they are computed in increasing value of the A2TR (i.e., the number of connected node pairs). There might exist multiple optimal CND solutions, i.e., all solutions next to the first one such that their optimal value z^* is equal to $\bar{z}$. Since these solutions are more damaging than the subsequent ones, a meaningful alternative is to consider only the optimal CND solutions and ignore the remaining ones. This is easily done by adding in line 12 of Algorithm 2.4 a third condition in the form $z^* = \bar{z}$. In the computational results, we also test this algorithm variant.

2.3.2 Local search approach

In the second task, a local search algorithm is applied to the solution provided by the first task. Note that in the Removing Phase of Algorithms 2.2 and 2.4, a link can only be removed if the resiliency value of the current network topology remains the same. Here, a local search algorithm (described in Algorithm 2.5) is proposed where each link $(i, j) \in E'$ is removed and excluded from the set of candidate links while re-running either Algorithm 2.2 or Algorithm 2.4. Removing the link from the graph decreases the resiliency value $\bar{z}$ but increases the remaining fiber budget B_R, which might enable to find an alternative topology with a better resiliency value.

Algorithm 2.5 Local search algorithm

```
 1: Input: $G = (N, E)$, $E'$, $\bar{z}$, $B_R$
 2: repeat
 3:     $\bar{z}_{\text{LS}} \leftarrow \bar{z}$, $E_{\text{LS}} \leftarrow E'$, $B_{\text{LS}} \leftarrow B_R$ and Update $\leftarrow$ false
 4:     for all $(i, j) \in E'$ do
 5:         $G' \leftarrow \big(N, (E \cup E') \backslash \{(i, j)\}\big)$
 6:         Run Algorithm 2.2 (or 2.4) starting from set $E' \backslash \{(i, j)\}$, fiber budget $B_R + l_{ij}$ and
            excluding link $(i, j)$ from the set of candidate links, obtaining a new set of selected
            links $E'_{ij}$, its resiliency value $\bar{z}_{ij}$ and fiber budget $B_{ij}$
 7:         if $\bar{z}_{ij} > \bar{z}_{\text{LS}}$ or $\big(\bar{z}_{ij} = \bar{z}_{\text{LS}}$ and $B_{ij} > B_{\text{LS}}\big)$ then
 8:             $\bar{z}_{\text{LS}} \leftarrow \bar{z}_{ij}$, $E_{\text{LS}} \leftarrow E'_{ij}$, $B_{\text{LS}} \leftarrow B_{ij}$ and Update $\leftarrow$ true
 9:         end if
10:     end for
11:     if $\bar{z}_{\text{LS}} > \bar{z}$ then
12:         $\bar{z} \leftarrow \bar{z}_{\text{LS}}$, $E' \leftarrow E_{\text{LS}}$ and $B_R \leftarrow B_{\text{LS}}$
13:     end if
14: until Update = false
```

The Inputs of Algorithm 2.5 are the original topology $G = (N, E)$, the added links E', the resiliency value of graph $(N, E \cup E')$ and the remaining fiber budget B_R of the solution provided by the first task. The main loop (steps 2-14) ensures that the local search runs until the resiliency value is not improved. Variables $\bar{z}_{\text{LS}}$, E_{LS} and B_{LS} store the best alternative topology in the present iteration and are accordingly updated (line 8) when a better topology is found. The inner loop (lines 4-10) removes each link $(i,j) \in E'$ from graph $(N, E \cup E')$ and runs the greedy deterministic algorithm (Algorithm 2.2 or 2.4) excluding the removed link to be selected. If two alternative topologies have the same resiliency value, the one with the highest remaining fiber budget is selected (line 7). Finally, in lines 11-13, the main variables $\bar{z}$, E' and B_R are updated if the best alternative topology has a higher resiliency value than the current topology.

After running some computational tests, we observed that in the network design problem, the local search approach is very inefficient as it does not provide relevant gains in the resiliency value and the running time becomes very high. Therefore, the second task is only included in the overall algorithm of the network upgrade problem.

2.3.3 Transparent optical networks application

In the previous tasks, the A2TR value was computed by solving the compact CND model. So, in the network design problem, it is necessary to check if the solution provided by the previous task is optically transparent, i.e., for each node pair, the optical shortest path between them is not higher than the transparent reach T (this is not an issue in the network upgrade problem since the optical transparency is guaranteed by the original network topology). If not, the aim is to use the unused fiber budget to turn the solution optically transparent. Moreover, it is also necessary to compute the A2TR value with the exact CND model and, if the two values are not equal, again we use the unused fiber budget to add new links so that the two values become as close as possible.

In our preliminary tests, we observed that, from the three stopping criteria used in Algorithms 2.2 and 2.4, the most common stopping criterion is the last one: $E'_{\text{rem}} = \big\{\text{last } |E'_{\text{rem}}|$ links added to set $E'_{\text{add}}\big\}$, i.e., the last added links do not improve the A2TR value of the solution and, therefore, they are removed. Thus, the solutions tend to have a reasonable amount of available fiber budget B_R. Algorithm 2.6 presents a deterministic method to use the remaining budget B_R in order to make an Input topology $G = (N, E)$ optically transparent. Initially, the shortest path distances between all node pairs without a direct link (i.e., $(i,j) \notin E$) are computed in loop 3-5. In line 6, variable M is set to the maximum distance between all node pairs $(i,j) \notin E$ and (i_M, j_M) is set to such a node pair. If M exceeds the transparent reach (line 7), the algorithm selects the shortest link (i,j) that, when added to the current topology, turns the distance between (i_M, j_M) within the transparent reach. If the selected link is within the available fiber budget, it is added to the topology (lines 9-11). The algorithm continues until no new link is added (line 13).

Algorithm 2.6 is run when we aim to design a new topology based on the fiber budget of an existing optical network and the existing optical network is not 2-connected (in the context of transparent optical networks, a topology is 2-connected if it is optically transparent for every single node deletion). On the other hand, when the existing network topology is 2-connected, we also require the solution obtained by the network design problem to be 2-connected. Algorithm 2.7 is a generalization of Algorithm 2.6 aiming to use the remaining budget to turn an Input topology $G = (N, E)$ into a 2-connected topology. In Algorithm 2.7, instead of computing the distance between all node pairs without a direct link in G, these distances are

Algorithm 2.6 Network validation algorithm

```
Input: $G=(N,E)$,  $B_R$
repeat
    for all node pairs $(i,j)\notin E$ do
        Compute shortest path $p_{ij}\in P_{ij}$ and its length $d_{ij}$
    end for
    Compute $M \leftarrow \max\{d_{ij} : (i,j)\notin E\}$ and the corresponding node pair $(i_M, j_M)$
    if $M > T$ then
        Compute link $(i,j)\notin E$ corresponding to $\min_{(i,j)}\{l_{ij} : d^{ij}_{i_M j_M} \leq T\}$, where $d^{ij}_{i_M j_M}$ is
        the distance between nodes $i_M$ and $j_M$ on graph $\big(N, E\cup\{(i,j)\}\big)$
        if $l_{ij} \leq B_R$ then
            $E \leftarrow E\cup\{(i,j)\}$ and $B_R \leftarrow B_R - l_{ij}$
        end if
    end if
until no new link added to set $E$
```

computed in loop 3-8 for all reduced graphs G_k, i.e., graphs without node k and its links, for all nodes $k\in N$. Then, variable M is computed (line 9) with the maximum distance between all node pairs over all reduced graphs G_k and the selected link (i,j) is computed in a way similar to Algorithm 2.6 but now considering the reduced graph G_k over which the maximum distance M was computed.

Algorithm 2.7 Network validation algorithm (2-connected)

```
1:  Input: $G=(N,E)$,  $B_R$
2:  repeat
3:      for all $k\in N$ do
4:          $G_k \leftarrow \big(N\backslash\{k\}, E_k\big)$, with $E_k=\{(i,j)\in E : i,j\neq k\}$
5:          for all node pairs $(i,j)\notin E_k$ with $i,j\in N\backslash\{k\}$ do
6:              Compute shortest path $p^k_{ij}$ (on graph $G_k$) and its length $d^k_{ij}$
7:          end for
8:      end for
9:      Compute $M \leftarrow \max\{d^k_{ij} : (i,j)\notin E_k, k\in N\}$, the corresponding node pair $(i_M, j_M)$
        and removed node $k_M$
10:     if $M > T$ then
11:         Compute new link $(i,j)\notin E_{k_M}$ corresponding to $\min_{(i,j)}\{l_{ij} : d^{k_M,ij}_{i_M j_M} \leq T\}$, where
            $d^{k_M,ij}_{i_M j_M}$ is the distance between nodes $i_M$ and $j_M$ on graph $\big(N\backslash\{k_M\}, E_{k_M}\cup\{(i,j)\}\big)$
12:         if $l_{ij} \leq B_R$ then
13:             $E \leftarrow E\cup\{(i,j)\}$ and $B_R \leftarrow B_R - l_{ij}$
14:         end if
15:     end if
16: until no new link added to set $E$
```

Finally, in Algorithm 2.8, we present a method that simultaneously solves the exact CND model (using Algorithm 2.1) and uses the remaining fiber budget B_R to move the resiliency value provided by the exact CND solution as close as possible to the resiliency value of the compact CND model. The Inputs of Algorithm 2.8 are the network topology G, the remaining fiber budget B_R, the target CND optimal value $\bar{z}$ and all the sets of critical nodes $\mathcal{K}$ previously generated by the greedy deterministic algorithm (either Algorithm 2.2 or 2.4). Similarly to Algorithm 2.1, the **MILP'** model is initialized without the path constraints (line 2). Then, in order to accelerate the row generation process, the path constraints associated to each set of critical nodes $K \in \mathcal{K}$ are added to **MILP'** model (lines 3-11). Next, the optimal solution of the exact CND model is solved as in Algorithm 2.1. In lines 15-17, if the exact resiliency value z^* is lower than the target value $\bar{z}$, the algorithm uses the remaining budget to compute new links to be added to the graph so that each component of the surviving graph induced by the optimal critical node set becomes optically transparent (this is equivalent to run Algorithm 2.6 in this surviving graph, line 16). Algorithm 2.6 is repeated until no new link is added (lines 13-18), which happens either if $z^* = \bar{z}$ (no need to add new links) or if no new link can be added due to the remaining fiber budget.

Algorithm 2.8 Exact CND upgrade algorithm

```
 1: Input: $G = (N, E)$,  $B_R$,  $\bar{z}$,  $\mathcal{K}$
 2: Initialize MILP' MILP model (2.1)-(2.6) without constraints (2.4)
 3: for all $K \in \mathcal{K}$ do
 4:    Compute subgraph $G_K = (N \backslash K, E_K)$ where $E_K = \{(i,j) \in E : \; i,j \notin K\}$
 5:    for all node pairs $(i,j) \notin E_K$ do
 6:       Compute shortest path $p_{ij}$ and its length $d_{ij}$
 7:       if $d_{ij} \leq T$ then
 8:          Add to MILP' constraint (2.4) corresponding to path $p_{ij}$
 9:       end if
10:    end for
11: end for
12: Solve the MILP' model. Let $z^*$ be the optimal value and $(u^*, v^*)$ the optimal solution
13: repeat
14:    [Lines 2-15 of Algorithm 2.1]
15:    if $z^* < \bar{z}$ then
16:       Run Algorithm 2.6 in the surviving graph induced by the current optimal critical
          nodes
17:    end if
18: until no new link added to set $E$
```

2.3.4 Overall algorithm

Recall that, for a given network $G = (N, E)$ with a total fiber length L and a fiber length budget of $B = L + L'$, with $L' \geq 0$, the network design problem aims to identify a new network topology connecting all nodes in N whose total fiber length is not higher than B and the network upgrade problem aims to identify a set of fiber links within the budget L' to be added to the existing topology. So, the overall algorithm is a combination of the previous algorithms that depends on the problem type (network design or network upgrade). Algorithms 2.9 and 2.10 describe how the different algorithms are put together to solve the network design and the network upgrade problem, respectively. As previously explained, the network design algorithm (Algorithm 2.9) does not include the local search algorithm

(Algorithm 2.5) and the network upgrade algorithm (Algorithm 2.10) does not need to run the network validation algorithms (Algorithms 2.6 and 2.7). On both Algorithms 2.9 and 2.10, we consider six algorithm variants: (i) Algorithm 2.2, (ii) Algorithm 2.4 considering S CND solutions and (iii) Algorithm 2.4 considering the optimal CND solutions, each case using either $f_1(i,j)$ or $f_2(i,j)$ as the criteria to select each new link.

Algorithm 2.9 Network design algorithm

```
Input: $G = (N, E)$,  $B$
Run Algorithm 2.2 (or 2.4) for graph $(N, \{\})$, with $E'$ the set of links of RNG topology
if $G$ is optically 2-connected then
    Run Algorithm 2.7 for graph $(N, E')$, with $E'$ and $B_R$ resulting from the previous method
else
    Run Algorithm 2.6 for graph $(N, E')$, with $E'$ and $B_R$ resulting from the previous method
end if
Run Algorithm 2.8 for graph $(N, E')$, with variables $\bar{z}$, $B_R$ and $\mathcal{K}$ resulting from the previous methods
```

Algorithm 2.10 Network upgrade algorithm

```
Input: $G = (N, E)$,  $L'$
Run Algorithm 2.2 (or 2.4) for graph $G$, with $B \leftarrow L'$ and $E' \leftarrow \{\}$
Run Algorithm 2.5 for graph $G$, with variables $E'$, $\bar{z}$ and $B_R$ resulting from the previous method
Run Algorithm 2.8 for graph $(N, E \cup E')$, with variables $\bar{z}$, $B_R$ and $\mathcal{K}$ resulting from the previous methods
```

2.4 Computational results

All results reported in this section were obtained using the optimization software *Gurobi Optimizer* version 8.0.0, with programming language *Julia* version 0.6.2, running on a PC with an Intel Core i7-8700, 3.2 GHz and 16 GB RAM. Following [RKD+13], we have assumed a transparent reach $T = 2000$ km corresponding to the use of OTU-4 lightpaths with a line rate of 100 Gbps. Moreover, we have considered $\Delta = 60$ km. This value considers an optical node architecture with an Input and an output WSS (Wavelength Selective Switch) per fiber port and assumes an attenuation of 6.0 dB inserted by each WSS. Then, assuming that the attenuation on each WSS is the main optical degradation factor suffered by a lightpath, an optical node introduces a total of 12.0 dB, equivalent to the attenuation on a fiber of 60 km, with an attenuation of 0.2 dB/km.

The network topologies used in these computational results are Germany50 [OWPT10], PalmettoNet [KNF+11] and Missouri Network Alliance (MissouriNA) [KNF+11]. Table 2.1 presents their topology characteristics in terms of number of nodes $|N|$ and fiber links $|E|$, total number of node pairs, minimum ($\delta_{\min}$), average ($\bar{\delta}$) and maximum ($\delta_{\max}$) node degree and an indication if the topology is (or is not) 2-connected.

Table 2.1: Topology characteristics of each tested network.

Network	$\lvert N\rvert$	$\lvert E\rvert$	no. Pairs	$\delta_{\min}$	$\bar{\delta}$	$\delta_{\max}$	2-Connected
Germany50	50	88	1225	2	3.52	5	Yes
PalmettoNet	45	64	990	1	2.84	5	No
MissouriNA	64	80	2016	1	2.50	5	No

In all cases, the geographical location of nodes is publicly available but the geographical routes of fiber links is not known. So, we have considered that each (existing or possible) link follows the shortest path over the surface of a sphere representing Earth. Table 2.2 presents the resulting length characteristics in terms of minimum ($l_{\min}$), average ($\bar{l}$), maximum ($l_{\max}$) and total link length (L), and diameter (i.e., the highest optical length among the shortest paths of all node pairs adding Δ for each intermediate node). Note that the three topologies are optically transparent for $T = 2000$ km since all diameter values are below 2000 km.

Table 2.2: Length characteristics (in km) of each tested network.

Network	$l_{\min}$	$\bar{l}$	$l_{\max}$	L	Diameter
Germany50	26	100.7	252	8859	1417
PalmettoNet	19	67.0	177	4286	1298
MissouriNA	7	50.0	307	4001	1301

In the computational experiments, we have considered $c \in \{2, 3, 4, 5, 6\}$ as the number of critical nodes. For each network and each c, we started by computing a topology with a fiber budget B equal to the total fiber length L of the original topology using Algorithm 2.9. Then, we computed an upgraded topology for each original topology assuming a fiber budget $L' = p \times L$ with $p = 10\%$ and 20% using Algorithm 2.10. Finally, we computed a topology with a fiber budget $B = L + p \times L$ also for $p = 10\%$ and 20% using Algorithm 2.9. These cases are the same as the ones considered in [BdSA18b] so that we can compare the efficiency of the methods proposed here with the ones proposed in [BdSA18b].

In all cases and in both types of problems (network design and network upgrade), we have run the six algorithm variants (see Section 2.3.4). In the variants with Algorithm 2.4 considering S CND solutions, we present the results with $S = 10$ as our preliminary tests have shown that this value is a good compromise between the running time and the algorithm efficiency. Tables 2.3, 2.4 and 2.5 present the resiliency values of the network upgrade solutions for the three network topologies. In these tables, in addition to the number of critical nodes c, column 'MS' refers to the solutions obtained by using the Multi-Start Greedy Randomized method proposed in [BdSA18b]. Columns 'S1' and 'S2' refer to the solutions obtained by Algorithm 2.2 (the values 1 and 2 mean the use of function $f_1(i, j)$ and $f_2(i, j)$, respectively). Columns 'A1' and 'A2' refer to the solutions obtained by Algorithm 2.4 considering the optimal CND solutions and columns 'M1' and 'M2' refer to the solutions obtained by Algorithm 2.4 considering $S = 10$ best CND solutions. Finally, the best values of each problem instance are highlighted in bold.

The first and most important observation of these computational results is that, with the

Table 2.3: Resiliency values z of the network upgrade solutions for Germany50.

	Germany50, with Upgrade = 10%							Germany50, with Upgrade = 20%						
c	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2
2	1081	1081	1081	1081	1081	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**
3	**991**	**991**	**991**	**991**	**991**	**991**	**991**	**1035**	**1035**	**1035**	**1035**	**1035**	**1035**	**1035**
4	830	830	830	830	**867**	795	**867**	906	946	**947**	946	**947**	906	**947**
5	640	616	640	640	640	**666**	**666**	756	756	756	**790**	**790**	**790**	**790**
6	498	483	478	478	478	**511**	487	**606**	583	543	**606**	**606**	583	**606**

Table 2.4: Resiliency values z of the network upgrade solutions for PalmettoNet.

	PalmettoNet, with Upgrade = 10%							PalmettoNet, with Upgrade = 20%						
c	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2
2	**821**	**821**	**821**	**821**	**821**	**821**	**821**	**861**	**861**	**861**	**861**	**861**	821	821
3	**616**	**616**	**616**	**616**	**616**	**616**	**616**	709	709	709	709	709	709	**744**
4	**427**	400	389	400	389	406	412	510	510	**532**	524	**532**	**532**	**532**
5	325	333	333	**337**	333	325	319	**380**	**380**	**380**	**380**	**380**	**380**	**380**
6	235	223	**238**	235	**238**	**238**	234	286	295	307	**325**	319	310	**325**

Table 2.5: Resiliency values z of the network upgrade solutions for MissouriNA.

	MissouriNA, with Upgrade = 10%							MissouriNA, with Upgrade = 20%						
c	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2
2	1555	**1659**	**1659**	**1659**	**1659**	1371	1371	1659	**1771**	**1771**	**1771**	**1771**	**1771**	1371
3	**1362**	**1362**	1242	**1362**	1172	**1362**	1320	1446	**1500**	**1500**	**1500**	**1500**	1452	**1500**
4	762	870	870	874	870	**906**	895	1039	1194	1246	1246	**1270**	**1270**	1194
5	618	667	653	711	653	**753**	733	758	843	841	861	871	896	**897**
6	457	505	460	505	460	**526**	520	550	701	688	**722**	681	701	**722**

exception of one instance (PalmettoNet topology for $c = 4$ and $p = 10\%$), the resiliency value obtained by at least one of the proposed algorithm variants is not lower (in many cases, it is significantly higher) than the resiliency value of the method proposed in [BdSA18b]. This means that the best obtained upgrade topologies, in general, have an higher resiliency to critical node failures when compared to the ones provided in [BdSA18b]. Additionally, the comparison of the different algorithm variants (proposed in this work) does not provide clear evidence that one of them is consistently better than the others. This means that, in practice, we might need to run all of them to compute the best upgrade solution.

Tables 2.6, 2.7 and 2.8 present the resiliency values of the network design solutions for the three network topologies (the meaning of each column is similar to the previous tables). In the Germany50 network, the strikeout values represent invalid solutions where the algorithm variant was not able to compute a 2-connected network design solution.

When comparing the results using the different algorithm variants with the method in [BdSA18b], it is possible to observe that, in general, the network topologies obtained in this work are much more resilient to critical node failures than the ones obtained in [BdSA18b]. In the Germany50 network, all invalid topologies were obtained using function $f_1(i, j)$. So, in this case, it is preferable to use function $f_2(i, j)$ in the link selection. The reason for the superior performance of $f_2(i, j)$ is because it favors the selection of candidate links connecting

Table 2.6: Resiliency values z of the network design solutions for Germany50.

	Network Design Problem							Network Design Problem + 10%							Network Design Problem + 20%						
c	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2
2	1081	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**	**1128**
3	991	**1035**	**1035**	961	**1035**	**1035**	**1035**	991	**1035**	**1035**	**1035**	**1035**	**1035**	**1035**	1035	1080	1035	1054	**1081**	**1081**	**1081**
4	830	906	**947**	906	**947**	946	906	906	**947**	**947**	**947**	**947**	**947**	**947**	906	947	**990**	**990**	**990**	**990**	**990**
5	640	724	790	756	787	790	**826**	756	790	826	826	**862**	826	826	790	862	826	864	**903**	864	**903**
6	498	~~573~~	631	~~623~~	651	~~651~~	**658**	606	631	687	658	**718**	~~717~~	718	658	687	718	**751**	745	**751**	**751**

Table 2.7: Resiliency values z of the network design solutions for PalmettoNet.

	Network Design Problem							Network Design Problem + 10%							Network Design Problem + 20%						
c	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2
2	**861**	**861**	**861**	**861**	**861**	**861**	**861**	861	861	902	900	**903**	**903**	**903**	861	**903**	**903**	**903**	**903**	**903**	**903**
3	676	709	**744**	709	**744**	709	709	709	780	744	744	**781**	**781**	744	744	781	781	**820**	781	781	781
4	510	510	**556**	**556**	490	**556**	**556**	582	582	610	636	**640**	**640**	**640**	582	605	672	669	672	640	**706**
5	379	373	**380**	**380**	**380**	**380**	379	409	429	380	429	**461**	**461**	444	480	461	**549**	444	524	**549**	**549**
6	266	295	246	315	297	**325**	313	322	342	337	325	342	**346**	337	358	346	361	367	**403**	391	381

Table 2.8: Resiliency values z of the network design solutions for MissouriNA.

	Network Design Problem							Network Design Problem + 10%							Network Design Problem + 20%						
c	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2	MS	S1	S2	A1	A2	M1	M2
2	1714	**1771**	**1771**	**1771**	**1771**	1714	**1771**	1714	**1830**	**1830**	**1830**	**1830**	1771	1771	1771	**1830**	**1830**	**1830**	**1830**	1771	**1830**
3	1495	**1550**	**1550**	**1550**	**1550**	**1550**	1452	1500	1599	**1654**	1599	1602	**1654**	**1654**	1550	**1656**	**1656**	**1656**	**1656**	**1656**	**1656**
4	1126	1231	1231	1231	1231	**1311**	**1311**	1194	1354	**1399**	1354	1354	1354	**1399**	1311	1389	1441	1491	**1495**	1491	1446
5	841	931	**1051**	1025	951	1023	**1051**	917	1081	1113	1091	**1147**	1113	**1147**	1081	1113	1147	1183	1221	**1261**	1221
6	694	**784**	732	764	768	742	776	717	893	861	842	893	918	**926**	784	972	992	956	992	1037	**1066**

nodes with lower degrees. So, there is a lower chance that the generated topology has leaves (nodes with degree one) and, even when this happens, Algorithm 2.7 needs, in general, a lower amount of fiber budget to make it 2-connected. Nevertheless, in the other networks (PalmettoNet and MissouriNA), there are some cases where the variants using $f_1(i,j)$ provide the best resiliency results. So, like in the network upgrade problem, in the network design problem there is no clear evidence that one of the variants is consistently better than the others.

Table 2.9 presents the resiliency value z of the best topologies obtained for each instance presented in Tables 2.3–2.8. Rows 'Original' refer to the original topologies (in column '0%') and upgraded topologies (in columns '10%' and '20%') while rows 'Alternative' refer to the best network design solutions with a fiber budget $B = L + p \times L$ with $p = 0\%$, 10% and 20%. For each case, columns 'UB' presents the trivial upper bound of the CND problem given by the number of pairs of $n - c$ surviving nodes, i.e., $(n-c)(n-c-1)/2$, with $n = |N|$.

An initial observation of these results is that the resiliency values are lower for higher number of critical nodes c, which is without surprise since more node failures disrupt an higher percentage of the network. Moreover, the resilience of the upgraded topologies is always significantly better for higher budget values.

The best topologies are always significantly better than the original/upgraded ones, with the exception of Germany50 for $c = 2$ and with $p = 10\%$ and 20%, where the trivial upper bound is reached in both cases. Nevertheless, when comparing the differences between the original/upgraded and the best topologies, it is significantly higher for PalmettoNet and MissouriNA topologies than for the Germany50 topology. This means that the latter topology is significantly more resilient to critical node failures than PalmettoNet and MissouriNA. To understand this fact, recall from the topology characteristics of the different networks (Table

Table 2.9: Best obtained resiliency value z for all tested instances.

c	Network	Germany50				PalmettoNet				MissouriNA			
	Instance	0%	10%	20%	UB	0%	10%	20%	UB	0%	10%	20%	UB
2	Original	1036	1128	1128	1128	513	821	861	903	946	1659	1771	1891
	Alternative	1128	1128	1128		861	903	903		1771	1830	1830	
3	Original	711	991	1035	1081	346	616	744	861	602	1362	1500	1830
	Alternative	1035	1035	1081		744	781	820		1550	1654	1656	
4	Original	640	867	947	1035	284	427	532	820	455	906	1270	1770
	Alternative	947	947	990		556	640	706		1311	1399	1495	
5	Original	496	666	790	990	176	337	380	780	338	753	897	1711
	Alternative	826	862	903		380	461	549		1051	1147	1261	
6	Original	415	511	606	946	123	238	325	741	253	526	722	1653
	Alternative	658	718	751		325	346	403		784	926	1066	

2.1) that Germany50 is the topology with the highest average node degree and the only one which is 2-connected. These two characteristics make this network more resilient than the two other networks.

More important than analyzing the absolute resiliency values, we need to analyze the resiliency gap between the original/upgraded topologies and the best topologies computed with the same fiber budget values. Figure 2.2 plots in a bar chart these gaps, for all networks and all values of c, computed as $\frac{z_{\mathrm{B}}-z_{\mathrm{O/U}}}{z_{\mathrm{B}}} \times 100\%$ where z_{B} is the resiliency value of the best topology and $z_{\mathrm{O/U}}$ is the resiliency value of the original/upgraded topology. Blue bars present the resiliency gap between the best topology and the original topology. The resiliency gaps between the best topologies and the upgraded topologies are presented in the red and green bars for $p = 10\%$ and 20%, respectively.

Firstly, the blue bars of Figure 2.2 show that the resiliency gaps are lower for Germany50 (but still significant for a number of critical nodes $c \geq 3$) and very large for PalmettoNet and MissouriNA. These results reinforce the previous conclusion that Germany50 is more resilient than the others but also show that, in general, existing network topologies are not resilient to critical node failures. Secondly, the resiliency gaps shown in the red bars (corresponding to topology designs with 10% more total fiber length) represent, in all cases, a significant gap reduction when compared with the blue bars. This means that for all tested instances, adding new links to an existing topology with a fiber budget of 10% enables solutions with resiliency to critical node failures much closer to a topology designed to maximize this resilience with the same amount of fiber. Thirdly, the results of the green bars (corresponding to topology designs with 20% more total fiber length) are mixed, i.e., in some cases, the additional 10% fiber budget enables a significant gap reduction while in other cases, the reduction is negligible.

Finally, we can distinguish two cases. For a number of critical nodes $c \leq 3$, the additional fiber budget of 20% allows in all cases the resiliency gap to become small (below 10%). For a number of critical nodes $c \geq 5$ (in the Germany50 network) and $c \geq 4$ (in the less resilient PalmettoNet and MissouriNA networks), the additional fiber budget of 20% is still not enough to make the resiliency gap small. This means that more fiber links are required in the upgrade of existing networks to reach the best resiliency to higher number of critical nodes.

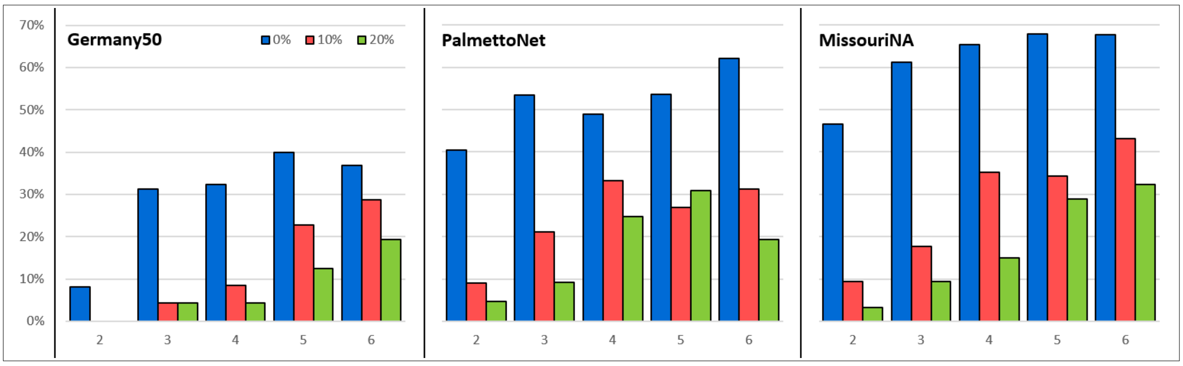


Figure 2.2: Resiliency gaps of all tested networks and for all $c \in \{2, ..., 6\}$.

For illustrative purposes, Figure 2.3 presents the original topologies, the best upgraded topologies with $L' = 10\%L$ and $L' = 20\%L$ (with the additional links highlighted in blue) and the best topologies with the same fiber budget L obtained considering $c = 4$ critical nodes. To highlight the differences, links of the best topology (and the best upgraded topologies) not in the original topology are highlighted in blue and, in all cases, critical nodes are represented with red squares. The analysis of these topologies show that:

Germany50: The critical node set splits the original network in three components (1, 10 and 35 nodes each) while it only isolates a pair of nodes from the others in the best topology. Moreover, the critical node set isolates 4 nodes from the others in the 10% upgraded topology and a pair of nodes in the 20% upgraded topology. So, an upgrade of 20% has the same resilience to 4 critical nodes as the best topology.

PalmettoNet: The critical node set splits the original network in four components (2, 6, 13 and 20 nodes each) while it splits the best topology in only two components (8 and 33 nodes each). Moreover, the critical node set splits the 10% upgraded topology in four components (2, 5, 5 and 29 nodes) and the 20% upgraded topology in two components (9 and 32 nodes). In this case, the resilience to 4 critical nodes of the 20% upgraded topology is still slightly lower than the resilience of the best topology.

MissouriNA: The critical node set splits the original network in four components (8, 16, 17 and 19 nodes each) while it splits the best topology in only two components (9 and 51 nodes each). Moreover, the critical node set splits the 10% upgraded topology in two components (24 and 36 nodes) and the 20% upgraded topology in two components (10 and 50 nodes). As in the previous case, the resilience to 4 critical nodes of the 20% upgraded topology is still slightly lower than the resilience of the best topology.

Concerning the running time of the proposed algorithm variants, Table 2.10 presents the average running time of the Network Upgrade Problem (Algorithm 2.10), among all five values $c = 2, ..., 6$ of each problem instance. In the instance name, ‘Ger’, ‘Pal’ and ‘Mis’ refers to the Germany50, PalmettoNet and MissouriNA networks, respectively, while the ‘10’ and ‘20’ refer to the fiber budget $L' = 10\%L$ and $20\%L$, respectively. Similarly, Table 2.11 presents the average running time of the Network Design Problem (Algorithm 2.9), among all five values $c = 2, ..., 6$ of each instance. In the instance name, the ‘0’, ‘10’ and ‘20’ refer to the fiber budget $B = L + 0\%L$, $B = L + 10\%L$ and $B = L + 20\%L$, respectively.

The analysis of the running times of Tables 2.10 and 2.11 let us draw the following con-

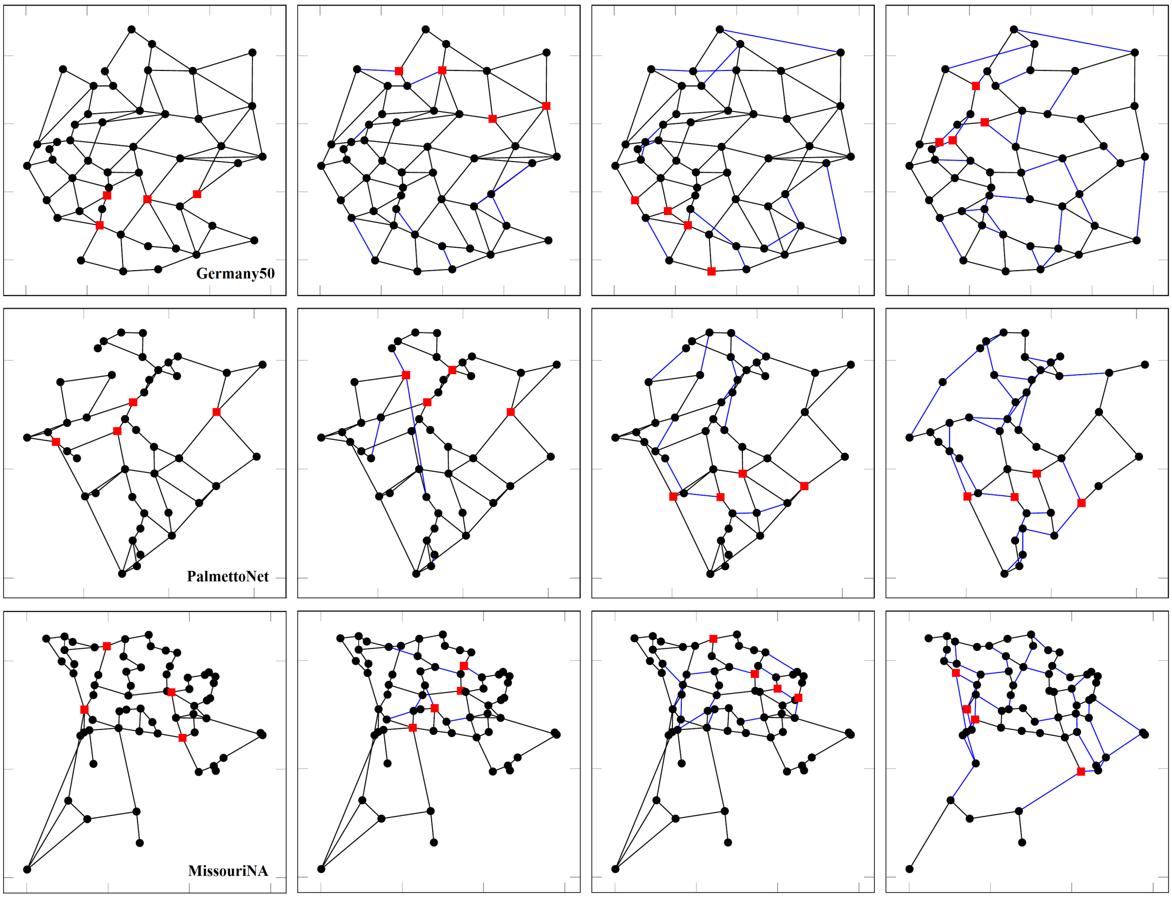


Figure 2.3: Original topologies (first column), best upgraded topologies with $L' = 10\%L$ and $20\%L$ (second and third columns, respectively) and the best topologies with $B = L$ (fourth column), considering $c = 4$ critical nodes (represented in red squares). Links not in the original topologies highlighted in blue.

Table 2.10: Average running time (HH:MM:SS) of the Network Upgrade Problem.

Instance	S1	S2	A1	A2	M1	M2
Ger_10	00:06:19	00:04:44	00:06:32	00:06:57	00:34:51	00:29:51
Ger_20	00:36:37	00:31:30	01:11:44	01:09:32	02:28:51	02:35:05
Pal_10	00:00:49	00:00:53	00:01:21	00:01:11	00:03:14	00:02:55
Pal_20	00:04:53	00:06:07	00:14:51	00:09:25	00:20:19	00:20:56
Mis_10	00:05:58	00:02:17	00:09:40	00:03:03	00:16:08	00:09:26
Mis_20	01:56:47	00:47:10	01:54:14	01:42:59	03:28:53	01:32:35

clusions. First, all algorithm variants have higher running times when the problems consider higher fiber budget values. This was expected since more links are added with an higher fiber budget and, therefore, the algorithms run a larger number of iterations.

Second, even without using the local search algorithm (Algorithm 2.5) in the Network Design Problem, this problem has much longer running times than the Network Upgrade Problem. The main reason is that Network Upgrade Problem starts with a fixed set of fiber

Table 2.11: Average running time (HH:MM:SS) of the Network Design Problem.

Instance	S1	S2	A1	A2	M1	M2
Ger_0	00:45:24	00:55:20	00:45:49	01:06:20	02:03:28	02:13:56
Ger_10	01:06:45	01:19:15	02:11:49	02:42:54	03:28:40	04:00:03
Ger_20	04:00:59	02:17:02	04:12:33	07:25:25	11:53:53	10:22:25
Pal_0	00:04:21	00:06:15	00:06:49	00:06:51	00:08:31	00:08:36
Pal_10	00:08:44	00:06:46	00:10:15	00:13:07	00:15:16	00:13:09
Pal_20	00:08:58	00:12:35	00:18:22	00:19:07	00:21:36	00:27:16
Mis_0	00:35:08	00:35:01	00:35:56	00:32:50	00:58:57	00:46:51
Mis_10	00:53:47	00:55:09	01:03:13	01:03:54	01:09:10	01:34:19
Mis_20	01:08:20	01:12:30	01:57:30	01:31:11	03:40:24	02:50:15

links (the links of the original topology), while the Network Design Problem has to built a solution from scratch.

Third, note that at each iteration, Algorithm 2.2 solves a single CND model, Algorithm 2.4 considering the optimal CND solutions solves a variable number of CND models and Algorithm 2.4 considering S CND solutions solves an even higher number of CND models (in our case, 10 CND models, as we consider $S = 10$). Moreover, solving the CND models is the most time-consuming part of all algorithms. As a consequence, the running times of both Algorithms 2.4 are higher, on average, than the running times of Algorithm 2.2 and the running times of Algorithm 2.4 considering S CND solutions are higher, on average, than the running times of Algorithm 2.4 considering the optimal CND solutions. Note that the use of $f_1(i,j)$ or $f_2(i,j)$ as the criterion to select each new link does not have a significant impact in the obtained running times.

Another aspect of interest is the comparison of the node degree distributions between the original topologies and the best topologies with the same total fiber length L. Figure 2.4 shows these distributions for the three network cases with the best topologies obtained for $c = 4$ critical nodes (original topologies in blue and best topologies in green). For example, in Germany50 original topology, there are 10 nodes with the minimum degree of 2 and 11 nodes with the maximum degree of 5 while in the best topology all nodes have a degree between 3 and 4. In the other two networks, we observe from the original topology to the best topology that the number of nodes with degree 1 and 2 decreases and the maximum network degree also decreases from 5 to 4 in both cases. So, the conclusion is that in the best topologies, there is a decrease in the number of nodes with the lowest and highest degrees and an increase in the number of nodes with degrees closer to the average. This observation also stands in the best topologies for the other values of c showing that resilient topologies tend to have more homogeneous node degrees.

2.5 Conclusions

In this work, we have addressed the topology design of transparent optical networks aiming to maximize their resilience to the simultaneous failure of their critical nodes. We have proposed different algorithm variants of a deterministic method that can be used both in the design of network topologies and in the upgrade of existing topologies. We have

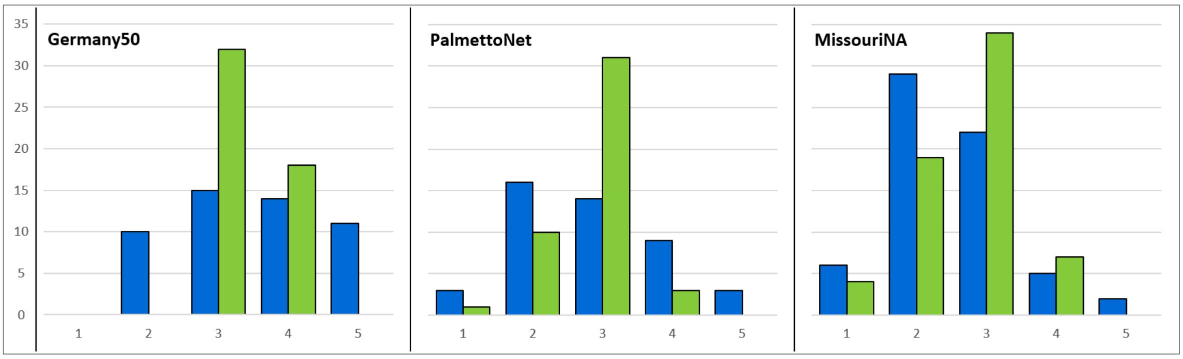


Figure 2.4: Node degree histograms of original topology (in blue) and the best topology (in green) for $c = 4$.

run the proposed algorithm on three network topologies with publicly available information comparing the resiliency gap between the existing and upgraded topologies with the best topologies designed to maximize its resilience with the same fiber budget.

The results have shown that the resiliency gap of existing topologies is significantly large but network upgrades with $L' = 10\%L$ can already reduce significantly the resiliency gaps provided that such upgrades are aimed at maximizing the network resiliency to the critical node failures. Finally, comparing the best topologies with the existing ones, the best topologies are characterized by a decrease of the number of nodes with the lowest and highest degrees and an increase of the number of nodes with degrees closer to the average node degree. This clearly shows that network topologies resilient to critical node failures tend to have more homogeneous degrees among all their nodes.

Bibliography

[ACEP09] A. Arulselvan, C. Commander, L. Elefteriadou, and P. Pardalos. *Detecting critical nodes in sparse graphs.* Computers & Operations Research, 36(7):2193–2200, 2009.

[AdSD16] A. Agra, A. de Sousa, and M. Doostmohammadi. *The minimum cost design of transparent optical networks combining grooming, routing, and wavelength assignment.* IEEE/ACM Transactions on Networking, 24(6):3702–3713, 2016.

[BdSA18a] F. Barbosa, A. de Sousa, and A. Agra. *The design of transparent optical networks minimizing the impact of critical nodes.* Electronic Notes in Discrete Mathematics, 64:165–174, 2018.

[BdSA18b] F. Barbosa, A. de Sousa, and A. Agra. *Topology design of transparent optical networks resilient to multiple node failures.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

[BGLR05] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish. *Improving network robustness by edge modification.* Physica A: Statistical Mechanics and its Applications, 357(3-4):593–612, 2005.

[dSMS17] A. de Sousa, D. Mehta, and D. Santos. *The robust node selection problem aiming to minimize the connectivity impact of any set of p node failures.* In 13th International Conference on Design of Reliable Communication Networks (DRCN), pages 138–145, 2017.

[DTM14] F. Dikbiyik, M. Tornatore, and B. Mukherjee. *Minimizing the risk from disaster failures in optical backbone networks.* Journal of Lightwave Technology, 32(18):3175–3183, 2014.

[FWG$^+$16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GTE$^+$16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[KNF$^+$11] S. Knight, H. Nguyen, N. Falkner, R. Bowden, and M. Roughan. *The internet topology zoo.* IEEE Journal on Selected Areas in Communications, 29(9):1765–1775, 2011.

[NYWF17] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek. *Link addition framework for optical CDNs robust to targeted link cut attacks.* In 9th International Workshop on Resilient Networks Design and Modeling (RNDM). IEEE, 2017.

[NZCM11] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano. *Assessing the vulnerability of the fiber infrastructure to disasters.* IEEE/ACM Transactions on Networking, 19(6):1610–1623, 2011.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[RCM17] D. Rueda, E. Calle, and J. Marzo. *Robustness comparison of 15 real telecommunication networks: structural and centrality measurements.* Journal of Network and Systems Management, 25(2):269–289, 2017.

[RHC$^+$16] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska. *RECODIS: Resilient communication services protecting end-user applications from disaster-based failures.* In 18th International Conference on Transparent Optical Networks (ICTON). IEEE, 2016.

[RKD$^+$13] F. Rambach, B. Konrad, L. Dembeck, U. Gebhard, M. Gunkel, M. Quagliotti, L. Serra, and V. López. *A multilayer cost model for metro/core networks.* Journal of Optical Communications and Networking, 5(3):210–225, 2013.

[SdSM18] D. Santos, A. de Sousa, and P. Monteiro. *Compact models for critical node detection in telecommunication networks.* Electronic Notes in Discrete Mathematics, 64:325–334, 2018.

[SGL12] M. Di Summa, A. Grosso, and M. Locatelli. *Branch and cut algorithms for detecting critical nodes in undirected graphs.* Computational Optimization and Applications, 53(3):649–680, 2012.

[STD15] K. Sabeh, M. Tornatore, and F. Dikbiyik. *Progressive network recovery in optical core networks.* In 7th International Workshop on Reliable Networks Design and Modeling (RNDM), pages 106–111. IEEE, 2015.

[Tou80] G. Toussaint. *The relative neighbourhood graph of a finite planar set.* Pattern Recognition, 12(4):261–268, 1980.

[VBP14] A. Veremyev, V. Boginski, and E. Pasiliao. *Exact identification of critical nodes in sparse networks via new compact formulations.* Optimization Letters, 8(4):1245–1259, 2014.

[VPP15] A. Veremyev, O. Prokopyev, and E. Pasiliao. *Critical nodes for distance-based connectivity and related problems in graphs.* Networks, 66(3):170–195, 2015.

[ZL12] A. Zeng and W. Liu. *Enhancing network robustness against malicious attacks.* Physical Review E, 85((6 Pt 2):066130), 2012.

Chapter 3

The Minimum Cost Network Upgrade Problem with Maximum Robustness to Multiple Node Failures

Abstract: The design of networks which are robust to multiple failures is gaining increasing attention in areas such as telecommunications. In this paper, we consider the problem of upgrading an existent network in order to enhance its robustness to events involving multiple node failures. This problem is modeled as a bi-objective mixed linear integer formulation considering both the minimization of the cost of the added edges and the maximization of the robustness of the resulting upgraded network. As the robustness metric of the network, we consider the value of the Critical Node Detection (CND) problem variant which provides the minimum pairwise connectivity between all node pairs when a set of c critical nodes are removed from the network. We present a general iterative framework to obtain the complete Pareto frontier that alternates between the minimum cost edge selection problem and the CND problem. Two different approaches based on a cover model are introduced for the edge selection problem. Computational results conducted on different network topologies show that the proposed methodology based on the cover model is effective in computing Pareto solutions for graphs with up to 100 nodes, which includes four commonly used telecommunication networks.

Keywords: Robust Network Design, Critical Node Detection, Mixed Integer Linear Programming, Pareto frontier Telecommunications

F. Barbosa, A. Agra, and A. de Sousa. *The minimum cost network upgrade problem with maximum robustness to multiple node failures.* Computers & Operations Research, 136:105453, 2021.

3.1 Introduction

The design of networks which are robust to multiple failures is gaining increasing attention. In the area of telecommunications, which has motivated this work, multiple failures can occur due to many different reasons, as natural disasters [GTE+16] or malicious human activities [FWG+16], and different techniques are being investigated to enhance the preparedness of telecommunication networks for such events [RH20]. Depending on the causes, multiple failures might involve only edges or nodes and edges (a node failure implies that its incident edges also fail). For example, in malicious human attacks, node shutdowns are harder to realize but they are the most rewarding in the attacker's perspective as the shutdown of a single node also shuts down its incident edges. Here, we address the case of multiple node failures as they are the most harmful cases of malicious human attacks.

In this work, we consider the minimum cost network upgrade problem with maximum robustness to multiple node failures (for short, robust network upgrade problem, RNUP). Given an undirected complete graph $G = (N, E_n)$ and a subset of edges $E_0 \subset E_n$, representing an existent network topology, the RNUP aims to determine a set of additional edges E' from $E_n \setminus E_0$, that maximizes the robustness of the upgraded graph $G^U = (N, E_0 \cup E')$ to multiple node failures while minimizing the total cost of the added edges. The robustness of the graph is measured by the lowest pairwise connectivity value (i.e., the lowest number of node pairs that have connectivity in the remaining graph) among all the possible scenarios of c removed nodes.

Concerning the robustness value of an upgraded graph, it can be computed with the optimal solution of an optimization problem, commonly named Critical Node Detection (CND). For a given graph and a given number c of nodes, the most common CND variant is the optimization problem that consists of computing the set of c nodes, named critical nodes, such that their deletion maximally degrades the network connectivity according to a given connectivity metric. Therefore, the optimal value of the CND variant considering the pairwise connectivity minimization represents the worst degradation that the deletion of any set of c nodes can impose in the given graph in our RNUP.

Note that, in some contexts, the determination of a set of critical nodes of a given graph is the ultimate goal of the optimization problem as, for example, the identification of the communities to be immunized in the spread of diseases [dSPRR19]. In other contexts, as the one addressed in this work, the CND problem is only one part of a more general problem.

The use of the CND value as a metric to evaluate the robustness of networks to multiple node failures has been recently used in the preparedness of telecommunication networks to large-scale failures, as in [dSMS17] where some nodes of the network are optimally selected to be made robust such that they never fail and in [BdSA20] where the network upgrade problem (i.e., the optimal selection of new edges to be added to an existent network) is addressed. In both cases, for a given budget (in the robust nodes and in the new edges, respectively), the aim is to improve as much as possible the worst degradation imposed by the failure of the critical nodes of the resulting upgraded network. By considering the budget as a constraint, these works address a single objective optimization problem.

When dealing with multi-objective optimization problems, the main objective is to obtain optimal Pareto solutions [CGL+02, SD07]. Instead of considering a given budget, the main goal of this work is to obtain the optimal Pareto frontier between minimizing the total cost of the edges added to the existent topology and maximizing the CND value of the upgraded topology G^U. This approach allows to generate detailed information regarding the trade-off between the upgrade cost and the gains in robustness resulting from that upgrade.

There are very few works that seek to enhance the robustness of a network to multiple node failures by increasing the topology connectivity through the addition of new links. To the best of our knowledge, in the context of network design, the recent paper [HB21] is the unique to consider two objectives. One of these objectives is common to our work (minimizing the link insertion cost). Regarding the other objective, the authors aim to maximize the network technical power (measured in terms of total potential for sending and receiving flow on all nodes) which leads to a simpler bi-objective problem. Different approaches are designed to find non-dominated solutions, but the purpose is not to obtain the complete Pareto frontier. In [NYWF19], at the infrastructure level of optical networks, the robustness to link cut attacks is enhanced by increasing the topology connectivity with sparse link addition. In [BdSA18, BdSA20], the network upgrade problem aims to identify a set of links, within a given link length budget, to be added to an existing topology in order to obtain the upgraded network that maximizes the robustness in case of a simultaneous failure of a set of c critical nodes. In these works, the problem is solved by resorting to heuristic methods: a multi-start greedy randomized method in [BdSA18] and a greedy deterministic algorithm in [BdSA20]. To the best of our knowledge, the robust network upgrade problem (as presented in this work) has never been addressed with exact methods.

Contrary to the RNUP, the CND problem has been extensively addressed in different network contexts where, depending on the context, different connectivity metrics have been considered, i.e., minimizing the pairwise connectivity, maximizing the number of connected components, minimizing the number of nodes of the largest connected component size, etc (see [LTK18], for a recent survey). Many of these variants assume a given number c of critical nodes, which, in our problem, represents the worst-case number of nodes that can simultaneously fail. Moreover, alternative formulations for the CND problem have been proposed with different objective functions and constraints as, for example, the beta-vertex disruptor [DXT$^+$10] and the component-cardinality-constrained [LTK16] CND variants. As already mentioned, we focus on the CND variant where, for a given number c of critical nodes, the aim is to compute a set of c nodes that minimizes the pairwise connectivity of the network [ACEP09, PC19, SGL11, SGL12, VBP14, Ven12], a variant that has been used in the vulnerability evaluation of telecommunication networks to multiple node failures [dSS20, SdSM18].

Recently, the CND problem itself has been modeled with multi-objective formulations. In [VHOB18], the CND problem is formulated as a bi-objective problem: maximizing the number of connected components in a graph while simultaneously minimizing the variance of their cardinalities by removing a subset of critical nodes. Six known multi-objective evolutionary algorithms are tested and compared. In [LPXC19], a bi-objective variant of the CND problem is studied, where the two conflicting objectives are the minimization of the pairwise connectivity of the induced graph and the cost of removing the critical nodes simultaneously. Two decomposition based multi-objective evolutionary algorithms are modified and improved. In [FOP$^+$19], a multi-objective formulation is proposed to obtain a Pareto frontier that considers different trade-offs between conflicting objectives of the attacker. Then, using the information from the Pareto front two indices are proposed to assess the robustness of a network and to identify the critical nodes. Case studies are reported using as objectives the minimization of the network connectivity, measured in terms of pairwise connectivity, and minimization of the attack total cost. The full defender/attacker approach, where the decision maker perspective is also taken into account, is left for future research.

On one hand, contrary to our work, in [FOP$^+$19, LPXC19], the minimization of the cost is considered as one of the objectives but from the point of view of the attacker (i.e. the cost of removing the critical nodes simultaneously). On the other hand, in our work, the CND problem is only considered as a tool to evaluate the network robustness to multiple node failures. Thus, we consider a standard single-objective formulation to the CND problem, and the second objective of the proposed RNUP is related to the cost of the edges added to the topology to increase its robustness to multiple node failures.

We model the RNUP as a bi-objective problem and provide a path formulation. Based on the proposed path formulation for the RNUP problem, we propose a general procedure to generate all the points belonging to the Pareto frontier that solves two subproblems (an edge selection problem and the CND problem) alternately. To enhance the procedure, we propose an approach that models the selection of edges as a set covering problem. Usually, path formulations are used to ensure connectivity. However, in our case, the computational results will show that the set covering constraints are much more effective in solving the edge selection problem. Two variants are proposed, one based on a row generation approach, where cover inequalities are added on the fly, and another approach where a characterization of the relevant cover inequalities is used to select all the inequalities.

The main computational experiments are conducted on 4 well-known network topologies commonly used in telecommunications [OWPT10]. The results show that using the general procedure can only solve very small size instances. However, using the enhanced procedures, all the tested instances are solved considering sets of $c \in \{2, 3, 4, 5, 6\}$ critical nodes and the complete Pareto frontier is obtained in instances up to $c = 4$ critical nodes. Additional computational tests are conducted on different topologies generated using three well-known graph algorithms: Erdos-Renyi model [ER59], Watts-Strogatz small-world model [WS98] and Barabasi-Albert scale-free model [BA99]. These tests aim at evaluating the impact of the size of the problem instances on the proposed solution procedures.

The original contributions of this work are summarized as follows:

- the RNUP is introduced and modeled as a bi-objective optimization problem using a path formulation;
- an upgrade algorithm is introduced to determine the complete Pareto frontier;
- a cover model is developed for the edge selection subproblem;
- two alternative algorithms based on the cover model are proposed;
- extensive computational results on different topologies and on different sizes are reported, showing the applicability of the solution approaches.

The paper outline is as follows. The RNUP is modeled as a bi-objective problem in Section 3.2. Then, a general approach to obtain the Pareto frontier is introduced in Section 3.3. In Section 3.4, we present two alternative approaches based on enhancements of the general algorithm. Computational results are reported and discussed in Section 3.5. In Section 3.6, we present the main conclusions of the conducted work.

3.2 Robust network upgrade problem

We consider a network represented by a connected undirected graph $G_n = (N, E_n)$ where $N = \{1, ..., n\}$ is the set of nodes and $E_n = \{\{i, j\} \in N \times N : \ i < j\}$ is the set of edges representing all possible edges. Additionally, we denote by $E_0 \subset E_n$ the subset of edges corresponding to the existing edges. For each candidate edge $\{i, j\} \in E_n \setminus E_0$, parameter l_{ij} represents the cost of installing an edge between the two nodes i and j in an upgraded solution.

The robust network upgrade problem (RNUP) consists of installing new edges to increase the robustness of a given network while minimizing the cost with the additional installed edges. We model this problem as a general bi-objective optimization problem in Section 3.2.1 and provide a mixed integer linear programming (MILP) path based formulation in Section 3.2.2.

3.2.1 Bi-objective optimization model

We model the RNUP as a bi-objective problem. The decisions are the new edges to add to the existing network (N, E_0). The objectives are the minimization of the cost of the added edges and the maximization of a robustness metric of the upgraded network.

Initially, we consider, for each candidate edge $\{i, j\} \in E_n \backslash E_0$, the binary decision variable y_{ij} that is 1 if edge $\{i, j\}$ is selected, and 0 otherwise. The proposed RNUP can be modeled as the following bi-objective problem:

$$min \quad L \ := \sum_{\{i,j\} \in E_n \backslash E_0} l_{ij} y_{ij} \tag{3.1}$$

$$max \quad z \ := \ f(E_0 \cup \{\{i, j\} \in E_n \backslash E_0 : y_{ij} = 1\}) \tag{3.2}$$

$$s.t. \quad y_{ij} \in \{0, 1\}, \quad \{i, j\} \in E_n \backslash E_0. \tag{3.3}$$

where $f(E)$ is a robustness metric of the network $G^U = (N, E)$. The first objective (3.1) is to minimize the total cost of the new edges.

In this work, the robustness metric is given by the objective function of the CND problem, that will be denoted by $\mathbf{CND}(E)$, i.e., $f(E) = \mathbf{CND}(E)$. The CND problem identifies a set of c nodes whose removal from G^U minimizes the pairwise connectivity on the remaining graph. So, the second objective (3.2) of the RNUP is to maximize the connectivity of the remaining graph assuming that the c critical nodes are removed.

3.2.2 Bi-objective mixed integer linear formulation

Next, we provide a MILP formulation for the bi-objective problem. Following the classical models to ensure connectivity between pair of nodes (see for instance [SSG12]), we propose a path based formulation where a path links each pair of nodes that have connectivity.

Consider the set $\mathcal{K}$ of all combinations of c nodes from N (i.e., set of all failure scenarios of c nodes). For each $K \in \mathcal{K}$, the binary parameter α_i^K is 1 if and only if node $i \in N$ belongs to the node set K. For each edge $\{i, j\} \in E_n$, we consider two arcs (i, j) and (j, i) obtained from the two possible orientations of the edge. The set of all arcs will be denoted by A.

In addition to variables y_{ij} introduced before, we consider the following two sets of binary decision variables. For each node pair $s, t \in N, s < t$, for each failure scenario $K \in \mathcal{K}$ and for each arc $(i, j) \in A$, variable x_{ij}^{stK} is 1 if arc (i, j) belongs to the path between s and t in the failure scenario K, and 0 otherwise. Additionally, for each node pair $s, t \in N, s < t$ and for each failure scenario $K \in \mathcal{K}$, variable u_{st}^K is 1 if nodes s and t remain connected in the failure scenario K, and 0 otherwise.

For ease of notation, we define variables y_{ij} also for the edge set E_0 which are set to 1. Then, the bi-level problem (3.1)–(3.3) can be defined by the following MILP formulation:

$$
\begin{aligned}
&min \quad L := \sum_{\{i,j\} \in E_n \setminus E_0} l_{ij} y_{ij} && && (3.4)\\
&max \quad z && && (3.5)\\
&s.t. \quad z \leq \sum_{s \in N} \sum_{t \in N, s<t} u_{st}^K, && K \in \mathcal{K}, && (3.6)\\
&\sum_{j \in N:(i,j) \in A} x_{ij}^{stK} + \alpha_i^K \leq 1, && s,t \in N, s<t,\ i \in N,\ K \in \mathcal{K}, && (3.7)\\
&\sum_{j \in N:(j,i) \in A} x_{ji}^{stK} + \alpha_i^K \leq 1, && s,t \in N, s<t,\ i \in N,\ K \in \mathcal{K}, && (3.8)\\
&\sum_{j \in N:(s,j) \in A} x_{sj}^{stK} = u_{st}^K, && s,t \in N, s<t,\ K \in \mathcal{K}, && (3.9)\\
&\sum_{j \in N:(i,j) \in A} x_{ij}^{stK} = \sum_{j \in N:(j,i) \in A} x_{ji}^{stK}, && s,t \in N, s<t,\ i \in N \setminus \{s,t\},\ K \in \mathcal{K}, && (3.10)\\
&\sum_{j \in N:(j,t) \in A} x_{jt}^{stK} = u_{st}^K, && s,t \in N, s<t,\ K \in \mathcal{K}, && (3.11)\\
&\sum_{j \in N:(j,s) \in A} x_{js}^{stK} = 0, && s,t \in N, s<t,\ K \in \mathcal{K}, && (3.12)\\
&x_{ij}^{stK} \leq y_{\{ij\}}, && s,t \in N, s<t,\ (i,j) \in A,\ K \in \mathcal{K}, && (3.13)\\
&y_{ij} = 1, && \{i,j\} \in E_0, && (3.14)\\
&y_{ij} \in \{0,1\}, && \{i,j\} \in E_n \setminus E_0, && (3.15)\\
&x_{ij}^{stK} \in \{0,1\}, && s,t \in N, s<t,\ (i,j) \in A,\ K \in \mathcal{K}, && (3.16)\\
&u_{st}^K \in \{0,1\}, && s,t \in N, s<t,\ K \in \mathcal{K}, && (3.17)\\
&z \geq 0. && && (3.18)
\end{aligned}
$$

Again, the objective (3.4) is to minimize the total cost L of the new edges. Then, the objective (3.5) is to maximize the robustness z of the upgraded topology. Constraints (3.6) guarantee that z is at most the pairwise connectivity of the remaining graph after each set K of critical nodes is removed. Thus, they ensure that variable z cannot exceed the robustness value of any failure scenario $K \in \mathcal{K}$. Combined with objective (3.5), which maximizes z, in an optimal solution, this upper bound is attained.

Constraints (3.7)–(3.8) ensure that arc (i, j) does not belong to any path if either nodes i or j are critical in each failure scenario $K \in \mathcal{K}$. Constraints (3.9)–(3.11) represent the flow conservation constraints if nodes s and t remain connected in the failure scenario $K \in \mathcal{K}$. Additionally, constraints (3.12) ensure that there will be no flow entering the source node s in the flow conservation constraints, i.e., removing the possibility of cycles.

Notation $y_{\{ij\}}$ represents decision variable y_{ij} if $i < j$, and variable y_{ji} otherwise, and then, constraints (3.13) guarantee that if either arc (i, j) or (j, i), with $i < j$, is used for any path in any failure scenario, then the edge $\{i, j\}$ must exist in the upgraded topology (i.e., $y_{ij} = 1$). Finally, constraints (3.14)–(3.18) are the variable domain constraints. Notice that this formulation assumes that edges from the original topology belong to the upgraded topology (i.e., $y_{ij} = 1$ for all $\{i, j\} \in E_0$).

We can observe that this formulation depends on the cardinality of $\mathcal{K}$ which increases exponentially as a function of the number of nodes if c is large. However, for small values of c, the size of $\mathcal{K}$ is small. Notice additionally that for each $K \in \mathcal{K}$, the resulting formulation is compact.

3.3 Solution approach: finding the Pareto frontier

When dealing with bi-objective problems, the most relevant information from the decision maker's point of view is to know the Pareto frontier allowing to compare the cost of a network upgrade with the gains in the given robustness metric. The proposed algorithms are designed to derive all the non-dominated solution pairs (L, z) in the Pareto frontier, where L is the cost of the added edges and z is the robustness value.

First, in Section 3.3.1, we present a general algorithm to obtain the Pareto frontier which uses two optimization problems, one for computing the robustness value of a topology (solving a CND problem) and another for selecting a set of edges for the upgraded topology, denoted as the Edge Selection Problem (ESP). An Integer Linear Programming (ILP) formulation for the CND problem is given in Section 3.3.2 and a path formulation for the ESP is given in Section 3.3.3.

3.3.1 A general algorithm for the RNUP

Here, we present a general algorithm that generates a set of pairs (L_s, z_s) that includes all the Pareto optimal solutions of the RNUP. The iterative algorithm considers the graph $G = (N, E_0)$ and starts with the trivial pair $(L_1, z_1) = (0, \mathbf{CND}(E_0))$ belonging to the Pareto frontier. In each iteration, a new pair (L_s, z_s) is obtained that strictly increases the value of z. The iterative step stops when the CND value of the upgraded topology (z_s) is maximal, i.e., when $z_s = \binom{n-c}{2}$. The full description of the algorithm is given in Algorithm 3.1.

This algorithm computes the CND value in Steps 3 and 7 and solves the ESP in Step 6. These two problems are solved using ILP formulations which are described in the following sections.

Algorithm 3.1 General upgrade algorithm

```
Input: $G = (N, E_0)$, $c \in \{1, \dots, |N|\}$
$s \leftarrow 1$
$(L_s, z_s) \leftarrow (0, \mathbf{CND}(E_0))$
while $z_s < \binom{n-c}{2}$ do
    $s \leftarrow s + 1$
    Compute set of edges $E' \subseteq E_n \backslash E_0$ such that $L_s \leftarrow \sum_{\{i,j\} \in E'} l_{ij}$ is minimized and $\mathbf{CND}(E_0 \cup E') > z_{s-1}$
    $z_s \leftarrow \mathbf{CND}(E_0 \cup E')$
end while
```

3.3.2 Critical node detection MILP formulation

Several MILP formulations have been proposed for the CND problem (see [ACEP09] and the more recent papers discussing formulations enhancements [Pav18, SdSM18]). Here, we consider the MILP formulation introduced in [SdSM18].

Aiming to minimize the pairwise connectivity of the graph without c critical nodes, consider the following two sets of decision variables: for each node $t \in N$, variable v_t is 1 if t is a critical node, and 0 otherwise; and for each node pair $s, t \in N, s < t$, variable u_{st} is 1 if nodes s and t remain connected (i.e., if exists a feasible path connecting end-nodes s and t) in graph $G^U = (N, E)$ after the removal of the critical nodes, and 0 otherwise. Additionally, for all $s, t \in N$ (with $s \neq t$), the notation $u_{\{st\}}$ represents the decision variable u_{st} if $s < t$, and variable u_{ts} otherwise.

Moreover, for each node pair $s, t \in N, s < t$, consider that the set $N_E^{st} \subseteq N$ represents the set of adjacent nodes to s, on graph $G^U = (N, E)$, if the node degree of s is not higher than the node degree of t, and the set of adjacent nodes to t otherwise.

Then, for a given number $c \in \{1, \dots, |N|\}$ of critical nodes, a compact formulation for the CND problem is given by the following MILP formulation:

$$min \quad z := \sum_{s,t \in N, s<t} u_{st} \tag{3.19}$$

$$s.t. \quad \sum_{t \in N} v_t = c, \tag{3.20}$$

$$u_{st} + v_s + v_t \geq 1, \qquad s, t \in N, s < t, \{s, t\} \in E, \tag{3.21}$$

$$u_{st} \geq u_{\{sk\}} + u_{\{tk\}} - 1 + v_k, \quad s, t \in N, s < t, \{s, t\} \notin E, \; k \in N_E^{st}, \tag{3.22}$$

$$v_t \in \{0, 1\}, \qquad t \in N, \tag{3.23}$$

$$u_{st} \in \{0, 1\}, \qquad s, t \in N, s < t. \tag{3.24}$$

The objective (3.19) is to minimize the pairwise connectivity, i.e., the total number of node pairs that have connectivity in the remaining graph $(N \backslash K, E^K)$, with $E^K = \{\{i, j\} \in E : i, j \notin K\}$ and where $K = \{i \in N : v_i^* = 1\}$ is the set of critical nodes. Constraint (3.20) ensures that exactly c nodes of N are selected as critical nodes.

Constraints (3.21) guarantee that a pair of adjacent nodes in graph $G^U = (N, E)$ is connected if none of the end-nodes is a critical node. Constraints (3.22) represent a generalization of constraints (3.21) for each pair of nodes s and t that are not adjacent, and guarantee that those nodes are connected if there is a non-critical node $k \in N_E^{st}$ connected to both s and t.

Constraints (3.23)-(3.24) are the variable domain constraints. As noted in [SdSM18], constraints (3.24) can be replaced by $u_{st} \geq 0$, reducing the number of binary variables. Henceforward, the optimal value z^* of this MILP problem will be represented by $\mathbf{CND}(E)$.

3.3.3 A path formulation for the ESP

Next, we consider the optimization problem defined in Step 6 of Algorithm 3.1. This optimization problem seeks a set of edges with the minimum cost that provides a CND value greater than a given threshold r (where, in Step 6, $r = z_{s-1}$).

We denote this problem by $\mathbf{ESP}(r)$ which can be modeled as an ILP path based formulation as follows:

$$\begin{aligned} min \quad & \sum_{\{i,j\} \in E_n \backslash E_0} l_{ij} y_{ij} && (3.25) \\ s.t. \quad & \sum_{\{s,t\} \in E_n} u_{st}^K \ \geq \ r+1, \ K \in \mathcal{K}, && (3.26) \\ & (y, x, u) \text{ satisfies (3.7)–(3.17).} \end{aligned}$$

Notice that, as the CND value must be integer and it must be greater than the threshold r, the right-hand side of (3.26) is $r+1$. The set of edges $E' = \{\{i,j\} \in E_n \backslash E_0 : y_{ij}^* = 1\}$ is the optimal solution of $\mathbf{ESP}(r)$ and $G^U = (N, E_0 \cup E')$ denotes the upgraded topology.

Theorem 3.3.1. *The pairs $(L_1, z_1), \ldots, (L_S, z_S)$ generated by Algorithm 3.1 include all the Pareto optimal solutions to the bi-objective optimization problem* (3.1)–(3.3)*.*

Proof. Let (L, z) be a Pareto optimal solution not generated by Algorithm 3.1.

Suppose that $L_s < L < L_{s+1}$, for some $s \in \{1, \ldots, S\}$. From Step 6, L_{s+1} is the optimal value of the subproblem $\mathbf{ESP}(z_s)$. Then, for each $E \subseteq E_n$, with $E_0 \subseteq E$, such that $\sum_{\{i,j\} \in E \backslash E_0} l_{ij} \leq L < L_{s+1}$, we have $z \leq z_s$. Thus, (L, z) is dominated by (L_s, z_s), which contradicts the assumption that (L, z) is a Pareto optimal solution.

Suppose $L = L_s$ for some $s \in \{1, \ldots, S\}$. If $z < z_s$, then (L, z) is dominated by (z_s, L_s) which contradict the assumption that (L, z) is a Pareto optimal solution. Consider now the case $z > z_s$. We may assume $L_{s+1} > L$, otherwise we could iteratively replace s by $s+1$ until the desirable condition $L_{s+1} > L$ is verified. Thus, at Step 6, L_{s+1} is the optimal value of the subproblem $\mathbf{ESP}(z_s)$ which contradicts $z \geq z_s + 1$ and $L < L_{s+1}$. Hence, the unique possible case is $z = z_s$. Then, (L, z) must coincide with (L_s, z_s) for some $s \in \{1, \ldots, S\}$, which shows that all the Pareto optimal solutions are generated by Algorithm 3.1. □

Although all the Pareto optimal solutions are generated with Algorithm 3.1, some of the solutions obtained with the algorithm may be dominated. Figure 3.1 presents such an example where solutions (b) and (c) are alternative optimal solutions to $\mathbf{ESP}(2)$ assuming that the cost parameters l_{ij} correspond to the Euclidean distance between nodes i and j. However, solution (b) is dominated by solution (c). Hence, if Algorithm 3.1 obtains (b) before (c), a dominated solution is generated.

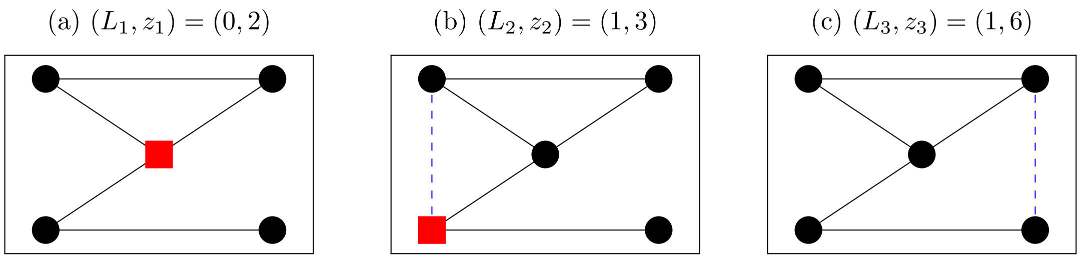

(a) $(L_1, z_1) = (0, 2)$ (b) $(L_2, z_2) = (1, 3)$ (c) $(L_3, z_3) = (1, 6)$

Figure 3.1: Example where solution (b) is dominated by solution (c) for $c = 1$ critical node and with $l_{ij} = 1$ in both selected new edges (critical node in a red square and selected edge in dashed blue).

The next result allows to identify all the dominated solutions generated by Algorithm 3.1.

Proposition 3.3.2. *A pair (L_s, z_s) generated by Algorithm 3.1 is dominated if and only if $z_s < z_{s+1}$ and $L_s = L_{s+1}$.*

Proof. Suppose that (L_s, z_s) is not a Pareto optimal solution. Since the robustness value is strictly increasing from each iteration to the next, the condition $z_s < z_{s+1}$ is straightforward.

Given that L_s and L_{s+1} are both the minimal objective function values of (3.25) for the thresholds z_s and z_{s+1}, respectively, we have that $L_s \leq L_{s+1}$. Suppose that $L_s < L_{s+1}$. Then, $L_{s-1} \leq L_s < L_{s+1}$ and $z_{s-1} < z_s < z_{s+1}$, which contradicts the assumption of (L_s, z_s) not being a Pareto optimal solution. Thus, $L_s = L_{s+1}$.

The converse implication is straightforward by definition of a Pareto optimal solution. □

Remark 3.3.3. Although it is theoretically possible to obtain a solution that is not a Pareto optimal solution, in all instances where the cost l_{ij} of new links is related with the distance between the nodes $i, j \in N$, none of the tested algorithms computed such a dominated solution. This shows how rare those dominated solutions are in real-world topologies when compared to academic scenarios like the one presented in Figure 3.1. Moreover, as checking if a solution is dominated can easily be done in linear time, we omit the step of verifying if a solution is dominated in all the algorithms presented in this paper.

3.4 Covering approach to the network upgrade problem

The path formulation for the **ESP**(r) presented in the previous section has the advantage of being a compact model for each set of critical nodes K. Nevertheless, it includes many variables, which implies to solve large size models in each iteration of Algorithm 3.1. As a consequence, the computational results will show (in Section 3.5.1) that it is only able to compute optimal Pareto solutions for a very limited range of instances. In order to use Algorithm 3.1 to obtain Pareto frontiers for larger instances, a different approach must be considered to optimally solve the RNUP.

In this section, we introduce an alternative ILP model to $\mathbf{ESP}(r)$. This model results from transforming the ESP into a set covering problem (see for instance [Chv79]) and will be called henceforward the *Cover* model. As will be described next, the Cover model has the advantage of having a small number of variables, but it has the disadvantage of including much more constraints (the cover inequalities). In order to use the Cover model efficiently, we need to address the issue of managing these constraints efficiently.

Next, we first define the Cover model (Section 3.4.1). Then, we introduce the general algorithm based on the Cover model (Section 3.4.2). Finally, we present two algorithms based on two different strategies to generate the cover inequalities: a row generation algorithm (Section 3.4.3) and an algorithm based on the partition of the network into components (Section 3.4.4). The advantages of using this alternative model will be discussed later.

3.4.1 Cover model for network upgrade

In order to define the Cover model, first we must introduce some notation. Given a set of edges E and a set of critical nodes $K \subset N$, consider the remaining graph $G_K^E = (N \backslash K, E^K)$, with $E^K = \{\{i,j\} \in E : i,j \notin K\}$. Let z_K^E be the robustness value of this graph, i.e., the total number of node pairs that have connectivity in graph G_K^E.

Moreover, consider the set of edges of an auxiliary graph $(N \backslash K, \overline{E}^K)$ where two nodes are adjacent if and only if they belong to the same connected component in graph G_K^E, i.e., $\overline{E}^K = \{\{i,j\} \in E_n : i,j \in N \backslash K$ have connectivity in $G_K^E\}$.

We are interested in those edges that link different connected components in G_K^E, in order to increase the robustness of the upgraded network. Given the introduced notation, we now consider the set:

$$\gamma_K^E \;:=\; \{\{i,j\} \in E_n : \; i,j \notin K \text{ and } \{i,j\} \notin \overline{E}^K\} \tag{3.27}$$

which corresponds to the set of candidate edges $\{i,j\} \in E_n$ such that nodes i and j have no connectivity in the remaining graph G_K^E.

Additionally, for a given threshold r for the robustness value, we define the family of sets of candidate edges $\Gamma(r)$ as follows:

$$\Gamma(r) \;:=\; \{\gamma_K^E : \; E \subset E_n, \text{ with } E_0 \subseteq E, \text{ and } K \in \mathcal{K} \text{ such that } z_K^E \leq r\}. \tag{3.28}$$

The family $\Gamma(r)$ considers all the topologies G_K^E resulting from a simultaneous failure of the nodes in K, whose robustness value does not exceed the threshold r. Thus, in order to increase the robustness of this topology, at least one additional edge from each of these γ_K^E sets must be added.

Using this observation, we define a set covering problem, denoted by $\mathbf{Cover}(\Gamma(r))$, which includes one cover constraint for each set of candidate edges $\gamma_K^E \in \Gamma(r)$ such that $z_K^E \leq r$:

$$min \quad \sum_{\{i,j\} \in E_n \backslash E_0} l_{ij} y_{ij} \tag{3.29}$$

$$s.t. \quad \sum_{\{i,j\} \in \gamma_K^E} y_{ij} \geq 1, \; \gamma_K^E \in \Gamma(r), \tag{3.30}$$

$$y_{ij} \in \{0,1\}, \qquad \{i,j\} \in E_n \backslash E_0. \tag{3.31}$$

The objective (3.29) is to minimize the total cost of the selected candidate edges to add to the current topology (N, E_0). For a given threshold r, constraints (3.30) are the cover inequalities for each set of edges $E \subset E_n$, with $E_0 \subseteq E$ (i.e., for each upgraded graph), and for each critical node set $K \in \mathcal{K}$ such that $z_K^E \leq r$. These cover inequalities cut off all infeasible solutions based on the remaining edge set E^K, i.e., a solution with $y_{ij} = 1$, if $(i,j) \in \gamma_K^E$, and $y_{ij} = 0$ otherwise (see Proposition 3.4.1 below). Finally, constraints (3.31) are the variable domain constraints.

Proposition 3.4.1. *Given $E \subset E_n$ and $K \in \mathcal{K}$, the incidence vector $\overline{y}$ of the remaining graph G_K^E, i.e., $\overline{y}_{ij} = 1$, for $\{i,j\} \in E^K$ and $\overline{y}_{ij} = 0$, for $\{i,j\} \in E_n \setminus E^K$, is violated by the cover inequality* (3.30) *defined for γ_E^K.*

Proof. If $\{i,j\} \in E^K$, then $\{i,j\} \notin \gamma_K^E$, since $E^K \subseteq \overline{E}^K$. Thus, $\overline{y}_{ij} = 0$ for all $\{i,j\} \in \gamma_K^E$, which implies that constraint (3.30) is violated by $\overline{y}$. □

The next result illustrates how the Cover ILP model (3.29)–(3.31) can be used to optimally solve Step 6 of Algorithm 3.1.

Theorem 3.4.2. *Let y^* be the optimal solution of* **Cover**$(\Gamma(z_{s-1}))$ *for a robustness value z_{s-1}. Then $z_s > z_{s-1}$, where $z_s =$* **CND**$(E_0 \cup \{\{i,j\} \in E_n \backslash E_0 : y^*_{ij} = 1\})$.

Proof. Suppose that $z_s \leq z_{s-1}$. Given $K = \{i \in N : v_i^* = 1\}$, then as $z_s \leq z_{s-1}$, it follows that $\gamma_K^{E_0 \cup E'} \in \Gamma(z_{s-1})$, where $E' = \{\{i,j\} \in E_n \backslash E_0 : y^*_{ij} = 1\})$. Setting $E = E_0 \cup E'$, and considering $\overline{y}_{ij} = 1$ for $\{i,j\} \in E_0$ and $\overline{y}_{ij} = y^*_{ij}$ for $\{i,j\} \in E_n \backslash E_0$, then by Proposition 3.4.1, the cover inequality $\sum_{\{i,j\} \in \gamma_K^E} y_{ij} \geq 1$ is violated. This contradicts the assumption that y^* is a feasible solution of **Cover**$(\Gamma(z_{s-1}))$. □

3.4.2 Cover-based upgrade algorithm

Here, we propose Algorithm 3.2 that uses the proposed Cover model to obtain the Pareto optimal solutions, i.e., in each iteration of the algorithm, a candidate solution (L_s, z_s) is computed.

Algorithm 3.2 Cover-based upgrade algorithm

```
1: Input: $G = (N, E_0)$, $c \in \{1, \dots, |N|\}$
2: $s \leftarrow 1$
3: $(L_s, z_s) \leftarrow (0, \mathbf{CND}(E_0))$
4: while $z_s < \binom{n-c}{2}$ do
5:     $s \leftarrow s + 1$
6:     $y^* \leftarrow$ optimal solution to $\mathbf{Cover}(\Gamma(z_{s-1}))$
7:     $L_s \leftarrow \sum_{\{i,j\} \in E_n \backslash E_0} l_{ij} y^*_{ij}$
8:     $z_s \leftarrow \mathbf{CND}(E_0 \cup \{\{i,j\} \in E_n \backslash E_0 : y^*_{ij} = 1\})$
9: end while
```

As input to the algorithm, we are given the network topology $G = (N, E_0)$ to be upgraded and the number of critical nodes $c \in \{1, \dots, |N|\}$. The algorithm starts by solving the CND problem for the original topology (Line 3) and by assigning the first (trivial) Pareto solution.

The main loop (Lines 4-9) stops when z_s reaches the upper bound of the problem, i.e., when the CND value of the upgraded topology is maximal. First, we increase the current index solution s. Then, the Cover model is optimized for the family of cover constraints $\Gamma(z_{s-1})$, i.e., with the threshold of the previous candidate solution z_{s-1}. Finally, the CND of the upgraded topology $(N, E_0 \cup E')$ is computed, where E' is the minimal cost of the corresponding upgraded topology.

Theorem 3.4.3. *The pairs* $(L_1, z_1), ..., (L_S, z_S)$ *generated by Algorithm 3.2 include all the Pareto optimal solutions of the bi-objective optimization problem* (3.1)–(3.3).

Proof. In order to prove that Algorithm 3.2 includes all the Pareto optimal solutions, using Theorem 3.3.1, it suffices to show that this algorithm generates the same points of Algorithm 3.1. Notice that Algorithm 3.2 is obtained by replacing Line 6 of Algorithm 3.1 with Lines 6-7. In each iteration of Algorithm 3.2, the Cover problem is solved allowing to obtain the minimum cost set of candidate edges with value L_s such that, by Theorem 3.4.2, $z_s = \mathbf{CND}(E_0 \cup \{\{i,j\} \in E_n \backslash E_0 : y^*_{ij} = 1\}) > z_{s-1}$. Therefore, both algorithms generate the same solutions. □

In contrast to the path formulation for the ESP, which is compact for a set K, the number of cover inequalities (3.30) increases exponentially with the size of the graph and leads to large size models that hardly can be solved to optimality even for relatively small instances. The main challenge is to devise approaches that use a small number of cover constraints to obtain the Pareto frontier. We address this challenge in two distinct ways: by using a row generation technique and by splitting the set of different topologies into equivalence classes and generate a cover constraint for each class.

3.4.3 Row generation approach

Here, we propose a row generation algorithm, where the family of inequalities (3.30) is initially ignored. In each iteration, the relaxed model is solved and an upgraded solution with edge set E is obtained. For a given threshold r, if $z^E_K \leq r$ for some $K \in \mathcal{K}$, then a new cut for the edge set γ^E_K is added. This procedure is described in Algorithm 3.3.

Similarly to Algorithm 3.2, the input is the original network topology $G = (N, E_0)$ and the number of critical nodes c. The algorithm starts by solving the CND problem for this topology and by assigning the initial Pareto optimal solution (Lines 3-4). Additionally, the family Γ of edge sets corresponding to the active cover constraints (3.30) is initialized (Line 5) with the set of candidate edges $\gamma^{E_0}_K$, where K is the set of critical nodes of the input graph.

The main loop (Lines 6-17) ensures that the algorithm stops when z_s reaches the upper bound. In each loop iteration, a new candidate solution (L_s, z_s) is generated.

The row generation phase is considered in the loop defined by Lines 8-15. The Cover model is optimized for the family of cover constraints Γ (Lines 9-10) and the CND of the current upgraded topology $(N, E_0 \cup E')$ is computed (Lines 12-13). Then, based on the optimal solutions of these two optimization problems, the cover cut set $\gamma^{E_0 \cup E'}_K$ is added to family Γ (Line 14). This process is repeated until the robustness value z^* of upgraded topology is higher than the robustness value of the previous solution z_{s-1}. When this happens, the next candidate solution (L_s, z_s) is assigned to the current solution (Line 16).

Algorithm 3.3 Row generation

```
**Input**: $G = (N, E_0)$, $c \in \{1, \dots, |N|\}$
$s \leftarrow 1$
$(L_s, z_s) \leftarrow (0, \mathbf{CND}(E_0))$
$v^* \leftarrow$ optimal solution to $\mathbf{CND}(E_0)$
$\Gamma \leftarrow \{\gamma_K^{E_0}\}$, where $K = \{i \in N : v_i^* = 1\}$
**while** $z_s < \binom{n-c}{2}$ **do**
    $s \leftarrow s + 1$
    **repeat**
        $y^* \leftarrow$ optimal solution to $\mathbf{Cover}(\Gamma)$
        $L_s \leftarrow \sum_{\{i,j\} \in E_n \backslash E_0} l_{ij} y_{ij}^*$
        $E' \leftarrow \{\{i, j\} \in E_n \backslash E_0 : y_{ij}^* = 1\}$
        $z^* \leftarrow \mathbf{CND}(E_0 \cup E')$
        $v^* \leftarrow$ optimal solution to $\mathbf{CND}(E_0 \cup E')$
        $\Gamma \leftarrow \Gamma \cup \{\gamma_K^{E_0 \cup E'}\}$, where $K = \{i \in N : v_i^* = 1\}$
    **until** $z^* > z_{s-1}$
    $(L_s, z_s) \leftarrow (L^*, z^*)$
**end while**
```

3.4.4 Cover inequalities from partitions of the set of nodes

Given a set of critical nodes $K \in \mathcal{K}$, the family of edge sets forms an equivalence class where two sets $E_1^K, E_2^K \subset E_n$ belong to the same class if and only if $\overline{E}_1^K = \overline{E}_2^K$, i.e., graphs $G_{E_1}^K = (N \backslash K, E_1^K)$ and $G_{E_2}^K = (N \backslash K, E_2^K)$ have the same connected components. Each set E^K is represented by the set $\overline{E}^K$. Figure 3.2 illustrates this concept.

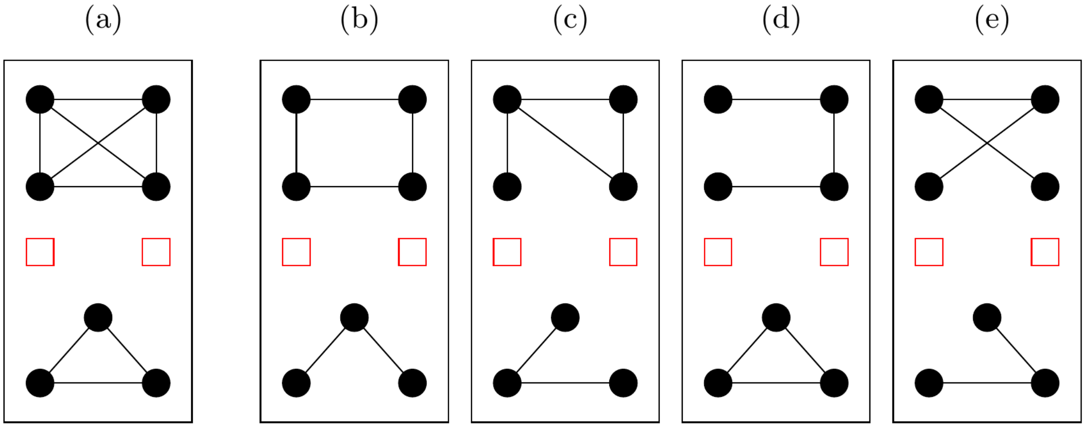


Figure 3.2: All the edge sets of the remaining graphs represented in the figure belong to the same class. This class is represented by the set of edges from the graph represented in (a).

Hence, if E_1^K, E_2^K belong to the same class, i.e., $\overline{E}_1^K = \overline{E}_2^K$, then $\gamma_K^{E_1} = \gamma_K^{E_2}$. Consequently, the cover inequality (3.30) is the same for all the topologies belonging to the same class and, in particular, for the topology where each component forms a clique. Thus, the inequality (3.30) can alternatively be defined from the node set partition corresponding to the topology.

Therefore, in order to compute the family of cover inequalities (3.30) for a given threshold r (and for each set of critical nodes $K \in \mathcal{K}$), we need to consider all the partitions of the node set $N \setminus K$ that take into account the existing edge set E_0 and whose robustness value is not higher than the threshold r. The next Example 1 illustrates how the robustness value of each partition is calculated.

Notice that, in general, the robustness value of any topology (and, by consequence, any components partition) has the format $z = \sum_{i=1}^{m} \binom{n_i}{2}$ with $\sum_{i=1}^{m} n_i = n - c$, where m represents the number of components in the remaining graph and each n_i represent the number of nodes of component i, with $i \in \{1, ..., m\}$. This is a particular property of the CND variant used in this work which considers the minimization of the pairwise connectivity.

Example 1: Given a node set $K \in \mathcal{K}$, suppose that the remaining graph $G_{E_0}^{K}$ has three connected components, i.e., $N \backslash K = C_1 \cup C_2 \cup C_3$, with $C_1, C_2, C_3 \subset N$ such that $C_1 \cap C_2 = C_1 \cap C_3 = C_2 \cap C_3 = \emptyset$. Additionally, $n_i = |C_i|$, for each $i \in \{1, 2, 3\}$. Thus, $n_1 + n_2 + n_3 = n - c$. The robustness values for the partitions with three and two components are given as follows:

- $z(C_1, C_2, C_3) = \binom{n_1}{2} + \binom{n_2}{2} + \binom{n_3}{2} = z_K^{E_0}$, corresponding to partition $\{C_1\}$, $\{C_2\}$, $\{C_3\}$;
- $z(C_1 \cup C_2, C_3) = \binom{n_1+n_2}{2} + \binom{n_3}{2}$, corresponding to partition $\{C_1 \cup C_2\}$, $\{C_3\}$;
- $z(C_1 \cup C_3, C_2) = \binom{n_1+n_3}{2} + \binom{n_2}{2}$, corresponding to partition $\{C_1 \cup C_3\}$, $\{C_2\}$;
- $z(C_1, C_2 \cup C_3) = \binom{n_1}{2} + \binom{n_2+n_3}{2}$, corresponding to partition $\{C_1\}$, $\{C_2 \cup C_3\}$.

Let $\mathcal{P}_{E_0}^{K}$ represent the set of all partitions of $N \setminus K$ such that two nodes connected by an edge in E_0 must belong to the same set. Associated to each partition $p \in \mathcal{P}_{E_0}^{K}$, we consider γ_p as the set of edges connecting pairs of nodes belonging to different sets in p and z_p its corresponding robustness value. The algorithm based on the set of components partitions is described in Algorithm 3.4.

Algorithm 3.4 Components separation

```
 1: Input: $G = (N, E_0)$ and $c \in \{1, \dots, |N|\}$
 2: $\mathcal{K}_0 \leftarrow \{K \in \mathcal{K} : z_{E_0}^{K} < \binom{n-c}{2}\}$
 3: $s \leftarrow 1$
 4: $(L_s, z_s) \leftarrow (0, \min\{z_{E_0}^{K} : K \in \mathcal{K}_0\})$
 5: while $z_s < \binom{n-c}{2}$ do
 6:     $s \leftarrow s + 1$
 7:     $\Gamma \leftarrow \{\gamma_p : p \in \mathcal{P}_{E_0}^{K}$ and $K \in \mathcal{K}_0$ such that $z_p \leq z_{s-1}\}$
 8:     $L_s \leftarrow \mathbf{Cover}(\Gamma)$
 9:     $y^* \leftarrow$ optimal solution to $\mathbf{Cover}(\Gamma)$
10:     $z_s \leftarrow \mathbf{CND}(E_0 \cup \{\{i, j\} \in E_n \backslash E_0 : y_{ij}^* = 1\})$
11: end while
```

Algorithm 3.4 is an extension of Algorithm 3.2 where the family of sets of edges Γ used to define the cover inequalities is computed in Line 7. In order to obtain this family Γ, initially, we need to compute every critical node set $K \in \mathcal{K}$ such that the remaining graph $G_{E_0}^{K}$ has multiple components (Line 2). Then, for each set $K \in \mathcal{K}_0$, the corresponding set of partitions $\mathcal{P}_{E_0}^K$ is defined. The family Γ is computed by including each partition p such that its robustness value z_p is not higher than the current threshold z_{s-1} (Line 7).

3.5 Computational results

All the computational tests reported in this section were obtained using the optimization software *Gurobi Optimizer* version 9.0.0, with programming language *Julia* version 1.4.1, running on a PC with an Intel Core i7-8700, 3.2 GHz and 16 GB RAM.

The main computational results are based on four telecommunication network topologies shown in Figure 3.3: Janos-US, Cost266, Germany50 and Coronet. The information of their nodes (and their geographical locations) and edges is publicly available information [OWPT10, Sim14].

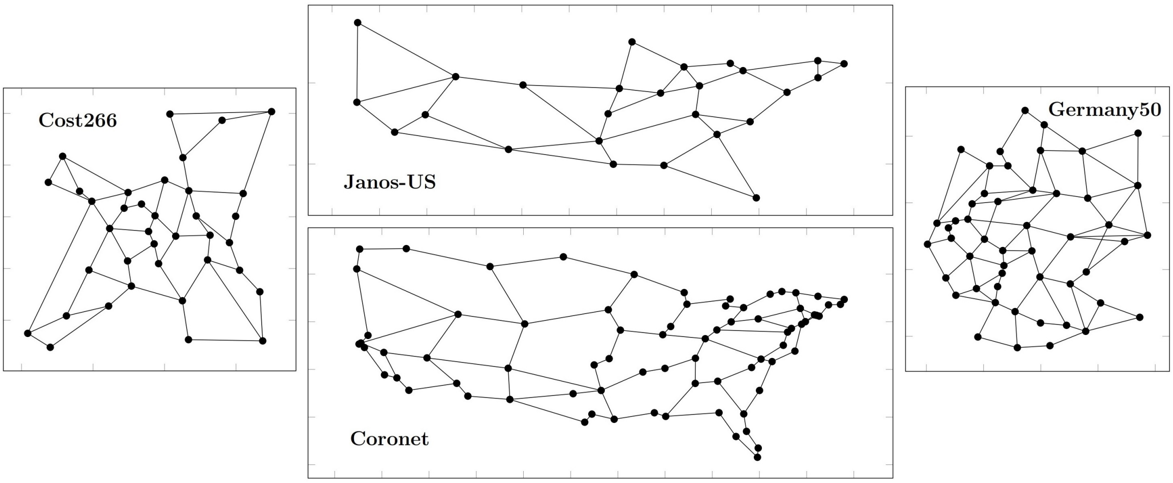


Figure 3.3: Network topologies.

In practice, the cost of a new edge between two given nodes in a telecommunication network requires the determination of the geographical route where the new edge is installed and this information is not available. However, there is a strong correlation between the distance between two network nodes and the cost of installing a new link connecting them and, thus, we assume that the cost l_{ij} of installing an edge between the two nodes i and j is given by the length (in kilometers) of the shortest path over the surface of a sphere representing Earth. Table 3.1 gives, for each network, the following topology characteristics: number of nodes $|N|$ and edges $|E_0|$ in the existing topologies, average node degree $\bar{\delta}$, total edge length of the original topology $L_0 = \sum_{(i,j)\in E_0} l_{ij}$, in kilometers, and average edge length $\bar{l}$. In addition, column '$|E_n \backslash E_0|$' represents the total number of candidate edges, i.e., the total number of binary variables y_{ij} in the proposed optimization models.

The remaining of this section is organized as follows. First, we report the results of the tests conducted with Algorithm 3.1 using formulation **ESP**(.) (Section 3.5.1) and show that only the smallest instance is solved with a runtime limit of 2 hours. Second, we compare the two algorithms based on the Cover model and provide numerical results based on the four network topologies previously presented (Section 3.5.2). Then, we provide some additional

Table 3.1: Topology characteristics of each network.

Network	$\lvert N\rvert$	$\lvert E_0\rvert$	$\bar{\delta}$	L_0	$\bar{l}$	$\lvert E_n\backslash E_0\rvert$
Janos-US	26	42	3.23	25224	600.6	283
Cost266	37	57	3.08	24970	438.1	609
Germany50	50	88	3.52	8859	100.7	1137
Coronet	75	99	2.64	32642	329.7	3729

insights on the Pareto frontier and on the performance of the two algorithms (Section 3.5.3). Finally, we test the proposed methodology on other well-known topologies in order to assess the scalability of both algorithms on larger graphs (Section 3.5.4), and analyze the effect of increasing the number of edges of the input topology (Section 3.5.5).

3.5.1 Testing Algorithm 3.1 using the path formulation ESP(.)

Table 3.2 presents the results for the Janos-US topology, with $c = 2$ critical nodes, obtained with Algorithm 3.1 where the selection of the edges is made by solving model **ESP**(.), as described in Section 3.3. This instance is the easiest one among all the instances reported in this paper.

Table 3.2: Results of Algorithm 3.1 using the **ESP**(.) model, considering Janos-US with $c = 2$.

L	z	$\lvert\mathcal{K}\rvert$	Rows (pre)	Rows (pos)	Total Runtime
0	181	0	-	-	0:00:01
1475	196	1	236968	172262	0:00:27
2357	213	3	710820	517198	0:02:36
2470	232	4	947746	688377	0:05:56
3940	253	8	1895450	1376043	0:26:18
4257	276	13	3080080	2235219	0:59:04

Columns 'L' and 'z' represent the respective values of all the Pareto optimal solutions for this instance. Column '$\lvert\mathcal{K}\rvert$' denotes the number of critical node sets that need to be considered to obtain each Pareto optimal solution (L, z). Notice that there is no need to define constraints for scenario failures $K \in \mathcal{K}$ whose robustness value in the original graph $z_K^{E_0}$ is higher than the current threshold since these constraints are guaranteed by the original topology itself. Columns 'Rows (pre)' and 'Rows (pos)' represent the total number of constraints in the path formulation **ESP**(.), before and after the preprocessing phase performed by the solver with the default options, respectively. Finally, column 'Total Runtime' gives the accumulated computational time (in the format H:MM:SS).

These results show that the **ESP**(.) models solved in each iteration have a large number of active constraints. Consequently, Algorithm 3.1 took about 1 hour to compute the Pareto frontier of this instance while the best proposed algorithm solves this instance in a second (results reported next). Moreover, this was the unique instance solved to optimality using the path formulation **ESP**(.) with the runtime limit of two hours. Henceforward, we will not report additional results using this model.

3.5.2 Row generation algorithm vs components separation algorithm

In order to compare the performance of Algorithm 3.3 (row generation algorithm) with Algorithm 3.4 (components separation algorithm), Table 3.3 presents detailed results of running both algorithms considering the Germany50 topology with $c = 4$ critical nodes.

Table 3.3: Comparison between algorithms, considering Germany50 topology with $c = 4$ critical nodes.

		Algorithm 3.3			Algorithm 3.4		
L	z	no. ILPs	Rows	Runtime	no. ILPs	Rows	Runtime
0	640	-	-	0:00:01	-	-	0:00:05
54	650	1	1	0:00:01	1	1	0:00:01
125	675	2	3	0:00:02	1	4	0:00:01
219	702	9	12	0:00:08	1	44	0:00:02
244	731	3	15	0:00:03	1	93	0:00:02
288	762	3	18	0:00:03	1	106	0:00:02
407	795	3	21	0:00:05	1	117	0:00:03
545	830	15	36	0:00:31	1	169	0:00:03
673	864	5	41	0:00:16	1	204	0:00:04
723	867	4	45	0:00:11	1	227	0:00:04
900	904	14	59	0:00:47	1	305	0:00:06
941	906	5	64	0:00:23	1	393	0:00:07
1294	946	38	102	0:02:36	1	714	0:00:08
1442	947	23	125	0:02:07	1	910	0:00:11
2104	990	93	218	0:14:16	1	3641	0:00:43
4781	1035	500	718	1:53:01	1	15155	0:02:09

Once again, columns 'L' and 'z' represent the respective values of all Pareto optimal solutions for this instance. For each algorithm, column 'no. ILPs' represents the number of times that the Cover model was optimized to obtain each Pareto optimal solution, column 'Rows' gives the total number of cover constraints added to the ILP model and column 'Runtime' gives the computational time (in the format H:MM:SS) to obtain the solution of each iteration.

In this instance, both algorithms obtain the complete Pareto frontier. Algorithm 3.4 is much faster than Algorithm 3.3 in computing the complete Pareto frontier, despite the total number of cover inequalities generated by Algorithm 3.4 being much higher than the number generated by Algorithm 3.3. This is justified by the fact that Algorithm 3.4 needs to optimize only one ILP problem per each Pareto optimal solution.

Notice also that, in general, Algorithm 3.4 takes a higher running time to compute the first Pareto optimal solution. This is due to the fact that every node set $K \in \mathcal{K}$ needs to be processed at the initialization step (Line 2 of Algorithm 3.4), in order to compute the family of critical node sets $\mathcal{K}_0$ that divide the original topology in multiple connected components.

Next, we show the results of testing both algorithms on the four topologies and considering a number of critical nodes $c \in \{2, 3, 4, 5, 6\}$. Moreover, a runtime limit is imposed, forcing the algorithm to stop whenever an iteration takes more than 2 hours to compute the next Pareto optimal solution.

Tables 3.4 and 3.5 present the total number of Pareto optimal solutions obtained and the total computational time (in the format H:MM:SS) used to get those solutions using Algorithms 3.3 and 3.4, respectively. The instances for which each algorithm was able to compute the complete Pareto frontier are represented in bold. Moreover, whenever the algorithm was able to compute only a partial Pareto frontier, the real total computational time is the one reported in these tables plus 2 hours.

Table 3.4: Number of Pareto optimal solutions obtained and the total runtime used to get those solutions using Algorithm 3.3 (row generation).

Network	c	2	3	4	5	6
Janos-US	Pareto points	**6**	**10**	20	17	19
	Runtime	0:00:02	0:01:27	0:59:04	1:30:09	2:00:59
Cost266	Pareto points	**5**	**12**	16	25	26
	Runtime	0:00:07	0:02:57	0:19:05	3:58:25	3:57:26
Germany50	Pareto points	**3**	**7**	**16**	17	16
	Runtime	0:00:20	0:07:53	2:14:31	2:58:22	1:20:57
Coronet	Pareto points	**6**	12	32	27	41
	Runtime	0:06:04	1:32:37	1:00:47	4:39:11	2:28:08

Table 3.5: Number of Pareto optimal solutions obtained and the total runtime used to get those solutions using Algorithm 3.4 (components separation).

Network	c	2	3	4	5	6
Janos-US	Pareto points	**6**	**10**	**24**	25	26
	Runtime	0:00:01	0:00:03	0:02:40	4:22:50	1:52:21
Cost266	Pareto points	**5**	**12**	**20**	30	27
	Runtime	0:00:02	0:00:12	0:08:06	1:21:00	3:25:36
Germany50	Pareto points	**3**	**7**	**16**	21	19
	Runtime	0:00:05	0:00:48	0:03:50	0:37:28	2:34:58
Coronet	Pareto points	**6**	**13**	38	26	0
	Runtime	0:00:38	0:08:48	0:57:38	3:22:32	-

These results show that, in general, Algorithm 3.4 is again much more time-efficient than Algorithm 3.3 when it is possible to compute the complete Pareto frontier within reasonable runtime. Additionally, there are three instances (Janos-US with $c = 4$, Cost266 with $c = 4$ and Coronet with $c = 3$) in which only Algorithm 3.4 was able to compute all Pareto optimal solutions.

Furthermore, when only a partial Pareto frontier was obtained, Algorithm 3.4 was able to obtain considerable more optimal solutions than Algorithm 3.3. There are two exceptions, i.e., two instances out of the 20 instances (4 topologies × 5 values of c) where Algorithm 3.3 performed better: Coronet topology for $c \in \{5, 6\}$. In these cases:

- for $c = 5$ critical nodes, Algorithm 3.4 exceeds the RAM limit when computing the 27th Pareto optimal solution;
- for $c = 6$ critical nodes, it is not possible to compute set $\mathcal{K}_0$ (Line 2 of Algorithm 3.4), i.e., processing the robustness value of each set of c nodes $K \in \mathcal{K}$ is not doable within the imposed runtime of two hours.

These two instances give us an indication of the scalability limit of Algorithm 3.4 (components separation). Conversely, as Algorithm 3.3 (row generation) does not require any prepossessing to obtain the initial Pareto optimal solutions, this algorithm is able to obtain a partial Pareto frontier in a wider range of input topologies.

3.5.3 Insights on the computational results

Next, we provide additional insights on the Pareto frontier of these instances.

First, recall that the robustness value of a solution is the number of node pairs that can still communicate if the critical nodes of the topology are deleted. Although this number can theoretically be any value between 0 and $\binom{n-c}{2}$, where n is the total number of nodes and c is the number of critical nodes, only a subset of these values can represent the robustness value of a Pareto optimal solution.

To illustrate this fact, Figure 3.4 presents a graphical representation of all Pareto-optimal topologies for Germany50 considering $c = 3$ critical nodes. The robustness value z_s of each topology is given by:

(a) $z_1 = \binom{37}{2} + \binom{10}{2} = 666 + 45 = 711$, that corresponds to two connected components with 37 and 10 nodes, respectively;

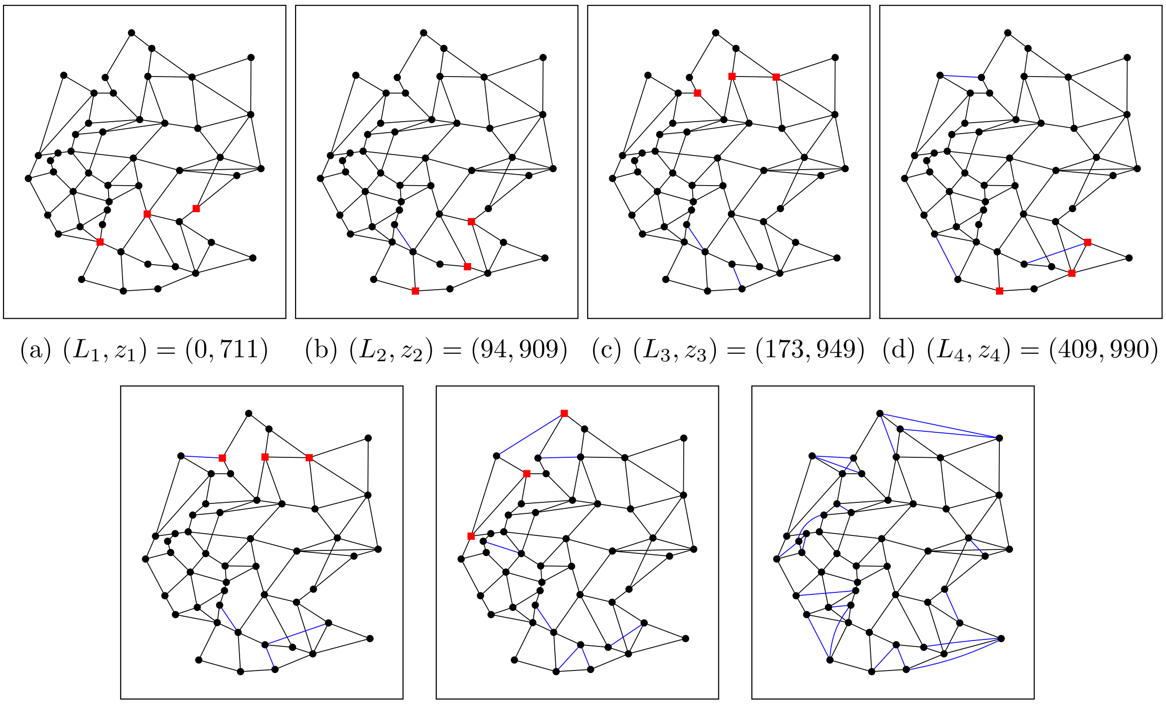
(b) $z_2 = \binom{43}{2} + \binom{4}{2} = 903 + 6 = 909$, that corresponds to two connected components with 43 and 4 nodes, respectively;

(c) $z_3 = \binom{44}{2} + \binom{3}{2} = 946 + 3 = 949$, that corresponds to two connected components with 44 and 3 nodes, respectively;

(d) $z_4 = \binom{45}{2} + \binom{1}{2} + \binom{1}{2} = 990 + 0 + 0 = 990$, that corresponds to a connected component with 45 nodes and two isolated nodes;

(e) $z_5 = \binom{45}{2} + \binom{2}{2} = 990 + 1 = 991$, that corresponds to two connected components with 45 and 2 nodes, respectively;

(f) $z_6 = \binom{46}{2} + \binom{1}{2} = 1035 + 0 = 1035$, that corresponds to a connected component with 46 nodes and an isolated node;


(a) $(L_1, z_1) = (0, 711)$ (b) $(L_2, z_2) = (94, 909)$ (c) $(L_3, z_3) = (173, 949)$ (d) $(L_4, z_4) = (409, 990)$

(e) $(L_5, z_5) = (432, 991)$ (f) $(L_6, z_6) = (884, 1035)$ (g) $(L_7, z_7) = (2482, 1081)$

Figure 3.4: Graphical illustration of the Pareto frontier for Germany50 topology and considering $c = 3$ critical nodes (optimal edges in blue and critical nodes in red squares).

(g) $z_7 = \binom{n-c}{2} = \binom{47}{2} = 1081$, that corresponds to the upper bound scenario where the upgraded topology is fully robust to any failure of 3 nodes.

In general, for a topology with $|N| = 50$ nodes and considering $c = 3$ critical nodes, it is impossible to obtain an upgraded topology with a robustness value $z \geq 946$ that does not belong to the set $\{946, 947, 949, 990, 991, 1035, 1081\}$ since these values represent all possible alternatives of separating a maximum of 3 nodes from the main component.

Next, in Figure 3.5, we represent all Pareto optimal values obtained (using Algorithm 3.3 or Algorithm 3.4, depending on which one obtained a higher number of Pareto points) with a set of scatter plots, one for each tested topology, with the robustness value (objective function value of the CND problem) as function of the edge upgrade cost percentage, i.e., $\frac{L}{L_0} \times 100$ (%). This represents the percentage of additional edge length added to the original topology (N, E_0).

As expected, from these scatter plots we can observe that there is no cross-over between Pareto frontiers for different numbers of critical nodes c, i.e., for similar upgrade percentages, the robustness value decreases with the increase of the number of critical nodes.

For $c \in \{2, 3, 4\}$ (with the exception of Coronet with $c = 4$ instance), the complete Pareto frontier of each instance is obtained. We observe that, in general, the last points represent a much higher edge length increase with a smaller robustness value increase than the previous points. This shows that, in general, we need smaller upgrade costs to reach higher robustness gains in the first Pareto optimal solutions and, when reaching the last

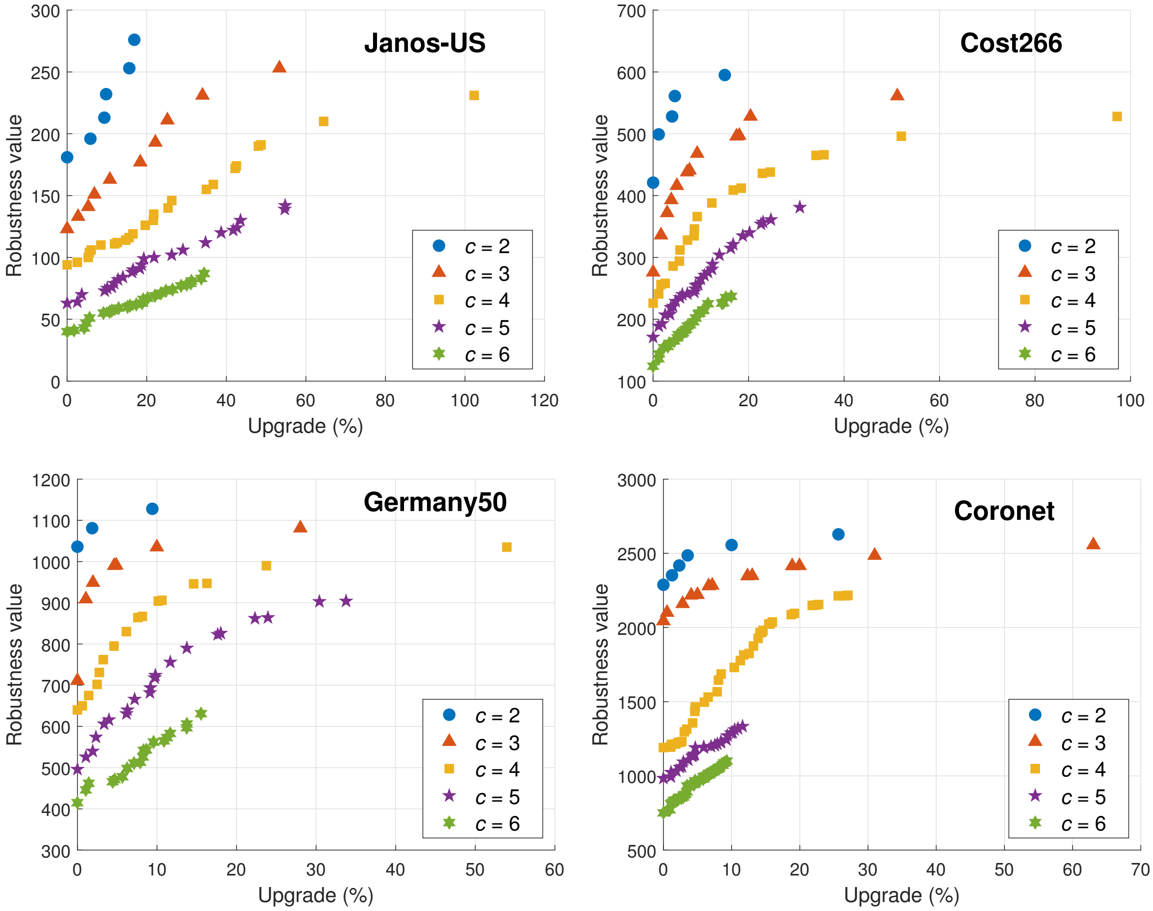


Figure 3.5: Scatter plots of all obtained Pareto optimal solution values.

Pareto optimal solutions, we need higher additional cost to reach full (or near full) robust solutions.

For $c \in \{5, 6\}$, these plots show how incomplete partial Pareto frontiers obtained are. For topologies representing real-world optical networks, the proposed algorithms do not obtain the complete Pareto frontier for more than $c = 4$ critical nodes. In practice, though, a partial Pareto frontier may be enough as, in general, upgrading a topology to have a high robustness value for large values of c implies incurring in huge costs.

Finally, across all tested instances, these Pareto frontiers show that it is within the initial 20% of edge upgrade cost that occurs the highest improvement in the robustness value of each topology. To further analyze this observation, Figure 3.6 represents each Pareto frontier obtained, in a stair plot format, up to 20% edge upgrade and considering the robustness value as a percentage of the upper bound $\binom{n-c}{2}$.

In these plots, we observe that the highest percentage increase in the robustness value of the topology (N, E_0) for a failure of $c \in \{4, 5, 6\}$ critical nodes occurs within the initial 20% of edge upgrade. Moreover, across the majority of tested instances, we observe that the initial 5% of edge upgrade provides the highest percentage of the robustness value to critical node failures for $c \in \{2, 3\}$.

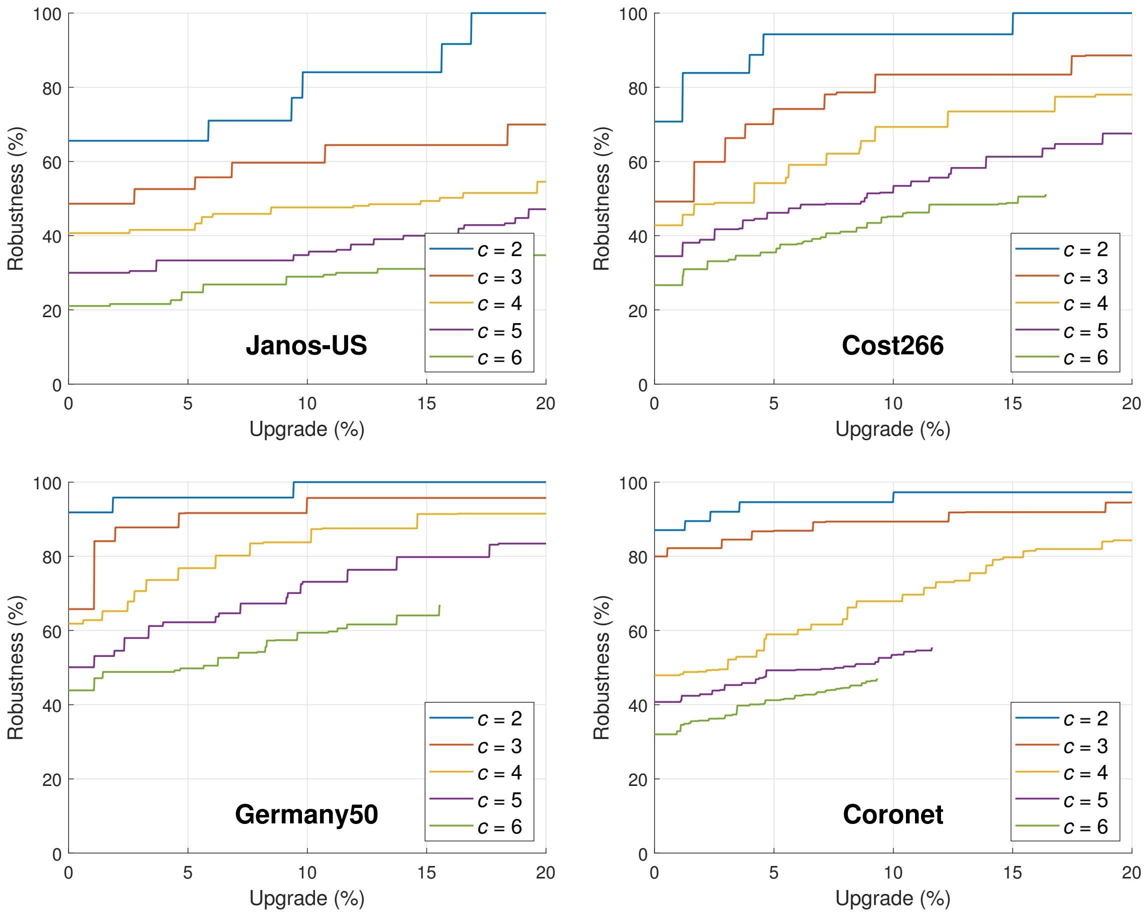
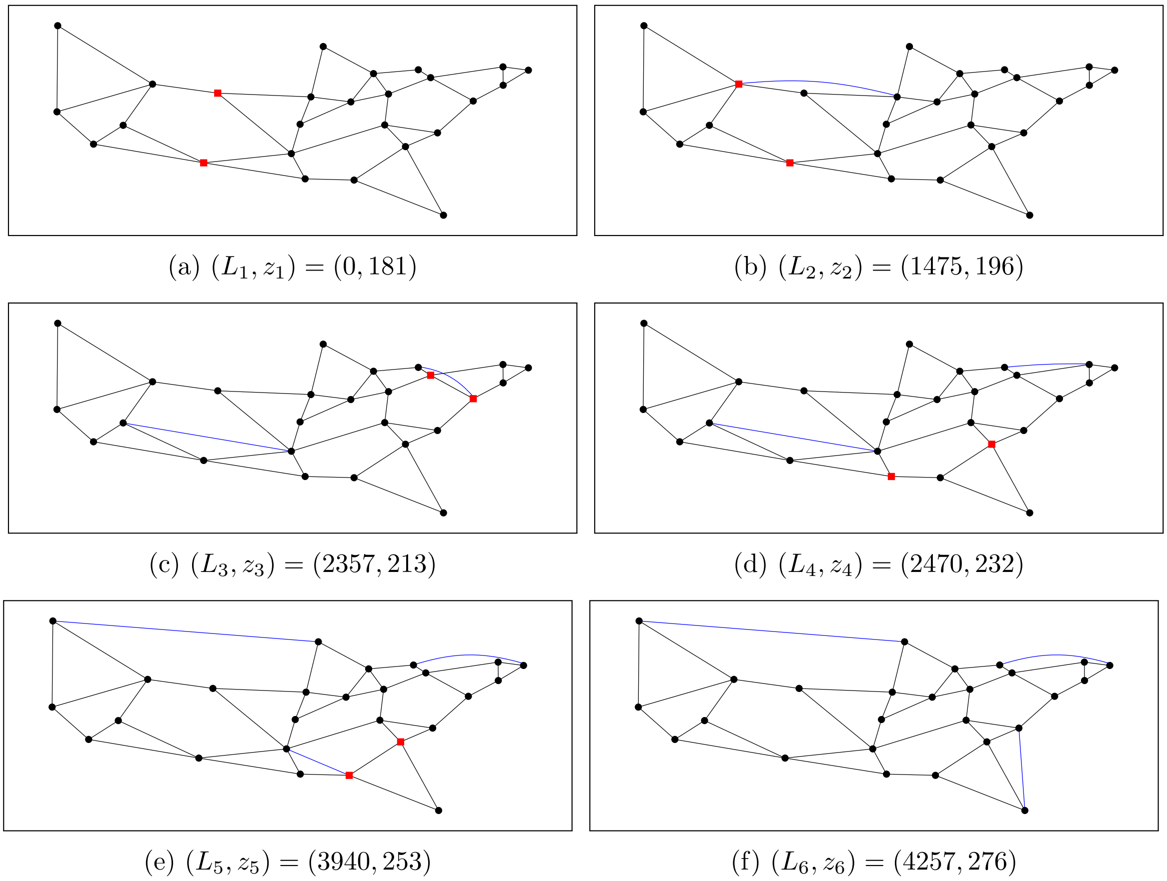


Figure 3.6: Stair plots of the Pareto frontiers obtained.

There exists a clear exception to this trend, which is Janos-US topology with $c = 2$ critical nodes (instance presented in Table 3.2). In order to understand this case, Figure 3.7 presents a graphical representation of all topologies, each one corresponding to a Pareto optimal solution. Analyzing these solutions, in order to upgrade the original topology (a) to one with higher robustness for $c = 2$ node failures, the upgraded topologies require the addition of at least one long edge across the network (compared with the average edge length of the original topology). This explains why this topology has different upgrade trends when compared to the other three topologies.

3.5.4 Testing other topologies and larger sizes

In this section, we present the results of testing the proposed algorithms on different topologies and, in order to assess the scalability of the methods, on larger graph sizes. We generated a set of 9 distinct topologies based on three well-known graph generation algorithms: Erdos-Renyi model [ER59] (Figure 3.8), Watts-Strogatz small-world model [WS98] (Figure 3.9) and Barabasi-Albert scale-free model [BA99] (Figure 3.10). In the process of generating these topologies, whenever a topology is not connected, it is discarded and a different topology is generated. This ensures that only connected topologies are considered.


(a) $(L_1, z_1) = (0, 181)$

(b) $(L_2, z_2) = (1475, 196)$

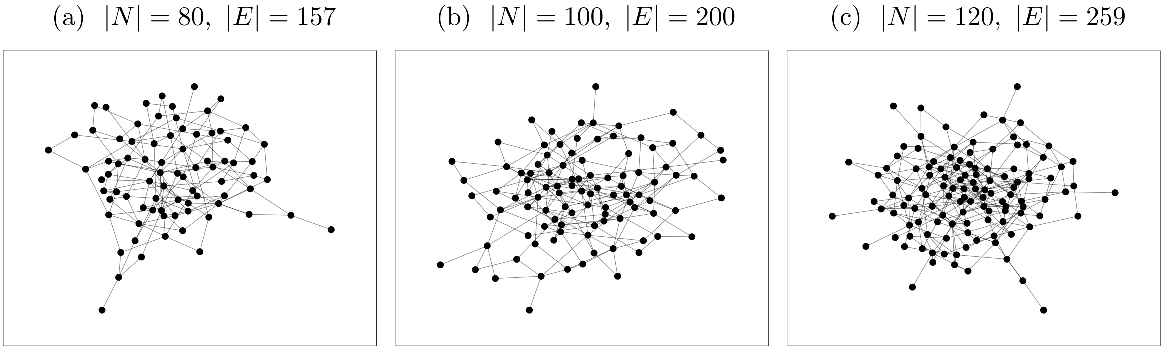
(c) $(L_3, z_3) = (2357, 213)$

(d) $(L_4, z_4) = (2470, 232)$

(e) $(L_5, z_5) = (3940, 253)$

(f) $(L_6, z_6) = (4257, 276)$

Figure 3.7: Graphical representation of the Pareto frontier solutions for Janos-US topology and considering $c = 2$ critical nodes (optimal edges in blue and critical nodes in red squares).

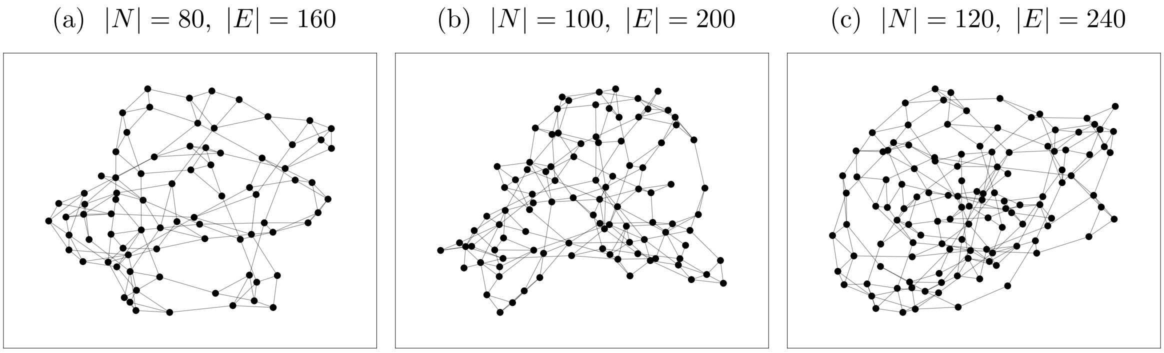

(a) $|N| = 80,\ |E| = 157$

(b) $|N| = 100,\ |E| = 200$

(c) $|N| = 120,\ |E| = 259$

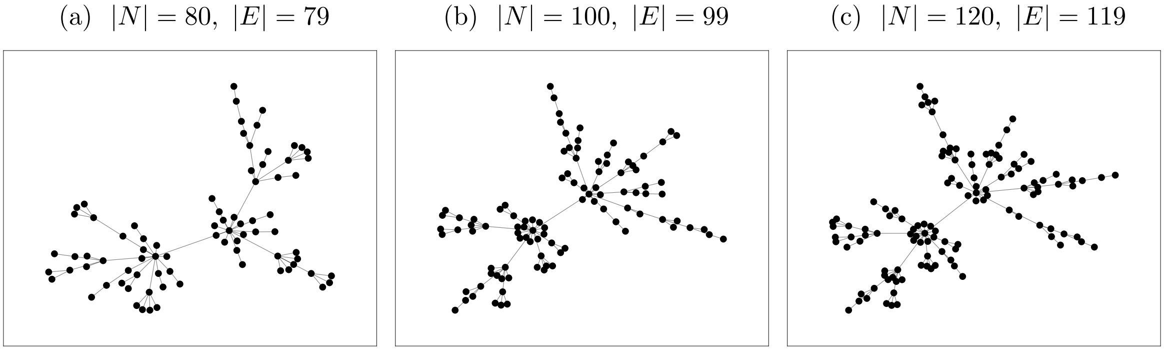
Figure 3.8: Erdos-Renyi randomly generated topologies with $|N| \in \{80, 100, 120\}$, considering a probability of selection of each edge of $p = 0.04$.

In order to test Algorithms 3.3 and 3.4 with these graphs, we considered a number of critical nodes $c \in \{2, 3, 4, 5\}$. Moreover, the previous runtime limit was again considered (the algorithm stops whenever an iteration reaches a 2 hours runtime to compute the next Pareto solution). Finally, we set unitary costs of installing new edges, i.e., $l_{ij} = 1$ for each $(i, j) \in E_n$, which means that the objective function (3.1) corresponds to minimizing the total number of



(a) $|N| = 80,\ |E| = 160$ (b) $|N| = 100,\ |E| = 200$ (c) $|N| = 120,\ |E| = 240$

Figure 3.9: Watts-Strogatz randomly generated topologies with $|N| \in \{80, 100, 120\}$, considering a total number of edges $|E| = 2|N|$ and a rewiring probability of $\beta = 0.2$.



(a) $|N| = 80,\ |E| = 79$ (b) $|N| = 100,\ |E| = 99$ (c) $|N| = 120,\ |E| = 119$

Figure 3.10: Barabasi-Albert randomly generated topologies with 80, 100 and 120 nodes, respectively.

additional edges.

Tables 3.6 and 3.7 present the results summary (similar to Tables 3.4 and 3.5) of the Erdos-Renyi topologies using Algorithms 3.3 and 3.4, respectively. For these instances, the complete Pareto frontier was obtained only when $c = 2$ critical nodes were considered (using Algorithm 3.4). Moreover, we observe that the number of Pareto optimal solutions obtained decreases with the increase of the number of nodes $|N|$. This fact gives us an indication that the partial Pareto frontier obtained tends to be more incomplete with the increase of the number of nodes of the input topology.

Next, Tables 3.8 and 3.9 present the results summary of the Watts-Strogatz small-world topologies using Algorithms 3.3 and 3.4, respectively. The computational results obtained with the Watts-Strogatz topologies are similar to the Erdos-Renyi topologies previously presented, with the main difference that Algorithm 3.4 is able to compute complete Pareto frontiers for $c = 3$ critical nodes with $|N| \leq 100$.

Regarding both algorithms, for the largest topologies (i.e., when $|N| = 120$), the results show that: on one hand, Algorithm 3.3 is barely able to compute any Pareto optimal solutions (besides the trivial one); on the other hand, Algorithm 3.4 is only able to compute solutions for $c \in \{2, 3\}$ (due to the 2 hours runtime limit constraint imposed to the preprocessing procedure of this algorithm). Therefore, although both algorithms have pros and cons when applied to topologies with $|N| \leq 100$, for larger topologies, the proposed methodology is not

Table 3.6: Erdos-Renyi results summary, i.e., number of Pareto optimal solutions obtained and the total runtime used to get those solutions using Algorithm 3.3 (row generation).

$\vert N\vert$	c	2	3	4	5
80	No. Pareto points	**5**	7	7	5
	Runtime	1:17:51	2:17:58	2:56:10	4:45:46
100	No. Pareto points	4	5	4	3
	Runtime	0:09:49	1:03:29	2:38:42	4:56:10
120	No. Pareto points	3	2	1	3
	Runtime	1:18:10	0:41:31	0:16:41	3:00:39

Table 3.7: Erdos-Renyi results summary, i.e., number of Pareto optimal solutions obtained and the total runtime used to get those solutions using Algorithm 3.4 (components separation).

$\vert N\vert$	c	2	3	4	5
80	No. Pareto points	**5**	7	9	0
	Runtime	0:01:13	0:03:20	0:18:35	-
100	No. Pareto points	**5**	7	7	0
	Runtime	0:07:19	0:24:56	0:44:20	-
120	No. Pareto points	**4**	5	0	0
	Runtime	0:21:26	0:26:33	-	-

Table 3.8: Watts-Strogatz results summary, i.e., number of Pareto optimal solutions obtained and the total runtime used to get those solutions using Algorithm 3.3 (row generation).

$\vert N\vert$	c	2	3	4	5
80	No. Pareto points	**2**	2	5	3
	Runtime	0:01:27	0:10:22	0:59:09	0:28:01
100	No. Pareto points	**2**	3	4	4
	Runtime	0:18:02	1:27:28	2:58:45	2:55:03
120	No. Pareto points	**2**	2	2	1
	Runtime	0:45:46	1:55:36	0:54:06	0:54:33

effective to compute the Pareto frontier.

Finally, Table 3.10 presents the results obtained using Algorithm 3.3 to the three topologies randomly generated using the Barabasi-Albert scale-free model. These results are quite straightforward. In all instances, Algorithm 3.3 is only able to compute two Pareto optimal solutions: the trivial solution (i.e. $L_1 = 0$) and the optimal Pareto pair that corresponds to adding only one new edge (i.e. $L_2 = 1$). This algorithm cannot compute the Pareto optimal solution with two (or more) additional edges within the runtime limit for any of the topologies

Table 3.9: Watts-Strogatz results summary, i.e., number of Pareto optimal solutions obtained and the total runtime used to get those solutions using Algorithm 3.4 (components separation).

$\|N\|$	c	2	3	4	5
80	No. Pareto points	**2**	**3**	7	0
	Runtime	0:00:50	0:16:56	2:25:38	-
100	No. Pareto points	**2**	**4**	7	0
	Runtime	0:04:36	1:47:55	3:38:19	-
120	No. Pareto points	**2**	2	0	0
	Runtime	0:19:43	0:40:28	-	-

generated with the Barabasi-Albert model.

Table 3.10: Barabasi-Albert results summary, i.e., number of Pareto optimal solutions obtained and the total runtime used to get those solutions using Algorithm 3.3 (row generation).

$\|N\|$	c	2	3	4	5
80	No. Pareto points	2	2	2	2
	Runtime	0:04:26	0:04:17	0:15:12	0:21:50
100	No. Pareto points	2	2	2	2
	Runtime	0:08:25	0:42:38	0:40:23	1:37:39
120	No. Pareto points	2	2	2	2
	Runtime	0:12:45	1:36:02	3:55:45	5:18:05

Moreover, we do not present the computational results using Algorithm 3.4 because this algorithm is not able to compute any Pareto optimal solution for these topologies (besides the trivial one). To understand the reason for this fact, consider the simplest instance (i.e., $c = 2$ critical nodes and the Barabasi-Albert topology with $|N| = 80$ nodes). When removing the critical nodes from this topology, it results in a remaining graph with 25 distinct components. Given that this algorithm is based on computing the partition set of all possible critical node sets, for this specific CND solution only, the Bell number of 25 is, approximately, 4.6×10^{18} (represents the cardinality of the partition set). Since Algorithm 3.4 requires to process all components partitions, this is unworkable due to both time and memory constraints.

3.5.5 Testing the effect of increasing the number of edges

Here, for a fixed number of nodes, we present the results of testing Algorithm 3.4 (components separation), which from the previous results is the best procedure, on graphs with different number of edges. To perform these tests, we considered the Erdos-Renyi model with $|N| = 50$ nodes and with a probability of selection of each edge of p that ranges from 0.05 to 0.11. Moreover, we have considered a fixed seed to this generation of topologies, in order to make each newly generated topology an upgrade of the previous one, i.e., if an edge is in the graph generated with a given p, then it is also in all the graphs generated with higher values for p. We tested different seeds until one of them ensured that the topology generated with $p = 0.05$ was connected (and by consequence, all topologies with $p > 0.05$).

In Table 3.11, we present the results obtained with Algorithm 3.4 (components separation) for each topology for $c \in \{2, 3, 4\}$ critical nodes considering, once again, unitary costs and the 2 hour stopping criteria. In the first two lines of this table, we present each tested probability p and the number of edges $|E|$ of the corresponding topology. In addition to the number of Pareto optimal solutions obtained, and the total runtime required to obtain all solutions found, we present the robustness value (in percentage to the upper bound) of each initial topology z_1 and the robustness value of the last Pareto optimal point computed z_{last}. Notice that connectivity robustness of 100% means that Algorithm 3.4 was able to compute the complete Pareto frontier of that instance.

Table 3.11: Results summary of increasing the number of edges using the Erdos-Renyi generation model (with probability $p \in \{0.05, 0.06, 0.07, 0.08, 0.09, 0.1, 0.11\}$) and Algorithm 3.4 (components separation).

c	p	0.05	0.06	0.07	0.08	0.09	0.10	0.11
	$\|E\|$	65	74	90	103	113	124	141
2	No. Pareto sol.	**8**	**6**	**5**	**3**	**3**	**2**	**2**
	Runtime	0:00:12	0:00:09	0:00:08	0:00:06	0:00:05	0:00:04	0:00:03
	z_1 (%)	80.2	87.8	87.8	91.8	91.8	95.8	95.8
	z_{last} (%)	100	100	100	100	100	100	100
3	No. Pareto sol.	9	7	6	**5**	**5**	**3**	**2**
	Runtime	0:57:25	0:00:25	0:00:31	0:00:31	0:00:25	0:00:19	0:00:12
	z_1 (%)	59.3	68.4	79.7	87.5	87.5	91.6	95.7
	z_{last} (%)	87.8	91.7	95.7	100	100	100	100
4	No. Pareto sol.	6	8	8	6	5	4	**3**
	Runtime	2:02:24	2:01:26	0:04:41	0:00:54	0:00:30	0:00:22	0:01:46
	z_1 (%)	48.0	62.8	75.5	83.3	87.2	87.2	91.4
	z_{last} (%)	73.0	87.3	91.5	95.7	95.7	95.7	100

Contrary to the effect of increasing the number of nodes, by increasing the number of edges of the input topology, the algorithm performs better. This can be easily explained by the following two related facts. By increasing the number of edges $|E|$, there is a tendency to increase the robustness value of the input topology z_1, and to decrease the total number of different combinations of c critical nodes that split the network into disjoint components. This causes a reduction in the number of Pareto optimal solutions, and therefore, the proposed approaches require fewer iterations to obtain the Pareto frontier.

3.6 Conclusions

In this work, we have addressed the robust network upgrade problem (RNUP) that aims to identify a set of new edges to add to the original topology in order to increase its robustness to simultaneous node failures. This problem is formulated as a bi-objective MILP problem with two distinct objectives: minimizing the total cost of the new edges, and maximizing the robustness of the resulting upgraded topology. As robustness metric, we have considered the objective function value of the CND problem which measures the pairwise connectivity between nodes when a set of c critical nodes are removed from the graph.

A general algorithm was presented to obtain the Pareto frontier where the robustness value is obtained by solving an ILP problem and the selection of the new edges is obtained solving a path formulation adapted from the bi-objective MILP problem. Since using this approach can only solve the smallest instances, we also presented an alternative formulation by modeling the selection of edges as a set covering problem. As the number of cover inequalities increases exponentially with the size of the instance, we proposed two algorithms to select the cover inequalities. One is a row generation algorithm that iteratively selects cover inequalities, and the other is a components separation algorithm that selects simultaneously all the cover inequalities that force the connection of different components in order to obtain a desire robustness value.

The computational tests have shown that the components separation algorithm is much more time-efficient than the row generation algorithm when it is possible to compute the complete Pareto frontier within a reasonable running time. In the telecommunication topologies, it was possible to obtain the complete Pareto frontier for all four tested topologies with $c \in \{2, 3\}$ critical nodes and for the Janos-US, Cost266 and Germany50 topologies with $c = 4$ critical nodes. Nevertheless, the components separation algorithm has scalability issues when considering a higher number of critical nodes. In contrast, the row generation algorithm is able to obtain a partial Pareto frontier for a wider range of instances. For example, it was able to compute 41 Pareto optimal solutions considering the Coronet topology with $c = 6$ critical nodes.

Finally, although both algorithms have advantages and disadvantages, when considering input topologies with larger sizes (more than 100 nodes), both algorithms present scalability issues. In this work, we have addressed the RNUP with exact procedures. For larger graphs, heuristic approaches have to be considered, aiming to obtain an approximation of the Pareto frontier.

Bibliography

[ACEP09] A. Arulselvan, C. Commander, L. Elefteriadou, and P. Pardalos. *Detecting critical nodes in sparse graphs.* Computers & Operations Research, 36(7):2193–2200, 2009.

[BA99] A. Barabási and R. Albert. *Emergence of scaling in random networks.* Science, 286(5439):509–512, 1999.

[BdSA18] F. Barbosa, A. de Sousa, and A. Agra. *Topology design of transparent optical* *networks resilient to multiple node failures.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

[BdSA20] F. Barbosa, A. de Sousa, and A. Agra. *Design/upgrade of a transparent optical network topology resilient to the simultaneous failure of its critical nodes.* Networks, 75(4):356–373, 2020.

[CGL$^+$02] R. Caballero, T. Gómez, M. Luque, F. Miguel, and F. Ruiz. *Hierarchical generation of Pareto optimal solutions in large-scale multiobjective systems.* Computers & Operations Research, 29(11):1537–1558, 2002.

[Chv79] V. Chvatal. *A greedy heuristic for the set-covering problem.* Mathematics of Operations Research, 4(3):233–235, 1979.

[dSMS17] A. de Sousa, D. Mehta, and D. Santos. *The robust node selection problem aiming to minimize the connectivity impact of any set of p node failures.* In 13th International Conference on Design of Reliable Communication Networks (DRCN), pages 138–145, 2017.

[dSPRR19] A. de Sousa, J. Piccini, F. Robledo, and P. Romero. *An interplay between critical node detection and epidemic models.* In 11th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–7, 2019.

[dSS20] A. de Sousa and D. Santos. *Vulnerability evaluation of networks to multiple failures based on critical nodes and links.* In J. Rak and D. Hutchison, editors, Guide to Disaster-Resilient Communication Networks, pages 63–86. Springer International Publishing, Cham, 2020.

[DXT$^+$10] T. Dinh, Y. Xuan, M. Thai, E. Park, and T. Znati. *On aproximation of new optimization methods for assessing network vulnerability.* In Proceedings IEEE INFOCOM, pages 1–9, 2010.

[ER59] P. Erdös and A. Rényi. *On random graphs I.* Publicationes Mathematicae Debrecen, 6:290–297, 1959.

[FOP$^+$19] L. Faramondi, G. Oliva, S. Panzieri, F. Pascucci, M. Schlueter, M. Munetomo, and R. Setola. *Network structural vulnerability: a multiobjective attacker perspective.* IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(10):2036–2049, 10 2019.

[FWG$^+$16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GTE$^+$16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[HB21] A. Hadian and M. Bagherian. *A Pareto frontier for node survivable computer network design problem.* Telecommunication Systems, 76:371–389, 2021.

[LPXC19] J. Li, P. Pardalos, B. Xin, and J. Chen. *The bi-objective critical node detection problem with minimum pairwise connectivity and cost: theory and algorithms.* Soft Computing, 23:12729–12744, 2019.

[LTK16] M. Lalou, M. Tahraoui, and H. Kheddouci. *Component-cardinality-constrained critical node problem in graphs.* Discrete Applied Mathematics, 210:150–163, 2016.

[LTK18] M. Lalou, M. Tahraoui, and H. Kheddouci. *The critical node detection problem in networks: a survey.* Computer Science Review, 28:92 – 117, 2018.

[NYWF19] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek. *Infrastructure upgrade framework for Content Delivery Networks robust to targeted attacks.* Optical Switching and Networking, 31:202–210, 2019.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[Pav18] K. Pavlikov. *Improved formulations for minimum connectivity network interdiction problems.* Computers & Operations Research, 97:48–57, 2018.

[PC19] D. Purevsuren and G. Cui. *Efficient heuristic algorithm for identifying critical nodes in planar networks.* Computers & Operations Research, 106:143–153, 2019.

[RH20] J. Rak and D. Hutchison. *Guide to disaster-resilient communication networks.* Computer Communications and Networks, Springer International Publishing, Cham, 2020.

[SD07] P. Shukla and K. Deb. *On finding multiple Pareto-optimal solutions using classical and evolutionary generating methods.* European Journal of Operational Research, 181(3):1630–1652, 2007.

[SdSM18] D. Santos, A. de Sousa, and P. Monteiro. *Compact models for critical node detection in telecommunication networks.* Electronic Notes in Discrete Mathematics, 64:325–334, 2018.

[SGL11] M. Di Summa, A. Grosso, and M. Locatelli. *Complexity of the critical node problem over trees.* Computers & Operations Research, 38(12):1766–1774, 2011.

[SGL12] M. Di Summa, A. Grosso, and M. Locatelli. *Branch and cut algorithms for detecting critical nodes in undirected graphs.* Computational Optimization and Applications, 53(3):649–680, 2012.

[Sim14] J. Simmons. *Optical network design and planning.* Springer, Switzerland, 2nd edition, 2014.

[SSG12] S. Shen, J. Smith, and R. Goli. *Exact interdiction models and algorithms for disconnecting networks via node deletions.* Discrete Optimization, 9(3):172–188, 2012.

[VBP14] A. Veremyev, V. Boginski, and E. Pasiliao. *Exact identification of critical nodes in sparse networks via new compact formulations.* Optimization Letters, 8(4):1245–1259, 2014.

[Ven12] M. Ventresca. *Global search algorithms using a combinatorial unranking-based problem representation for the critical node detection problem.* Computers & Operations Research, 39(11):2763–2775, 2012.

[VHOB18] M. Ventresca, K. Harrison, and B. Ombuki-Berman. *The bi-objective critical node detection problem.* European Journal of Operational Research, 265(3):895–908, 2018.

[WS98] D. Watts and S. Strogatz. *Collective dynamics of 'small-world' networks.* Nature, 393:440–442, 1998.

Chapter 4

Provision of Maximum Connectivity Resiliency with Minimum Cost to Telecommunication Networks through Third-Party Networks

Abstract: In telecommunication networks, full connectivity resilience to multiple link failures is too costly as it requires a network topology with too many redundant links. Alternatively, the connectivity resilience of a telecommunications network can be improved resorting to available third-party networks for temporary additional connectivity until the failing links are restored. In this approach, some nodes of the network must be selected in advance to act as gateway nodes to the third-party networks when a multiple link failure event occurs. For a given network topology and a cost associated to each node to turn it into a gateway node, the aim is to select the gateway nodes providing maximum connectivity resilience at minimum cost. So, the Gateway Node Selection is defined as a bi-objective optimization problem such that its Pareto-optimal solutions represent different trade-offs between cost and connectivity resilience improvement. In this work, the connectivity resilience is modeled by the Critical Link Detection optimization problem. An exact optimization algorithm is proposed, based on a row generation algorithm and on set cover cuts. The computational results demonstrate the effectiveness of the proposed algorithm on four well-known telecommunication network topologies.

Keywords: Connectivity Resilience, Critical Link Detection, Gateway Node Selection, Bi-objective optimization, Pareto frontier, Telecommunication networks

F. Barbosa, A. de Sousa, and A. Agra. *Provision of Maximum Connectivity Resiliency with Minimum Cost to Telecommunication Networks through Third-Party Networks.* Submitted to: Networks, 2021.

4.1 Introduction

In the context of telecommunications networks, the resilience to failures is defined as the capacity of the network to maintain as much as possible its services in a failure scenario. In terms of connectivity, current telecommunication networks are fully resilient to single link failures. However, large-scale failures are becoming a serious concern to operators due to different reasons, as natural disasters [GTE$^+$16] or malicious human activities [FWG$^+$16]. In the latter case, evidence is growing that such activities are associated with social, political, economic and cultural conflicts [GSM$^+$11]. Nowadays, telecommunication networks resort to optical infrastructures which are unprotected against several physical-layer attacks [SKFZW16]. Particularly, link cuts are a straightforward attack method on the network physical-layer that can severely disrupt the supported services.

The impact of multiple link failures in telecommunication networks has been considered in different contexts in the literature. In [RSM03, ZZM06], the capacity of different protection schemes in providing resilience to multiple random link failures is accessed in the context of optical networks based on wavelength division multiplexing. More recently, the backup network design against multiple random link failures has been addressed in [HHSO20, JLM15] where some capacity on the different network links is reserved to act as a backup capacity to be used only in case of multiple link failures.

In [JH13, YW11], multiple link failures are modeled as shared risk link groups (i.e., groups of links with high probability of simultaneous failure). The typical example is when multiple links share a single duct and, thus, the unattended cut of the duct makes all links to be simultaneously cut. In [GTE$^+$16, NGGGS18, TRVG17], simultaneous link failures are modeled in the context of natural disasters. In those works, there exists correlation between the failing links. Concerning uncorrelated failures, protecting telecommunication networks against dual link failures has been addressed in several works [BLL$^+$12, GSB16, LT11, RC08]. Furthermore, malicious human activities scenarios, where more than two simultaneous uncorrelated failures can easily occur in a telecommunication network, has only been considered in very few works [DXT$^+$12, NdSWF18, YHG$^+$17].

In the perspective of the telecommunication network operator, achieving full connectivity resilience against multiple link failures is, in practice, impossible since it requires too many physical links, which would be too expensive to install and operate. Alternatively, aiming to improve the connectivity resilience against such failures, operators resort to solutions that search for a trade-off between cost and resilience gains. The common emergency packet transport network proposed in [XYS$^+$17] for disaster recovery is one of such examples. In that proposal, a third-party entity builds an emergency network with the surviving resources of multiple network operators (affected by a regional disaster) that can be jointly used by them. The emergency network is built in several steps to avoid confidential information leakage between telecommunication network operators.

In [BdSA20], the network upgrade problem is addressed, and it aims to identify a set of new links (within a given budget) to add to the network topology aiming to maximize its network resilience against multiple node failures (measured resorting to a Critical Node Detection problem). Here, instead of improving the network resilience to multiple failures with new physical links, we follow the proposal of [dS20] which resorts to a third-party entity that provides temporary virtual links (when a multiple failure occurs).

The approach is as follows. Consider a telecommunication operator of a network deployed on a geographical region where other networks (of other operators) coexist. In a multiple link failure scenario, in order to obtain temporary connectivity between some network nodes (while the failing links are not reestablished), the operator resorts to those third-party networks available in that region. With this approach, some nodes of one network must be selected to act as gateway nodes to third-party networks. The business relation between network operators can be one-way (the third-party operator charges the temporary connectivity provided when needed) or two-way (each operator provides the temporary connectivity when needed by the other), which could eliminate the service costs charged between operators depending on their Service Level Agreement (SLA).

Consider a given positive integer l representing the number of simultaneous link failures for which the network operator aims to improve the resilience of its network. Consider also a connectivity weight assigned to each pair of network nodes representing the importance of the connectivity between the node pair (such weights can be defined by the traffic demand between the nodes, the number of interconnected users, etc). The connectivity resilience of the network is assumed to be the minimum total weight of the node pairs that can still communicate after any set of l simultaneous link failures. The connectivity resilience value is obtained by solving the Critical Link Detection (CLD) optimization problem, whose optimal solution identifies a set of l critical links [dSS20].

For a given network topology, the Gateway Node Selection (GNS) is a bi-objective optimization problem that aims to compute different optimal trade-off solutions between the total cost of the selected gateway nodes to a third-party network and the connectivity resilience gains provides by those gateway nodes. In the GNS problem, instead of assigning costs to the candidate links as in [BdSA20], the costs are assigned to the network nodes that can act as gateway nodes to the third-party network. In order to compute all Pareto-optimal solutions of the GNS problem, an exact optimization algorithm is proposed, based on a row generation algorithm and on set cover cuts. Dealing with bi-objective optimization problems and developing algorithms to identify the Pareto-optimal solutions has been investigated also in other telecommunication network contexts, as in [BBH$^+$17, LGZ$^+$15]. In order to evaluate the proposed algorithm, we present computational results demonstrating its effectiveness on four well-known telecommunication network topologies.

Finally, the edge-connectivity augmentation problem [ET76, Nag04], a widely known problem in graph theory, is related to the one that we are addressing in this work. Its objective is to obtain the minimum number of new edges to be added to a given graph so that the edge-connectivity (i.e., the minimum number of edges whose removal disconnects the graph) of the augmented graph increases to a given target value. Note that, although adding a single edge (in the edge-augmentation connectivity problem) is equivalent to selecting its 2 end-nodes as gateway nodes (in the GNS problem), this is not true when multiple edges are added (for example, adding two edges is different from selecting their end-nodes as gateway nodes since in the latter case, there is full connectivity between all 4 nodes in the third-party network, and not just between 2 pairs of nodes). On the other hand, regarding its complexity, the edge-connectivity augmentation problem has been solved with polynomial-time algorithms [BK00, WN87], while the GNS problem is NP-hard (this can be easily proved since the CLD subproblem itself is NP-complete [SNXT13]).

The original contributions of this paper can be summarized as follows:

- the Gateway Node Selection (GNS) problem is proposed and modeled as a bi-objective optimization;
- a general GNS algorithm is introduced aiming to obtain the complete Pareto frontier;
- the Critical Link Detection (CLD) optimization problem, used in this work as a subproblem of the main bi-objective GNS problem, is adapted to a scenario where a subset of nodes are selected as gateway nodes;
- a set cover model is developed to optimally solve the subproblem of selecting a set of gateway nodes with a given connectivity resilience threshold;
- a row generation algorithm, based on a lower dimensional set cover model, is proposed to compute all Pareto-optimal solutions;
- the proposed methodology is extended to the case that multiple third-party networks are available to the telecommunications operator;
- extensive computational results on 4 different telecommunications topologies are reported, considering different parameters and both single third-party and multiple third-parties cases, showing the applicability of the proposed algorithms.

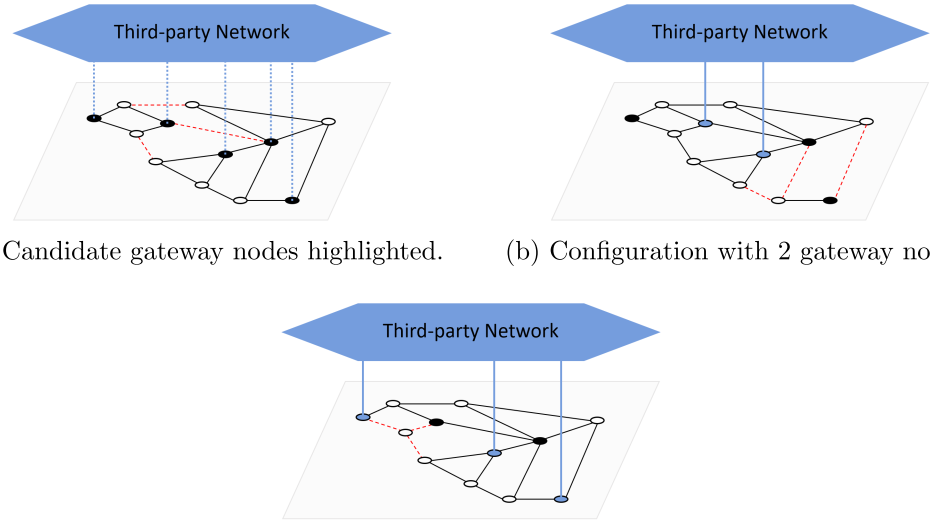
The paper is organized as follows. In Section 4.2, we describe the GNS problem as a bi-objective optimization problem, presenting a general algorithm framework to compute its Pareto frontier. The same section also describes how the connectivity resilience of a given network topology is evaluated (resorting to the CLD optimization problem, with a given set of gateway nodes to a third-party network), and presents a set cover model to obtain the minimal cost gateway node set for a given connectivity resilience threshold. Then, in Section 4.3, we propose an efficient exact optimization algorithm for the GNS problem, based on a row generation algorithm that resorts to a lower dimensional set cover model. Section 4.4 describes how the previous algorithm is extended for the case when multiple third-party networks are available. The computational results are presented and discussed in Section 4.5 highlighting the importance to the network operator of the trade-off solutions provided by the algorithm. Finally, Section 4.6 summarizes the main conclusions of the work.

4.2 Gateway node selection problem

Consider the network defined by an undirected graph $G = (N, E)$, where $N = \{1, ..., n\}$ and $E \subseteq \{\{i, j\} : i, j \in N, i < j\}$ represent the sets of nodes and links, respectively. Moreover, consider $N_1 \subseteq N$ as the subset of all possible nodes that can act as gateway nodes to the third-party network and let $c_i > 0$, for each $i \in N_1$, represent the cost of turning node i into a gateway node.

The Gateway Node Selection (GNS) problem aims to compute the minimum cost set of gateway nodes to the third-party network with maximum connectivity resilience. To better understand the GNS problem, consider the example illustrated in Figure 4.1.

Figure 4.1(a) represents a given telecommunication network with a third-party network available whose connectivity weights are unitary for all node pairs. Moreover, consider that the 5 nodes in black can be used as gateway nodes to this third-party network. Without resorting to the additional connectivity provided by the third-party network, the $l = 3$ critical links (highlighted in dashed red in Figure 4.1(a)) split the network into one component of 4



(a) Candidate gateway nodes highlighted.

(b) Configuration with 2 gateway nodes.

(c) Configuration with 3 gateway nodes.

Figure 4.1: Illustration of a third-party network, with provision of temporary virtual links between the gateway nodes for the simultaneous failure of 3 links (highlighted in dashed red).

nodes and another of 8 nodes (with a total pairwise connectivity of 34).

In Figure 4.1(b), two gateway nodes are selected so that if the previous critical links fail, the two network components can be connected through the third-party network. In this solution, the resulting set of critical links, highlighted in dashed red in Figure 4.1(b), can only split the network into two components of 2 and 10 nodes, respectively (with a total connectivity of 46). Finally, in Figure 4.1(c), three gateway nodes are selected and, in this solution, the resulting set of critical links can only isolate one node from all other nodes (with a total connectivity of 55).

As illustrated in the example, we obtain different trade-offs between the cost of selecting gateway nodes and the connectivity resiliency gains provided by that selection showing that minimizing cost and maximizing connectivity resiliency are conflicting objectives. To address this problem, we first model the GNS problem as a bi-objective optimization problem and then, we present a general algorithm framework to compute the complete Pareto frontier to the GNS problem.

4.2.1 Bi-objective optimization model

Initially, consider that, for each node $i \in N_1$, the binary decision variable x_i is 1 if node i is selected as a gateway node, and 0 otherwise. The GNS problem can be modeled as the following bi-objective optimization problem:

$$min \quad B := \sum_{i \in N_1} c_i x_i \tag{4.1}$$

$$max \quad z := \textbf{CLD}(\{i \in N_1 : x_i = 1\}) \tag{4.2}$$

$$s.t. \quad x_i \in \{0, 1\}, \quad i \in N_1. \tag{4.3}$$

There are two objectives: objective function (4.1) is the minimization of the total cost B of the selected set of gateway nodes and objective function (4.2) is the maximization of the connectivity resilience to up to l simultaneous link failures z, as provided by CLD problem, with the selected set of gateway nodes $M = \{i \in N_1 : x_i = 1\}$, i.e., notation $\mathbf{CLD}(M)$ represents the connectivity resilience value of considering M as the selected set of gateway nodes.

In this bi-objective optimization problem, a given solution with a cost B and a connectivity resilience z is a Pareto-optimal solution if it is better than any other solution in at least one of its values (i.e., either lower on its cost B or higher on its connectivity resilience z). So, computing the Pareto frontier to the GNS problem provides multiple solutions with different trade-offs between the two objective functions and the decision-maker can correctly identify the connectivity resilience improvement obtained by each possible investment (i.e., each different cost value of all Pareto-optimal solutions).

4.2.2 A general GNS algorithm

Here, we propose an algorithm framework to compute the complete Pareto frontier of the GNS bi-objective optimization problem (4.1)–(4.3).

Algorithm 4.1 is a general algorithm (that will be further detailed in Section 4.3 in the form of a row generation algorithm) to compute all Pareto-optimal solutions. Parameter s indicates the index of each Pareto candidate solution, i.e., $s \in \{1, 2, 3, ...\}$. A candidate solution s is defined by its set of gateway nodes $M_s \subseteq N_1$ and the associated pair of solution values (B_s, z_s).

Algorithm 4.1 General algorithm for GNS

```
1: $s \leftarrow 1$
2: $(B_s, z_s) \leftarrow \big(0, \mathbf{CLD}(\emptyset)\big)$
3: while $z_s < \mathbf{CLD}(N_1)$ do
4:     $s \leftarrow s + 1$
5:     Compute gateway node set $M_s \subseteq N_1$ such that $\sum_{i \in M_s} c_i$ is minimized and $\mathbf{CLD}(M_s) >$
       $z_{s-1}$
6:     $(B_s, z_s) \leftarrow \big(\sum_{i \in M_s} c_i,\ \mathbf{CLD}(M_s)\big)$
7: end while
```

The algorithm starts (lines 1–2) by computing the first Pareto-optimal solution $s = 1$ which is the solution without gateway nodes whose values are $(0, \mathbf{CLD}(\emptyset))$.

Then, in each iteration of the while loop (lines 3–7), a new pair (B_s, z_s) is obtained that strictly increases the resilience value (line 5), i.e., $z_s > z_{s-1}$. The while loop ends when the upper bound of the CLD problem is reached, i.e., when the resilience value z_s of the current solution s has the same resilience value as selecting all nodes of set N_1 as gateway nodes, which is the optimal value $\mathbf{CLD}(N_1)$.

Remark 4.2.1. At the end of Algorithm 4.1, the obtained solutions $s \in \{1, 2, 3, ...\}$ include all Pareto-optimal solutions. However, some of these solutions might be non Pareto-optimal: although the resilience value strictly increases from one solution to the next one in the while cycle (line 5), it is possible that the 2 solutions have the same cost value, i.e., $B_s = B_{s-1}$ for some index s. When this happens, the solution with index $s-1$ is not Pareto-optimal and is excluded from the Pareto frontier.

In line 5 of Algorithm 4.1, a minimal cost set of gateway nodes M_s must be computed such that its resilience value $\mathbf{CLD}(M_s)$ is strictly higher than the previous value z_{s-1}. In the next subsections, we first present a compact model to evaluate the connectivity resilience, and then we propose a set cover model to optimally select each set M_s.

4.2.3 Connectivity resilience evaluation

Given a subset of network nodes selected as gateway nodes, in this subsection, we discuss how to evaluate the connectivity resilience to multiple link failures.

Let $w_{ij} > 0$ be the connectivity weight of node pair $i, j \in N, i < j$, which represents the importance to the network operator of the connectivity between nodes i and j. Moreover, consider a given positive integer l representing the number of simultaneous link failures for which the network operator aims to improve the resilience of its network.

The network connectivity resilience for l simultaneous link failures is defined as the minimum total weight of all node pairs that can communicate whatever set of l links fails. The connectivity resilience is given by the optimal solution of the Critical Link Detection (CLD) optimization problem.

Additionally, consider that this network has a set of gateway nodes $M \subseteq N$ connected to a third-party network. Let G^M represent the augmented graph obtained by adding to graph G one extra link per pair of gateway nodes, i.e., $G^M = (N, E^M)$, where $E^M = E \cup \{\{i,j\} : i,j \in M, i < j\}$. Additionally, we assume that these extra links never fail (since they represent the virtual links provided by the third-party operator).

Finally, consider the following two sets of decision variables: for each link $\{i,j\} \in E$, variable v_{ij} is 1 if $\{i,j\}$ is selected as a critical link, and 0 otherwise; and, for each node pair $i,j \in N, i < j$, variable u_{ij} is 1 if nodes i and j can communicate (i.e., if exists a path between nodes i and j on the augmented graph G^M without the critical links), and 0 otherwise.

Therefore, the CLD problem is defined by the following mixed integer linear programming (MILP) model:

$$\begin{aligned}
&min \quad z := \sum_{i,j \in N, i<j} w_{ij} u_{ij} && (4.4)\\
&s.t. \quad \sum_{\{i,j\} \in E} v_{ij} \le l, && (4.5)\\
&\qquad u_{ij} + v_{ij} \ge 1, \qquad \{i,j\} \in E^M, && (4.6)\\
&\qquad u_{ij} \ge u_{\{ik\}} + u_{\{jk\}} - 1, \quad i,j \in N, i<j,\ k \in N_{ij}^M, && (4.7)\\
&\qquad v_{ij} = 0, \qquad i,j \in M, i<j, && (4.8)\\
&\qquad v_{ij} \in \{0,1\}, \qquad \{i,j\} \in E, && (4.9)\\
&\qquad u_{ij} \ge 0, \qquad i,j \in N, i<j. && (4.10)
\end{aligned}$$

The objective function (4.4) is the minimization of the connectivity resilience of the solution defined as the total weight of the node pairs that can communicate in the surviving network. Note that, if the connectivity weights are set as unitary, the connectivity resilience z measures the minimum number of node pairs that can still communicate in any failure of at most l links.

Constraint (4.5) guarantees that the number of critical links is not higher than l. Constraints (4.6) ensure that the end-nodes of a link (either from the network itself or a virtual link provided by the third-party network) $\{i, j\} \in E^M$ can communicate if the link is not critical (i.e., if $v_{ij} = 0$).

Constraints (4.7) guarantee that each pair of nodes $i, j \in N$, with $i < j$, can communicate if there is a third node k such that k can communicate with both i and j. In these inequalities, the notation $u_{\{st\}}$ represents variable u_{st} if $s < t$, or variable u_{ts} otherwise. To obtain the minimum number of such constraints, it is enough to consider k as the neighbor nodes of either i or j. Thus, set N_{ij}^M represents the set of neighbor nodes of node i, if node i has a lower degree than node j on the augmented graph G^M, or node j otherwise. If nodes i and j are neighbors (i.e., if $\{i, j\} \in E^M$), they are excluded from N_{ij}^M.

In constraints (4.8), we set all temporary virtual links $\{i, j\}$, with $i, j \in M, i < j$, to non-critical links (because these links are provided by the available third-party network). Finally, constraints (4.9)–(4.10) are the variable domain constraints. Notice that variables u_{ij} are set to real non-negative values since they assume binary values in any optimal solution.

The connectivity resilience of the network, with the given set of gateway nodes M, is the optimal solution value z of the CLD model (4.4)–(4.10). Notation $\mathbf{CLD}(M)$ represents the optimal value of this MILP model. Finally, note that $\mathbf{CLD}(\emptyset)$ represents the connectivity resilience of the network without gateway nodes to a third-party network.

4.2.4 Set cover model

Here, we propose an ILP model, based on set cover constraints, to optimally select the set of gateway nodes M_s such that $\mathbf{CLD}(M_s) > z_{s-1}$ (line 5 of Algorithm 4.1).

First, consider that, for a given set of gateway nodes $M \subseteq N_1$, the set of critical links E' is provided by the optimal solution of $\mathbf{CLD}(M)$. Then, let $C_1, ..., C_m \subset N$ represent the disjoint connected components of the augmented graph G^M without the set of critical links E'. We denote by $\gamma(M)$ the set of these components, i.e., $\gamma(M) = \{C_1, ..., C_m\}$. Additionally, we denote by E_M the set of node pairs of N_1 that belong to different components of $\gamma(M)$.

Then, for a given connectivity resilience threshold z_{s-1}, we define:

$$\Gamma(z_{s-1}) \ := \ \{M \subseteq N_1 : \mathbf{CLD}(M) \leq z_{s-1}\} \tag{4.11}$$

i.e., $\Gamma(z_{s-1})$ represents all the GNS solutions whose connectivity resilience value is not higher than the threshold.

In order to compute a minimal cost set of gateway nodes M_s such that its resilience value $\mathbf{CLD}(M_s)$ is strictly higher than z_{s-1}, we introduce the following ILP model:

$$
\begin{aligned}
min \quad & \sum_{i \in N_1} c_i x_i && (4.12)\\
s.t. \quad & \sum_{\{i,j\} \in E_M} y_{ij} \geq 1, \quad M \in \Gamma(z_{s-1}), && (4.13)\\
& y_{ij} \leq x_i, \qquad \{i,j\} \in E_M,\ M \in \Gamma(z_{s-1}), && (4.14)\\
& y_{ij} \leq x_j, \qquad \{i,j\} \in E_M,\ M \in \Gamma(z_{s-1}), && (4.15)\\
& x_i + x_j \leq 1 + y_{ij}, \ \{i,j\} \in E_M,\ M \in \Gamma(z_{s-1}), && (4.16)\\
& x_i \in \{0,1\}, \qquad i \in N_1, && (4.17)\\
& y_{ij} \in \{0,1\}, \qquad \{i,j\} \in E_M. && (4.18)
\end{aligned}
$$

where x_i is a binary variable indicating whether node $i \in N_1$ is selected or not and variables y_{ij} indicate whether a link between i and j is established or not.

The objective function (4.12) is the minimization of the total cost of the selected gateway nodes. For each set of gateway nodes $M \in \Gamma(z_{s-1})$, constraints (4.13) impose at least an additional link between a pair of gateway nodes linking two components in the corresponding augmented graph G^M (without the set of critical links E'). Constraints (4.14)–(4.15) ensure that if a link between two gateway nodes is established, then the two gateway nodes are selected.

Constraints (4.16) ensure that if two gateway nodes are selected a link between them must be considered. These inequalities are necessary to model correctly the solutions but are always satisfied by any optimal solution of the model obtained by discarding these constraints. Thus, henceforward, constraints (4.16) will not be considered as part of this model.

Finally, constraints (4.17)–(4.18) represent the variable domain constraints.

Remark 4.2.2. Since by definition of gateway nodes, all nodes of M are connected to each other in the augmented graph G^M, and since it is assumed that those links never fail, all nodes of a set of gateway nodes M belong to the same connected component of the augmented graph G^M without the optimal set of critical links.

Remark 4.2.3. For simplicity, we considered that **CLD**(M) has a single optimal solution. In the case that this optimization problem has alternative optimal solutions, $\gamma(M)$ represents the union of all sets of components (associated to each alternative solution) and, similarly, E_M represents the union of all sets of node pairs of N_1 that belong to different components for each optimal set of critical links E' (associated to each alternative solution).

Although this set cover model optimally solves the GNS problem, on our preliminary computational results, model (4.12)–(4.18) prove to be inefficient to compute the complete Pareto frontier (even when an approach such as row generation is considered). Thus, in the next section of this paper, we deduce a lower dimensional set cover model that proved to be considerably better than the previous one.

4.3 Solution approach to the GNS problem

In this section, we proposed an efficient row generation algorithm, based on an alternative set cover model, in order to solve the GNS problem previously proposed. First, a lower dimensional set cover model is deduced resorting to the Fourier-Motzkin elimination [Sch98], and then, we propose a row generation algorithm to compute its Pareto frontier (i.e., its complete set of Pareto-optimal solutions).

4.3.1 A lower dimensional set cover model

Here, our goal is to derive an alternative cover model using only variables x_i (i.e., eliminating all variables y_{ij}). For a given set of gateway nodes $M \in \Gamma(z_{s-1})$, suppose that we intend to eliminate variable y_{st} associated to $\{s,t\} \in E_M$. By rewriting the corresponding inequalities (4.13)–(4.15), we obtain:

$$1 \;-\; \sum_{\{i,j\}\in E_M\setminus\{s,t\}} y_{ij} \;\leq\; y_{st} \;\leq\; \min\{x_s, x_t\} \tag{4.19}$$

Variables y_{st} can be eliminated, using the Fourier-Motzkin elimination, by combining this lower bound of y_{st} with both upper bounds. The following two inequalities are obtained:

$$x_s \;+\; \sum_{\{i,j\}\in E_M\setminus\{s,t\}} y_{ij} \;\geq\; 1 \qquad \text{and} \qquad x_t \;+\; \sum_{\{i,j\}\in E_M\setminus\{s,t\}} y_{ij} \;\geq\; 1 \tag{4.20}$$

These two inequalities can be rewritten in a more compact way as follows:

$$a_{st}x_s \;+\; (1-a_{st})x_t \;+\; \sum_{\{i,j\}\in E_M\setminus\{s,t\}} y_{ij} \;\geq\; 1, \;\text{ with }\; a_{st} \in \{0,1\}, \tag{4.21}$$

When $a_{st} = 1$, we obtain the inequality with variable x_s, and when $a_{st} = 0$, we obtain the inequality with variable x_t. Repeating the elimination process for a subset of variables y_{ij} with $\{i,j\} \in F$, where $F \subseteq E_M$, we obtain

$$\sum_{\{i,j\}\in F} \big(a_{ij}x_i + (1-a_{ij})x_j\big) \;+\; \sum_{\{i,j\}\in E_M\setminus F} y_{ij} \geq 1, \quad a_{ij} \in \{0,1\} \quad \text{for all } \; \{i,j\} \in F. \tag{4.22}$$

Additionally, these inequalities must be iteratively combined with $y_{ij} \leq x_i$ and $y_{ij} \leq x_j$ for all $\{i,j\} \in F$.

The next theorem presents the cover ILP model obtain by using this Fourier-Motzkin elimination procedure for all variables y_{ij}, i.e., for all $\{i,j\} \in E_M$.

Theorem 4.3.1. *Projecting out variables y_{ij} we obtain the model:*

$$\min \quad \sum_{i\in N_1} c_i x_i \tag{4.23}$$

$$s.t. \quad \sum_{\{i,j\}\in E_M} \big(a_{ij}x_i + (1-a_{ij})x_j\big) \geq 1,\; a_{ij} \in \{0,1\} \textit{ for all } \{i,j\}{\in}E_M,\; M{\in}\Gamma(z_{s-1}), \tag{4.24}$$

$$x_i \in \{0,1\}, \quad i \in N_1. \tag{4.25}$$

Proof. Using the Fourier-Motzkin elimination to project out variables y_{ij}, inequalities (4.24) result directly from inequalities (4.13)–(4.15). Inequalities (4.14)–(4.15) imply $x_i \leq 1$, which are dominated by the domain inequalities (4.17), and therefore, omitted. □

For each set of gateway nodes $M \in \Gamma(z_{s-1})$, we obtain a model with $2^{|E_M|}$ constraints (4.24). Each one of these constraints can be rewritten as follows:

$$\sum_{i \in N_1} k_i x_i \geq 1, \text{ where } k_i = \sum_{j \in N_1 : \{i,j\} \in E_M} a_{ij} + \sum_{j \in N_1 : \{j,i\} \in E_M} (1 - a_{ji}) \text{ for each } i \in N_1. \tag{4.26}$$

Notice that, with these parameters, we deduce that, for each $i \in N_1$, $k_i \in \{0, \dots, \delta_i\}$, and that $\sum_{i \in N_1} k_i = |E_M|$, where δ_i is the degree of node i in graph (N_1, E_M).

Let $\sigma(k_i) = 1$, if $k_i \geq 1$, and $\sigma(k_i) = 0$ otherwise. Considering the domain constraints (4.25), a (feasible) solution satisfies (4.26) if and only if it satisfies

$$\sum_{i \in N_1} \sigma(k_i) x_i \geq 1, \text{ where } k_i = \sum_{j \in N_1 : \{i,j\} \in E_M} a_{ij} + \sum_{j \in N_1 : \{j,i\} \in E_M} (1 - a_{ji}) \text{ for each } i \in N_1. \tag{4.27}$$

As $\sum_{i \in N_1} k_i x_i \geq \sum_{i \in N_1} \sigma(k_i) x_i \geq 1$, inequalities (4.26) are dominated by (4.27). Therefore, a tighter model is obtained using the cover-type inequalities (4.27) instead of inequalities (4.26).

A deeper look into the cover-type inequalities shows that some of these inequalities are redundant and can be eliminated. Observe that, for instance, if $R_1 \subset R_2 \subseteq N_1$ inequality $\sum_{i \in R_1} x_i \geq 1$ implies inequality $\sum_{i \in R_2} x_i \geq 1$, and therefore the latter inequality can be eliminated as it is dominated.

To find the non-dominated inequalities, let N_1 be partitioned as $\{S_1, \dots, S_m\}$, where S_t is the set of nodes in N_1 belonging to component C_t (i.e., $S_t = N_1 \cap C_t$). Then, we have the following lemma:

Lemma 4.3.2. *If $\sigma(k_i) = 0$ for some $i \in S_t$, then $\sigma(k_j) = 1$ for all $j \in N_1 \setminus S_t$.*

Proof. If $\sigma(k_i) = 0$ then $k_i = 0$. Thus, $a_{ij} = 0$ for all $j \in N_1 : \{i,j\} \in E_M$ and $a_{ji} = 1$ for all $j \in N_1 : \{j,i\} \in E_M$ (node j is selected to the cover inequality in both cases). As node i is in component C_t, it must be connected with all nodes in N_1 outside C_1, which means that $k_j \geq 1$ for all $j \in N_1 \setminus S_t$. □

Lemma 4.3.2 shows that only coefficients in one component can be null. Now, we can observe that constraints (4.27) with $\sigma(k_i) = 0$ for all $i \in C_t$ do exist, since the constraint (4.27) exists with $k_i = 0$ for all $i \in S_t$. Hence, the set of non-dominated constraints is given by:

$$\sum_{i \in N_1 \setminus C} x_i \geq 1, \quad C \in \gamma(M), \; M \in \Gamma(z_{s-1}). \tag{4.28}$$

For completeness, we present the resulting covering model, represented as $\mathbf{Cover}(z_{s-1})$, which includes only the non-dominated constraints:

$$\begin{aligned} min \quad & \sum_{i\in N_1} c_i x_i && (4.29)\\ s.t. \quad & \sum_{i\in N_1\setminus C} x_i \geq 1, \ \ C\in\gamma(M), \ M\in\Gamma(z_{s-1}), && (4.30)\\ & x_i\in\{0,1\}, \ i\in N_1. && (4.31)\end{aligned}$$

The objective function (4.29) is the minimization of the total cost of the selected gateway nodes. Constraints (4.30) represent a set of cover cuts for each set of gateway nodes $M \subseteq N_1$ with connectivity resilience not higher than the threshold z_{s-1}, i.e., each $M \in \Gamma(z_{s-1})$. Moreover, each set of cover cuts include one constraint for each component in the corresponding augmented graph G^M without their set of critical links, i.e., each $C \in \gamma(M)$. Finally, each constraint (4.30) guarantees that, for each disjoint connected component $C \in \gamma(M)$, a gateway node i belonging to N_1 is selected in the complement node set $N_1\setminus C$. This is a necessary and sufficient condition to guarantee that the resilience value of the solution is strictly higher than z_{s-1}. Finally, constraints (4.31) are the variable domain constraints.

The following example gives a better understanding on how model (4.29)–(4.31) can be deduced from (4.12)–(4.18).

Example 4.3.3. Consider a graph $G = (N, E)$ and a set of candidate gateway nodes $N_1 = \{1, 2, 3, 4, 5\} \subseteq N$. Given a set of gateway nodes M, suppose that C_1, C_2 and C_3 represent all disjoint connected components of the graph G^M without its optimal critical links. Additionally, suppose that these components are such that $\{1, 2\} \subset C_1$, $\{3, 4\} \subset C_2$ and $\{5\} \subset C_3$. Then, the set of node pairs of N_1 that belong to different components is defined by $E_M = \{\{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}$.

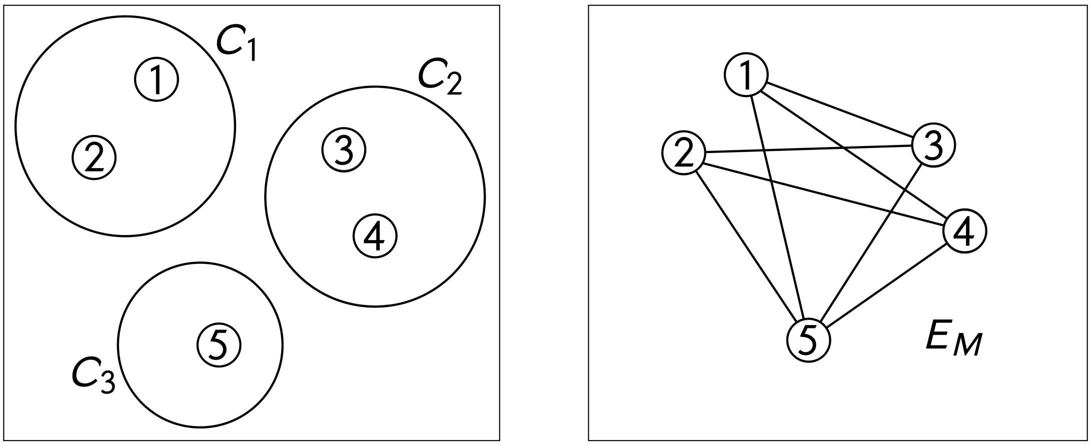


Figure 4.2: Illustration of the components separation of graph G^M without its optimal critical links (left), and representation of graph (N_1, E_M) (right).

First, model (4.12)–(4.18) is given by:

$$\begin{aligned}
min\quad & c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5\\
s.t.\quad & y_{13} + y_{14} + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35} \geq 1,\\
& y_{13} \leq x_1,\ y_{14} \leq x_1,\ y_{15} \leq x_1,\ y_{23} \leq x_2,\ y_{24} \leq x_2,\ y_{25} \leq x_2,\ y_{35} \leq x_3,\ y_{45} \leq x_4,\\
& y_{13} \leq x_3,\ y_{14} \leq x_4,\ y_{15} \leq x_5,\ y_{23} \leq x_3,\ y_{34} \leq x_4,\ y_{25} \leq x_5,\ y_{35} \leq x_5,\ y_{45} \leq x_5,\\
& x_1, x_2, x_3, x_4, x_5 \in \{0, 1\},\\
& y_{13}, y_{14}, y_{15}, y_{23}, y_{24}, y_{25}, y_{35}, y_{45} \in \{0, 1\}.
\end{aligned}$$

In order to remove variable y_{13}, by rearranging the inequalities that involve this variable, we obtain:

$$1 - (y_{14} + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35}) \ \leq\ y_{13} \ \leq\ \min\{x_1, x_3\}$$

Using the Fourier-Motzkin elimination to eliminate variable y_{13} from the model, we have:

$$\begin{aligned}
min\quad & c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5\\
s.t.\quad & x_1 + y_{14} + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35} \geq 1,\\
& x_3 + y_{14} + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35} \geq 1,\\
& y_{14} \leq x_1,\ y_{15} \leq x_1,\ y_{23} \leq x_2,\ y_{24} \leq x_2,\ y_{25} \leq x_2,\ y_{35} \leq x_3,\ y_{45} \leq x_4,\\
& y_{14} \leq x_4,\ y_{15} \leq x_5,\ y_{23} \leq x_3,\ y_{34} \leq x_4,\ y_{25} \leq x_5,\ y_{35} \leq x_5,\ y_{45} \leq x_5,\\
& x_1, x_2, x_3, x_4, x_5 \in \{0, 1\},\\
& y_{14}, y_{15}, y_{23}, y_{24}, y_{25}, y_{35}, y_{45} \in \{0, 1\}.
\end{aligned}$$

Similarly, by eliminating variable y_{14} from the model, we obtain:

$$\begin{aligned}
min\quad & c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5\\
s.t.\quad & 2x_1 + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35} \geq 1,\\
& x_1 + x_4 + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35} \geq 1,\\
& x_1 + x_3 + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35} \geq 1,\\
& x_3 + x_4 + y_{15} + y_{23} + y_{24} + y_{25} + y_{34} + y_{35} \geq 1,\\
& y_{15} \leq x_1,\ y_{23} \leq x_2,\ y_{24} \leq x_2,\ y_{25} \leq x_2,\ y_{35} \leq x_3,\ y_{45} \leq x_4,\\
& y_{15} \leq x_5,\ y_{23} \leq x_3,\ y_{34} \leq x_4,\ y_{25} \leq x_5,\ y_{35} \leq x_5,\ y_{45} \leq x_5,\\
& x_1, x_2, x_3, x_4, x_5 \in \{0, 1\},\\
& y_{15}, y_{23}, y_{24}, y_{25}, y_{35}, y_{45} \in \{0, 1\}.
\end{aligned}$$

Projecting out all variables y_{ij} using the Fourier-Motzkin elimination, we obtain the following cover model, where all inequalities are written with the proposed compact notation.

$$\begin{aligned}
min\quad & c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5\\
s.t.\quad & a_{13}x_1 + (1 - a_{13})x_3 + a_{14}x_1 + (1 - a_{14})x_4 + a_{15}x_1 + (1 - a_{15})x_5 + a_{23}x_2\\
& + (1 - a_{23})x_3 + a_{24}x_2 + (1 - a_{24})x_4 + a_{25}x_2 + (1 - a_{25})x_5 + a_{35}x_3 + (1 - a_{35})\\
& + x_5 + a_{45}x_4 + (1 - a_{45})x_5 \geq 1\\
& \quad \text{for all } \ a_{13}, a_{14}, a_{15}, a_{23}, a_{24}, a_{25}, a_{35}, a_{45} \in \{0, 1\},\\
& x_1, x_2, x_3, x_4, x_5 \in \{0, 1\}.
\end{aligned}$$

By rearranging the set of constraints and using the σ function previously defined on the coefficients of each x_i, we obtain the following set cover model with constraints (4.27):

$$\begin{aligned} \mathit{min} \quad & c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5 \\ s.t. \quad & \sigma(a_{13} + a_{14} + a_{15})x_1 + \sigma(a_{23} + a_{24} + a_{25})x_2 \\ & \quad + \sigma((1 - a_{13}) + (1 - a_{23}) + a_{34})x_3 + \sigma((1 - a_{14}) + (1 - a_{24}) + a_{45})x_4 \\ & \quad + \sigma((1 - a_{15}) + (1 - a_{25}) + (1 - a_{35}) + (1 - a_{45}))x_5 \geq 1 \\ & \qquad \text{for all } \ a_{13}, a_{14}, a_{15}, a_{23}, a_{24}, a_{25}, a_{35}, a_{45} \in \{0, 1\}, \\ & x_1, x_2, x_3, x_4, x_5 \in \{0, 1\}. \end{aligned}$$

The coefficients k_i, defined in (4.26), of each node $i \in N_1$ are given by: $k_1 = a_{13}+a_{14}+a_{15}$, $k_2 = a_{23} + a_{24} + a_{25}$, $k_3 = (1 - a_{13}) + (1 - a_{23}) + a_{34}$, $k_4 = (1 - a_{14}) + (1 - a_{24}) + a_{45}$, and $k_5 = (1-a_{15})+(1-a_{25})+(1-a_{35})+(1-a_{45})$. Notice that there exists a subset of constraints (4.27) such that $k_i \geq 1$ (i.e., $\sigma(k_i) = 1$) for all $i \in N_1$. Each one of these, when simplified with the σ function, is simply the inequality $x_1 + x_2 + x_3 + x_4 + x_5 \geq 1$.

All the remaining constraint are such that exists (at least one) $i \in N_1$ such that $k_i = 0$ (i.e. $\sigma(i) = 0$). For example, if $k_1 = 0$, then $a_{13} = a_{14} = a_{15} = 0$, which means that $\sigma(k_3) = \sigma(k_4) = \sigma(k_5) = 1$. We obtain the set of constraints $\sigma(a_{23} + a_{24} + a_{25})x_2 + x_3 + x_4 + x_5 \geq 1$, for all $a_{23}, a_{24}, a_{25} \in \{0, 1\}$. Using this process for each $i \in N_1$, we obtain the following model:

$$\begin{aligned} \mathit{min} \quad & c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5 \\ s.t. \quad & x_1 + x_2 + x_3 + x_4 + x_5 \geq 1, \\ & \sigma(a_{23} + a_{24} + a_{25})x_2 + x_3 + x_4 + x_5 \geq 1, && \forall a_{23}, a_{24}, a_{25} \in \{0, 1\}, \\ & \sigma(a_{13} + a_{14} + a_{15})x_1 + x_3 + x_4 + x_5 \geq 1, && \forall a_{13}, a_{14}, a_{15} \in \{0, 1\}, \\ & x_1 + x_2 + \sigma((1 - a_{14}) + (1 - a_{24}) + a_{45})x_4 + x_5 \geq 1, && \forall a_{14}, a_{24}, a_{45} \in \{0, 1\}, \\ & x_1 + x_2 + \sigma((1 - a_{13}) + (1 - a_{23}) + a_{35})x_3 + x_5 \geq 1, && \forall a_{13}, a_{23}, a_{35} \in \{0, 1\}, \\ & x_1 + x_2 + x_3 + x_4 \geq 1, \\ & x_1, x_2, x_3, x_4, x_5 \in \{0, 1\}. \end{aligned}$$

In some inequalities of this model, some coefficients $\sigma()$ can still be either 0 or 1 according to the values of parameters a_{ij}. However, the constraints with all of these coefficients at 0 are the non-dominated ones, and therefore, we can set all of these coefficients to 0. Finally, by eliminating all redundant inequalities, we obtain the set cover model (4.29)–(4.31):

$$\begin{aligned} \mathit{min} \quad & c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5 \\ s.t. \quad & x_3 + x_4 + x_5 \geq 1, \\ & x_1 + x_2 + x_5 \geq 1, \\ & x_1 + x_2 + x_3 + x_4 \geq 1, \\ & x_1, x_2, x_3, x_4, x_5 \in \{0, 1\}, \end{aligned}$$

where each inequality corresponds to the cover constraint associated to $N_1\backslash C_1 = \{3, 4, 5\}$, $N_1\backslash C_2 = \{1, 2, 5\}$ and $N_1\backslash C_3 = \{1, 2, 3, 4\}$, respectively.

Remark 4.3.4. Note that the proposed set cover model (4.29)–(4.31) can become unfeasible. That condition is reached when a constraint (4.30) is added for a component $C \in \gamma(M)$ and a set of gateway nodes $M \in \Gamma(r)$ such that $N_1 \backslash C = \emptyset$, i.e., a constraint in the form $\sum_{i \in \emptyset} x_i \geq 1$ which turns the problem unfeasible. This condition is reached when all possible gateway nodes N_1 belong to the same component C, i.e., $N_1 \subseteq C$.

Furthermore, when this condition is reached for a given threshold resilience z_s, it means that the connectivity resilience value z_s is the highest possible connectivity resilience that can be obtained with the set of possible gateway nodes N_1. Therefore, this condition defines the stopping criteria of the proposed algorithm, i.e., when $z_s = \mathbf{CLD}(N_1)$, the algorithm reaches the last Pareto-optimal solution.

4.3.2 Row generation algorithm

The main challenge of solving $\mathbf{Cover}(z_{s-1})$ is that the total number of constraints (4.30) increases exponentially with the increase of the connectivity resilience threshold z_{s-1}.

Here, we use a row generation technique to solve the GNS problem where constraints (4.30) are initially ignored and, then, they are iteratively added to the set cover model. Algorithm 4.2 describes the proposed approach where, when compared with Algorithm 4.1, two initial steps are added (lines 3–4) and the general step in Algorithm 4.1 (line 5) is replaced by a repeat until loop (lines 7–11) and a final step (line 12) in Algorithm 4.2.

Algorithm 4.2 Row generation based algorithm for GNS

```
 1: $s \leftarrow 1$
 2: $(B_s, z_s) \leftarrow \big(0, \mathbf{CLD}(\emptyset)\big)$
 3: Initialize Cover() with objective (4.29) and domain constraints (4.31)
 4: $M \leftarrow \emptyset$
 5: while $z_s < \mathbf{CLD}(N_1)$ do
 6:     $s \leftarrow s + 1$
 7:     repeat
 8:         Add constraints (4.30) to Cover() for each $C \in \gamma(M)$
 9:         $x^* \leftarrow$ optimal solution of Cover()
10:         $M \leftarrow \{i \in N_1 : x_i^* = 1\}$
11:     until $\mathbf{CLD}(M) > z_{s-1}$
12:     $M_s \leftarrow M$
13:     $(B_s, z_s) \leftarrow \big(\sum_{i \in M_s} c_i,\ \mathbf{CLD}(M_s)\big)$
14: end while
```

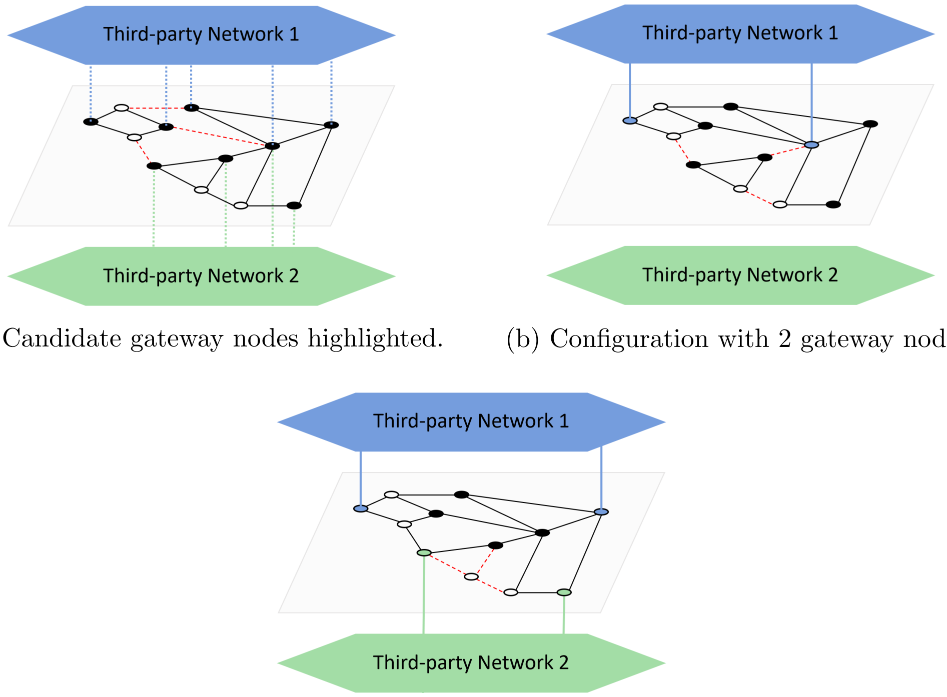
Again, Algorithm 4.2 starts (lines 1–2) by computing the first Pareto-optimal solution $s = 1$ which is the solution without gateway nodes. Then, the **Cover**() model is initialized (line 3) only with the objective function (4.29) and the variable domain constraints (4.31) and the initial set of selected gateway nodes M is initialized empty (line 4).

In each iteration of the main while loop (lines 5–14), a new candidate solution s is obtained with solution values (B_s, z_s) such that $z_s > z_{s-1}$. In the inner repeat until cycle, the constraints (4.30) corresponding to the previous gateway node set M are first added in line 8 to the **Cover**() model. Then, **Cover**() is solved to compute its optimal solution (line 9) defining the new set of gateway nodes M (line 10). Finally, if its resilience value, given by $\mathbf{CLD}(M)$, is not strictly higher than z_{s-1}, the repeat until cycle is repeated. Otherwise, set M becomes the candidate solution s (line 12), with the solution values (B_s, z_s) (line 13).

Note that the repeat until cycle (lines 7–11) is the row generation algorithm that solves the **Cover**(z_{s-1}) presented in the previous subsection.

4.4 GNS problem with multiple third-party networks

In this section, we explain how to generalize the solution approach presented in the previous sections to the case where multiple third-party networks are available to provide additional connectivity. Figure 4.3 presents an illustration of this problem with two third-party networks.



(a) Candidate gateway nodes highlighted.

(b) Configuration with 2 gateway nodes.

(c) Configuration with 4 gateway nodes.

Figure 4.3: Illustration of two distinct third-party networks, with provision of temporary virtual links between the gateway nodes for the simultaneous failure of $l = 3$ links (highlighted in dashed red).

Consider the example in Figure 4.3(a) of a given network with two available third-party networks whose connectivity weights are unitary for all node pairs. This representation also indicates (in black) the nodes that can be used as gateway nodes to each third-party network (in general, a node can be a gateway node to more than one third-party networks). Without resorting to any third-party network, the $l = 3$ critical links (highlighted in dashed red) split the network into one components of 4 nodes and another of 8 nodes (with a total connectivity of 34).

In Figure 4.3(b), two gateway nodes are used to third-party Network 1 so that if the previous critical links fail, the two network components can be connected through Network 1. In such solution, the resulting set of critical links can only split the network into two components of 3 and 9 nodes, respectively (with a total connectivity of 39).

Finally, in Figure 4.3(c), two additional gateway nodes are used to third-party Network 2 so that if the previous critical links fail, the two network components can be connected through Network 2. In such solution, the resulting set of critical links can only isolate one node from all other nodes (with a total connectivity of 55). Associating a cost value for each possible gateway node, we obtain in this way two different solutions, with two different trade-offs between the solution cost and the connectivity resilience increase.

In order to solve this extended GNS problem, consider that $|T|$ different third-party networks are available to the telecommunication operator. Consider $N_\theta \subseteq N$ as the subset of all nodes that can act as gateway nodes to the third-party network $\theta \in T$. Let $c_i^\theta > 0$, with $i \in N_\theta$, represent the cost of turning node i into a gateway node to the third-party network $\theta \in T$ (we consider that the same node can be configured to become a gateway node to more than one third-party networks).

A GNS solution to this problem is represented by a family of sets $\mathcal{M} = \{M_1, ..., M_{|T|}\}$, where $M_\theta \subseteq N_\theta$ is the set of selected gateway nodes for third-party network $\theta \in T$. Aiming to extend to multiple third-party networks the row generation algorithm previously proposed for a single third-party network, first, we must redefine the CLD problem for a family of gateway node sets $\mathcal{M}$.

4.4.1 Connectivity resilience evaluation

Considering the GNS solution $\mathcal{M} = \{M_1, ..., M_{|T|}\}$, let $G^{\mathcal{M}}$ now represent the augmented graph obtained by adding to graph G, for each set of gateway nodes $M \in \mathcal{M}$, one extra link per pair of gateway nodes, i.e., $G^{\mathcal{M}} = (N, E^{\mathcal{M}})$, where $E^{\mathcal{M}} = E \cup \bigcup_{M \in \mathcal{M}} \{\{i,j\} : i,j \in M, i < j\}$.

Thus, the CLD problem can be redefined as the following MILP model:

$$\begin{aligned}
min \quad & z := \sum_{i,j \in N, i<j} w_{ij} u_{ij} && && (4.32)\\
s.t. \quad & \sum_{\{i,j\} \in E} v_{ij} \leq l, && && (4.33)\\
& u_{ij} + v_{ij} \geq 1, && \{i,j\} \in E^{\mathcal{M}}, && (4.34)\\
& u_{ij} \geq u_{\{ik\}} + u_{\{jk\}} - 1, && i,j \in N, i<j,\ k \in N_{ij}^{\mathcal{M}}, && (4.35)\\
& v_{ij} = 0, && i,j \in M, i<j,\ M \in \mathcal{M}, && (4.36)\\
& v_{ij} \in \{0,1\}, && \{i,j\} \in E, && (4.37)\\
& u_{ij} \geq 0, && i,j \in N, i<j. && (4.38)
\end{aligned}$$

This extended MILP model to the CND problem is identical to MILP model (4.4)–(4.10), with the main difference that constraints are now defined over the augmented $G^{\mathcal{M}}$ (that considered the GNS solution with multiple third-parties).

In constraints (4.35), set $N_{ij}^{\mathcal{M}}$ now represents the set of neighbor nodes of node i, if node i has lower degree than node j on the augmented graph $G^{\mathcal{M}}$, or node j otherwise. Furthermore, in constraints (4.36), for each set of gateway nodes selected $M \in \mathcal{M}$ (to each distinct third-party network), we set all temporary virtual links $\{i,j\}$, with $i,j \in M, i<j$, to non-critical links.

The connectivity resilience of a network with a family of gateway node sets $\mathcal{M}$ is the optimal solution of the CLD model (4.32)–(4.38), and the optimal value of this model will be referred henceforward as $\mathbf{CLD}(\mathcal{M})$. Finally, notice that if $|T| = 1$ (i.e. case with a single third-party network), both MILP models (4.4)–(4.10) and (4.32)–(4.38) are exactly the same, and therefore, there is no need to distinguish the notation used to represent the connectivity resilience.

4.4.2 Row generation algorithm

Given a family of gateway node sets $\mathcal{M}$, consider that, in the augmented graph $G^{\mathcal{M}}$ without the set of critical links given by the optimal solution of $\mathbf{CLD}(\mathcal{M})$, the set of nodes N is split into m disjoint connected components $C_1, ..., C_m$. Again, denote by $\gamma(\mathcal{M})$ the set of these components, i.e., $\gamma(\mathcal{M}) = \{C_1, ..., C_m\}$.

First, for each third-party network $\theta \in T$, consider that the binary decision variable x_i^θ is 1 if $i \in N_\theta$ is selected as a gateway node for the third-party network θ, and 0 otherwise.

Algorithm 4.3 generalizes the previous row generation algorithm (i.e. Algorithm 4.2) to solve the GNS problem with multiple third-party networks. The initial set cover model is defined (line 3) as:

$$min \quad \sum_{\theta \in T} \sum_{i \in N_\theta} c_i^\theta x_i^\theta \tag{4.39}$$

$$s.t. \quad x_i^\theta \in \{0, 1\}, \ \ i \in N_\theta, \ \ \theta \in T. \tag{4.40}$$

Additionally, on each iteration $\varepsilon \in \{1, 2, 3, ...\}$ of the row generation algorithm (lines 8–16), the following set of $|T|$ binary variables (one for each third-party network) is introduced:

$$y_\varepsilon^\theta = \begin{cases} 1, & \text{if third-party network } \theta \text{ is selected in iteration } \varepsilon; \\ 0, & \text{otherwise.} \end{cases}$$

For a given family of gateway node sets $\mathcal{M}$, the following constraints represent the generalization of constraints (4.30) to multiple third-party networks:

$$\sum_{i \in N_\theta \setminus C} x_i^\theta \geq y_\varepsilon^\theta, \quad \theta \in T, \ C \in \gamma(\mathcal{M}), \tag{4.41}$$

$$\sum_{\theta \in T} y_\varepsilon^\theta \geq 1, \tag{4.42}$$

$$y_\varepsilon^\theta \in \{0, 1\}, \quad \theta \in T. \tag{4.43}$$

Constraints (4.41) represent the set cover constraints (4.30) when the third-party network $\theta \in T$ is selected to cover the GNS solution in iteration ε (i.e., if $y_\varepsilon^\theta = 1$). Constraints (4.42) guarantee that at least one third-party network is selected to cover that iteration. Finally, constraints (4.43) are the variable domain constraints of the new variables y_ε^θ, for each $\theta \in T$. These constraints are added iteratively by Algorithm 4.3 (lines 10–12).

Algorithm 4.3 Row generation based algorithm for GNS with multiple third-party networks

```
$s \leftarrow 1$
$(B_s, z_s) \leftarrow \big(0, \mathbf{CLD}(\emptyset)\big)$
Initialize Cover() ILP with objective (4.39) and domain constraints (4.40)
$\mathcal{M} \leftarrow \emptyset$
$\varepsilon \leftarrow 0$
while $z_s < \mathbf{CLD}(\{N_1, ..., N_{|T|}\})$ do
    $s \leftarrow s + 1$
    repeat
        $\varepsilon \leftarrow \varepsilon + 1$
        Add variables $y^\theta_\varepsilon \in \{0, 1\}$ to Cover() for each $\theta \in T$
        Add constraints (4.41) to Cover() for each $C \in \gamma(\mathcal{M})$
        Add constraint (4.42) to Cover()
        $x^* \leftarrow$ optimal solution of Cover()
        $M_\theta \leftarrow \{i \in N_\theta : (x^\theta_i)^* = 1\}$ for each $\theta \in T$
        $\mathcal{M} \leftarrow \{M_1, ..., M_{|T|}\}$
    until $\mathbf{CLD}(\mathcal{M}) > z_{s-1}$
    $\mathcal{M}_s \leftarrow \mathcal{M}$
    $(B_s, z_s) \leftarrow \big(\sum_{\theta \in T} \sum_{i \in M_\theta} c^\theta_i,\ \mathbf{CLD}(\mathcal{M})\big)$
end while
```

4.5 Computational Results

All computational results reported in this section were obtained using the optimization software *Gurobi Optimizer* version 9.0.2, with programming language *Julia* version 1.4.1, running on a PC with an Intel Core i7-8700, 3.2 GHz and 16 GB RAM. The computational results are based on 4 network topologies with publicly available information (Cost266, Janos-US and Germany50 in [OWPT10], Coronet in [Sim14]) and shown in Figure 4.4. Table 4.1 presents the number of nodes $|N|$, number of edges $|E|$ and the average node degree $\bar{\delta}$ of each topology. In addition, the total number of node pairs of each network is shown in column 'No. node pairs' (which is the maximum connectivity resilience value when considering unitary connectivity weights).

Table 4.1: Topology characteristics of each network.

Network	$\|N\|$	$\|E\|$	$\bar{\delta}$	No. node pairs
Janos-US	26	42	3.23	325
Cost266	37	57	3.08	666
Germany50	50	88	3.52	1225
Coronet	75	99	2.64	2775

After running several preliminary computational tests over different node cost values c_i, we have concluded that the computational complexity of the problem with unitary costs and non-unitary costs is quite similar. Moreover, by considering unitary costs, the objective function (4.29) value represents the selected number of gateway nodes, which allows an easier

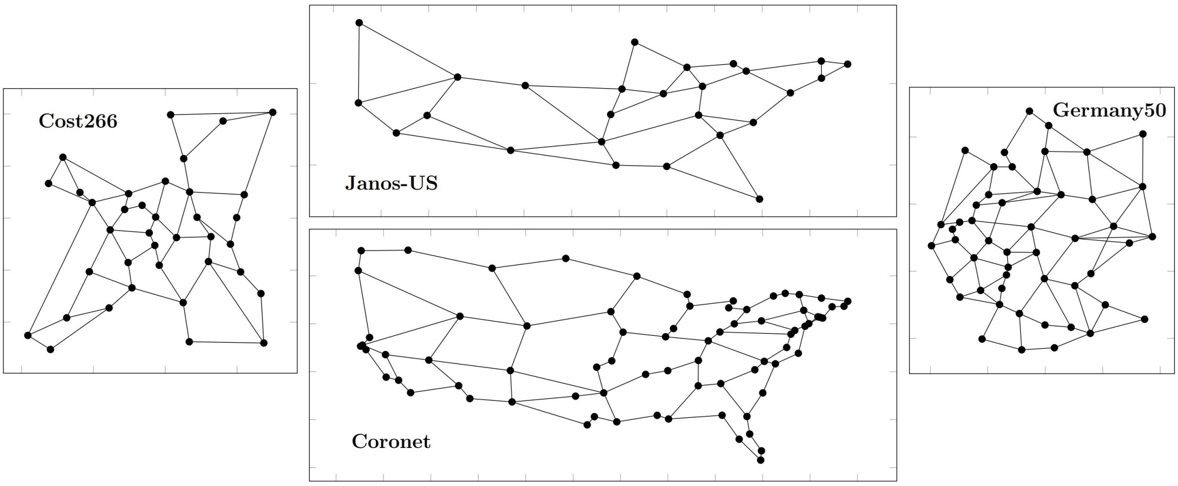


Figure 4.4: Network topologies.

interpretation of the results. Therefore, we will consider $c_i = 1$ for all $i \in N$ henceforward.

In the remaining of this section, we first present and discuss the numerical results of Algorithm 4.2 considering two cases: unitary connectivity weights (Section 4.5.1) and different connectivity weights (Section 4.5.2). Then, Section 4.5.3 provides additional insights on the Pareto frontiers of both cases. Finally, Section 4.5.4 presents and discusses the numerical results of Algorithm 4.3 for multiple third-party networks.

4.5.1 Single third-party network: unitary connectivity weights

Table 4.2 presents the results for the particular case of Germany50 topology and $l = 6$ critical links, obtained with Algorithm 4.2. These results consider the most challenging scenario in terms of optimization, which is to consider $N_1 = N$ (i.e., all network nodes can be selected as gateway nodes).

Columns 'B' and 'z' present the 2 objective values of each obtained candidate solution, with Pareto-optimal solutions highlighted in bold. Column 'z (%)' presents the connectivity resilience as a percentage of its maximum value $\binom{N}{2} = 1225$. For each obtained candidate solution, column 'No. Iterations' presents the number of row generation iterations (repeat until loop in lines 7–11 of Algorithm 4.2), column 'No. Cuts' presents the number of cover constraints (4.30) added in such iterations and column 'Time (sec)' presents the running time of the method (in seconds). The last row presents the total values (with the total runtime in the format HH:MM:SS).

The most significant conclusion is that Algorithm 4.2 was able to compute the complete Pareto frontier, in a total of 13 Pareto-optimal solutions, in 6 minutes and 26 seconds. The results of this case illustrate many trends that are common to the majority of the tested instances.

First, Algorithm 4.2 has computed 18 candidate solutions, from which a significant percentage (5 in total) are not Pareto-optimal solutions. Moreover, the majority of these solutions are within the initial computed candidates. This is because the number of cover constraints (4.30) is low at the beginning, which results in many alternative optimal solutions to the set

Table 4.2: Germany50 results with $l = 6$ critical links.

B	z	z (%)	No. Iterations	No. Cuts	Runtime (sec)
0	**681**	55,6	-	-	0,2
2	825	67,3	1	2	0,7
2	**856**	69,9	4	8	2,9
4	889	72,6	5	10	3,1
4	914	74,6	2	4	3,1
4	924	75,4	5	11	4,7
4	**961**	78,4	5	10	5,1
5	**994**	81,1	3	6	5,6
6	**1000**	81,6	16	37	12,8
7	**1037**	84,7	24	51	30,5
8	**1041**	85,0	5	12	9,5
11	**1081**	88,2	35	87	47,3
12	1082	88,3	5	17	9,8
12	**1084**	88,5	33	96	43,4
16	**1128**	92,1	67	185	57,9
25	**1129**	92,2	173	522	104,3
28	**1176**	96,0	45	117	26,1
50	**1225**	100,0	81	184	19,2
			509	1359	6 min 26 sec

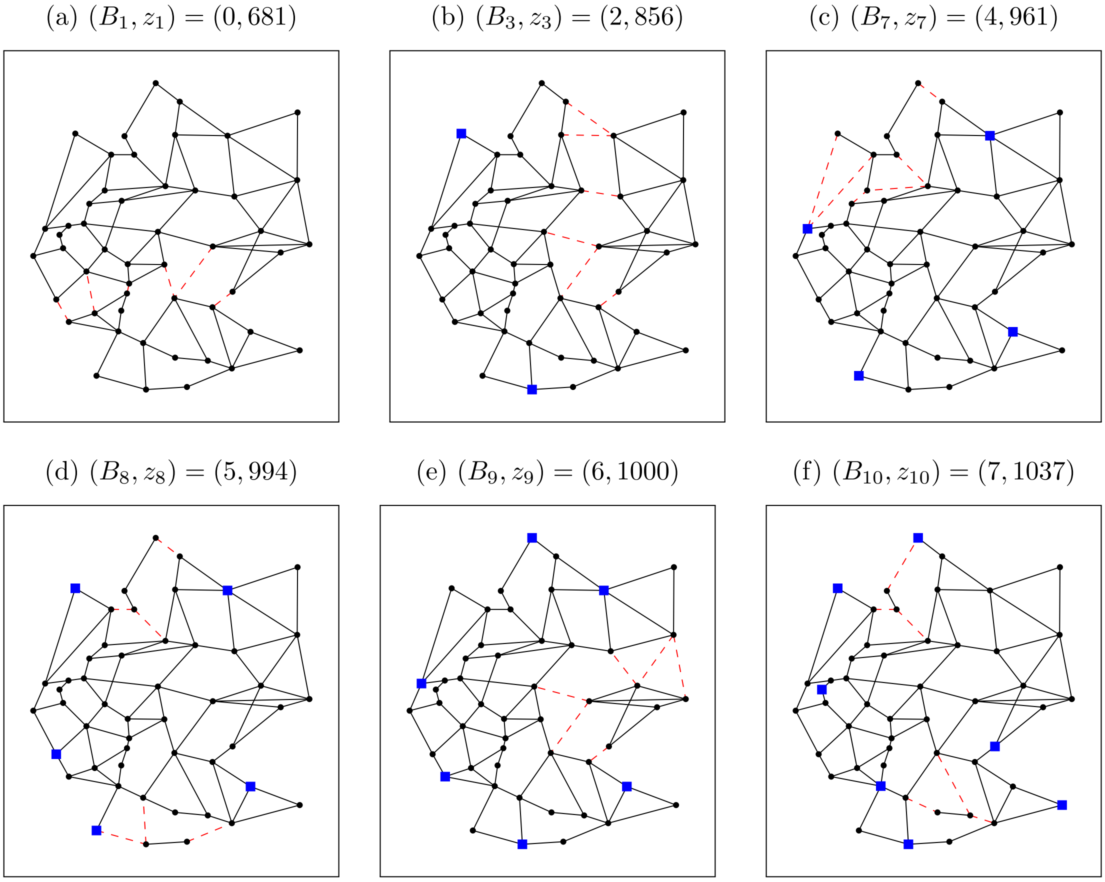
cover problem.

Second, because all nodes can be selected as gateway nodes, the connectivity resilience maximum value is always reached in the last Pareto-optimal solution, i.e., $\binom{50}{2} = 1225$. Note that, since Germany50 topology has a maximum node degree of 5, with 6 critical links, the maximal resilience value is only obtained when all nodes are selected as gateway nodes.

Third, although the total number of cover constraints (4.30) keeps increasing from one computed candidate solution to the next one, by analyzing the runtime column combined with the number of iteration of each computed solution, we conclude that the maximum complexity of the proposed algorithm is when the set cover optimal solution selects about $N/2$ gateway nodes (in this case, 25 gateway nodes).

Figure 4.5 presents the first 6 Pareto-optimal solutions of Table 4.2. Two interesting observations from Figure 4.5 are that the gateway nodes in these Pareto-optimal solutions are mainly in the network periphery and, from one solution to the next one, the optimal gateway nodes can completely change as it happens in some cases.

To compute the full set of computational results, we have considered $l \in \{2, 3, 4, 5, 6, 7\}$ critical links for all 4 network topologies. Note that all topologies are 2-connected (i.e., there are at least 2 node disjoint paths between every pair of nodes) and, therefore, the case of $l = 1$ critical link is not considered (no single link failure degrades the connectivity resilience of the network). We have considered again the most challenging case, which is to consider $N_1 = N$ (all nodes can be selected as gateway nodes). The solutions obtained for these problem instances define the best possible Pareto frontier, i.e., all optimal pairs of solution



(a) $(B_1, z_1) = (0, 681)$

(b) $(B_3, z_3) = (2, 856)$

(c) $(B_7, z_7) = (4, 961)$

(d) $(B_8, z_8) = (5, 994)$

(e) $(B_9, z_9) = (6, 1000)$

(f) $(B_{10}, z_{10}) = (7, 1037)$

Figure 4.5: Illustration of the first 6 Pareto-optimal solutions, for Germany50 with unitary weights and $l = 6$ critical links (gateway nodes highlighted in blue squares and critical links in dashed red).

values (B, z) considering $N_1 = N$ cannot be worst than considering other cases of possible gateway nodes, even when multiple third-party networks are available. Furthermore, since we consider unitary gateway costs, each obtained Pareto-optimal pair of values (B, z) represents the minimum number of gateway nodes B required to reach the connectivity resilience z.

Table 4.3 presents the most relevant data of the full set of results obtained with Algorithm 4.2. For each network topology and each value of l, row 'No. Candidate solutions' presents the number of pairs (B, z), row 'No. Pareto-optimal solutions' presents the number of Pareto-optimal solutions, row 'No Iterations' presents the total number of row generation iterations and row 'No. Cover Cuts (4.30)' presents the total number of cover cuts added to reach the complete Pareto frontier. Finally, 'Runtime (HH:MM:SS)' is the total computational time of Algorithm 4.2 for each case.

These results show that Algorithm 4.2 was able to compute the complete Pareto frontier for all cases. For each network topology, the increase in the number l of critical links also increases the problem complexity (due to the increase of the number of candidate and Pareto-optimal solutions and the number of iterations and added cover cuts), which makes the running times to become larger (in fact, we observe an exponential increase of the running times with respect

Table 4.3: Computational results summary (unitary case).

Network	l	2	3	4	5	6	7
Janos-US	No. Candidate sol.	3	6	10	15	24	25
	No. Pareto-optimal sol.	3	4	6	9	11	15
	No. Iterations	5	25	54	140	391	774
	No. Cover Cuts (4.30)	10	50	109	327	1029	2146
	Runtime (HH:MM:SS)	00:00:01	00:00:02	00:00:04	00:00:09	00:00:24	00:00:54
Cost266	No. Candidate sol.	3	6	11	17	25	27
	No. Pareto-optimal sol.	3	5	9	11	14	16
	No. Iterations	10	47	94	239	773	1803
	No. Cover Cuts (4.30)	20	94	207	584	2162	5322
	Runtime (HH:MM:SS)	00:00:03	00:00:11	00:00:21	00:00:50	00:02:03	00:04:36
Germany50	No. Candidate sol.	3	4	8	11	18	26
	No. Pareto-optimal sol.	3	4	7	10	13	17
	No. Iterations	11	36	71	209	509	1282
	No. Cover Cuts (4.30)	22	72	161	519	1359	3672
	Runtime (HH:MM:SS)	00:00:19	00:00:47	00:01:32	00:03:38	00:06:26	00:11:55
Coronet	No. Candidate sol.	6	11	19	27	46	70
	No. Pareto-optimal sol.	5	8	15	20	28	33
	No. Iterations	64	160	957	2820	14179	32901
	No. Cover Cuts (4.30)	128	327	2597	7968	46833	111173
	Runtime (HH:MM:SS)	00:01:53	00:04:10	00:22:24	00:54:42	06:59:44	43:40:43

to the value of l). Anyway, for the 3 smallest topologies, the total running times were always short, with the harder cases in the order of a few minutes, indicating that larger values of l can also be solved.

For the Coronet topology, the running times become very large with the two most challenging cases ($l = 6$ and 7) in the order of hours, indicating that for topologies of equivalent dimension, $l = 7$ critical links is very close to the scalability limit of Algorithm 4.2 in computing the complete Pareto frontier. Note, though, that computing the complete Pareto frontier is hardly useful in practice. When the operator has a budget, it is only interested in computing the Pareto frontier up to its budget. In this case, Algorithm 4.2 can stop in the first candidate solution whose cost B is above the budget, which reduces significantly the total running time of the algorithm.

4.5.2 Single third-party network: different connectivity weights

In this section, the aim is to test Algorithm 4.2 when the connectivity weights w_{ij} are not unitary. Since each network topology is defined over a given geographical region (either a country or a continent), we have used the population size of each node closest city to derive realistic weight values.

First, we have estimated the city population p_i associated to each node $i \in N$ (using

WolframAlpha). Then, given p_{med} as the median value of $\{p_i : i \in N\}$, we have assigned a weight value for each node $i \in N$ given by $w_i = \lceil p_i / p_{\text{med}} \rceil$. The aim is that half of the nodes have unitary weights (associated to the smallest city population nodes) and the other half have integer node weights proportional to the city population (these weight values are illustrated in Figure 4.6). Finally, the connectivity weight of each node pair $i, j \in N, i < j$ is given by $w_{ij} = w_i \times w_j$ (i.e., the connectivity importance is higher between nodes serving larger populations).

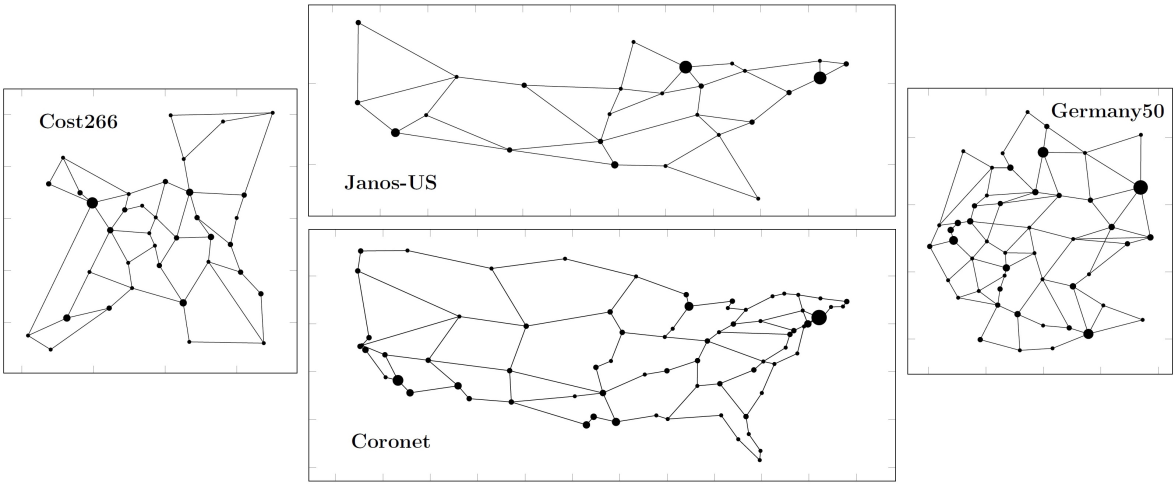


Figure 4.6: Network topologies with node weights (area of each node proportional to its weight value).

To compute the full set of computational results with these weights, we have again considered $l \in \{2, 3, 4, 5, 6, 7\}$ critical links for all 4 network topologies. Table 4.4 presents the most relevant data of the results obtained with Algorithm 4.2.

Like before, these results show that Algorithm 4.2 was able to compute the complete Pareto frontier for all cases and the total running times became much shorter. For example, in the worst case of Coronet topology with $l = 7$ critical links, the runtime was reduced from more than 43 hours in the unitary weight case to less than 14 hours in this case.

Comparing the results of the two cases (unitary and weighted) for each individual instance, the number of candidate and Pareto-optimal solutions is higher. Nevertheless, the number of iterations and added cover cuts is almost the same, which means that the row generation technique requires similar running times. The reason why the running times are shorter is that the critical link detection problem, i.e., the **CLD** model, is solved in much shorter times with different connectivity weights when compared with unitary weights.

4.5.3 Pareto frontiers of single third-party network scenarios

Figures 4.7, 4.8, 4.9 and 4.10 present the pairs of solution values (B, z) of all Pareto-optimal solutions obtained in both unitary and weighted scenarios for the 4 topologies. Each Pareto frontier is presented with the pairs of solution values (B, z) highlighted differently for each value l and showing the connectivity resilience as its percentage relative to the maximum resilience value (recall that B represents the number of selected gateway nodes).

Table 4.4: Computational results summary (weighted case).

Network	l	2	3	4	5	6	7
Janos-US	No. Candidate sol.	4	11	16	22	30	32
	No. Pareto-optimal sol.	3	7	10	13	17	19
	No. Iterations	6	24	55	112	232	477
	No. Cover Cuts (4.30)	12	48	115	257	596	1332
	Runtime (HH:MM:SS)	00:00:02	00:00:04	00:00:05	00:00:09	00:00:15	00:00:23
Cost266	No. Candidate sol.	4	8	16	24	33	46
	No. Pareto-optimal sol.	4	7	11	16	19	23
	No. Iterations	10	47	94	239	956	1935
	No. Cover Cuts (4.30)	20	94	211	597	2708	5834
	Runtime (HH:MM:SS)	00:00:05	00:00:12	00:00:24	00:00:46	00:01:49	00:03:44
Germany50	No. Candidate sol.	4	9	16	24	33	49
	No. Pareto-optimal sol.	4	7	12	17	23	29
	No. Iterations	11	37	77	254	668	1451
	No. Cover Cuts (4.30)	22	75	171	651	1898	4461
	Runtime (HH:MM:SS)	00:00:23	00:01:11	00:01:13	00:02:00	00:03:55	00:06:45
Coronet	No. Candidate sol.	9	23	37	64	80	105
	No. Pareto-optimal sol.	8	15	24	32	39	47
	No. Iterations	62	159	998	2739	11130	25787
	No. Cover Cuts (4.30)	124	327	2741	7825	37695	91101
	Runtime (HH:MM:SS)	00:02:04	00:03:50	00:15:52	00:38:39	03:27:44	13:54:54

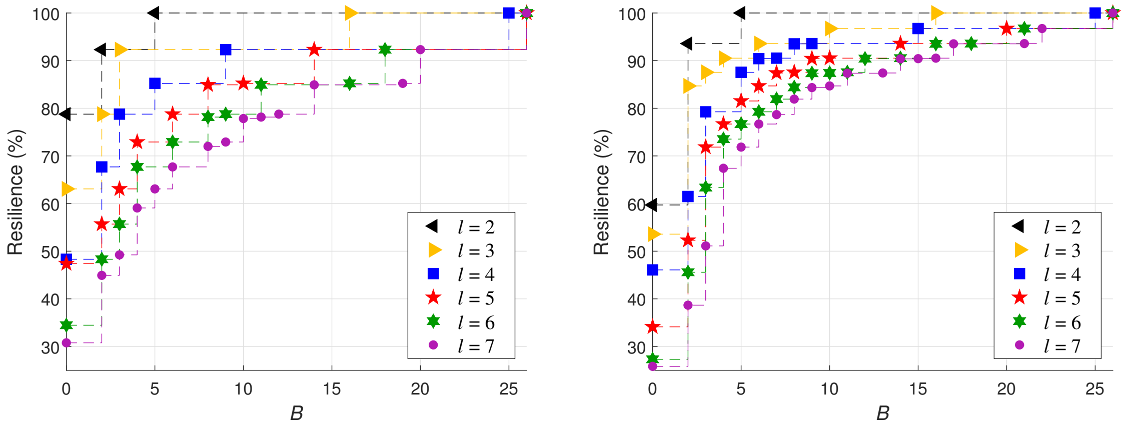


Figure 4.7: Scatter plots of the Pareto frontiers obtained for Janos-US topology (unitary case left and weighted case right).

In all cases, we can observe that the highest resilience gains are obtained with the lowest cost values (i.e, the first Pareto-optimal solutions). This is an important observation to network operators since it indicates that with the smaller investment costs, they can obtain the highest connectivity resilience gains. Then, the resilience gains become smaller until the maximum possible resilience value is obtained.

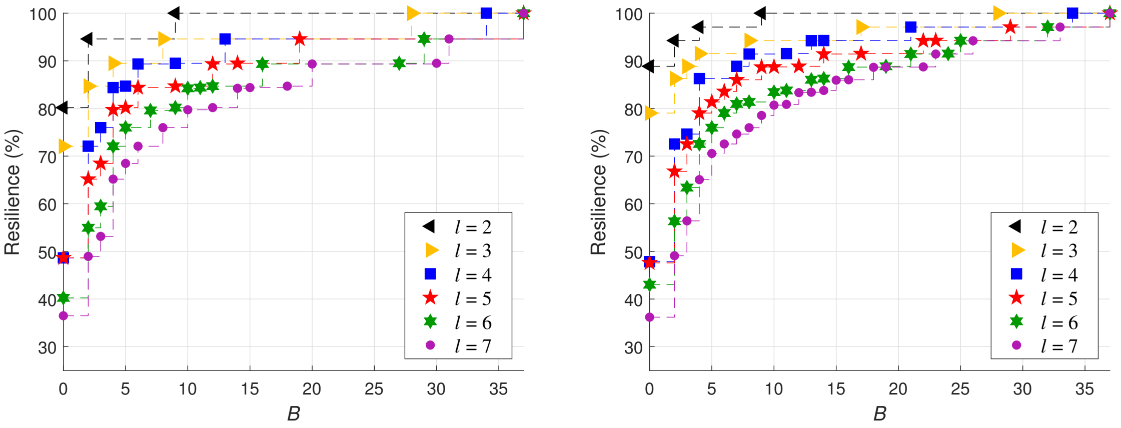


Figure 4.8: Scatter plots of the Pareto frontiers obtained for Cost266 topology (unitary case left and weighted case right).

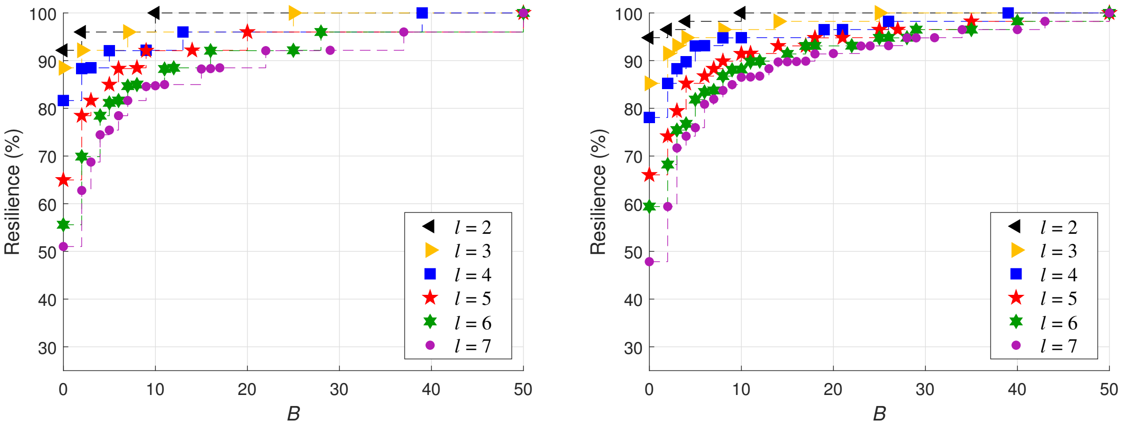


Figure 4.9: Scatter plots of the Pareto frontiers obtained for Germany50 topology (unitary case left and weighted case right).

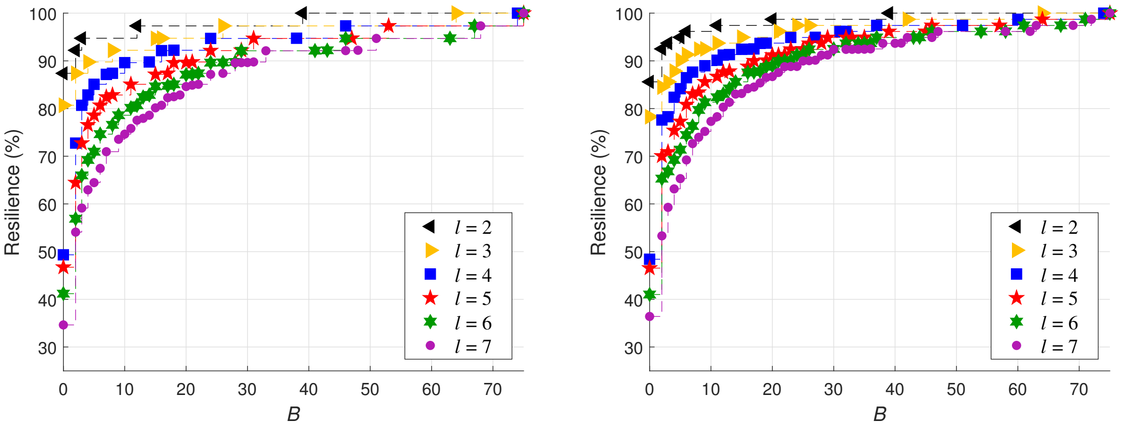


Figure 4.10: Scatter plots of the Pareto frontiers obtained for Coronet topology (unitary case left and weighted case right).

As already observed before, full connectivity resilience can always be obtained when all network nodes can be selected as gateway nodes (i.e., $N_1 = N$). In all topologies, full connectivity resilience requires all nodes to be gateway nodes for $l \geq 5$ critical links. Nevertheless, for smaller values of l, full connectivity resilience is many times obtained with less number of gateway nodes. For example, for $l = 2$ in Janos-US topology, the full connectivity resilience of 100% is obtained with 5 gateway nodes (Figure 4.7) in both unitary and weighted scenarios (the gateway nodes are the 5 nodes with node degree 2 of this topology, see Figure 4.6).

Comparing the Pareto frontiers between the two scenarios (unitary and weighted) for each network topology and each value l, the most significant difference is that, in the weighted scenarios, there are more Pareto-optimal solutions providing to the network operator more trade-offs between cost and connectivity resilience. Consider the example of $l = 3$ in Janos-US topology (Figure 4.7). For the unitary scenario, there are 4 Pareto-optimal solutions with $B = 0$, 2, 3 and 16 gateway nodes, while in the weighted scenario, there are 7 Pareto-optimal solutions with $B = 0$, 2, 3, 4, 6, 10 and 16 gateway nodes (in both cases, 16 gateway nodes provide full connectivity resilience). So, in the weighted scenario, the solutions with $B = 4$, 6 and 10 gateway nodes represent trade-off alternatives between cost and connectivity resilience that do not exist in the unitary scenario.

4.5.4 Multiple third-party networks

To generate these computational results, we have considered the largest Coronet topology. Since both Coronet and Janos-US networks are defined over the USA, we have selected Janos-US as one of the third-party networks and the common nodes to both networks (nodes in the same location) were considered as the set of possible gateway nodes of Coronet to Janus-US. Then, we have considered 2 artificial regional third-party networks, one covering the East coast region (named East network) and the other covering the West coast region (named West network). Figure 4.11 shows the Coronet nodes that can be selected as gateway nodes to each of the 3 third-party networks.

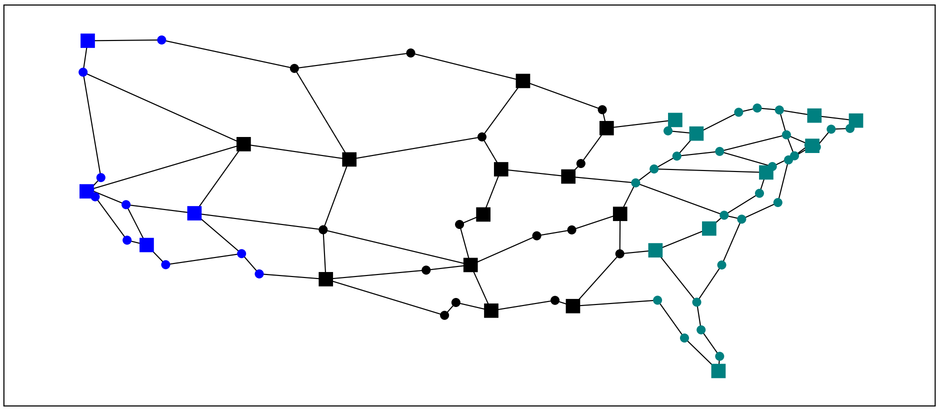


Figure 4.11: Possible Coronet gateway nodes to each third-party network (highlighted with squares to 'Janos-US', in green to 'East' and in blue to 'West').

To compute the full set of computational results, we have considered unitary connectivity weights and $l \in \{2, 3, 4, 5, 6, 7\}$. Moreover, we have considered 3 cases:

1. 'Janos-US only': a single available third-party network provided by 'Janos-US' (this is not a multiple third-party network scenario but its results are used for comparison reasons);
2. 'Regional only': two available third-party networks provided by East and West networks;
3. 'Janos-US + Regional': three available third-party networks provided by all 3 networks.

Table 4.5 presents the most relevant data of the results obtained with Algorithm 4.3 for the 3 third-party network cases. These results show that Algorithm 4.3 was able to compute the complete Pareto frontier for all cases. Moreover, the total running times are shorter than the ones of the previous subsections for Coronet, showing that these cases are easier to be solved. The main reason for this fact is that in the previous cases we have considered all network nodes as possible gateway nodes (the most challenging case in terms of optimization) while in these cases, the set of possible gateway nodes is only a percentage of the total node set.

In general, the Pareto frontiers of these 3 cases contain less number of Pareto-optimal solutions than the Pareto frontier of Coronet network considering all nodes as possible gateway nodes (shown in Section 4.5.2). In particular, the 'Regional only' case has a very small number of Pareto-optimal solutions. The reason for this is that the set of $l = 4$ critical links of Coronet (highlighted in dashed red in Figure 4.12) splits the network in a way that neither the East nor the West network can provide additional connectivity between the two split parts. So, for $l \geq 4$, the regional networks alone are not very helpful.

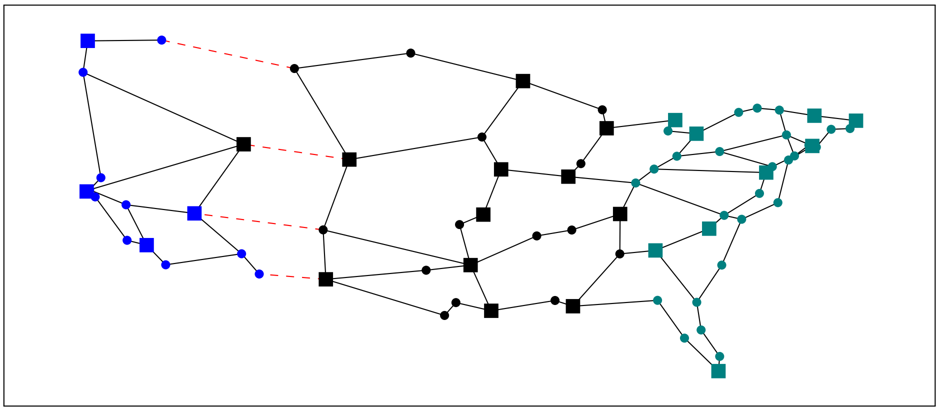


Figure 4.12: Coronet third-party networks study-case, with $l = 4$ critical links in dashed red.

Figure 4.13 presents, for each $l \in \{2, 3, 4, 5, 6, 7\}$, the Pareto frontiers for all cases based on the Coronet network topology: the 3 third-party cases of this subsection and the case considering all nodes as possible gateway nodes of Section 4.5.2. Recall that the latter case provides the best possible Pareto frontier and, so, we use it to analyze how close the Pareto-optimal solutions provided by the multiple third-party networks are from the best possible solutions.

The comparison of the Pareto frontiers of the 'Janos-US only' (blue line) and the 'Regional only' (green line) cases shows that: for $l = 2$, the regional networks are slightly better; for $l = 3$, the 2 cases are similar; and for $l \geq 4$, the Janos-US allows significant resilience improvements, while, for the reasons already explained, the regional networks are almost useless.

Table 4.5: Computational results summary (3 third-party networks cases).

Instance	l	2	3	4	5	6	7
Janos-US only	No. Candidate solutions	2	4	8	11	18	28
	No. Pareto-optimal sol.	2	3	4	7	8	12
	No. Iterations	2	6	10	37	82	231
	Runtime (HH:MM:SS)	00:00:08	00:00:33	00:00:36	00:01:48	00:02:06	00:05:50
Regional only	No. Candidate solutions	4	5	1	2	5	4
	No. Pareto-optimal sol.	3	3	1	2	3	3
	No. Iterations	7	10	0	1	7	9
	Runtime (HH:MM:SS)	00:00:29	00:01:16	00:00:01	00:00:06	00:00:16	00:00:09
Janos-US + Regional	No. Candidate solutions	4	8	12	18	36	53
	No. Pareto-optimal sol.	3	5	8	13	19	21
	No. Iterations	10	45	92	362	1042	3022
	Runtime (HH:MM:SS)	00:00:42	00:03:50	00:08:57	00:23:23	01:10:56	07:58:53

On the other hand, when we consider the 'Janos-US + Regional' case, we obtain connectivity resilience improvements considerably higher than the ones of the 'Janos-US only' case. This means that, although the regional networks alone do not allow significant connectivity resilience, when they are available together with the Janos-US network (which covers a wider geographical range), they become effective in allowing higher connectivity resilience values.

Finally, when comparing the Pareto frontier of the 'Janos-US + Regional' case (red line) with the best Pareto frontier (black line), we observe in Figure 4.13 that the two sets of Pareto-optimal solutions are very close for a significant range of the lowest cost values (which are the solutions providing the highest connectivity resilience gains). So, at least for the case of Coronet topology, the 3 considered third-party networks can altogether provide trade-off solutions (between cost and connectivity resilience) close to the Pareto-optimal solutions.

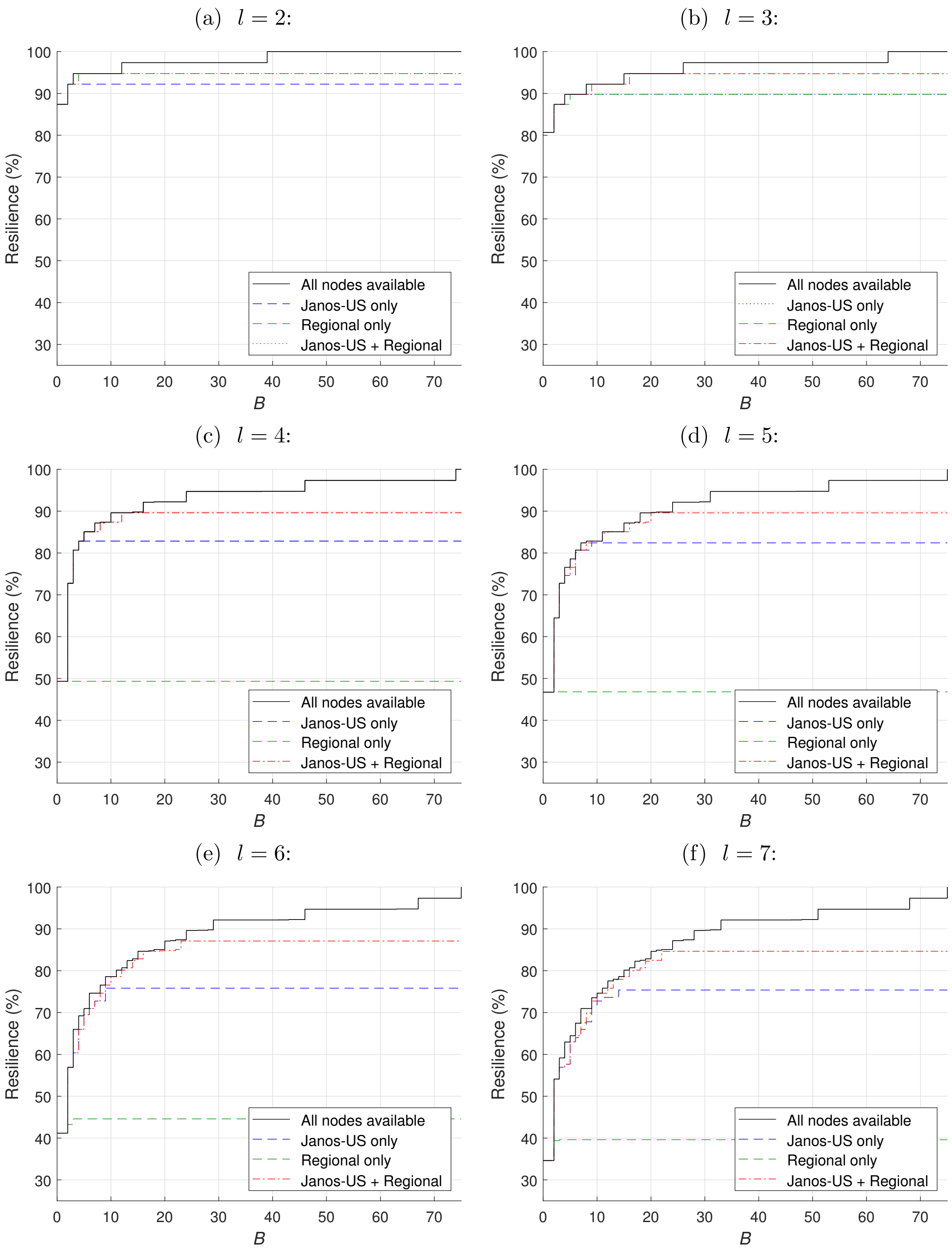
4.6 Conclusions

In this work, we have proposed an algorithm able to provide different GNS solutions which are different trade-offs between the total cost of the gateway nodes to third-party networks and the connectivity resilience increase provided by the selected gateway nodes.

The computational results have shown that the algorithm was able to compute all Pareto-optimal solutions of the underlying bi-objective optimization problem for four well-known network topologies, the largest one with 75 nodes and 99 links, and considering up to $l = 7$ simultaneous link failures.

One important observation from the different obtained Pareto-optimal solutions is that the highest resilience gains are obtained with the lowest cost values in the first Pareto-optimal solutions, which clearly indicates that the smaller investment costs allow to obtain the highest connectivity resilience gains.

Finally, the Pareto-optimal solutions computed when multiple third-party networks are available showed that, for the lowest cost values (which are the solutions providing the highest connectivity resilience gains), having multiple third-party networks, even if they cannot



(a) $l = 2$:

(b) $l = 3$:

(c) $l = 4$:

(d) $l = 5$:

(e) $l = 6$:

(f) $l = 7$:

Figure 4.13: Stair plots of the Pareto frontiers on the Coronet network topology.

cover all network nodes, can allow trade-off solutions which are close to the optimal trade-off solutions when all network nodes can be selected as gateway nodes for a single third-party network.

Bibliography

[BBH$^+$17] A. Basta, A. Blenk, K. Hoffmann, H. Morper, M. Hoffmann, and W. Kellerer. *Towards a cost optimal design for a 5G mobile core network based on SDN and NFV.* IEEE Transactions on Network and Service Management, 14(4):1061–1075, 2017.

[BdSA20] F. Barbosa, A. de Sousa, and A. Agra. *Design/upgrade of a transparent optical network topology resilient to the simultaneous failure of its critical nodes.* Networks, 75(4):356–373, 2020.

[BK00] A. Benczúr and D. Karger. *Augmenting undirected edge connectivity in $\tilde{O}(n2)$ time.* Journal of Algorithms, 37(1):2–36, 2000.

[BLL$^+$12] N. Bao, L. Li, H. Luo, Z. Zhang, and H. Yu. *On exploiting sharable resources with resource contention resolution for surviving double-link failures in optical mesh networks.* Journal of Lightwave Technology, 30(17):2788–2795, 2012.

[dS20] A. de Sousa. *Improving the connectivity resilience of a telecommunications network to multiple link failures through a third-party network.* In 16th International Conference on the Design of Reliable Communication Networks (DRCN), pages 1–6, 2020.

[dSS20] A. de Sousa and D. Santos. *Vulnerability evaluation of networks to multiple failures based on critical nodes and links.* In J. Rak and D. Hutchison, editors, Guide to Disaster-Resilient Communication Networks, pages 63–86. Springer International Publishing, Cham, 2020.

[DXT$^+$12] T. Dinh, Y. Xuan, M. Thai, P. Pardalos, and T. Znati. *On new approaches of assessing network vulnerability: hardness and approximation.* IEEE/ACM Transactions on Networking, 20(2):609–619, 2012.

[ET76] K. Eswaran and R. Tarjan. *Augmentation problems.* SIAM Journal on Computing, 5(4):653–665, 1976.

[FWG$^+$16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GSB16] H. Guo, G. Shen, and S. Bose. *Routing and spectrum assignment for dual failure path protected elastic optical networks.* IEEE Access, 4:5143–5160, 2016.

[GSM$^+$11] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante. *Dimensions of cyber-attacks: cultural, social, economic, and political.* IEEE Technology and Society Magazine, 30(1):28–38, 2011.

[GTE$^+$16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde,

A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[HHSO20] Y. Hirano, F. He, T. Sato, and E. Oki. *Backup network design against multiple link failures to avoid link capacity overestimation.* IEEE Transactions on Network and Service Management, 17(2):1254–1267, 2020.

[JH13] B. Jaumard and H. Hoang. *Design and dimensioning of logical survivable topologies against multiple failures.* IEEE/OSA Journal of Optical Communications and Networking, 5(1):23–36, 2013.

[JLM15] M. Johnston, H. Lee, and E. Modiano. *A robust optimization approach to backup network design with random failures.* IEEE/ACM Transactions on Networking, 23(4):1216–1228, 2015.

[LGZ$^+$15] S. Lange, S. Gebert, T. Zinner, P. Tran-Gia, D. Hock, M. Jarschel, and M. Hoffmann. *Heuristic approaches to the controller placement problem in large scale SDN networks.* IEEE Transactions on Network and Service Management, 12(1):4–17, 2015.

[LT11] V. Liu and D. Tipper. *Spare capacity allocation using shared backup path protection for dual link failures.* In 8th International Workshop on the Design of Reliable Communication Networks (DRCN), pages 118–125, 2011.

[Nag04] H. Nagamochi. *Graph algorithms for network connectivity problems.* Journal of the Operations Research Society of Japan, 47(4):199–223, 2004.

[NdSWF18] C. Natalino, A. de Sousa, L. Wosinska, and M. Furdek. *On the trade-offs between user-to-replica distance and CDN robustness to link cut attacks.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–7, 2018.

[NGGGS18] B. Nedic, M. Gunkel, T. Gomes, and R. Girão-Silva. *SRLG-disjointness and geodiverse routing – a practical network study and operational conclusions.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[RC08] S. Ramasubramanian and A. Chandak. *Dual-link failure resiliency through backup link mutual exclusion.* IEEE/ACM Transactions on Networking, 16(1):157–169, 2008.

[RSM03] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee. *Survivable WDM Mesh Networks.* Journal of Lightwave Technology, 21(4):870–883, 2003.

[Sch98] A. Schrijver. *Theory of linear and integer programming.* Wiley, 1998.

[Sim14] J. Simmons. *Optical network design and planning*. Springer, Switzerland, 2nd edition, 2014.

[SKFZW16] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska. *Physical-layer security in evolving optical networks.* IEEE Communications Magazine, 54(8):110–117, 2016.

[SNXT13] Y. Shen, N. Nguyen, Y. Xuan, and M. Thai. *On the discovery of critical links and nodes for assessing network vulnerability.* IEEE/ACM Transactions on Networking, 21(3):963–973, 2013.

[TRVG17] J. Tapolcai, L. Rónyai, B. Vass, and L. Gyimóthi. *List of shared risk link groups representing regional failures with limited size.* In IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, pages 1–9, 2017.

[WN87] T. Watanabe and A. Nakamura. *Edge-connectivity augmentation problems.* Journal of Computer and System Sciences, 35(1):96–144, 1987.

[XYS$^+$17] S. Xu, N. Yoshikane, M. Shiraiwa, T. Tsuritani, H. Harai, Y. Awaji, and N. Wada. *Multi-carrier interconnection-based emergency packet transport network planning in disaster recovery.* In 13th International Conference on the Design of Reliable Communication Networks (DRCN), pages 1–8, 2017.

[YHG$^+$17] S. Yin, S. Huang, B. Guo, Y. Zhou, H. Huang, M. Zhang, Y. Zhao, J. Zhang, and W. Gu. *Shared-protection survivable multipath scheme in flexible-grid optical networks against multiple failures.* Journal of Lightwave Technology, 35(2):201–211, 2017.

[YW11] S. Yuan and B. Wang. *Highly available path routing in mesh networks under multiple link failures.* IEEE Transactions on Reliability, 60(4):823–832, 2011.

[ZZM06] J. Zhang, K. Zhu, and B. Mukherjee. *Backup reprovisioning to remedy the effect of multiple link failures in WDM mesh networks.* IEEE Journal on Selected Areas in Communications, 24(8):57–67, 2006.

Chapter 5

RMSA Algorithms Resilient to Multiple Node Failures in Dynamic Elastic Optical Networks

Abstract: In Elastic Optical Networks (EONs), the way different service demands are supported in the network is ruled by the Routing, Modulation and Spectrum Assignment (RMSA) algorithm, which decides how the spectrum resources of the optical network are assigned to each service demand. In a dynamic EON, demand requests arrive randomly one at a time and the accepted demands last in the network for a random time duration. So, one important goal of the RMSA algorithm is the efficient use of the spectrum resources to maximize the acceptance probability of future demand requests. On the other hand, multiple failure events are becoming a concern to network operators as such events are becoming more frequent in time. In this work, we consider the case of multiple node failure events caused by malicious attacks against network nodes. In order to obtain RMSA algorithms resilient to such events, a path disaster availability metric was recently proposed which takes into account the probability of each path not being disrupted by an attack. This metric was proposed in the offline variant of the RMSA problem where all demands are assumed to be known at the beginning. Here, we exploit the use of the path disaster availability metric in the RMSA of dynamic EONs. In particular, we propose RMSA algorithms combining the path disaster availability metric with spectrum usage metrics in a dynamic way based on the network load level. The aim is that the efficient use of the resources is relaxed for improved resilience to multiple node failures when the EON is lightly load, while it becomes the most important goal when the EON becomes heavily loaded. We present simulation results considering a mix of unicast and anycast services in 3 well-known topologies. The results show that the RMSA algorithms combining the path disaster availability metric with spectrum usage metrics are the best trade-off between spectrum usage efficiency and resilience to multiple node failures.

Keywords: Elastic Optical Networks, RMSA, Multiple Node Failures, Disaster Resilience, Simulation

F. Barbosa, A. de Sousa, A. Agra, K. Walkowiak, and R. Goścień. *RMSA algorithms resilient to multiple node failures in dynamic EONs.* Optical Switching and Networking, 42:100633, 2021.

5.1 Introduction

The support of different service demands in Elastic Optical Networks (EONs) is ruled by the Routing, Modulation and Spectrum Assignment (RMSA) algorithm, which decides how the network resources are assigned to each service demand. In a dynamic EON, demand requests arrive randomly one at a time and the accepted demands last in the network for a random time duration.

One of the main goals of the RMSA algorithm is to use the resources in an efficient way, i.e., by keeping the spectrum resources usage low so that future demands can be accommodated with higher probability [AR17, CTV11, KW11, TR17, WK13]. However, other goals are also important due to the continuous advances of EONs in terms of node architectures and transceiver characteristics (bit-rate and transmission reach). This is particularly important in the RMSA offline problem where all demands to be supported by the EON are estimated at the beginning and the RMSA efficient use of the network resource also considers other goals as the minimization of transceiver costs or of the network power consumption [CSO15, GWK15, PAK+12].

On the other hand, large-scale failure events are becoming a concern to network operators as such event are becoming more frequent in time [RH20]. Large-scale failure events can have different causes, as natural disasters [GTE+16] or human malicious activities [FWG+16], which might involve a significant number of simultaneous failures. Network resilience to failure events is, broadly speaking, the ability of the network to keep supporting the service demands after a failure event and many works have addressed this problem for single link (or single node) failures considering protection mechanisms to guarantee that all demands can be maintained after the failure event [CZJZ15, GK19, WNG17]. However, the guarantee that all demands are maintained in a large-scale failure event involving multiple failures is infeasible in practice as the required network resources become too costly. In this case, the aim becomes to improve the network preparedness to large-scale failure events as much as possible by maximizing the amount of demand that can still be maintained in face of such events.

In this work, we consider the case of multiple node failure events caused by human malicious attacks against network nodes. In terrorist attacks, although node shutdowns are harder to realize than link cuts, they are the most rewarding in the attackers' perspective since the shutdown of a node also shuts down all its fiber links. So, we deal with multiple node failures as they are the most harmful case. The topology design of optical networks resilient to multiple node failures was addressed in [BdSA18, BdSA20]. In those works, though, the RMSA is not considered and the resilience of the network topology is evaluated by the impact of the simultaneous failure of its critical nodes, i.e., the nodes with the highest impact on the connectivity of the network.

Meanwhile, a family of RMSA algorithms resilient to multiple node failures caused by attacks against multiple nodes has been recently proposed for EONs in [BdSA+19] assuming that the attacker "discovers" with some probability a set of nodes to be attacked. The proposed algorithms use a metric, named *path disaster availability*, in the RMSA decision which takes into account the probability that each path is not disrupted by the attack. While the work in [BdSA+19] considers the offline version of the RMSA problem (i.e., all service demands are assumed to be known at the beginning), we exploit in this work the use of the path disaster availability metric in the RMSA of dynamic EONs. In particular, we propose RMSA algorithms combining the path disaster availability metric with spectrum usage metrics in a dynamic way based on the network load level. The aim is that the efficient use of the resources is relaxed for improved resilience to multiple node failures when the EON is lightly loaded, while it becomes the most important goal when the EON is heavily loaded.

To evaluate the proposed RMSA algorithms, we have developed an event-driven simulator (in this type of simulation, only the time instants at which the state of the system changes need to be simulated, i.e., the system is modeled as a series of time instants when a state-change occurs, called *events* [Rob04]). The simulator is used to estimate the spectrum usage efficiency of each RMSA algorithm (assessed by the bit-rate amount of all requests that are blocked due to insufficient free spectrum resources) and the network resilience to multiple node failures. In the latter case, the resiliency is evaluated by 2 parameters: the average non-disrupted demand (the bit-rate percentage that is not disrupted after a failure, averaged over all failures) and the average surviving demand (the bit-rate percentage that is supported after a failure, averaged over all failures). Both resiliency parameters are important in practice. On one hand, higher average surviving demand values are important for non-critical services as they are less penalized by short-term disruptions. On the other hand, higher average non-disrupted demand values are important for critical services (which require high availability) and for minimizing the number of disrupted lightpaths requiring reconfiguration.

We present a set of computational results considering a mix of unicast and anycast services in 3 well-known topologies. All algorithms are evaluated through simulation considering a restoration mechanism where, upon a multiple node failure event, the non-affected lightpaths remain unchanged and the demands of the affected lightpaths are reassigned as much as possible with new lightpaths in the spectrum resources of the surviving network. The results show that the RMSA algorithms combining the path disaster availability metric with spectrum usage metrics are the best trade-off between spectrum usage efficiency and resilience to multiple node failures.

The paper is organized as follows. Section 5.2 describes how the malicious node attacks are modeled and how the path disaster availability metric is computed based on the attack model. Section 5.3 describes the RMSA algorithms in the regular state and in the failure state. Section 5.4 describes the simulation procedure used to assess the different RMSA algorithms. The computational results are presented and discussed in Section 5.5. Finally, Section 5.6 draws the main conclusions of the work.

5.2 Modeling node attacks and path disaster availability

In this work, a malicious attack against multiple nodes corresponds to the case when a malicious organization discovers some nodes that it is able to attack. By shutting down these nodes, the organization aims to disrupt as much as possible the services supported by the network.

In general, different levels of public information exist related to the location of each network node. For example, the location of Data Centers is usually publicly known and most likely a network node is nearby, which results in a higher probability of such nodes being discovered by malicious organizations. Moreover, the set of nodes discovered by a malicious organization depends on its resources (human cells and geographical base locations) and operational capabilities. However, different malicious organizations might exist, each one with its own resources and capabilities. So, from the perspective of the network operator, since it does not know which organization is planning an attack on its network (or how nodes are discovered by the organization), any set of uncorrelated nodes can be attacked. In modeling terms, it is similar to multiple unintended failures with the difference that single failures are much more likely than multiple failures in unintended failure events, while the failure of multiple nodes is more likely in malicious attacks.

Following these assumptions, we describe in separate subsections, first, how a malicious node attack is modeled and, then, how the path disaster availability metric is computed for each routing path based on the attack model. In both subsections, we consider an EON topology defined by a graph $G = (N, E)$, with a set of $n = |N|$ nodes and a set of $|E|$ undirected links.

5.2.1 Modeling a malicious node attack

We consider the following malicious node attack model. An attacker discovers with a given probability a set of nodes that can be attacked (almost) simultaneously. Each node $i \in N$ has an associated positive weight w_i proportional to the probability of the node being discovered by the attacker and, as discussed before, there is no correlation between discovered nodes. The number s of discovered nodes is between a minimum number s_m below which its destructive impact in the network is considered not worthy by the attacker and a maximum number s_M above which the probability of such number of nodes being attacked is negligible. Moreover, we assume that the effort required to attack s nodes is proportional to the number of nodes and, therefore, the probability P_s of s nodes being attacked, with $s_m \leq s \leq s_M$, is inversely proportional to the number of attacked nodes, i.e.:

$$P_s = \frac{\frac{1}{s}}{\sum_{t=s_m}^{s_M} \frac{1}{t}} \quad , \; s = s_m, ..., s_M \tag{5.1}$$

5.2.2 Computing the path disaster availability

Consider a given path p on graph $G = (N, E)$ defined by its set of nodes $i \in p$ (including source and destination nodes). The path disaster availability a_p of path p is the probability that p is available (i.e., not disrupted) after an attack. Due to the assumption of no correlation between attacked nodes, the path disaster availability a_p is given by:

$$a_p = \prod_{i \in p} (1 - \pi_i) \tag{5.2}$$

where π_i is the probability of node $i \in N$ to be attacked when an attack is realized. Then, π_i is given by:

$$\pi_i = \sum_{s=s_m}^{s_M} \pi_i^s \times P_s \tag{5.3}$$

where π_i^s is the probability of node i being attacked on an attack to s nodes and P_s, previously defined in (5.1), is the probability of an attack to s nodes. Finally, probability π_i^s is computed by the sum of the probabilities of all sequences without repetitions of s nodes out of n $(= |N|)$ nodes that include node i in one of its positions, given by:

$$\begin{aligned}\pi_i^s \;=\; & \frac{w_i}{W_N} + \sum_{j \in N\backslash\{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N\backslash\{j\}}} \\ & + \sum_{j \in N\backslash\{i\}} \frac{w_j}{W_N} \Big(\sum_{k \in N\backslash\{i,j\}} \frac{w_k}{W_{N\backslash\{j\}}} \times \frac{w_i}{W_{N\backslash\{j,k\}}} \Big) + ...\end{aligned} \tag{5.4}$$

where W_M denotes the sum of the node weights of a set $M \subseteq N$, i.e., $W_M = \sum_{i \in M} w_i$. The first term $\frac{w_i}{W_N}$ in (5.4) is the probability of all sequences such that i is the first node of the sequence. The second term $\sum_{j \in N\backslash\{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N\backslash\{j\}}}$ is the probability of all sequences such that i is the second node of the sequence, i.e., all sequences composed by a node $j \in N\backslash\{i\}$ in the first position and node i in the second position. The third term is the generalization of the previous term for the sequences such that i is the third node of the sequence.

The probability π_i^s defined in (5.4) has s terms and can be computed recursively as follows. For a given set of nodes N and associated weights $w = \{w_i, i \in N\}$, a given number of attacked nodes s and a given node i, the probability π_i^s is computed as:

$$\pi_i^s \;=\; prob(N, w, i, 0, s) \tag{5.5}$$

where $prob()$ is the recursive function defined in Algorithm 5.1. The input parameters of Algorithm 5.1 are a set of nodes M which were still not selected (in the first call in (5.5), this parameter is the complete node set N), the set w of node weights, the node i whose probability we want to compute, the number z of already selected nodes (in the first call in (5.5), this parameter is $z = 0$) and the number of attacked nodes s.

Algorithm 5.1 Recursive function to compute π_i^s

```
function $\pi = prob(M, w, i, z, s)$
$z \leftarrow z + 1$
$W_M \leftarrow \sum_{j \in M} w_j$
$\pi \leftarrow \frac{w_i}{W_M}$
if $z < s$ then
    for all $j \in M\backslash\{i\}$ do
        $\pi \leftarrow \pi + \frac{w_j}{W_M} \times prob(M\backslash\{j\}, w, i, z, s)$
    end for
end if
return $\pi$
```

For illustration purposes, consider the example of graph $G = (N, E)$ presented in Figure 5.1, with $n = 12$ nodes and $|E| = 18$ edges and assume that the nodes highlighted in gray are 10 times more probable of being discovered than the other nodes. Therefore, $w_i = 10$ for nodes $i \in \{2, 5, 11\}$ and $w_i = 1$ for all other nodes. Note that the probabilities π_i^s given by (5.4) are equal for nodes with equal weight values w_i. In this example, since there are only two different weight values, all probabilities of nodes $i \in \{2, 5, 11\}$ are equal and all probabilities of the other nodes are also equal. Table 5.1 presents the probability values of this example computed by Algorithm 5.1 for a number of attacked nodes s from 2 up to 6. As expected, these results show that the more the attacked nodes s are, the higher the probabilities π_i^s of

Table 5.1: Probability value π_i^s of each node $i \in N$ for each s in the example.

s	2	3	4	5	6
π_i^s $(w_i = 10)$	0.494	0.700	0.845	0.929	0.971
π_i^s $(w_i = 1)$	0.058	0.100	0.163	0.246	0.343

all nodes become. Moreover, for all values of s, the nodes i with the highest weight value $w_i = 10$ have always a higher probability of being attacked than the other nodes.

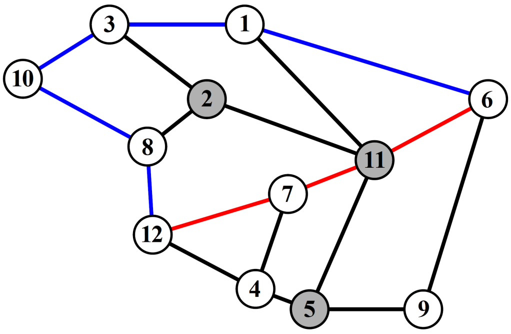


Figure 5.1: Polska network topology [OWPT10].

Then, for a given range $[s_m, s_M]$ in the number of attacked nodes, the probability π_i of each node i to be attacked when an attack is realized is given by (5.3). Table 5.2 presents the probability values π_i of all nodes (third and fourth columns) for different $[s_m, s_M]$ ranges (first and second columns) assuming a constant minimum number of attacked nodes $s_m = 2$ an an increasing maximum number of attacked nodes $s_M = 3, 4, 5$ and 6. Again, an increasing average number of attacked nodes increases the probability values π_i of all nodes and the probability values of the nodes with the highest weight value are always higher than the probability values of the nodes with the lowest weight values.

Now consider in the example of Figure 5.1 the end-nodes $s = 6$ and $t = 12$ and the following two candidate paths: $p_1 = \{6-11-7-12\}$ (highlighted in red) and $p_2 = \{6-1-3-10-8-12\}$ (highlighted in blue). The path disaster availability of these two candidate paths is given by (5.2), whose values are presented in Table 5.2 (fifth and sixth columns) for the different considered $[s_m, s_M]$ ranges. For any of the considered ranges, although path p_1 is shorter (in number of links), its probability of not being affected by an attack (i.e., its path disaster availability) is lower than the probability of p_2 not being affected by an attack. This is because p_1 includes one of the nodes (node 11) with higher probability of being discovered while p_2 does not include any of such nodes.

Note that the values of π_i^s computed with Algorithm 5.1 and π_i computed with (5.3) only depend on the EON topology and on the parameters defining the malicious node attack model. So, they are computed once (in advance) and, then, the path disaster availability a_p of each candidate path p considered by the RMSA algorithms is efficiently computed with (5.2).

Table 5.2: Probability value π_i of each node $i \in N$ and path disaster availability of p_1 and p_2 for different $[s_m, s_M]$ ranges.

s_m	s_M	π_i $(w_i = 10)$	π_i $(w_i = 1)$	a_{p_1}	a_{p_2}
2	3	0.577	0.074	0.336	0.628
2	4	0.638	0.095	0.268	0.550
2	5	0.684	0.118	0.217	0.469
2	6	0.717	0.144	0.178	0.393

5.3 RMSA algorithms

In a dynamic EON, demand requests arrive one at a time in the regular state. When a new request arrives, there is a set of lightpaths already established in the network (occupying some spectrum on the different fiber links) and the RMSA algorithm decision is either to assign a lightpath to the incoming request or to block it if there are not enough spectrum resources in the network. On the other hand, in a failure state (caused by an attack to multiple nodes), we consider a restoration mechanism where the non-affected lightpaths remain unchanged and the RMSA algorithm has to assign as much as possible new lightpaths to the affected demands in the available resources of the surviving network (i.e., the network without the attacked nodes). Next, we address the regular state and the failure state in separate subsections.

5.3.1 RMSA algorithm in the regular state

Recall that we consider an EON topology defined by a graph $G = (N, E)$, with a set of $n = |N|$ nodes and a set of $|E|$ undirected links. Consider also $F = \{1, 2, ..., |F|\}$ as the ordered set of Frequency Slots (FSs) available on each fiber link to be assigned to lightpaths. In the regular state, a set of lightpaths is already established and there is a request d for a new demand to be accepted.

The type of request d can be either unicast or anycast. An unicast request d is characterized by a pair of end-nodes (s_d, t_d) and its required bit-rate b_d. In anycast requests, the network supports a set R of services and each anycast service $r \in R$ is provided by a set of Data Centers (DCs) located in nodes $C_r \subseteq N$. Then, an anycast request d is characterized by a source node s_d, an anycast service $r_d \in R$ and a required bit-rate b_d (the anycast request d can be satisfied by any of the DCs in C_{r_d}).

Consider $\mathcal{P}_d$ as the set of candidate paths that can be selected for request d. If d is of unicast type, $\mathcal{P}_d$ is a set of different routing paths between s_d and t_d. If d is of anycast type, $\mathcal{P}_d$ is a set of different routing paths between s_d and one of the nodes in C_{r_d}. When the incoming request d is accepted, the RMSA decision is the specification of a lightpath to support d, which is defined by a routing path p selected from $\mathcal{P}_d$, a modulation format (MF) for electrical-optical-electrical conversion on the end-nodes of the lightpath and a set of contiguous FSs occupied by the lightpath in all fiber links of the selected routing path p.

In all RMSA algorithms, a set of parameters is associated to each candidate path $p \in \mathcal{P}_d$ and the path of the lightpath is selected as the candidate path with the best parameter values. One of the associated parameters is a_p indicating the path disaster availability of each candidate path $p \in \mathcal{P}_d$ as already defined in (5.2) of section 5.2.2.

Note that each MF has an associated transmission reach, which specifies an optical length threshold above which the lightpath does not work. So, another parameter associated to each candidate path $p \in \mathcal{P}_d$ is n_p indicating the number of FSs of the most efficient MF (the one requiring less FSs able to support the bit-rate b_d of request d) whose transmission reach is not lower than the optical length of p. We consider the optical length of each candidate path $p \in \mathcal{P}_d$ as the sum of its link lengths plus a given length value Δ per intermediate node (modeling the optical degradation suffered by a lightpath while traversing an intermediate optical switch).

Finally, based on the required number of FSs, given by the value of parameter n_p, and on the free FSs in all the links of each candidate path $p \in \mathcal{P}_d$ at the time instant of request d, another associated parameter is f_p indicating the highest FS index of the lowest set of n_p free contiguous FSs available in path p (this parameter is only considered in the candidate paths $p \in \mathcal{P}_d$ with enough available resources, i.e., with at least one set of n_p free contiguous FSs).

First, we describe three basic RMSA algorithms where the first two (FF and LFS) are well-known algorithms and the third one aims to obtain the best resilience to multiple node failures.

First-Fit (FF): Request d is routed in the first path $p \in \mathcal{P}_d$ with enough available resources and assigned with the lowest set of n_p free contiguous FSs (in this algorithm, $\mathcal{P}_d$ is ordered from the shortest to the longest optical length).

Lowest Frequency Slot (LFS): Among the paths $p \in \mathcal{P}_d$ with enough available resources, request d is routed in the path p with lowest f_p and assigned with the set of n_p free contiguous FSs whose highest FS index is f_p. If multiple paths have the same value of f_p, the path among them with the shortest optical length is selected.

Path Disaster Availability (PDA): Among the paths $p \in \mathcal{P}_d$ with enough available resources, request d is routed in the path p with the highest path disaster availability a_p and assigned with the lowest set of n_p free contiguous FSs. If multiple paths have the same value of a_p, one of them is selected with the **LFS** rule.

In [BdSA$^+$19], one of the main findings (in the offline variant of the RMSA problem) is that **LFS** is the best RMSA in terms of spectrum usage efficiency (as it keeps a larger portion of the highest spectrum completely free) and **PDA** is the best RMSA in terms of resilience to multiple node failures (as it avoids the selection of paths involving the nodes with higher probability of being attacked).

In general, the best trade-off between spectrum usage efficiency and resilience to multiple node failures depends on the load level of the network: (i) when the EON is lightly loaded, there are plenty of free resources and the spectrum usage efficiency can be relaxed to reach a better resilience to multiple node failures; (ii) when the EON is heavily loaded, the spectrum must be used in the most efficient way to maximize the acceptance probability of future demand requests.

In order to reach the best trade-off between these two aims in a dynamic EON (where, typically, the network oscillates over time between different load levels), we also propose RMSA algorithms combining the path disaster availability metric with two spectrum usage metrics in three different possible options. In all three options, we compute an additional parameter m_p for each path $p \in \mathcal{P}_d$ with enough available resources and the aim is to select the path p with the highest value of m_p.

The way parameter m_p is computed in each option is as follows. In the first option, parameter m_p is given by:

$$m_p = \Big(1 - \frac{H}{|F|}\Big)a_p \ + \ \frac{H}{|F|}\Big(1 - \frac{f_p}{|F|}\Big) \tag{5.6}$$

where H is the current highest FS occupied in at least one fiber link (which is used as a measure of the current network load). In this option, we combine the maximization of the path disaster availability a_p with the minimization of the spectrum usage metric given by f_p. Note that a higher value of $\Big(1 - \frac{f_p}{|F|}\Big)$ represents a lower value of f_p as desired by maximizing the combined parameter m_p. Moreover, both a_p and $\Big(1 - \frac{f_p}{|F|}\Big)$ terms are normalized as both values are between 0 and 1. So, when H is lower, the path disaster availability a_p has a higher weight in the determination of m_p, while when H is higher, the FS index f_p has a higher weight in the determination of m_p. In the second option, parameter m_p is given by:

$$m_p = \Big(1 - \frac{H}{|F|}\Big)a_p \ + \ \frac{H}{|F|}\frac{1}{\log_\beta(\alpha_p)} \tag{5.7}$$

where α_p is total number of FSs occupied by the lightpath to support request d in candidate path p (i.e., α_p is given by n_p multiplied by the number of fiber links of path p). In this second option, the spectrum usage metric α_p aims to give preference to paths using less spectrum resources so that more resources remain free for future requests. Again, a higher value of $\frac{1}{\log_\beta(\alpha_p)}$ represents a lower value of α_p as desired by maximizing the combined parameter m_p. In order to normalize the term $\frac{1}{\log_\beta(\alpha_p)}$ between 0 and 1, we consider β as the minimum number of FSs that can be required by any lightpath in any candidate path. Finally, in the third option, parameter m_p is given by:

$$m_p = \Big(1 - \frac{H}{|F|}\Big)a_p \ + \ \frac{H}{|F|}\left(\frac{1}{2}\Big(1 - \frac{f_p}{|F|}\Big) \ + \ \frac{1}{2}\frac{1}{\log_\beta(\alpha_p)}\right) \tag{5.8}$$

where the two previous spectrum usage metrics (the minimization of the highest FS index f_d used in (5.6) and minimization of the total number of required FSs α_p used in (5.7)) are combined with equal weight in the second term of (5.8). The resulting combined RMSA algorithms are as follows.

Mixed RMSA: Among the paths $p \in \mathcal{P}_d$ with enough available resources, request d is routed in the path p with the highest m_p and assigned with the lowest set of n_p free contiguous FSs. If multiple paths have the same value of m_p, the path among them with the shortest optical length is selected. Depending on the option to compute the values m_p, we obtain three different variants – Variant 1, 2 and 3 – of the **Mixed RMSA**, using eqs. (5.6), (5.7) and (5.8), respectively.

Assuming that the set of candidate paths is computed in advance for all possible demand requests (which is possible as the network topology does not change over time in the regular state), all algorithms require in the worst case the computation of the different parameters for all candidate paths and the processing of each parameter is linear with the number of nodes included in each candidate path (which is at most n). So, the complexity of all RMSA algorithms is $\mathcal{O}(n \times |\mathcal{P}_d|)$. Note that the **FF** algorithm has lower complexity when compared with all other algorithms as it needs to run up to the first candidate path that can be used to assign the lightpath while all the others require the computation of all candidate paths.

5.3.2 RMSA algorithm in a failure state

In a failure state caused by an attack to multiple nodes, the non-affected lightpaths remain unchanged and the RMSA algorithm tries to assign as much as possible new lightpaths to the affected demands in the available resources of the surviving EON, i.e., the network without the attacked nodes.

In this case, the resilience to node failures is not a priority and the RMSA must have the lowest possible complexity as it has to assign lightpaths not for a single request but for all affected demands. So, we consider the **FF** algorithm adapted to the failure cases. The complete algorithm has 3 phases.

First phase: the algorithm computes the FSs occupied by the non-affected lightpaths and runs a k-shortest paths algorithm for each affected demand to compute its set of candidate paths in the surviving network.

Second phase: the set of affected demands d with a non-empty set of candidate paths (i.e., the ones such that the k-shortest path has returned at least one candidate path) is ordered following the next three hierarchical orders (from the most important to the least important):

1. decreasing order of its bit-rate b_d;
2. decreasing order of the number of links of the shortest optical length path;
3. decreasing order of the optical length of the shortest optical length path.

Third phase: starting with the FSs occupied by the non-affected lightpaths (computed in Phase 1), the algorithm tries to assign iteratively a lightpath to each demand by the order computed in Phase 2 and using the **FF** algorithm; at each iteration, when a new lightpath is assigned to a demand, the set of occupied FSs is updated before the next iteration.

The hierarchical order used in the second phase was shown in our preliminary tests to provide the best performance in terms of total surviving demand. Note that, in a failure state, it is no longer possible to compute in advance the set of candidate paths as the set of failing nodes cannot be predicted. The complexity of the algorithm is mainly imposed by the first phase where a k-shortest paths algorithm must be run between many node pairs and its complexity is $\mathcal{O}(kn(|E| + n\log(n)))$ for each pair of nodes [BELR07] when using Yen's algorithm [Yen71].

5.4 Simulation description

An event-driven simulator was developed to evaluate the spectrum usage efficiency and the resilience to multiple node failures of the different RMSA algorithms in dynamic EONs. The spectrum usage efficiency is assessed by the bit-rate amount of all requests that are blocked in the regular state due to insufficient free spectrum resources. The resilience to multiple node failures is evaluated by the average non-disrupted demand (the average bit-rate percentage that is not disrupted after a multiple node failure) and the average surviving demand (the average bit-rate percentage that is supported after a multiple node failure) among all failure events of each simulation.

A simulation is composed by two modules, one simulating the regular state and another simulating the failures states, which are described separately in the next subsections.

5.4.1 Simulation of the regular state

In the regular state, events are associated with time instants when the EON has either to assign a lightpath to a new request or to tear down a previously assigned lightpath. In each simulation, λ is the arriving request rate (per time unit) at the end of the simulation and the lightpath duration is exponentially distributed with an average duration of one time unit.

Each simulation runs a total number of events given by $\mathcal{E}$ and the arriving request rate is $\frac{e}{\mathcal{E}} \times \lambda$, where $e = 1, 2, ..., \mathcal{E}$ is the current event number. In this way, a single run simulates all network load values from a very lightly loaded network (at the beginning of the simulation) up to a heavily loaded network (at the end of the simulation). Parameter λ is tuned for each network case so that the blocking probability at the end of the simulation is around 10% for the worst RMSA algorithm.

Each unicast request d has its end-nodes (s_d, t_d) randomly generated with a uniform distribution among all node pairs and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set $\{50, 100, 150, 200\}$ resulting in an average bit-rate request of 125 Gbps. On the other hand, each anycast request d has its source node s_d randomly generated with a uniform distribution among all nodes, its anycast service r_d randomly generated with a uniform distribution among all anycast services and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set $\{50 \times \omega : \omega \in \mathbb{N},\ \omega \leq 20\} = \{50, 100, ..., 1000\}$ resulting in an average bit-rate request of 525 Gbps.

At each request event, first the request type is randomly selected between unicast with probability p_{uni} or anycast (with probability $1 - p_{uni}$). Then, the request of each type is randomly generated as described before. In all simulations, we have considered that the total generated bit-rate is equally split between unicast and anycast services. Since the average bit-rate request is 125 Gbps for unicast and 525 Gbps for anycast, p_{uni} was set to:

$$p_{uni} = \frac{525}{125 + 525} = \frac{21}{26}.$$

In the simulations reported in the computational results, we have set $\mathcal{E} = 10^5$ events. Moreover, for a fair evaluation between the different RMSA algorithms, we have randomly generated all parameters associated with request events once for each network, and used the same values when simulating the different RMSA algorithms for the same network.

5.4.2 Simulation of the failure states

When the regular state reaches the event numbers in set $\mathcal{E}_f$, the failure state simulation module is launched and, when this module ends, the regular state simulation continues from the state it was before. The simulation of a failure state has the following 3 steps:

1. generate a random multiple node failure event;
2. run the RMSA algorithm (as described in section 5.3.2) taking into account the regular state at the moment of the failure event and the set of failure nodes;
3. compute the resulting total non-disrupted bit-rate and surviving bit-rate of the current failure event.

The random generation of a multiple node failure event in step 1 follows the attack model described in section 5.2.1. First, the number of attacked nodes s is randomly generated between s_m and s_M with the probabilities given by (5.1). Then, a set of s nodes is randomly selected (without replacement) with a probability of each node $i \in N$ being selected proportional to its weight w_i.

At the end of the regular state simulation, the average non-disrupted demand and the average surviving demand performance parameters are computed based on the values obtained on all failure events run in the set $\mathcal{E}_f$ of event numbers.

In the simulations reported in the computational results, we have considered set $\mathcal{E}_f$ composed by the event numbers multiple of 100 in the range $10^3 < e \leq \mathcal{E}(= 10^5)$, which gives a total of 990 multiple node failure events per simulation. The aim was to select the set $\mathcal{E}_f$ uniformly from a minimum number (below which the network load is very low) until $\mathcal{E}$ so that the resilience performance parameters are assessed over the whole range of network loads. Again, for a fair evaluation between the different RMSA algorithms, we have randomly generated all multiple node failure events once for each network and used the same node failures when simulating the different RMSA algorithms for the same network.

5.5 Computational results

The computational results presented in this section are based on 3 network topologies with public available information [OWPT10] and shown in Figure 5.2: Germany50, Cost266 and Janos-US. Table 5.3 presents their topology characteristics in terms of number of nodes n and fiber links $|E|$, average node degree $\bar{\delta}$, average link length $\bar{l}$ (in Km) and diameter D, i.e., the highest optical length (in Km) among all shortest paths adding Δ per intermediate node (the length Δ modeling the degradation suffered by a lightpath on each intermediate node was set to 60 km).

Table 5.3: Topology characteristics of each network.

Network	$n = \|N\|$	$\|E\|$	$\bar{\delta}$	$\bar{l}$ (km)	D (km)	$\|C\|$
Germany50	50	88	3.52	100.7	1417	11
Cost266	37	57	3.08	438.1	4574	9
Janos-US	26	42	3.23	600.6	5094	7

In each network, we have considered a set of five anycast services ($|R| = 5$) and each service $r \in R$ is run on five randomly selected DC nodes. We restricted the possible DC locations of each anycast service to set $C \subset N$ (highlighted in large circles in Figure 5.2) which was selected among the nodes with largest node degree (the number of such nodes is also provided in the last column of Table 5.3). Then, the DC node locations (set C_r) providing each anycast service $r \in R$ were randomly selected with a uniform distribution among the nodes in C.

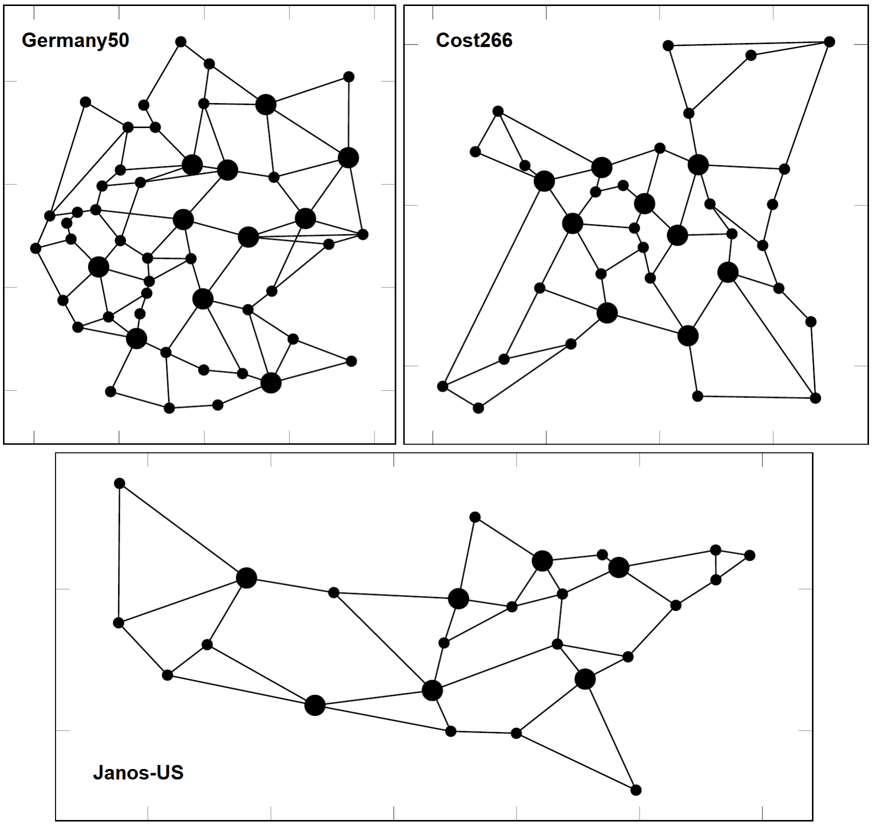


Figure 5.2: Network topologies.

In the regular state, the set of candidate paths associated to each incoming unicast request d was computed with a k-shortest paths algorithm (considering $k = 30$) and the same set was used for all RMSA algorithms. In anycast requests, we have considered the union of the sets of the $k = 30$ shortest paths from the source node s_d to each DC node of its anycast service r_d, and then excluded from the union set the paths that have intermediate DC nodes of the same service. In each failure state, we have considered up to $k = 5$ shortest paths as the candidate paths in the surviving topology. Notice that, in both states, if the number of feasible paths is lower than k, we consider all possible paths as the set of candidate paths.

We have considered a capacity of $|F| = 320$ FSs on all fiber links of the network, which corresponds to a spectral grid of granularity 12.5 GHz. We have assumed 4 available MFs whose transmission reach and bit-rate capacity are presented in Table 5.4 (transceiver model based on [RBMT17] and transmission reaches based on [KRS$^+$16]).

The number n_p of FSs required by each candidate path $p \in \mathcal{P}_d$ for a request d requiring a bit-rate b_d is computed based on the distance-adaptive transmission (DAT) rule as follows. We first select the highest bit-rate MF whose transmission reach is not lower than the optical length of p (the assumptions are that transceivers support polarization division multiplexing, operate at a fixed baud rate of 28 Gbaud, and transmit/receive on an optical channel occupying 37.5 GHz). If the bit-rate b_d of request d is not higher than the selected MF bit-rate,

Table 5.4: Transmission reach and bit-rate capacity of each MF.

Modulation Format (MF)	BPSK	QPSK	8-QAM	16-QAM
Transmission reach (km)	6300	3500	1200	600
Bit-rate capacity (Gbps)	50	100	150	200

one single transceiver is required. Otherwise, multiple optical channels (each one used by one transceiver with the previous selected MF) are grouped in a single spectral super-channel (SCh). We assume that lightpaths require a 12.5 GHz guard-band and, so, the required number of contiguous FSs is $n_d = 3t + 1$, where t denotes the minimum number of transceivers with a total bit-rate not lower than b_d. Consequently, we set $\beta = 4$ in expressions (5.7) and (5.8) of the Mixed RMSA algorithm as $n_d = 3t + 1$ has a minimum of 4 when $t = 1$.

As explained in Section 5.4.1, parameter λ was tuned for each network case so that the blocking probability at the end of the simulation is around 10% for the worst RMSA algorithm. After preliminary tests with each topology, we have considered $\lambda = 1200$ for Germany50, $\lambda = 550$ for Cost266 and $\lambda = 500$ for Janos-US.

Concerning the multiple node attacks, we have considered that the number of attacked nodes s is between $s_m = 2$ and $s_M = 6$ (we have excluded $s = 1$ since typical topologies are already resilient to single node failures). Moreover, the node weights (defining the probability of each node being discovered by the attacker) were assumed to be $w_i = 10$ for the DC nodes (set C) and $w_i = 1$ for all other nodes (set $N \backslash C$).

Concerning the obtained simulation results, Table 5.5 presents for each network the total rejected bit-rate obtained by each RMSA algorithm, i.e., the sum of the bit-rate values of all requests that were blocked in the regular state (the best values are highlighted in bold for each network). In this table (and in the following ones), Mv1, Mv2 and Mv3 refers to the Mixed RMSA Variants 1, 2 and 3, respectively, as described in section 5.3.1.

Table 5.5: Total rejected bit-rate (in Gbps) results

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	46800	2600	49150	3650	35100	**1700**
Cost266	43900	19350	36500	18700	33950	**14350**
Janos-US	35250	19900	42600	18700	33500	**12400**

The results in Table 5.5 clearly show that the Mixed RMSA Variant 3 algorithm is the best alternative in terms of spectrum usage efficiency. Note that it is even better than the LFS algorithm which does not use the path disaster availability metric and selects the path only based on assigning the FSs on the lowest possible spectrum. Recall that the Mixed RMSA Variant 3 algorithm combines with equal weights two spectrum usage metrics (the minimization of the highest assigned FS and minimization of the total number of assigned FSs). Moreover, the rejected bit-rates happen when the network is heavily loaded. In these cases, the weight of the spectrum usage metrics becomes close to 1 (and the weight of the path disaster availability metric becomes close to 0) in the Mixed RMSA algorithms. So, the results in Table 5.5 show that the combination of the two spectrum usage metrics with equal weights (of the Mixed RMSA Variant 3 algorithm) uses more efficiently the spectrum resources than considering only the minimization of the highest assigned FS (of the LFS algorithm).

On the other hand, both FF (which uses the basic first-fit approach) and PDA algorithms (which use the path disaster availability metric as the first criterion) are the ones that, overall, are the least efficient in terms of spectrum usage. Finally, the other RMSA algorithms present intermediate results.

Concerning the resilience to multiple node failures, Table 5.6 presents for each network the average non-disrupted demand, in percentage, obtained by each RMSA algorithm, i.e., the average bit-rate percentage that is not disrupted after a multiple node failure (again, best values highlighted in bold). As expected, the PDA algorithm is the best RMSA algorithm since, by using the path disaster availability metric, minimizes the probability of the selected routing paths to be affected by the multiple node failures. On the other hand, the FF and LFS algorithms are worst, on average, than the PDA algorithm.

Table 5.6: Average non-disrupted demand (%) results

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	67.61	64.96	**70.98**	67.88	69.24	68.86
Cost266	58.71	57.17	**62.10**	59.85	60.76	60.46
Janos-US	53.86	50.97	**55.03**	53.01	54.81	53.88

Concerning the Mixed RMSA algorithms (which combine the path disaster availability metric with spectrum usage metrics), they do not seem to be as good as the PDA algorithm. Nevertheless, these values represent percentages over the total bit-rate accepted in the network at the time instant of each failure event. Recall from the previous Table 5.5 that the Mixed RMSA Variant 3 has a much smaller total rejected demand. So, for this RMSA algorithm, the percentage values in Table 5.6 represent absolute non-disrupted demands which are closer to the ones of the best PDA algorithm.

Finally, Table 5.7 presents for each network the average surviving demand, in percentage, obtained by each RMSA algorithm, i.e., the average bit-rate percentage that is supported after a multiple node failure (again, best values highlighted in bold). In this case, the Mixed RMSA Variant 3 is the best, on average, although for each network the results are very close between the different RMSA algorithms. This is due to the fact that in a multiple node failure, many of the affected lightpaths have end-nodes which become disconnected in the surviving network. Like in the previous table, the values of Table 5.7 represent percentages over the total bit-rate accepted in the network at the time instant of each multiple node failure. So, since the Mixed RMSA Variant 3 has a much smaller total rejected demand (seen in Table 5.5), we reach the conclusion that the Mixed RMSA Variant 3 is the best algorithm concerning the average surviving demand parameter.

In overall, the best algorithm among all tested ones is the Mixed RMSA Variant 3 as it is the most efficient in terms of spectrum usage (reaching the lowest level of rejected bit-rate) and, concerning the resiliency to multiple node failures, it is the most efficient in terms of average surviving demand and almost as efficient as the PDA algorithm in terms of average non-disrupted demand.

Note that, upon a multiple node failure event, there are demands that cannot survive

Table 5.7: Average surviving demand (%) results

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	89.46	89.70	89.31	89.70	89.48	**89.74**
Cost266	83.56	83.58	83.40	83.58	83.57	**83.59**
Janos-US	**75.17**	75.12	74.82	75.14	75.04	75.15

in the surviving network whatever RMSA is adopted. The obvious ones are the demands such that at least one of their end-nodes has failed. Moreover, if the multiple node failure event splits the network in different components: (i) unicast demands cannot survive if their end-nodes are in different components and (ii) anycast demands cannot survive if their source nodes are in a network component without any of the DC nodes of their anycast service.

In the results of both Tables 5.6 and 5.7, the performance values obtained by all RMSA algorithms are always better for Germany50, intermediate for Cost266 and worst for Janos-US. In order to better understand these results, we have also analyzed the type of surviving networks that were imposed by all failure events on each network. In graph theory, a disconnected network is a graph that does not contain a path for at least one of its node pairs. Moreover, a 1-connected network is a graph such that the minimum number of elements (nodes and edges) whose removal makes the network disconnected is 1. Finally, a 2-connected network is a graph such that the minimum number of elements whose removal makes the network disconnected is 2. Table 5.8 presents, for each network, the relative frequency (in percentage) of each type of surviving network among all 990 simulated failure events.

Table 5.8: Relative frequency (in %) of each type of surviving network.

Network	Disconnected	1-connected	2-connected
Germany50	4.24	60.51	35.25
Cost266	17.07	72.12	10.81
Janos-US	40.61	55.15	4.24

Note that a 2-connected surviving network is more likely to have enough resources to assign lightpaths to the affected demands than a 1-connected surviving network. In Table 5.8, although most of the surviving networks are 1-connected for all networks, the network with the best resilience to multiple node failures (i.e., Germany50) is the one with the lower percentage of disconnected surviving networks and the highest percentage of 2-connected surviving networks. On the other hand, the network with the worst resilience to multiple node failures (i.e., Janus-US) is the one with the highest percentage of disconnected surviving networks and the lowest percentage of 2-connected surviving networks.

Next, we present different visualizations of the conducted simulations to further analyze the reasons for the best performance of the Mixed RMSA Variant 3 algorithm. The different simulations are visualized comparing this algorithm with the LFS (whose decision aims only the best spectrum usage efficiency) and with the PDA (whose decision aims primarily the best resiliency to multiple node failures).

Using the highest allocated FS (parameter H in section 5.3.1) as a measure of the network load, Figure 5.3 visualizes the evolution of the highest allocated FS as a function of the event number for the three RMSA algorithms on each of the three networks (in each plot, the plotted value on each event number is the average value of H in the last 1000 events).

Figure 5.3 shows that, for all networks, the spectrum usage is the lowest in most of the events with LFS reaching the highest load values only at the events very close to the end of the simulation. On the other hand, the spectrum usage is the highest in all events with PDA reaching the highest load values much sooner than LFS (the reason why the PDA algorithm has a poor performance in terms of total rejected bit-rate). Finally, the Mixed RMSA Variant 3 algorithm is similar to PDA at the lower network load values (when there are plenty of free resources and the spectrum usage efficiency can be relaxed to reach a better multiple node failure resiliency) and gets slightly lower (i.e., better), on average, than LFS as the network load becomes very high (when the free spectrum resources become very scarce and the spectrum resources must be efficiently used).

As already discussed, there are affected demands that cannot survive whatever RMSA is adopted. In the simulations, we have also computed the total bit-rate that can survive in terms of connectivity on each failure event. Next figures visualize the evolution of the non-disrupted demand (Figure 5.4) and the surviving demand (Figure 5.5) as a function of the consecutive failure events for the three RMSA algorithms on each of the three networks. Both non-disrupted and surviving demands are computed as the ratio (in percentage) between their absolute bit-rate values and the total bit-rate that can survive at each failure event (in each plot, the plotted value on each failure event is the average value over the last 100 failure events).

As expected, the visualizations in Figure 5.4 show that PDA is always the best and LFS is always the worst algorithm concerning the non-disrupted demand. Moreover, the Mixed RMSA Variant 3 algorithm is as good as the best in the initial failure events (as it gives a higher weight to the path disaster availability metric when the network load is low) and becomes worse than the best PDA algorithm but still always better than the LFS algorithm (as it keeps using the path disaster availability metric on its decision although with a lower weight).

Regarding the surviving demand, the visualizations in Figure 5.5 show that all RMSA algorithms are able to maintain 100% of all survivable bit-rate for the lower values of network load. This is not surprising as there is plenty of the resources in the surviving network in these cases and this is the reason why the average surviving demand results shown in Table 5.6 are so close between the different RMSA algorithms. Then, when failure events happen in higher network load values, only part of the survivable bit-rate can survive and the Mixed RMSA Variant 3 becomes consistently better than the two other algorithms.

Concerning simulation running times, Table 5.9 presents the total running time of each simulation, including the regular state and all failure states. Recall that we have considered the same number of events (both in terms of request and failure events) for all simulations of all networks. However, the runtime values in Table 5.9 increase with the size of the network. The reason for this increase is a combination of two factors. One in that bigger networks accommodate more lightpaths and so, in multiple node failure events, the RMSA algorithm has to deal with more affected demands, on average. The other is that the k-shortest paths algorithm which is run in every RMSA decision takes longer runtime in bigger networks.

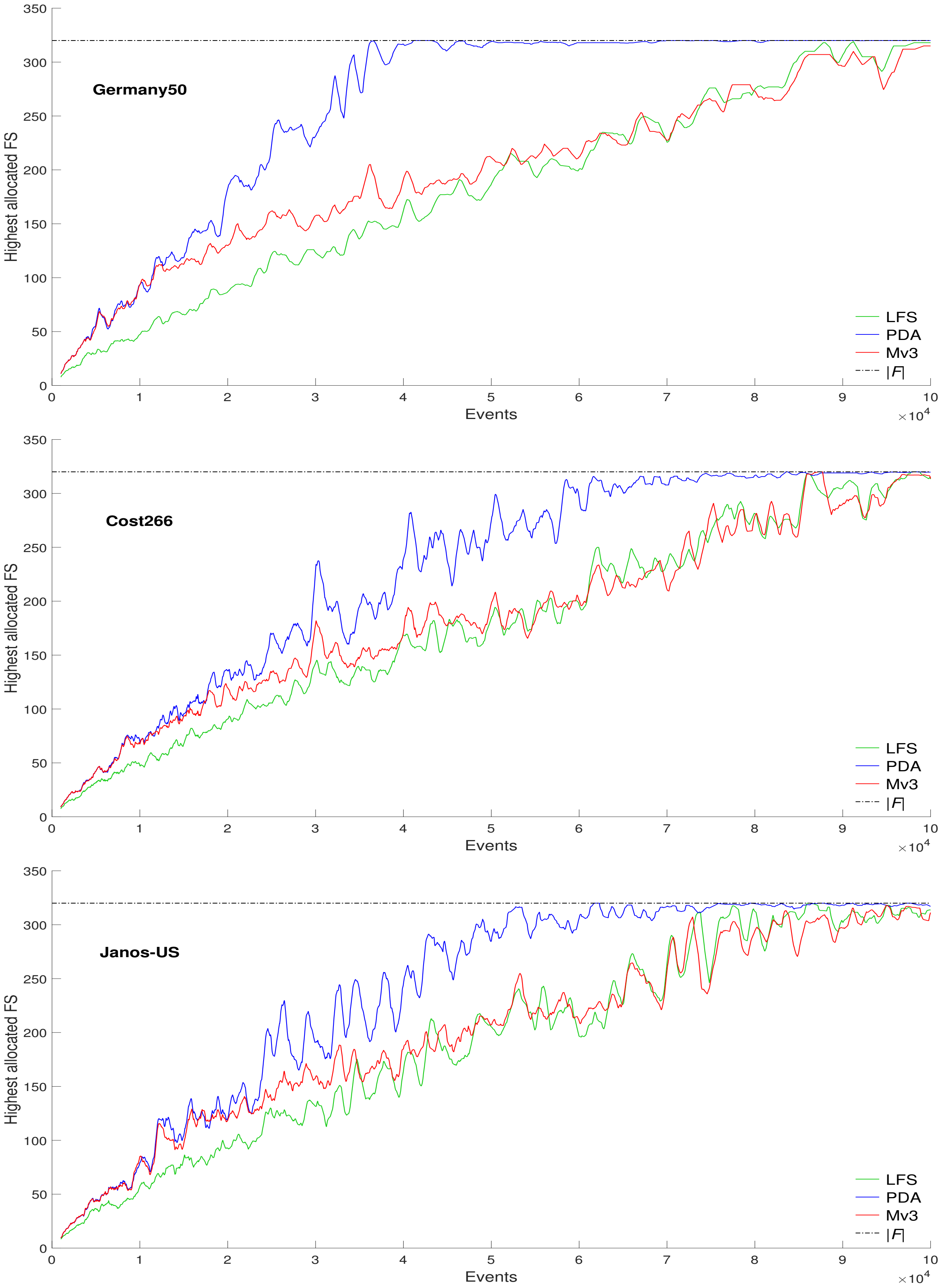


Figure 5.3: Evolution of the highest allocated FS as a function of the event number in the regular state ($|F|$ is the number of FSs on each fiber link).

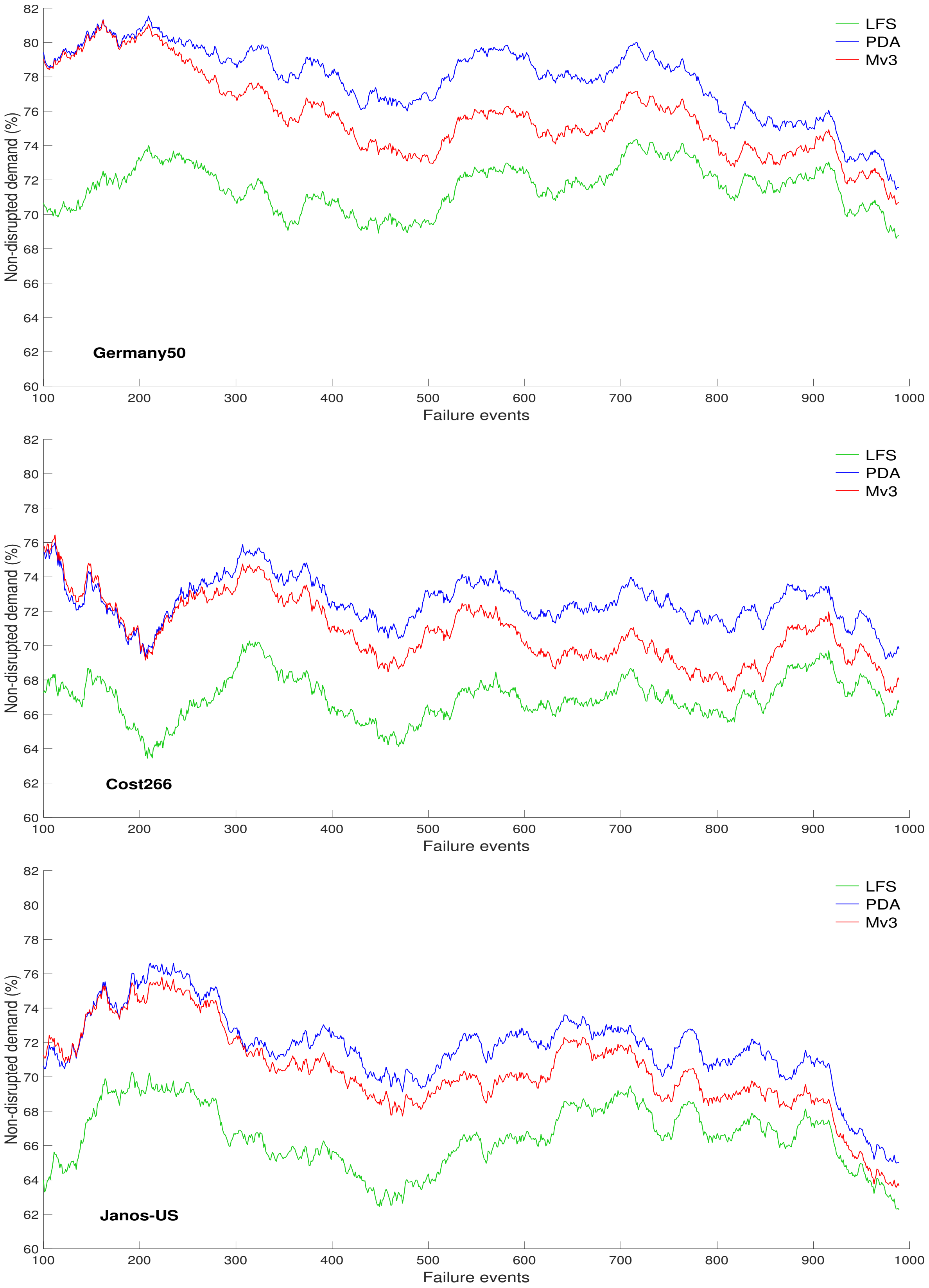


Figure 5.4: Evolution of the non-disrupted demand, in percentage, as a function of the consecutive failure events.

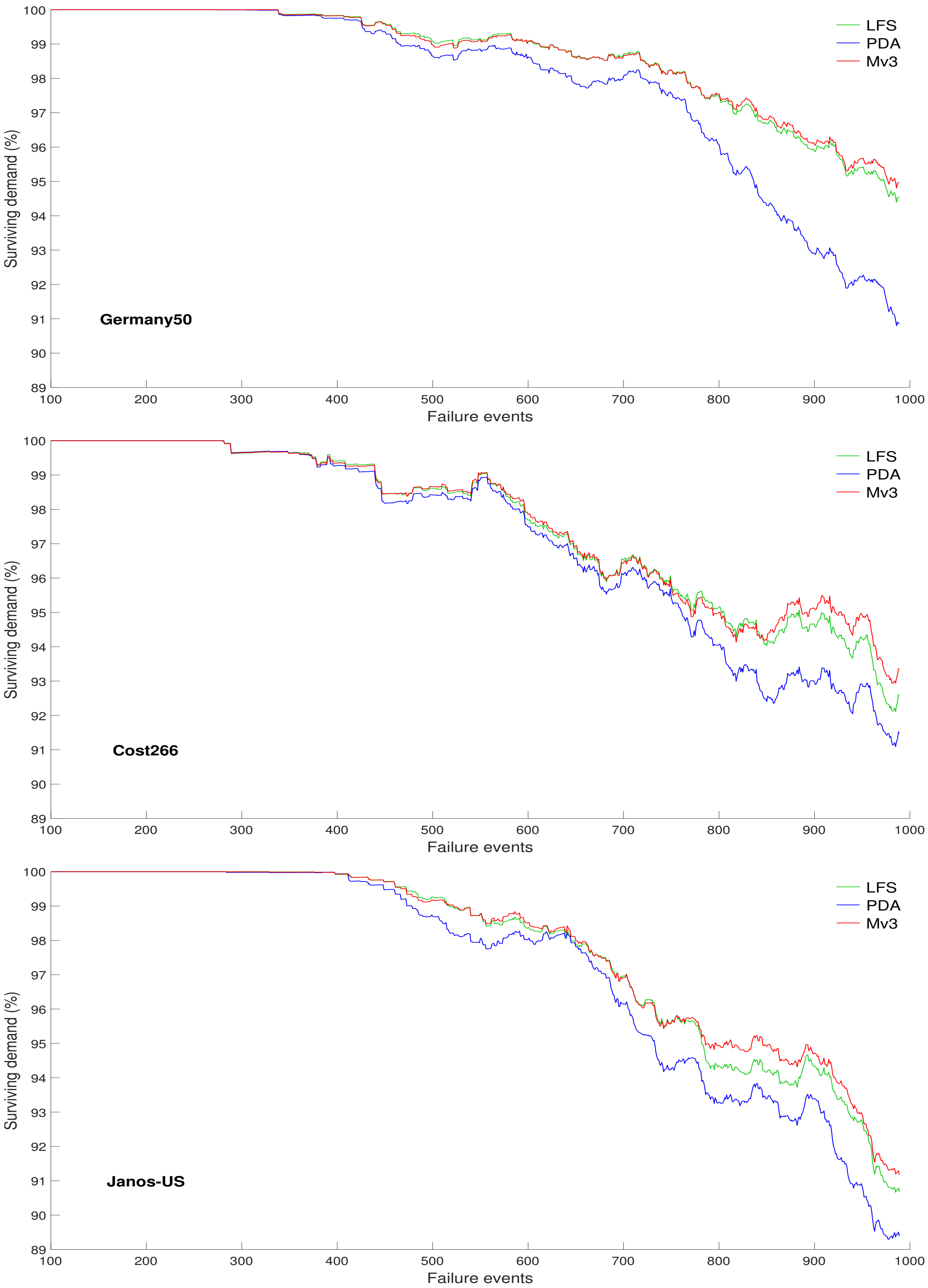


Figure 5.5: Evolution of the surviving demand, in percentage, as a function of the consecutive failure events.

Table 5.9: Total running time (in the format H:MM:SS) of each simulation.

Network	FF	LFS	PDA	Mv1	Mv2	Mv3
Germany50	1:00:33	1:08:51	0:52:10	1:04:27	0:59:11	1:04:44
Cost266	0:20:11	0:22:57	0:18:52	0:22:04	0:20:23	0:21:43
Janos-US	0:06:17	0:08:10	0:06:56	0:07:57	0:07:06	0:07:47

Moreover, there are some visible differences between the runtime values of the different RMSA algorithms for the same network. The reason for these differences is again a combination of two factors. One is the complexity of each RMSA decision: FF is clearly the less complex algorithm while the Mixed RMSA variants are the more complex ones. The second is the performance of each algorithm in terms of non-disrupted demand: the most efficient algorithms minimize the number of disrupted lightpaths and the required RMSA decision in the failure state becomes quicker as it involves a smaller number of affected demands.

As a final note, recall that the node weights defining the probability of each node being discovered by the attacker were assumed to be $w_i = 10$ for the DC nodes and $w_i = 1$ for all other nodes. Some additional simulation tests were conducted (not reported here) with different weight sets. The conclusions between the different proposed RMSA algorithms are similar to the ones reported here as long as the ratio between the highest weight and the lowest weight is significant. When this ratio is small, the probability of each node being attacked (when an attack is realized) becomes similar among all nodes and the path disaster availability of candidate paths becomes inversely proportional to the number of links of the path. In this case, the maximization of the path disaster availability tends to select the same paths as the minimization of the number of assigned FSs in all links of the path (the second considered spectrum usage metric used in the Mixed RMSA Variant 3) as the number of links of the path becomes the main optimization factor of both metrics. Again the Mixed RMSA Variant 3 is the best overall algorithm but the difference between its performance and the performance of the other RMSA algorithms becomes smaller than the ones reported here. In particular, the FF algorithm becomes better as it selects the first path with enough available spectrum resources considering the paths ordered from the shortest to the longest optical length and there is a strong positive correlation between the optical length of a path and its number of links.

5.6 Conclusions

In EONs, the RMSA algorithm rules the way the optical spectrum of the EON is assigned to each service demand with the primary goal of using the spectrum resources in an efficient way. Then, other goals can also be addressed as long as the spectrum usage efficiency is not jeopardized. One such goal is the resilience of the EON to large-scale failures and one source of such failures is malicious human activities. In terrorist attacks, although node shutdowns are harder to realize than link cuts, they are the most rewarding in the attackers' perspective since the shutdown of one node also shuts down all its fiber links.

In a previous work, a path disaster availability metric was proposed for the RMSA decision which takes into account the probability of each path not being disrupted by a multiple node failure. Here, we have proposed a set of RMSA algorithms that make use of the path disaster availability metric for dynamic EONs where requests arrive randomly one at a time and the accepted ones last in the network for a random time duration.

To evaluate the proposed RMSA algorithms, we have developed an event-driven simulator able to assess the spectrum usage efficiency of the different RMSA algorithms and also their resilience to multiple node failures assessed by 2 parameters: the average non-disrupted demand and the average surviving demand. All algorithms were evaluated through simulation considering a mix of unicast and anycast services in 3 well-known topologies and, in the failure cases, a restoration mechanism where the non-affected lightpaths remain unchanged and the demands of the affected lightpaths are reassigned as much as possible in the spectrum resources of the surviving network.

In the simulations, we have compared two commonly used RMSA algorithms (FF and LFS) with different proposed RMSA algorithms using the path disaster availability metric: the PDA algorithm and the 3 variants of the Mixed RMSA algorithm. PDA uses the path disaster availability metric as its primary criterion. The 3 variants of the Mixed RMSA combine in three different ways the path disaster availability metric with 2 spectrum usage metrics: the lowest assigned frequency slot and the number of assigned frequency slots. Moreover, the combination takes into consideration the current load of the EON so that the resilience to multiple node failures has a higher weight in the RMSA decision when the EON is lightly loaded while the spectrum usage metrics have a higher weight in the RMSA decision when the EON is heavily loaded.

The simulation results have shown that the RMSA algorithm that combines the path disaster availability with the two spectrum usage metrics (named Mixed RMSA Variant 3 algorithm) is the best trade-off between the spectrum usage efficiency and the resilience of the EON to multiple node failures: this algorithm is the most efficient in terms of spectrum usage (reaching the lowest level of rejected bit-rate) and, concerning the resiliency to multiple node failures, it is the most efficient in terms of average surviving demand and almost as efficient as the PDA algorithm in terms of average non-disrupted demand.

Bibliography

[AR17] F. Abkenar and A. Rahbar. *Study and analysis of routing and spectrum allocation (RSA) and routing, modulation and spectrum allocation (RMSA) algorithms in elastic optical networks (EONs).* Optical Switching and Networking, 23:5–39, 2017.

[BdSA18] F. Barbosa, A. de Sousa, and A. Agra. *Topology design of transparent optical networks resilient to multiple node failures.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

[BdSA$^+$19] F. Barbosa, A. de Sousa, A. Agra, K. Walkowiak, and R. Goścień. *A RMSA algorithm resilient to multiple node failures on elastic optical networks.* In 11th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2019.

[BdSA20] F. Barbosa, A. de Sousa, and A. Agra. *Design/upgrade of a transparent op-*

tical network topology resilient to the simultaneous failure of its critical nodes. Networks, 75(4):356–373, 2020.

[BELR07] E. Bouille, G. Ellinas, J. Labourdette, and R. Ramamurthy. *Path routing in mesh optical networks.* Wiley, 2007.

[CSO15] B. Chatterjee, N. Sarma, and E. Oki. *Routing and spectrum allocation in elastic optical networks: a tutorial.* IEEE Communications Surveys Tutorials, 17(3):1776–1800, 2015.

[CTV11] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos. *Elastic bandwidth allocation in flexible OFDM-based optical networks.* Journal of Lightwave Technology, 29(9):1354–1366, 2011.

[CZJZ15] X. Chen, S. Zhu, L. Jiang, and Z. Zhu. *On spectrum efficient failure-independent path protection p-cycle design in elastic optical networks.* Journal of Lightwave Technology, 33(17):3719–3729, 2015.

[FWG$^+$16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GK19] R. Goścień and M. Kucharzak. *On the efficient optimization of unicast, anycast and multicast flows in survivable elastic optical networks.* Optical Switching and Networking, 31:114–126, 2019.

[GTE$^+$16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[GWK15] R. Goścień, K. Walkowiak, and M. Klinkowski. *Tabu search algorithm for routing, modulation and spectrum allocation in elastic optical network with anycast and unicast traffic.* Computer Networks, 79:148–165, 2015.

[KRS$^+$16] P. Khodashenas, J. Rivas-Moscoso, D. Siracusa, F. Pederzolli, B. Shariati, D. Klonidis, E. Salvadori, and I. Tomkos. *Comparison of spectral and spatial super-channel allocation shemes for SDM networks.* Journal of Lightwave Technology, 34(11):2710–2716, 2016.

[KW11] M. Klinkowski and K. Walkowiak. *Routing and Spectrum Assignment in Spectrum Sliced Elastic Optical Path Network.* IEEE Communications Letters, 15(8):884–886, 2011.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[PAK$^+$12] E. Palkopoulou, M. Angelou, D. Klonidis, K. Christodoulopoulos, A. Klekamp, F. Buchali, E. Varvarigos, and I. Tomkos. *Quantifying spectrum, cost, and energy efficiency in fixed-grid and flex-grid networks* [invited]. IEEE/OSA Journal of Optical Communications and Networking, 4(11):B42–B51, 2012.

[RBMT17] C. Rottondi, P. Boffi, P. Martelli, and M. Tornatore. *Routing, modulation format, baud rate and spectrum allocation in optical metro rings with flexible grid and few-mode transmission.* Journal of Lightwave Technology, 35(1):61–70, 2017.

[RH20] J. Rak and D. Hutchison. *Guide to disaster-resilient communication networks.* Computer Communications and Networks, Springer International Publishing, Cham, 2020.

[Rob04] S. Robinson. *Simulation: the practice of model development and use*. John Wiley & Sons, Inc., Hoboken, NJ, USA, 2004.

[TR17] S. Talebi and G. Rouskas. *On distance-adaptive routing and spectrum assignment in mesh elastic optical networks.* IEEE/OSA Journal of Optical Communications and Networking, 9(5):456–465, 2017.

[WK13] K. Walkowiak and M. Klinkowski. *Joint anycast and unicast routing for elastic optical networks: Modeling and optimization.* In IEEE International Conference on Communications (ICC), pages 3909–3914, 2013.

[WNG17] J. Wu, Z. Ning, and L. Guo. *Energy-efficient survivable grooming in software-defined elastic optical networks.* IEEE Access, 5:6454–6463, 2017.

[Yen71] J. Yen. *Finding the k-shortest loopless paths in a network.* Management Science, 17(11):712–716, 1971.

Appendix A: Critical Node Detection with Connectivity based on Bounded Path Lengths

Abstract: For a given graph representing a transparent optical network, a given weight associated to each node pair and a given positive integer c, the Critical Node Detection problem variant addressed here is the determination of the set of c nodes that, if removed from the graph, minimizes the total weight of the node pairs that remain connected. In the context of transparent optical networks, a node pair is considered connected only if the surviving network provides it with a shortest path not higher than a given positive value T representing the optical transparent reach of the network. Moreover, the length of a path depends both on the length of its links and on its number of intermediate nodes. A path-based Integer Linear Programming model is presented together with a row generation approach to solve it. We present computational results for a real-world network topology with 50 nodes and 88 links and for $c = 2$ up to 6. The optimal results are compared with node centrality based heuristics showing that such approaches provide solutions which are far from optimal.

Keywords: Critical node detection, Transparent optical networks, Path model, Decomposition approach

F. Barbosa, A. Agra, and A. de Sousa. *Critical node detection with connectivity based on bounded path lengths.* In XIX Congresso da Associação Portuguesa de Investigação Operacional, Aveiro, Portugal, 2018.

A.1 Introduction

For a given network, Critical Node Detection (CND) problems aim to optimally remove a subset of nodes (the critical nodes) in order to optimize or restrict a given network degradation metric. The problem can be defined either by upper-bounding the number of critical nodes and maximizing the degradation metric, or by lower-bounding the degradation metric and minimizing the number of critical nodes.

One most used network degradation metric is the pairwise connectivity defined as the number of node pairs that remain connected when the critical node set is removed, as in [ACEP09]. This work considers a given number c and define CND as the identification of c critical nodes minimizing the pairwise connectivity showing that the problem is NP-hard. It proposes a compact Integer Linear Programming (ILP) model which is not able to solve realistic sized instances, and a multi-start local search heuristic as an alternative for large problem instances. The work in [VBP14] addresses two CND variants. The first variant is the same as defined in [ACEP09]. In the second variant, for a given integer L, the aim is to identify a minimum set of critical nodes, so that the largest connected component in the remaining graph contains no more than L nodes. For both variants, the authors propose alternative more compact ILP models, together with reformulations and valid inequalities. In [SGL12], an ILP model with a non-polynomial number of constraints is proposed to the minimum pairwise connectivity CND version and a branch-and-cut method is described exploiting the fact that the linear relaxation of the model can be solved in polynomial time. In [SdSM18], a weighted version of the pairwise connectivity is used as the network degradation metric, *i.e.*, a weight is associated to each node pair and the aim is to minimize the total weight of the connected node pairs. This work proposes ILP models which are more efficiently solved by standard solvers than the ones proposed in [ACEP09, VBP14] and presents computational results showing that realistic sized networks up to 75 nodes and 99 edges can be solved within seconds.

In [VPP15], the CND problem is dealt with considering a distance-based connectivity metric, *i.e.*, to take into consideration not only the node pairs that become disconnected but also the shortest path distance penalties between node pairs that remain connected. For a given graph with associated node costs and a given cost budget, this work considers the identification of a set of nodes within the budget whose removal maximally degrades the connectivity metric. It proposes a general ILP model that can be adapted to different distance-based metrics by proper parameter definition. In [DXT$^+$12], the critical elements can be either nodes or links. In this work, the aim is to identify a minimum cardinality critical set of elements, referred to as a $\beta-$disruptor, whose removal results in a given pairwise connectivity target ($0 \leq \beta < 1$ denotes the connectivity fraction target). More recently, [DT15] assumes a budget constraint considering associated link and node costs, and extends the previous work in [DXT$^+$12] to the case where the $\beta-$disruptor can be a mix of links and nodes. In both works, approximation methods are proposed to solve the different problem variants.

CND problems have been considered in different contexts (social networks, power grids, military networks, biology, and so on). Recently, CND problems are gaining special attention in the vulnerability evaluation of telecommunication networks to large-scale disasters. Disaster based failures can seriously disrupt any telecommunication network due to either natural, technological or malicious human causes [RHC$^+$16] and a key component when dealing with these issues is the vulnerability evaluation of current networks against such failures [GTE$^+$16]. In the particular case of malicious human attacks, node shutdowns, although harder to realize, are the most rewarding in the attackers perspective. The solutions provided by CND for a given number c are a worst-case scenario for simultaneous failures of up to c nodes and, when comparing different network topologies, the higher the CND value is, the more robust the network becomes to such failures.

In here, we study the CND problem in the context of transparent optical networks. In such networks, data is converted at the source into light, routed to the destination through an all-optical path, named *lightpath*, and converted back to electronic domain at the destination. To work properly, the routing path from source to destination of a ligthpath must be bounded by a *transparent reach* value which is imposed by the optical degradation suffered by the lightpath both on fibre links and on intermediate optical nodes. The optical degradation suffered by a lightpath while traversing an intermediate node is usually modelled by a given fibre length value δ, *i.e.* by considering it equivalent to the degradation incurred due to the transmission over a given fibre of length δ.

If some network nodes are considered critical due to some reason, then, the optical network design must take into consideration this fact. An example is [BdSA18] where the network design approach proposed in [AdSD16] is adapted to the design of a transparent optical network minimizing the impact of the simultaneous failure of a given set of critical nodes. In that work, the critical node set is given while here the aim is to determine the set of critical nodes of a given transparent optical network.

The CND variant addressed here considers, as in [SdSM18], a given weight associated to each node pair and a given positive integer c defining the number of critical nodes. Nevertheless, differently from all previous works, in this problem variant, a node pair is considered connected only if the surviving network provides it with a shortest path not higher than a given positive value T representing the transparent reach of the optical network. Moreover, the length of a path depends both on the length of its links and on its number of intermediate nodes. To describe the problem in a compact way, we would need an arc-based ILP model which requires for each pair of nodes many additional arc variables and flow conservation constraints to define the associated path. Instead, we define the problem with a path-based formulation, as in [SGL12], and we propose an exact algorithm based on row generation to solve it. Finally, as in other works for other CND problem variants ([DT15, DXT$^+$12, VBP14]) , we compare the optimal solutions of the exact method with node centrality based heuristics showing that such approaches provide solutions which are far from optimal.

The paper is organized as follows. Section A.2 describes the path-based ILP model defining the CND problem in the context of transparent optical networks. Section A.3 describes the row generation based approach used to solve the problem. Section A.4 describes the node centrality based heuristics used in the computational results. The computational results are presented and discussed in Section A.5. Finally, Section A.6 presents the main conclusions of the work.

A.2 Path-based ILP model

Consider a transparent optical network represented by a graph $G = (N, E)$ where $N = \{1, ..., n\}$ is the set of network nodes and $E \subseteq \{(i, j) \in N \times N : \; i < j\}$ is the set of fibre links. For each link $(i, j) \in E$, parameter l_{ij} represents its length. For each pair of nodes (i, j), with $i \in N, j \in N, i < j$, parameter w_{ij} represents the connectivity weight of the node pair. The transparent reach of the network is denoted by parameter $T > 0$ and the fibre length equivalent to the degradation suffered by a lightpath while traversing an intermediate node is denoted by parameter $\delta > 0$. We assume that $l_{ij} \leq T$ for all fibre links; otherwise, such link is worthless and can be removed.

The set of all paths in G between $i \in N$ and $j \in N, i < j$, with length not greater than T, is denote by P_{ij}. This set is defined only for non adjacent nodes, *i.e.*, for $(i, j) \notin E$. For each path $p \in P_{ij}$ the following binary parameters are defined: parameter β_k^p indicates whether node k (which can be an end node) is in path p or not, and parameter α_{kt}^p indicates whether link $(k, t), k < t$ is in path p or not. So, P_{ij} is composed by all paths p such that $\sum_{k=1}^{n-1} \sum_{t=k+1}^{n} \alpha_{kt}^p l_{kt} + \delta\big(\sum_{k=1}^{n} \beta_k^p - 2\big) \leq T$. Although δ can be incorporated in the link length and, therefore, the use of parameters β_k^p could be omitted, we opted to include them in order to ease the reading.

Parameter $c \in \mathbb{N}$ represents the number of critical nodes. For each node $i \in N$, we consider a binary variable v_i indicating whether i is a critical node or not. For each node pair (i, j), with $i, j \in N : i < j$, the binary variable u_{ij} is 1 if nodes i and j are connected through a path satisfying the transparent reach T, and 0 otherwise.

A path formulation for the CND problem is given by the following ILP model.

$$\min \quad z := \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} w_{ij}\ u_{ij} \tag{A.1}$$

$$s.t. \quad \sum_{i=1}^{n} v_i \leq c \tag{A.2}$$

$$u_{ij} + v_i + v_j \geq 1, \quad (i, j) \in E, \tag{A.3}$$

$$u_{ij} + \sum_{k=1}^{n} \beta_k^p v_k \geq 1,\ (i, j) \notin E,\ \ p \in P_{ij}, \tag{A.4}$$

$$v_i \in \{0, 1\}, \qquad i \in N, \tag{A.5}$$

$$u_{ij} \in \big\{0, 1\big\}, \qquad i, j \in N:\ \ i < j. \tag{A.6}$$

The objective (A.1) is to minimize the total weighted connectivity in the surviving graph, *i.e.* the sum of the weights of the node pairs that remain connected after the critical nodes are removed. Constraint (A.2) ensures that at most c nodes are selected as critical nodes (in any optimal solution, c nodes are selected). Constraints (A.3) guarantee that a pair of adjacent nodes is connected if none of the two nodes is a critical node. Constraints (A.4) are the generalization of constraints (A.3) for the node pairs that are not adjacent in G: the node pair (i, j), with $i < j$, is connected if there is a path $p \in P_{ij}$ such that none of its nodes is a critical node. Finally, constraints (A.5)-(A.6) are the variable domain constraints.

Notice that constraints (A.6) can be replaced by $u_{ij} \geq 0$. Since variables v_i are binary, constrains (A.3)–(A.4) impose $u_{ij} \geq 1$ if (i, j) is a connected node pair, and will be redundant in presence of constraints $u_{ij} \geq 0$, otherwise. As the objective function is a minimization function, then $u_{ij} = 1$ if (i, j) is a connected pair and $u_{ij} = 0$ otherwise. The resulting mixed integer linear problem (MILP) will be considered henceforward.

A.3 A row generation approach

The path formulation presented in the previous section includes the family of constraints (A.4) whose number increases exponentially with the input data. The exact number of constraints depends on the graph topology, the length of the links and on the parameters T and δ. However, the MILP can become too large for relative small size instances. Here we propose an exact algorithm, based on row generation, where inequalities (A.4) are initially ignored and the relaxed MILP problem is solved. Then, the separation problem associated with inequalities (A.4) is solved. If a violated inequality is found, it is added to the model and the MILP is solved again. The process is repeated until no violated inequality is found. The exact algorithm is described in Algorithm A.1.

The separation problem associated with constraints (A.4) is solved in the following way. First, we compute the subgraph that results from G when the critical nodes and the corresponding incident edges are removed and we add δ to the length of all non-removed edges. Then, we determine the shortest paths between all pairs of nodes in this subgraph with the new lengths. Finally, each shortest path whose length is not higher than $T + \delta$ is used to generate a new inequality (A.4) that is added to the model (by adding δ to each edge length and since, for each path, the number of intermediate nodes is equal to the number of edges minus one, the shortest path value with the new lengths is equal to the length value with the original lengths plus δ).

Algorithm A.1 Exact algorithm for the CND problem.

```
Solve MILP model without constraints (A.4) and let $(u^*, v^*)$ be the optimal solution
**repeat**
  Set NCuts ← 0 and $C \leftarrow \{i \in N : v_i^* = 1\}$
  Update the subgraph graph $G^C = (N \setminus C, E^C)$ where $E^C = \{(i,j) \in E : \ i,j \notin C\}$
  **for all** node pair $(i,j) \notin E^C$ with $i < j$ **do**
    Run Dijkstra algorithm (adding $\delta$ to the length of each edge) to find the shortest
    path $p_{ij} \in P_{ij}$ and its length $d_{ij}$
    **if** $d_{ij} \leq T + \delta$ and $u^*_{ij} + \sum_{k=1}^{n} \beta_k^{p_{ij}} v_k^* = 0$ **then**
      Add constraint (A.4) corresponding to path $p_{ij}$
      NCuts ← NCuts +1
    **end if**
  **end for**
  **if** NCuts $> 0$ **then**
    Solve MILP model with the added constraints. Update $(u^*, v^*)$
  **end if**
**until** Ncuts $= 0$
```

A.4 Node centrality based heuristics

Heuristic methods based on node centrality measures are commonly used in the literature to quickly compute sets of critical nodes. Algorithm A.2 presents a general heuristic framework for using these measures. In each iteration a node is selected according to the chosen node centrality measure (step 3) and removed from the graph (step 4). The heuristic finishes when c nodes are selected.

Algorithm A.2 Iterative heuristic approach based on node centrality .

```
1: Set $C \leftarrow \emptyset$ and $G' \leftarrow (N, E)$
2: **for all** $k = 1$ to $c$ **do**
3:     Using the selected node centrality measure, select the central node $i$ of graph $G'$
4:     Remove from graph $G'$ node $i$ and all edges incident to node $i$
5:     Set $C \leftarrow C \cup \{i\}$
6: **end for**
```

We consider three node centrality measures to select the central nodes in graph G':

- Node degree centrality. The selected node is the one with highest degree in graph G'.
- Node closeness centrality. The closeness of node i is defined as the sum of the inverse of the distances between i and each of the remaining nodes: $c(i) = \sum_{j \in N \setminus \{i\}} \frac{1}{\mathrm{d}_{ij}(G')}$, where $\mathrm{d}_{ij}(G')$ is the shortest path length between nodes i and j in G'. The node with highest closeness is selected.
- Node betweenness centrality. For graph G', the betweenness of node i is the number of shortest paths between all nodes in G', with length not greater than T, that include node i as an intermediate node. The node with highest betweenness is selected.

Again, the shortest path lengths computed for the Closeness and Betweenness centralities consider the length δ associated to each intermediate node and are computed in the same way as described in the previous section for the separation problem.

A.5 Computational results

Here we report the computational experiments carried out to test the proposed exact solution approach for the CND problem and to compare it with the centrality based heuristics. Additionally, some insight on the solutions for the CND problem is given.

All computations were performed using the optimization software *Gurobi Optimizer* version 7.5.1, with programming language *Julia* version 0.6.0, running on a PC with a Intel Core i5, 1.7 GHz (up to 2.4 GHz) and 6 GB RAM.

The test instances are based on the Germany50 network topology, a telecommunication backbone network with 50 nodes and 88 edges [OWPT10]. The transparent reach depends on the Optical Transport Units installed. Current values go up to 2500 km. Hence, for the transparent reach parameter T we consider values in $\{1417, 1500, 1600, 1800, 2000, 2500\}$, where value 1417 is the maximum length among the shortest paths between all node pairs of

Germany50 (a smaller value does not allow the network to be optically transparent between all node pairs). In all cases, we have considered $\delta = 60$ km.

Table A.1 presents the results obtained for $c \in \{2, 3, 4, 5, 6\}$ and considering the scenario where each pair of nodes has an unitary connectivity weight *i.e.* $w_{ij} = 1$ for all $i, j \in N$ with $i < j$. In addition to the number of critical nodes c and the transparent reach T given in the first two columns, column UB provides the trivial upper bound when all pairs of remaining nodes are connected (*i.e.*, the critical nodes do not turn the surviving network into more than one component), which is given by $\frac{(n-c)\times(n-c-1)}{2}$. The next three columns show the objective function value (in this case of unitary weights it coincides with the total number of connected node pairs after the removal of the critical nodes) of the feasible solution obtained with the heuristic based on the corresponding centrality measure. Hence, a feasible solution with value equal to UB means that all the remaining nodes are connected after the critical nodes have been removed. The last four columns are obtained with the exact approach. Column *CND* gives the optimal value, column *Iterations* gives the number of times the relaxed MILP was solved running Algorithm A.1, column *Time* gives the total elapsed running time in seconds, and column *Cuts* gives the total number of constraints (A.4) added to the model in order to reach the optimal solution.

Although the node centrality measures are commonly used in the literature to quickly compute critical node sets, it is possible to conclude from the results that these sets are not minimizing the global connectivity of the graph. Nevertheless, the total running time of all heuristics based on the node centrality take less than half a second (not presented in the table), while the exact approach, in some cases, take almost one minute.

Figure A.1 presents a graphical scaled representation of the network and the optimal critical node sets for each $c \in \{2, 3, 4, 5, 6\}$. Figure A.2 gives a similar representation of the critical node sets selected using the node centrality based heuristics for $c = 6$. These figures illustrate the reason behind the difference between the CND objective values and the number of connected node pairs obtained using node centrality based methods. On one hand, if the critical node set is optimally selected (*i.e* minimizing the global connectivity), the graph resulting from the removal of the critical nodes is disconnected into several components. On the other hand, node centrality based methods do not aim to disconnect the graph but only to select the most influential nodes (using node centrality criteria), which results is less disconnected graphs. When the resulting graph is not disconnected, the total number of connected node pairs increases for larger transparent reach values up to a point such that its value becomes equal to the upper bound.

Regarding the impact of the transparent reach value T in the results, Table A.1 shows that this parameter has little impact on the CND optimal value for this network. This can be explained by observing that when the critical nodes are removed from graph G, the resulting graph becomes disconnected and each resulting component fully satisfies connectivity for any $T \geq 1417$ km. However, this behaviour is not observed when node centrality based methods are used. In several instances the total number of connected node pairs increases for larger transparent reach values T to a point that the upper bound of the problem is reached. In this case, the graph resulting from the removal of the selected critical nodes is totally connected, as can be seen in Figure A.2 for the Degree and Closeness cases.

In order to test the effect of having different connectivity weights between different pairs of nodes, next we consider the case where the nodes corresponding to the five largest German

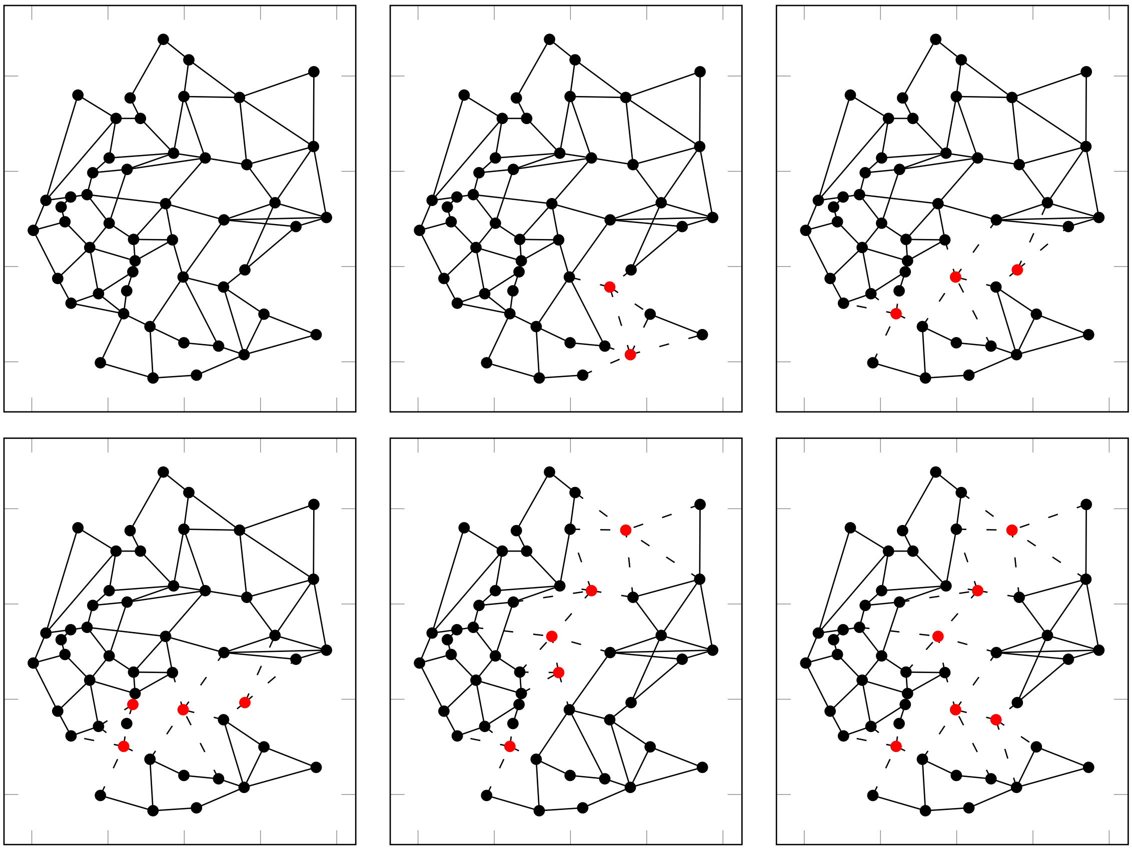


Figure A.1: Germany50 on top left, and the network resulting from the removal of the optimal critical node set for each size $c \in \{2, 3, 4, 5, 6\}$ (for any $T \geq 1500$).

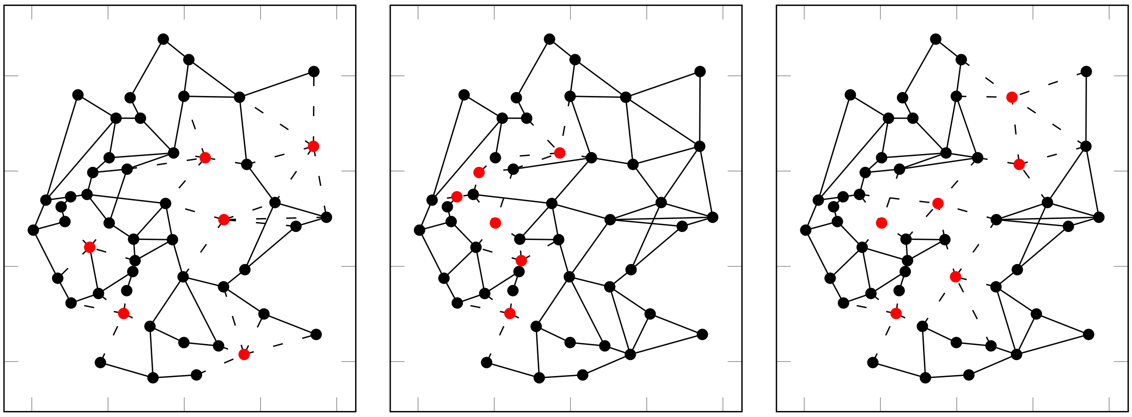


Figure A.2: The network resulting from the removal of node sets computed using centrality methods: Degree, Closeness and Betweenness, respectively (for $c = 6$).

Table A.1: Computational results for unitary weights.

c	T (km)	UB	Degree	Closeness	Between.	CND	Iterations	Time (s)	Cuts
2	1417	1128	1126	1127	1126	1026	17	36	3645
	1500		1128	1128	1128	1036	18	46	3689
	1600		1128	1128	1128	1036	18	49	3756
	1800		1128	1128	1128	1036	18	57	3816
	2000		1128	1128	1128	1036	18	54	3826
	2500		1128	1128	1128	1036	18	54	3826
3	1417	1081	1076	1076	1060	711	5	3	2557
	1500		1081	1081	1071	711	5	3	2603
	1600		1081	1081	1081	711	5	3	2593
	1800		1081	1081	1081	711	5	3	2620
	2000		1081	1081	1081	711	5	3	2620
	2500		1081	1081	1081	711	5	3	2620
4	1417	1035	1025	880	834	640	11	20	2892
	1500		1032	907	869	640	11	25	2969
	1600		1034	929	908	640	10	19	3031
	1800		1035	976	950	640	10	21	3157
	2000		1035	1010	989	640	10	22	3273
	2500		1035	1035	1035	640	10	22	3359
5	1417	990	980	809	682	496	7	9	3092
	1500		987	836	711	496	7	10	3196
	1600		989	867	743	496	7	11	3296
	1800		990	924	804	496	7	12	3429
	2000		990	959	862	496	7	14	3518
	2500		990	990	990	496	7	14	3600
6	1417	946	933	653	486	415	12	36	3319
	1500		940	678	487	415	12	38	3407
	1600		944	708	487	415	12	37	3492
	1800		946	766	487	415	12	35	3574
	2000		946	825	487	415	12	37	3607
	2500		946	946	487	415	12	36	3615

cities (in terms of population) have higher impact than all other 45 nodes. First, we assign a node weight of 4 to the nodes corresponding to the five larger cities and a node weight of 1 to all other nodes. Then, the connectivity weight w_{ij} between node i and node j is given by the multiplication of the weights of the two nodes.

In Table A.2, we present the results obtained with the exact approach for the CND problem with the weights computed as explained above. For these weight values an upper bound (column UB) is obtained when the critical nodes are c nodes that do not correspond to the largest cities and the resulting subgraph is fully connected. In these cases, the upper bound is given by the number of node pairs with two largest cities multiplied by 4^2 plus the number of node pairs with one largest city multiplied by 4 plus the number of node pairs with no largest cities multiplied by 1, *i.e.* UB $:= 4^2 \times \frac{5\times4}{2} + 4 \times 5 \times (45-c) + \frac{(45-c)\times(45-c-1)}{2}$. The remaining columns have the same meaning as the corresponding ones in Table A.1. The last two columns were added to compare these cases against the unitary weights cases. Column *Con. Pairs* gives the total number of connected node pairs after the removal of the critical

Table A.2: Computational results for different weights.

c	T (km)	UB	CND	Iterations	Time (s)	Cuts	Con. Pairs	Prev. CND
2	1417	1923	1577	15	24	2755	1127	1026
	1500		1577	14	21	2798	1127	1036
	1600		1578	14	23	2830	1128	1036
	1800		1578	14	23	2862	1128	1036
	2000		1578	14	23	2868	1128	1036
	2500		1578	14	22	2868	1128	1036
3	1417	1861	1224	6	6	2647	711	711
	1500		1224	6	6	2672	711	711
	1600		1224	6	6	2688	711	711
	1800		1224	6	6	2698	711	711
	2000		1224	6	6	2702	711	711
	2500		1224	6	6	2702	711	711
4	1417	1800	1044	8	11	3291	675	640
	1500		1044	8	12	3368	675	640
	1600		1044	8	12	3432	675	640
	1800		1044	8	12	3511	675	640
	2000		1044	8	12	3525	675	640
	2500		1044	8	12	3526	675	640
5	1417	1740	850	12	35	3902	526	496
	1500		850	11	31	4052	526	496
	1600		850	11	29	4184	526	496
	1800		850	11	32	4374	526	496
	2000		850	11	32	4507	526	496
	2500		850	11	33	4697	526	496
6	1417	1681	653	10	26	3823	446	415
	1500		653	10	27	3981	446	415
	1600		653	10	29	4125	446	415
	1800		653	10	29	4179	446	415
	2000		653	10	30	4278	446	415
	2500		653	10	31	4377	446	415

nodes of these cases. Column *Prev. CND* gives the (previous) CND optimal value for the unitary weights cases.

Concerning the performance of the exact algorithm proposed in Section A.3, by comparing the number of iterations, running time and number of added cuts between Table A.1 and Table A.2, one can observe that the results are nearly identically. That means the weights do not have a great impact on the performance of CND method presented in Algorithm A.1. Concerning the number of connected node pairs of the CND solutions, as expected, the number of connected node pairs considering different weights is higher than in the previous cases. This is because now the optimal set of critical nodes is a mixture between selecting nodes representing the largest cities and nodes that disconnect more the network.

Table A.3, presents the ratio between the optimal values and the corresponding theoretical upper bounds. These results show that the more realistic scenario with different weights show

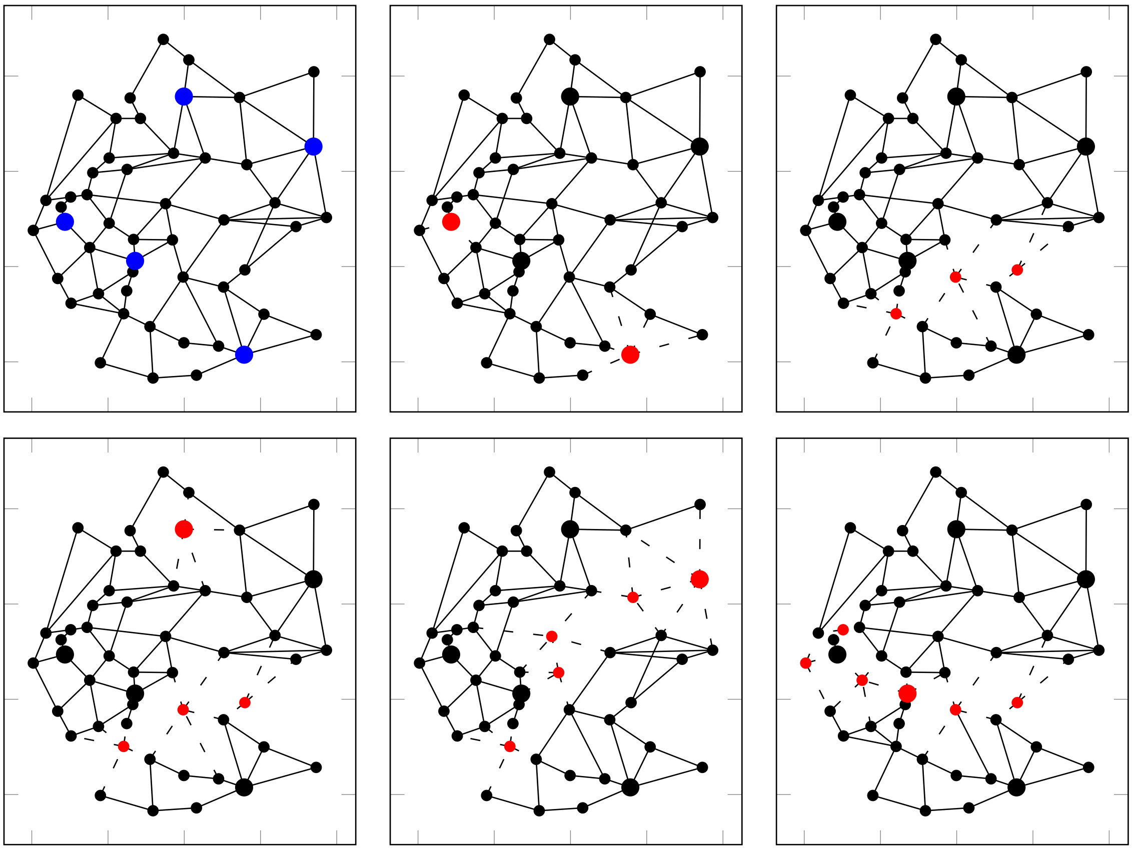


Figure A.3: Germany50 with the five main cities highlighted on top left, and the network obtained with the removal of the optimal node set for $c \in \{2, 3, 4, 5, 6\}$ ($T \geq 1600$).

that the network under consideration is less resilient to multiple node failures than the simplest scenario of considering equal importance to all node pairs. Moreover, as expected for both cases, the percentage of non-critical node pairs that remain connected decreases for larger values of critical nodes c.

Table A.3: Ratio (%) between CND optimal value and the upper bound ($T \geq 1600$).

c	2	3	4	5	6
Unitary	91.8	65.8	61.8	50.1	43.9
Weighted	82.1	65.8	58.0	48.9	38.9

Figure A.3 depicts the network where the five nodes corresponding to the largest cities are highlighted in blue, and the optimal critical node sets obtained for the weighted values and for the different values of c.

Comparing Figure A.3 with Figure A.1, one can observe that, with exception of $c = 3$, the optimal critical node set changes when different weights are considered. For example, with just two critical nodes, instead of disconnecting the graph (as in Figure A.1), the optimal solution is obtained by selecting two nodes corresponding to largest cities. In the last scenario with

6 critical nodes, the set of critical nodes changes considerably from the unitary weights to the different weights case. With unitary weights, the CND solution splits the network into three components each one with a large number of nodes. With different weights, the optimal solution is also obtained by splitting the graph into three components but the components are not balanced in terms of number of nodes (there is one component with only two nodes). Instead, one node corresponding to a largest city is selected as a critical node and the other four nodes representing largest cities are split among the 3 components.

A.6 Conclusions

In this work, we have addressed the Critical Node Detection (CND) problem in the context of a real transparent optical backbone network, a problem which is gaining a special interest in the vulnerability evaluation of networks. A path-based ILP model was proposed. Although path-based ILP formulations are not as efficient as the compact models for the traditional CND problem, such compact formulations do not allow to include directly the connectivity constraints based on bounded path lengths, as imposed by transparent optical networks. Based on the path formulation, an exact approach, based on row generation, was described allowing to compute the optimal set of critical nodes for the Germany50 network topology. The computational results also showed that the heuristics derived from the commonly used node centrality measures to quickly identify critical nodes, are not able, in general, to identify the optimal critical node set. Moreover, the results have shown that the tested backbone network has not a topology resilient to multiple node failures. In fact, with a simultaneous failure of only 10% of the network nodes ($c = 5$), it is possible to reduce the global connectivity of the network in about 50%. On top of that, the computational results show that in the more realistic scenario where node pairs have different weights, the simultaneous failure of the critical nodes is able to reduce the network connectivity even more than in the unitary weights case.

For a given network topology, the CND solution provides a worst-case measure of the network vulnerability to multiple node failures. As future research, we aim to develop efficient methods, both deterministic and stochastic, to upgrade the current network topology aiming to improve its CND value turning it more robust to multiple node failures.

Bibliography

[ACEP09] A. Arulselvan, C. Commander, L. Elefteriadou, and P. Pardalos. *Detecting critical nodes in sparse graphs.* Computers & Operations Research, 36(7):2193–2200, 2009.

[AdSD16] A. Agra, A. de Sousa, and M. Doostmohammadi. *The minimum cost design of transparent optical networks combining grooming, routing, and wavelength assignment.* IEEE/ACM Transactions on Networking, 24(6):3702–3713, 2016.

[BdSA18] F. Barbosa, A. de Sousa, and A. Agra. *The design of transparent optical networks minimizing the impact of critical nodes.* Electronic Notes in Discrete Mathematics, 64:165–174, 2018.

[DT15] T. Dinh and M. Thai. *Network under joint node and link attacks: vulnerability assessment methods and analysis.* IEEE/ACM Transactions on Networking, 23(3):1001–1011, 2015.

[DXT$^+$12] T. Dinh, Y. Xuan, M. Thai, P. Pardalos, and T. Znati. *On new approaches of assessing network vulnerability: hardness and approximation.* IEEE/ACM Transactions on Networking, 20(2):609–619, 2012.

[GTE$^+$16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[RHC$^+$16] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska. *RECODIS: Resilient communication services protecting end-user applications from disaster-based failures.* In 18th International Conference on Transparent Optical Networks (ICTON). IEEE, 2016.

[SdSM18] D. Santos, A. de Sousa, and P. Monteiro. *Compact models for critical node detection in telecommunication networks.* Electronic Notes in Discrete Mathematics, 64:325–334, 2018.

[SGL12] M. Di Summa, A. Grosso, and M. Locatelli. *Branch and cut algorithms for detecting critical nodes in undirected graphs.* Computational Optimization and Applications, 53(3):649–680, 2012.

[VBP14] A. Veremyev, V. Boginski, and E. Pasiliao. *Exact identification of critical nodes in sparse networks via new compact formulations.* Optimization Letters, 8(4):1245–1259, 2014.

[VPP15] A. Veremyev, O. Prokopyev, and E. Pasiliao. *Critical nodes for distance-based connectivity and related problems in graphs.* Networks, 66(3):170–195, 2015.

Appendix B: Topology Design of Transparent Optical Networks Resilient to Multiple Node Failures

Abstract: Consider the resilience of a network defined by the average 2-terminal reliability (A2TR) against a set of critical node failures. Consider an existing transparent optical network with a total fibre length L. The first goal of this paper is to assess the resiliency gap between the existing topology and a new network topology designed to maximize its resilience with the same fibre budget L. The resiliency gap gives us a measure of how good the resilience of existing network topologies are. Consider now that an existing network is upgraded with new links aiming to maximize its resiliency improvement with a fibre budget L'. The second goal of this paper is to assess how much the resiliency gap can be reduced between a good upgraded solution and a network topology designed to maximize its resiliency with the same fibre budget $L + L'$. The gap reduction gives us a measure of how close to the best resilience the upgraded solutions can get for different values of L'. To reach these goals, we first describe how the Critical Node Detection problem is defined and solved in the context of transparent optical networks. Then, we propose a multi-start greedy randomized method to generate network topologies, with a given fibre length budget, that are resilient to critical node failures. This method is also adapted to the upgrade of an existing network topology. At the end, we run the proposed methods on network topologies with public available information. The computational results show that the resiliency gap of existing topologies is significantly large but network upgrades with $L' = 10\%L$ can significantly reduce the resiliency gaps provided that such upgrades are aimed at maximizing the network resilience to multiple node failures.

Keywords: Transparent Optical Networks; Critical Node Detection; Resilient Network Design; Disasters

F. Barbosa, A. de Sousa, and A. Agra. *Topology design of transparent optical networks resilient to multiple node failures.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

B.1 Introduction

Large-scale failures can seriously disrupt any telecommunications network due to either natural, technological or malicious human activities [RHC$^+$16] (two surveys conducted within COST Action RECODIS are [GTE$^+$16] on strategies to protect networks against large-scale natural disasters and [FWG$^+$16] on security challenges in communication networks). So, an emerging research topic is the design of telecommunication networks enhancing their resilience to large-scale failures. To reach this goal, we must first adopt a proper resiliency evaluation metric and, then, we must investigate proper network design methods aiming to maximize the network resiliency metric to large-scale failures.

This work addresses the design of resilient network topologies in the context of transparent optical networks. Note that, in general, multiple failures might involve only links or nodes and links (a node failure implies that its links also fail). For example, in malicious human attacks, node shutdowns are harder to realize but are the most rewarding in the attackers perspective (the shutdown of a single node is also able to shut down multiple links). Node failures are more harmful to the resilience of networks and, so, we address the topology design of transparent optical networks which must be resilient to multiple node failures.

For a given topology, if some nodes are considered critical due to some reason, the network design should take this into consideration, as in [BdSA18] where the approach proposed in [AdSD16] is adapted to the design of a transparent optical network minimizing the failure impact of a given set of critical nodes. Here, we consider the resiliency metric defined by the average 2-terminal reliability (A2TR) and, for a given network topology, we evaluate this metric against a set of critical node failures. A2TR is defined as the number of node pairs that remain connected if all critical nodes fail and the set of critical nodes is the optimal solution of a Critical Node Detection (CND) optimization problem.

CND problems have been considered in different contexts and are gaining special attention in the vulnerability evaluation of telecommunication networks to large-scale failures [GTE$^+$16]. In [ACEP09], CND is defined as the detection of a given number c of critical nodes aiming to minimize the number of connected node pairs. More recently, this and other variants of CND have also been addressed [SdSM18, SGL12, VBP14, VPP15] but none of these works addresses the CND problem in the context of transparent optical networks.

In these networks, data is converted into light in the source node and transmitted through an all optical path, named *lightpath*, towards the destination node. Due to many optical degradation factors, like attenuation, dispersion, crosstalk and other non-linear factors, there is a maximum length, named *transparent reach*, for each lightpath to work properly. Moreover, the length of a path depends both on the length of its links and on its number of hops. The optical degradation suffered by a lightpath while traversing an intermediate node is usually modelled by a given fibre length value d, i.e., by considering it equivalent to the degradation incurred due to the transmission over a given fibre of length d. So, when accounting the A2TR metric, the CND problem has to consider that two nodes are connected only if the surviving network provides it with a shortest path within the transparent reach. Here, a proper Integer Linear Programming (ILP) description of this CND problem variant is provided together with a row generation approach to compute its optimal solution.

Other metrics have been used to evaluate the vulnerability of networks in other contexts [RCM17] or assuming multiple failures with geographical correlation between failing elements [NZCM11]. There are also works on improving the preparedness of networks to multiple failures, some by changing the network topology [BGLR05, NYWF17, ZL12], while others by proposing strategies to recover from failures [DTM14, STD15]. None of these works, though, uses the optimal solution of CND to assess the vulnerability of networks. On the other hand, in [dSMS17], CND is used but resiliency improvement is exploited by optimal robust node selection on a given topology. The advantage of using CND is that it provides a worst case resiliency analysis, i.e., in any failure involving the same number of failing nodes, the resulting A2TR is never worse than the value provided by the solution of CND.

Here, we propose a multi-start greedy randomized method to generate network topologies, with a given fibre length budget, that are resilient to critical node failures. The method is also adapted to the upgrade of an existing topology. For an existing network with a total fibre length L, the first aim is to assess the resiliency gap between the existing topology and a new network topology designed to maximize its resilience with the same fibre budget L. If the existing network is to be upgraded with new links within a fibre budget L', the second aim is to assess how much the resiliency gap can be reduced between a good upgraded topology and a network topology designed to maximize its resiliency with the same fibre budget $L + L'$.

The paper is organized as follows. Section B.2 describes a path-based Mixed ILP (MILP) model defining the CND problem, a row generation approach used to solve it and centrality based heuristics combined with a local search method to approximate it. Section B.3 proposes the multi-start greedy randomized method to generate network topologies resilient to critical node failures. The computational results are presented and discussed in Section B.4. Finally, Section B.5 presents the main conclusions of this work.

B.2 Critical node detection problem

Consider a transparent optical network represented by an undirected graph $G = (N, E)$ where $N = \{1, ..., n\}$ is the set of nodes and $E \subseteq \{(i, j) \in N \times N : \ i < j\}$ is the set of fibre links. For each link $(i, j) \in E$, parameter l_{ij} represents its length.

The transparent reach of the network is denoted by parameter $T > 0$ and the fibre length equivalent to the degradation suffered by a lightpath while traversing an intermediate node is denoted by parameter $d > 0$. We assume that $l_{ij} \leq T$ for all $(i, j) \in E$; otherwise, such link is worthless and can be removed from G.

The set of all paths in G between $i \in N$ and $j \in N$ (with $i < j$ and $(i, j) \notin E$) with length not greater than T is denoted by P_{ij}. Each path $p \in P_{ij}$ is defined by the binary parameters β_k^p, indicating whether node k (which can be an end node) is in p or not, and α_{kt}^p indicating whether link $(k, t), k < t$ is in p or not. So, P_{ij} is composed by all paths p such that $\displaystyle\sum_{k=1}^{n-1} \sum_{t=k+1}^{n} \alpha_{kt}^p l_{kt} + d\big(\sum_{k=1}^{n} \beta_k^p - 2\big) \leq T$.

B.2.1 Path-based MILP model

For each node $i \in N$, we consider a binary variable v_i indicating whether i is a critical node or not. For each node pair (i, j), with $i, j \in N : i < j$, the binary variable u_{ij} is 1 if nodes i and j are connected through a path satisfying the transparent reach T, and 0 otherwise.

Then, for a given number $c \in \mathbb{N}$ of critical nodes, a path formulation for the CND problem is given by the following ILP model.

$$\min \quad z := \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} u_{ij} \tag{B.1}$$

$$s.t. \quad \sum_{i=1}^{n} v_i \leq c, \tag{B.2}$$

$$u_{ij} + v_i + v_j \geq 1, \quad (i,j) \in E, \tag{B.3}$$

$$u_{ij} + \sum_{k=1}^{n} \beta_k^p v_k \geq 1, \;\; (i,j) \notin E, \;\; p \in P_{ij}, \tag{B.4}$$

$$v_i \in \{0,1\}, \qquad i \in N, \tag{B.5}$$

$$u_{ij} \in \{0,1\}, \qquad i,j \in N: \; i < j. \tag{B.6}$$

The objective (B.1) is to minimize z defined as the total number of connected node pairs in the surviving graph (*i.e.* the graph given by removing all critical nodes from G). Constraint (B.2) ensures that at most c nodes are selected as critical nodes (in any optimal solution, c nodes are selected). Constraints (B.3) guarantee that a pair of adjacent nodes is connected if none of the two nodes is a critical node. Constraints (B.4) are the generalization of constraints (B.3) for the node pairs that are not adjacent in G: node pair (i,j) is connected if there is one path $p \in P_{ij}$ such that none of its nodes is a critical node. Constraints (B.5)-(B.6) are the variable domain constraints.

Note that, since variables v_i are binary, constrains (B.3)–(B.4) impose $u_{ij} \geq 1$ when nodes i and j are connected, which then, due to the objective function, forces $u_{ij} = 1$. Therefore, constraints (B.6) can be replaced by $u_{ij} \geq 0$. The resulting Mixed Integer Linear Programming (MILP) model will be considered henceforward.

B.2.2 Row generation approach

The exact number of constraints (B.4) of the MILP model depends on the graph topology, the link lengths and the values of T and d. However, the model becomes too large for relative small sized instances. Here, we propose a row generation approach to solve it. The exact algorithm is described in Algorithm B.1.

Initially, inequalities (B.4) are ignored and the relaxed MILP problem is solved. Then, the separation problem associated with inequalities (B.4) is solved, all violated inequalities are added to the model and the MILP is solved again. The process is repeated until no violated inequality is found.

The separation problem associated with constraints (B.4) is solved in the following way. We determine a subgraph G^C removing from G the critical nodes and the corresponding incident edges ($G^C = (N \setminus C, E^C)$) and adding d to the length of each edge in E^C. Note that the number of intermediate nodes of a path is equal to the number of edges minus one. As a consequence, the shortest path value in G^C is equal to the path length plus d. So, we determine the shortest path in G^C between all pairs of nodes i and j in $N \setminus C$, such that $(i,j) \notin E^C$, using Dijkstra algorithm, and each shortest path whose length is not higher than $T + d$ is used to generate a new inequality (B.4) that is added to the model.

Algorithm B.1 Exact algorithm for the CND problem

```
Solve the MILP model without constraints (B.4); let $(u^*, v^*)$ be the optimal solution
repeat
  Set NCuts $\leftarrow 0$ and $C \leftarrow \{i \in N : v_i^* = 1\}$
  Compute subgraph $G^C = (N \setminus C, E^C)$ where $E^C = \{(i,j) \in E : \ i,j \notin C\}$
  for all node pair $(i,j) \notin E^C$ with $i < j$ do
    Run Dijkstra algorithm (adding $d$ to the length of each edge) to find the shortest
    path $p_{ij} \in P_{ij}$ and its length $d_{ij}$
    if $d_{ij} \leq T + d$ and $u_{ij}^* + \sum_{k=1}^{n} \beta_k^{p_{ij}} v_k^* = 0$ then
      Add constraint (B.4) corresponding to path $p_{ij}$
      NCuts $\leftarrow$ NCuts $+1$
    end if
  end for
  if  NCuts $> 0$ then
    Solve MILP model with the added constraints. Update $(u^*, v^*)$
  end if
until Ncuts $= 0$
```

B.2.3 Centrality based heuristics

Heuristic methods based on centrality measures can be used to compute critical node sets because they run very quickly although not providing optimal solutions.

Algorithm B.2 presents a general heuristic framework for using these measures: in each iteration of the **For** cycle, a node is selected according to the centrality measure chosen (steps 3 and 4) and removed from the graph (step 5). These heuristics will be used later on in the network design task as a means to shorten the evaluation runtime of solutions. Preliminary tests have shown that these heuristics are worthwhile with the following centrality measures:

- Degree centrality. The central node in step 3 is the node with highest degree in the current graph G'.

- Betweenness centrality. In the current graph G', the betweenness of node i is the number of shortest paths (adding d for each intermediate node) between all nodes with length not greater than T that include node i as an intermediate node. The central node in step 3 is the node with highest betweenness.

Algorithm B.2 Iterative heuristic based on a centrality measure

```
1: Set $C \leftarrow \emptyset$ and $G' \leftarrow (N, E)$
2: for all $k = 1$ to $c$ do
3:   Select the central node $i \in N$ of graph $G'$
4:   Set $C \leftarrow C \cup \{i\}$
5:   Remove from $G'$ node $i$ and all its incident edges
6: end for
```

B.2.4 Local search approach

Note that, for a given set of nodes $C \subset N$ with $|C| = c$, we can compute in polynomial time its CND value z by determining the total number of shortest paths with length not higher than T between all node pairs in the surviving graph (i.e., the graph that results from G by removing the set of nodes C and corresponding incident edges). So, in order to potentially improve the solutions obtained with the previous heuristics, we also consider a node based local search method (described in Algorithm B.3) that evaluates each swap of a critical node by a non-critical neighbour node in G.

Algorithm B.3 Local Search Method

```
Given a critical node set $C \subset N$ with $|C| = c$ and its CND value $z$
repeat
    for all $i \in C$, $j \in N \backslash C$ : $\big(\min(i,j), \max(i,j)\big) \in E$ do
        $C_i^j \leftarrow (C \backslash \{i\}) \cup \{j\}$ and compute its CND value $z_i^j$
    end for
    if $\min\{z_i^j\} < z$ then
        Update $z \leftarrow \min\{z_i^j\}$, and $C \leftarrow C_i^j$ accordantly
    end if
until $z$ is not updated
```

B.3 Network design problem

In this section, we propose a multi-start greedy randomized algorithm to generate network topologies, with a fibre length budget given by B, that are resilient to critical node failures. In the proposed algorithm, the evaluation of each network topology uses the methods described in the previous section.

In general, a greedy randomized algorithm builds a network topology by starting with a graph with an empty set of fibre links $G = (N, \emptyset)$ and randomly selecting one link at a time until no new link can be added within the given budget B.

A key issue of this approach is how to define the probability $\mathrm{P}\big((i,j)\big)$ of each new link (i,j), with $i < j$, being selected so that the method can efficiently find good network topologies. After testing multiple strategies, the best results were obtained by guaranteeing that at least one end node of each new link is one of the lowest degree nodes of the current partial topology and by giving an higher probability to shorter links.

After fine-tuning, the best algorithm was obtained considering the probabilities as follows. First, consider that at each step the set of already selected links is E, δ_i is the degree of node i in $G = (N, E)$ and the remaining budget is $B_R = B - \sum_{(i,j)\in E} l_{ij}$. Then, for all node pairs $(i,j) \notin E$ such that $l_{ij} \leq B_R$ and at least one of the nodes (i or j) has the lowest degree in $G = (N, E)$ (i.e., $\min\{\delta_i, \delta_j\} = \min\{\delta_k : k \in N\}$), the probability is:

$$\mathrm{P}\big((i,j)\big) = \frac{1}{(|\delta_i - \delta_j| + 1)\ {l_{ij}}^2} \tag{B.7}$$

while for all other node pairs (i,j), $\mathrm{P}\big((i,j)\big) = 0$.

Nevertheless, starting from an empty set of fibre links still did not allow to reach an efficient algorithm. Instead, we have investigated different criteria to adopt an initial non-empty set E_0 of fibre links. The most efficient algorithm was obtained by using the Relative Neighbourhood Graph (RNG) [Tou80] as E_0 which is defined as follows: nodes $i, j \in N$ are connected by a link if and only if there is no other node $k \in N \backslash \{i, j\}$ such that $l_{ik} \leq l_{ij}$ and $l_{jk} \leq l_{ij}$. Our preliminary tests have shown that this graph provides a good initial balance between connectivity and amount of used fibre.

The resulting algorithm is described in Algorithm B.4. Note that this algorithm can be easily adapted to the upgrade of an existing network topology by setting E_0 in step 1 with the link set of the existing topology instead of using the RNG.

Algorithm B.4 Greedy Randomized Generation

```
1: Compute initial graph $G = (N, E_0)$
2: Set $B_R \leftarrow B - \sum_{(i,j) \in E} l_{ij}$
3: **repeat**
4:     Select a new link $(i, j)$ with probabilities given by (B.7)
5:     $E \leftarrow E \cup \{(i, j)\}$
6:     $B_R \leftarrow B_R - l_{ij}$
7: **until** $\mathrm{P}\big((i, j)\big) = 0$, for all $i, j \in N : i < j$
```

Multiple runs of Algorithm B.4 generate different topologies. So, in a multi-start greedy randomized algorithm, we run multiple times Algorithm B.4, evaluate the CND value z of each generated topology and store the topology with the highest z among all. The resulting algorithm is presented in Algorithm B.5 with a stopping criteria given by maximum runtime.

Depending on the purpose of the algorithm, the initial topology $\bar{G} = (N, \bar{E})$ is set differently in step 1. When the algorithm is used to upgrade an existing topology, the initial topology is set to $\bar{G} = (N, \emptyset)$ with its CND value $\bar{z} = 0$. When the algorithm is used to generate a topology better than a given one defined by a graph G and with a CND value z, then, $\bar{G}$ is set to G and its CND value $\bar{z}$ is set to z.

Recall that in the design of transparent optical networks, a topology is only valid if it is optically transparent, i.e., if the shortest path (adding d for each intermediate node) between each node pair is not higher than T for all node pairs. So, each topology generated in step 3 is first validated in step 4 and discarded before evaluation if it is not optically transparent. Moreover, when the initial topology $\bar{G}$ is 2-connected, we also require the solution of the algorithm to be 2-connected and discard the topologies accordingly. In the context of transparent optical networks, a topology is 2-connected if it is optically transparent for every removal of a single node.

In steps 5-19, each valid topology is evaluated saving as best topology the solution with the highest CND value $\bar{z}$. Note that the most time consuming part of Algorithm B.5 is the evaluation. The rationale of this algorithm is to use the heuristics described in the previous section to evaluate each generated topology and discard it whenever its objective value is lower than the current best solution $\bar{z}$. As a consequence, the exact method to detect the critical nodes only runs if none of the heuristics discard the topology under evaluation. Moreover, they are run from the fastest (Degree centrality), in terms of runtime, to the most time consuming (Exact CND method).

Algorithm B.5 Multi-Start Greedy Randomized Algorithm

```
Initialize $\bar{G} = (N, \bar{E})$ and its CND value $\bar{z}$
repeat
  Generate a new graph $G = (N, E)$ using Algorithm B.4.
  if $G$ is a valid topology then
    Run Algorithm B.2, using Degree centrality
    Compute CND value $z_{Deg}$ from that node set
    if $z_{Deg} \geq \bar{z}$ then
      Run Algorithm B.2, using Betweenness centrality
      Compute CND value $z_{Bet}$ from that node set
      if $z_{Bet} \geq \bar{z}$ then
        Run Algorithm B.3, using node set corresponding to $\min\{z_{Deg}, z_{Bet}\}$, and compute $z_{LS}$
        if $z_{LS} \geq \bar{z}$ then
          Run Algorithm B.1, obtaining $z_{MILP}$
          if $z_{MILP} \geq \bar{z}$ then
            $\bar{G} \leftarrow G$ and $\bar{z} \leftarrow z_{MILP}$
          end if
        end if
      end if
    end if
  end if
until maximum runtime reached
```

B.4 Computational results

All computational results were obtained using the optimization software *Gurobi Optimizer* version 7.5.1, with programming language *Julia* version 0.6.0, running on a PC with an Intel Core i7, 2.3 GHz and 6 GB RAM. Following [RKD$^+$13], we have assumed a transparent reach $T = 2000$ km corresponding to the use of OTU-4 lightpaths with a demand capacity of 100 Gbps. Moreover, we have considered $d = 60$ km.

The network topologies selected in our computational experiments are all optically transparent for $T = 2000$ km and are: Germany50 [OWPT10], PalmettoNet [KNF$^+$11] and Missouri Network Alliance (MissouriNA) [KNF$^+$11]. Table B.1 presents their topology characteristics in terms of number of nodes $|N|$ and fibre links $|E|$, total number of node pairs, minimum ($\delta_{\min}$), average ($\bar{\delta}$) and maximum ($\delta_{\max}$) node degree and an indication (in column '2-C') if the topology is (or is not) 2-connected.

Table B.1: Topology characteristics of each network.

Network	$\|N\|$	$\|E\|$	Pairs	$\delta_{\min}$	$\bar{\delta}$	$\delta_{\max}$	2-C
Germany50	50	88	1225	2	3.52	5	Yes
PalmettoNet	45	64	990	1	2.84	5	No
MissouriNA	64	80	2016	1	2.50	5	No

In all cases, the geographical location of nodes is publicly available but the geographical routes of fibre links is not known. So, we have considered that each link follows the shortest path over the surface of a sphere representing Earth. Table B.2 presents the resulting length characteristics in terms of minimum ($l_{\min}$), average ($\bar{l}$), maximum ($l_{\max}$) and total (L) link length, and diameter, i.e., the highest length among the shortest paths (adding d for each intermediate node) of all node pairs (all topologies are optically transparent for $T = 2000$ km since all diameter values are below 2000).

Table B.2: Length characteristics (in km) of each network.

Network	$l_{\min}$	$\bar{l}$	$l_{\max}$	L	Diameter
Germany50	26	100.7	252	8859	1417
PalmettoNet	19	67.0	177	4286	1298
MissouriNA	7	50.0	307	4001	1301

In the computational experiments, we have considered $c \in \{2, 3, 4, 5, 6\}$ as the number of critical nodes used to compute the resiliency metric z of each topology. For each network and each c, we started by computing (with Algorithm B.5) a topology with a fibre budget B equal to the total fibre length L of the original topology. Then, we computed an upgraded topology for each original topology assuming a fibre budget $L' = p \times L$ with $p = 10\%$ and 20%. Finally, we computed a topology with a fibre budget $B = L + p \times L$ also for $p = 10\%$ and 20%. In each case, we gave a runtime limit of 5 hours to Algorithm B.5.

Table B.3 presents the resiliency value z of the best topologies obtained by the multi-start greedy randomized algorithm. Rows 'Original' refer to the original topologies (in column '0%') and upgraded topologies (in columns '10%' and '20%') while rows 'Generated' refer to the best topology solutions with a fibre budget $B = L + p \times L$ with $p = 0\%$, 10% and 20%. For each case, columns 'UB' presents the trivial upper bound of z given by the number of pairs of $|N| - c$ surviving nodes.

Table B.3: Resiliency value z of all cases obtained by the multi-start greedy randomized algorithm.

c	Network	Germany50				PalmettoNet				MissouriNA			
	Instance	0%	10%	20%	UB	0%	10%	20%	UB	0%	10%	20%	UB
2	Original	1036	1081	1128	1128	513	821	861	903	946	1555	1659	1891
	Generated	1128	1128	1128		861	861	861		1714	1714	1771	
3	Original	711	991	1035	1081	346	616	709	861	602	1362	1446	1830
	Generated	991	991	1035		676	709	744		1495	1500	1550	
4	Original	640	830	906	1035	284	427	510	820	455	762	1039	1770
	Generated	867	906	906		510	582	582		1126	1194	1311	
5	Original	496	640	756	990	176	325	380	780	338	618	758	1711
	Generated	666	756	790		379	409	480		841	917	1081	
6	Original	415	498	606	946	123	235	286	741	253	457	550	1653
	Generated	543	606	658		266	322	358		694	717	784	

The first observation of these results is that the resiliency values are lower for higher number of critical nodes c, which is without surprise since more node failures disrupt an higher percentage of the network. Moreover, the resilience of the upgraded topologies is always significantly better for higher budget value L'. Finally, the best topologies are always significantly better than the original/upgraded ones for PalmettoNet and MissouriNA. Nevertheless, this is not the case for Germany50 where the difference between the two types of solutions is already small for higher values of c and even null for many cases of the lower values of c. So, one major conclusion is that Germany50 is significantly more resilient to critical node failures than PalmettoNet and MissouriNA. To understand this fact, recall from the topology characteristics of the different networks (Table B.1) that Germany50 is the topology with the highest average node degree and the only one which is 2-connected. These two characteristics make this network more resilient than the two other networks.

More important then analysing the absolute resiliency values z, we need to analyse the resiliency gap between the original/upgraded topologies and the best topologies computed with the same fibre budget values. Figure B.1 plots in a bar chart these gaps, for all networks and all values of c, computed as $\frac{z_B - z_{O/U}}{z_B}$ where z_B is the resiliency value of the best topology and $z_{O/U}$ is the resiliency value of the original/upgraded topology. Blue bars present the resiliency gap between the best topology and the original topology. The resiliency gaps between the best topologies and the upgraded topologies are presented in the purple and green bars for $p = 10\%$ and 20%, respectively.

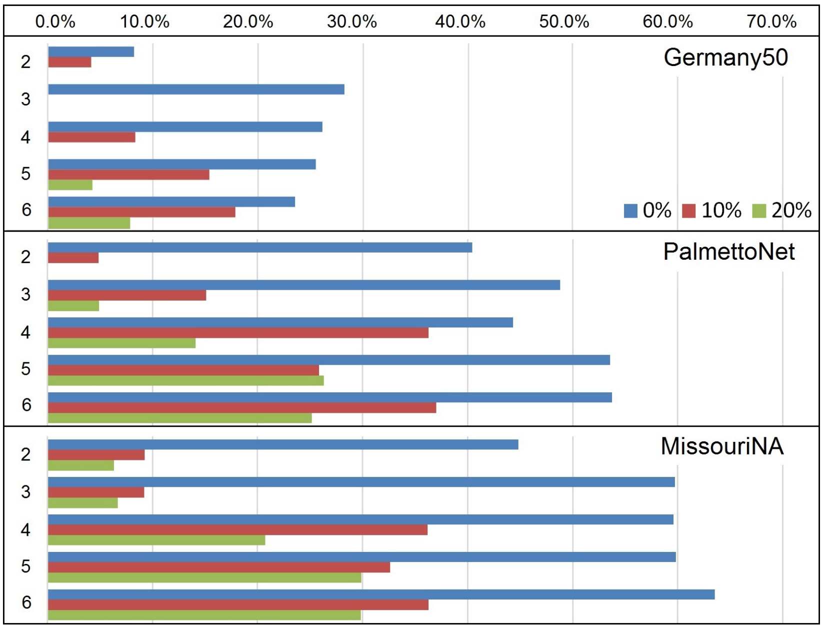


Figure B.1: Resiliency gaps $\frac{z_B - z_{O/U}}{z_B}$(%) of all cases.

The blue bars of Figure B.1 show that the resiliency gaps are lower for Germany50 (but still significant for a number of critical nodes $c \geq 3$) and very large for PalmettoNet and MissouriNA. These results reinforce the previous conclusion that Germany50 is more resilient than the others but also show that, in all cases, existing network topologies are not resilient to critical node failures. On the other hand, the resiliency gaps shown in the purple bars (corresponding to topology designs with 10% more total fibre length) represent, in all cases, a significant gap reduction when compared with the blue bars. This means that in all topologies and for all considered number of critical nodes, adding new links to an existing topology with a fibre budget of 10% enables solutions whose resiliency to critical node failures becomes closer to a topology designed to maximize this resilience. Interestingly, the results of the green bars (corresponding to topology designs with 20% more total fibre length) are mixed, i.e., in some cases, the additional 10% fibre budget enables a significant gap reduction while in other cases, the reduction is negligible.

Finally, we can distinguish two groups of results. For a number of critical nodes $c \leq 3$, the additional fibre budget of 20% makes in all networks the resiliency gap to become very small. For a number of critical nodes $c \geq 4$, and in the less resilient PalmettoNet and MissouriNA networks, the additional fibre budget of 20% is still not enough to make the resiliency gap small. This means that more fibre links are required in the upgrade of existing networks to reach the best resiliency to higher number of critical nodes.

Table B.4 presents, for each tested instance, the percentage of the total fibre length L of the original topology that is common to the best topology computed with the same fibre budget L. These results show that these percentage values are around 50%, with some small differences, for all topologies and all values of c, showing that the best topologies, in terms of resiliency to multiple node failures, are significantly different from the existing ones.

Table B.4: Percentage of the total fibre length of the original topology common to the best topology.

c	Germany50	PalmettoNet	MissouriNA
2	43.6%	52.6%	47.1%
3	49.1%	52.1%	50.2%
4	45.8%	52.7%	49.5%
5	43.5%	51.1%	47.1%
6	46.3%	51.3%	48.0%
Average	45.7%	52.0%	48.4%

For illustrative purposes, Figure B.2 presents the original topologies and the best topologies with the same fibre budget L obtained for $c = 3$ critical nodes. To understand the differences, links of the best topology not in the original topology are highlighted in dashed blue and, in both cases, critical nodes are represented with red squares. Also, Figure B.3 presents the best upgraded solutions with $L' = 10\%L$ and $20\%L$ obtained also for $c = 3$ with the additional links highlighted in dashed blue (again, critical nodes represented with red squares). The analysis of these topologies show that:

Germany50: The critical node set splits the original network in two components (10 and 37 nodes each) while it only isolates two nodes from the others in the best topology. Moreover, the critical node set isolates 2 nodes from the others in the 10% upgraded topology and a single node in the 20% upgraded topology.

PalmettoNet: The critical node set splits the original network in three components (6, 13 and 23 nodes each) while it splits the best topology in only two components (5 and 37 nodes each). Moreover, the critical node set splits the 10% upgraded topology in two components (7 and 35 nodes) and the 20% upgraded topology in two components (4 and 38 nodes). In this case, both the best topology and the two upgraded topologies are 2-connected.

MissouriNA: The critical node set splits the original network in three components (17, 20

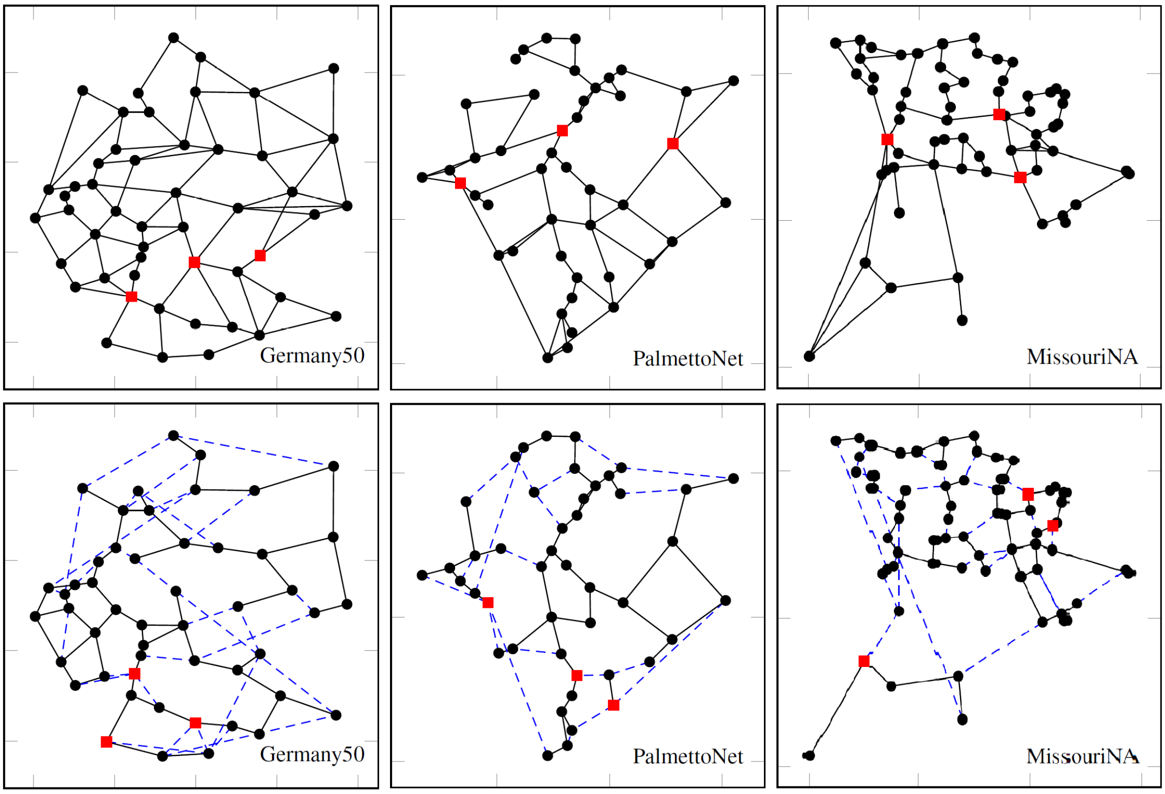


Figure B.2: Original topologies (top) and best topologies (bottom) for $c = 3$. Links not in the original topology highlighted in dashed blue in the best topology (critical nodes in red squares).

and 24 nodes each) while it splits the best topology in three components (1, 5 and 55 nodes each). Moreover, the critical node set splits the 10% upgraded topology in two components (9 and 52 nodes) and the 20% upgraded topology in two components (6 and 55 nodes). In this case, the 20% upgraded topology is 2-connected but neither the best topology nor the 10% upgraded topology are, showing that the original MissouriNA is much less connected and, therefore, requires more fibre length upgrades to become 2-connected.

This analysis clearly highlights that the best topologies with the same total fibre of existing ones are much more resilient to critical node failures and the resiliency of existing topologies can be improved with the addition of new links.

Another aspect of interest is the comparison of the node degree distributions between the original topologies and the best topologies with the same total fibre. Figure B.4 shows these distributions for the three network cases with the best topologies obtained for $c = 3$ critical nodes (original topologies in black and best topologies in blue). Interestingly, in the best topologies, there is a decrease of the number of nodes with the lowest and highest degrees and an increase of the number of nodes with degrees closer to the average. This observation also stands in the best topologies for the other values of c showing that resilient topologies tend to have more homogeneous node degrees.

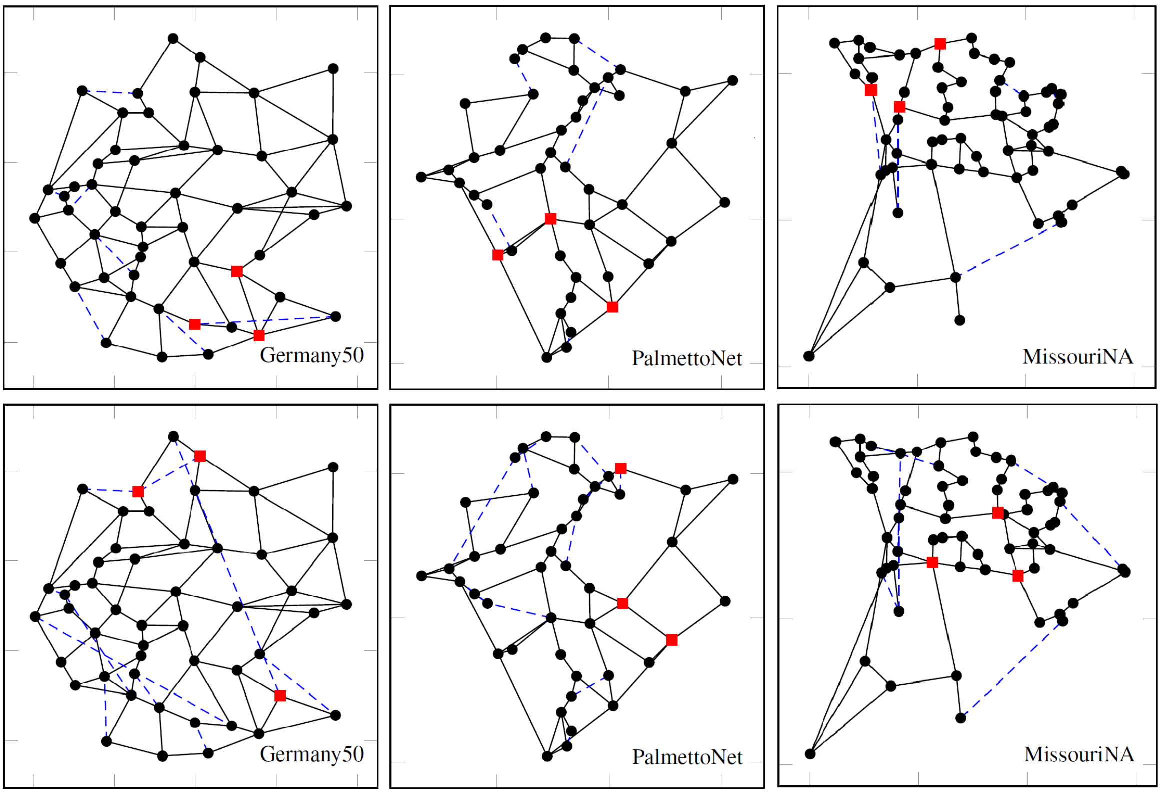


Figure B.3: Best upgraded topologies with $L' = 10\%L$ (top) and $20\%L$ (bottom) for $c = 3$. Links added to the original topologies highlighted in dashed blue (critical nodes in red squares).

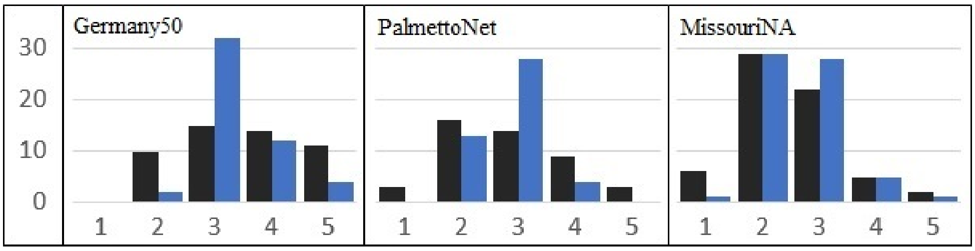


Figure B.4: Node degree histograms of original topology (in black) and the best topology (in blue) for $c = 3$.

Finally, recall that Algorithm B.5 (see Section B.3) uses heuristics in the evaluation of the CND value z of each valid topology as a means to minimize the number of times the exact method is used. In order to evaluate the efficiency of this strategy, Table B.5 presents the average percentage of valid solutions that were discarded by the heuristics, row ’Success (%)’, and the average runtime percentage the algorithm has spent while running the heuristics, row ’Success (%)’, among all cases of each network topology and also among all cases of all topologies (column ’Average’).

The results of Table B.5 show that both percentage values vary significantly between the

Table B.5: Average percentage of discarded solutions and average runtime percentage of the heuristics running Algorithm B.5.

	Germany50	PalmettoNet	MissouriNA	Average
Success (%)	36.8	71.8	65.0	57.9
Time (%)	19.2	57.7	51.0	42.6

different network topologies. Nevertheless, in all cases, the percentage of discarded solutions is always higher than the percentage of runtime spent by the heuristics. In the overall, almost 60% of the solutions were discarded at the cost of 42,6% of computational effort, showing that indeed the use of heuristics has improved the overall computational efficiency of the proposed multi-start greedy randomized algorithm.

B.5 Conclusions

In this work, we have addressed the topology design of transparent optical networks aiming to maximize their resilience against critical node failures. We have proposed a multi-start greedy randomized algorithm resorting to a MILP based method, using row generation, to compute the critical nodes of each topology. The algorithm can be used both in the design of network topologies and in the upgrade of existing topologies.

We have run the proposed algorithm on three network topologies with publicly available information comparing the resiliency gap between the existing/upgraded topologies with the best topologies designed to maximize its resilience with the same fibre budget.

The results have shown that the resiliency gap of existing topologies is significantly large but network upgrades with $L' = 10\%L$ can already reduce significantly the resiliency gaps provided that such upgrades are aimed at maximizing the network resiliency to multiple node failures.

Finally, comparing the best topologies with the existing ones, the best topologies are characterised by a decrease of the number of nodes with the lowest and highest degrees and an increase of the number of nodes with degrees closer to the average node degree. This clearly shows that network topologies resilient to critical node failures tend to have more homogeneous degrees among all their nodes.

Bibliography

[ACEP09] A. Arulselvan, C. Commander, L. Elefteriadou, and P. Pardalos. *Detecting critical nodes in sparse graphs.* Computers & Operations Research, 36(7):2193–2200, 2009.

[AdSD16] A. Agra, A. de Sousa, and M. Doostmohammadi. *The minimum cost design of transparent optical networks combining grooming, routing, and wavelength assignment.* IEEE/ACM Transactions on Networking, 24(6):3702–3713, 2016.

[BdSA18] F. Barbosa, A. de Sousa, and A. Agra. *The design of transparent optical networks minimizing the impact of critical nodes.* Electronic Notes in Discrete Mathematics, 64:165–174, 2018.

[BGLR05] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish. *Improving network robustness by edge modification.* Physica A: Statistical Mechanics and its Applications, 357(3-4):593–612, 2005.

[dSMS17] A. de Sousa, D. Mehta, and D. Santos. *The robust node selection problem aiming to minimize the connectivity impact of any set of p node failures.* In 13th International Conference on Design of Reliable Communication Networks (DRCN), pages 138–145, 2017.

[DTM14] F. Dikbiyik, M. Tornatore, and B. Mukherjee. *Minimizing the risk from disaster failures in optical backbone networks.* Journal of Lightwave Technology, 32(18):3175–3183, 2014.

[FWG$^+$16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GTE$^+$16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[KNF$^+$11] S. Knight, H. Nguyen, N. Falkner, R. Bowden, and M. Roughan. *The internet topology zoo.* IEEE Journal on Selected Areas in Communications, 29(9):1765–1775, 2011.

[NYWF17] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek. *Link addition framework for optical CDNs robust to targeted link cut attacks.* In 9th International Workshop on Resilient Networks Design and Modeling (RNDM). IEEE, 2017.

[NZCM11] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano. *Assessing the vulnerability of the fiber infrastructure to disasters.* IEEE/ACM Transactions on Networking, 19(6):1610–1623, 2011.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[RCM17] D. Rueda, E. Calle, and J. Marzo. *Robustness comparison of 15 real telecommunication networks: structural and centrality measurements.* Journal of Network and Systems Management, 25(2):269–289, 2017.

[RHC$^+$16] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska. *RECODIS: Resilient communication services protecting end-user applications from disaster-based failures.* In 18th International Conference on Transparent Optical Networks (ICTON). IEEE, 2016.

[RKD$^+$13] F. Rambach, B. Konrad, L. Dembeck, U. Gebhard, M. Gunkel, M. Quagliotti, L. Serra, and V. López. *A multilayer cost model for metro/core networks.* Journal of Optical Communications and Networking, 5(3):210–225, 2013.

[SdSM18] D. Santos, A. de Sousa, and P. Monteiro. *Compact models for critical node detection in telecommunication networks.* Electronic Notes in Discrete Mathematics, 64:325–334, 2018.

[SGL12] M. Di Summa, A. Grosso, and M. Locatelli. *Branch and cut algorithms for detecting critical nodes in undirected graphs.* Computational Optimization and Applications, 53(3):649–680, 2012.

[STD15] K. Sabeh, M. Tornatore, and F. Dikbiyik. *Progressive network recovery in optical core networks.* In 7th International Workshop on Reliable Networks Design and Modeling (RNDM), pages 106–111. IEEE, 2015.

[Tou80] G. Toussaint. *The relative neighbourhood graph of a finite planar set.* Pattern Recognition, 12(4):261–268, 1980.

[VBP14] A. Veremyev, V. Boginski, and E. Pasiliao. *Exact identification of critical nodes in sparse networks via new compact formulations.* Optimization Letters, 8(4):1245–1259, 2014.

[VPP15] A. Veremyev, O. Prokopyev, and E. Pasiliao. *Critical nodes for distance-based connectivity and related problems in graphs.* Networks, 66(3):170–195, 2015.

[ZL12] A. Zeng and W. Liu. *Enhancing network robustness against malicious attacks.* Physical Review E, 85((6 Pt 2):066130), 2012.

Appendix C: Evaluation and Design of Elastic Optical Networks Resilient to Multiple Node Failures

Abstract: Consider an existing Elastic Optical Network (EON) with a given topology composed by nodes and connecting fibers, each fiber with a given spectrum capacity. Consider an estimated set of demands to be supported and a routing, modulation and spectrum assignment (RMSA) policy adopted by the operator both for the regular state and for the failure states. First, we address the resilience evaluation of the EON to multiple node failures. We adopt a worst-case approach by identifying the nodes (named critical nodes) whose simultaneous failure maximally reduce the demand percentage that is supported by the network and we use this percentage as the resilience metric. Then, for the same estimated demands, the same RMSA policy and a fiber budget equal to the total fiber length of the existing network, we address the design problem aiming to determine a new EON maximizing the resilience metric imposed by its critical nodes. We use a multi-start greedy randomized method that generates multiple EONs and returns the best one, i.e., the EON with the highest resilience metric. We run the evaluation and design methods on known network topologies. The computational results let us (i) analyze the efficiency of the methods and (ii) assess how far the resilience of existing networks are from the best ones.

Keywords: Elastic Optical Networks; Transparent Optical Networks; Critical Node Detection; Resilient Network Design; Disasters

F. Barbosa, A. de Sousa, and A. Agra. *Evaluation and design of elastic optical networks resilient to multiple node failures.* In 15th International Conference on the Design of Reliable Communication Networks (DRCN), pages 154–161, 2019.

C.1 Introduction

Large-scale failures are becoming more frequent in time and wider in scope severely disrupting telecommunication networks and services [RHC$^+$16]. So, both the impact evaluation of large-scale failures on existing networks and the design of networks more resilient to large-scale failures are becoming key issues (two surveys addressing these issues are [GTE$^+$16] on strategies to protect networks against large-scale natural disasters and [FWG$^+$16] on security challenges in communication networks).

Large-scale failures might involve only network links or network nodes and links (a node failure implies that its links fail). For example, in malicious human attacks, node shutdowns are harder to realize than link cuts but are the most rewarding in the attacker's perspective (a node shutdown also shuts down multiple links). Moreover, power outages shut down nodes since fiber links do not require power supply. Here, we consider as large-scale failures the case of multiple node failures as they are the most harmful.

In EONs, the optical spectrum of each fiber link is organized in frequency slots (FSs). Each demand between a pair of nodes is routed over an end-to-end *lightpath* (we assume a transparent optical network). On each direction of a lightpath, data is converted in the source from electrical to optical domain using a modulation format (MF) emitting on a set of contiguous FSs, transmitted through a routing path over the optical network and converted back to electrical domain in the target node. At the network level, multiple lightpaths can be set up if their FSs do not overlap on any fiber link.

Due to many factors, there is a maximum length, named *transparent reach*, for the routing path of a lightpath. Also, the MF of a lightpath impacts both its transparent reach and its number of FSs. For example, in a single carrier lightpath, a 16-QAM MF carries twice the number of bits/symbol of the QPSK MF but imposes a shorter transparent reach. So, in a shorter routing path, the same line rate (in bits/second) can be transmitted by 16-QAM instead of QPSK with a half symbol rate which occupies less FSs [JKT$^+$10]. Moreover, OFDM enables each lightpath to be composed by a bunch of sub-carriers, which can be partially overlapping in the spectrum domain reaching spectrum gains [CSO15, WCP11]. In this case, multiple sub-carriers with uniform symbol rate and bits/symbol can be selected for a required line rate so that the transparent reach of the lightpath is enough to the length of its routing path [JKT$^+$10].

So, for a required demand line rate, a more spectrum efficient MF configuration is one that requires a smaller number of FSs but imposes a shorter transparent reach (the main principle behind the distance-adaptive spectrum allocation strategies [JKT$^+$10, TR17]). When the MF of each required lightpath is fixed, the decision on the routing path and FSs of each lightpath is known as the routing and spectrum assignment (RSA) problem. When multiple MFs are available, the assignment problem includes the selection of the MF configuration to each lightpath, which is known as the routing, modulation and spectrum assignment (RMSA) problem and has been addressed in many works and different contexts [AFM$^+$18, AR17, CSO15, CTV11, GWK15, GZLZ12, JKT$^+$10, KW11, TR17, WCP11, YZZY13, ZWA15].

The failure of multiple nodes on an EON has three different impact factors. First, all demands with one end node which is a failure node are lost. Second, if the failure nodes disconnect the network into different components, all demands with end nodes in different components are also lost. Third, a demand whose routing path of its lightpath contains at least one failure node, if the demand is in the same network component, it might be reassigned with a different lightpath. Then, its reassignment might require a different MF in a longer routing path which, in turn, might require more FSs in more links. So, the network might not have enough spectrum resources to reassign lightpaths to all such demands.

Consider an existing EON with a given topology composed by nodes and connecting fibers, each fiber with a given capacity in number of FSs. Consider an estimated demand set and a RMSA policy adopted by the operator both for the regular and for the failure states. First, we address the resilience evaluation of the EON to multiple node failures. If the critical nodes are given, the RMSA can maximize the total demand still supported when all critical nodes fail, as in [BdSA18a] where the approach in [AdSD16] is adapted to such case. Here, the critical nodes are not given. Instead, our resilience evaluation adopts a worst-case approach by identifying the critical nodes as the set of nodes whose simultaneous failure maximally reduce the demand percentage that is still supported. So, the critical nodes are the result of an optimization problem and the obtained demand percentage is used as the resilience metric. Then, for the same set of estimated demands, the same RMSA policy and a fiber budget equal to the total fiber length of an existing EON, we address the design problem aiming to determine a new EON maximizing the resilience metric imposed by its critical nodes.

Critical Node Detection (in short, CND) problems have been considered in different contexts [ACEP09, SdSM18, SGL12, VBP14] and are gaining special attention in the vulnerability evaluation of telecommunication networks to large-scale failures [GTE$^+$16]. Other metrics have been used to evaluate the network vulnerability in other contexts [RCM17] or assuming multiple geographical correlated failures [NZCM11]. There are also works on improving the preparedness of networks to multiple failures, some by changing the network topology [BGLR05, NYWF17, ZL12], while others by proposing strategies to recover from failures [DTM14, STD15]. CND is used in [dSMS17] as a resilience metric in the optimal robust node selection problem. Both the evaluation and network design of optical networks resilient to multiple node failures were addressed in [BdSA18b]. In that work, though, the RMSA is not considered as spectrum capacity of links is assumed to be infinite, i.e., the third impact factor is ignored in the resilience evaluation.

The paper is organized as follows. Section C.2 describes the RMSA policy considered both for the regular and for the failure states. Section C.3 presents the resilience evaluation method while Section C.4 presents the EON design method. The computational results are discussed in Section C.5. Finally, Section C.6 draws the main conclusions of the work.

C.2 Routing, modulation and spectrum assignment

For a given EON and a given set of demands, the RMSA policy rules the way lightpaths are assigned both in the regular state and in any failure state. Here, we adapt the proposal in [KW11] to both cases. Consider the EON topology represented by an undirected graph $G = (N, E)$ with a set of nodes $N = \{1, ..., |N|\}$ and a set of links $E \subseteq \{(i, j) \in N{\times}N : i < j\}$ whose lengths are represented as l_{ij}. Set $F = \{1, 2, ..., |F|\}$ is the ordered set of FSs available on each fiber link.

Set D is the estimated set of demands. Each $d \in D$ is defined by its source node s_d

and target node t_d, $s_d < t_d$ (multiple demands between the same end nodes can exist and we let their supporting lightpaths to have different routing paths). Here, we assume a single line rate optical network (i.e., all demands require the same line rate in bits/second) but its generalization to multiple line rates is straightforward.

To model the RMSA solution, we need two additional sets. Set M is the set of MF configurations for the considered line rate. Each $m \in M$ is defined by its number of contiguous FSs n_m (this value includes the required guard band between lightpaths) and its transparent reach T_m. Set P_d is the set of lightpath candidate paths to demand $d \in D$. The optical length of path $p \in P_d$ is the sum of its link lengths plus a length value Δ per intermediate node (which models the optical degradation suffered by a lightpath while traversing an intermediate optical switch). Each path $p \in P_d$ is defined by:

- the binary parameters β_k^p which are equal to 1 if node k (which can be an end node) is in p or equal to 0 otherwise;
- the binary parameters α_{ij}^p which are equal to 1 if link $(i, j), i < j$ is in p or equal to 0 otherwise;
- the integer parameter n_p indicating the number of FSs of the most efficient MF configuration whose transparent reach is not smaller than the optical length of p.

In [KW11], each demand has a fixed required number of FSs. In our case, the required number of FSs is n_p which depends on the candidate path $p \in P_d$. We associate to each $d \in D$ the parameter n_d which gives the minimum number of FSs required by any of its candidate paths $p \in P_d$, i.e., $n_d = \min_{p \in P_d} n_p$. Consider set P_e as the set of all candidate paths of all demands that include link $e \in E$. Similar to [KW11], a collision metric c_e is computed for each link $e \in E$ given by $c_e = \sum_{d \in D} \sum_{p \in (P_d \cap P_e)} n_p$. Then, each candidate path $p \in \cup_{d \in D} P_d$ has an associated path length $l_p = \sum_{e \in P} c_e$ used to break ties when selecting candidate paths. All l_p values are precomputed and used as parameters in the RMSA.

The RMSA policy for the regular state is given by Algorithm C.1, a greedy algorithm that starts with an empty network (i.e., all FSs are free in all links) and assigns iteratively to a demand $d \in D$, a lightpath $p \in P_d$ and a set of n_p contiguous FSs. Each assignment is the one that packs as much as possible the lightpaths in the lowest spectrum. Algorithm C.1 starts by computing the maximum value n among the n_d values of all demands (Step 1) and initializes set $\bar{D}$ with all demands such that $n_d = n$ (Step 3). Then, for each candidate path p of each demand in $\bar{D}$ (Step 6), the algorithm computes the lowest set of n_p contiguous FSs that can be assigned without overlap with previous assignments. The algorithm selects the candidate path whose highest selected FS index is the lowest among all and, as a tiebreaker, the one with the shorter path length l_p (Steps 8 and 9). The selected path and associated set of FSs is used to assign the lightpath to the corresponding demand (Step 12) and the demand is removed from set $\bar{D}$ (Step 13). When $\bar{D}$ becomes empty, n is decreased and the algorithm continues until n reaches 0.

A key issue in the RMSA is the set of candidate paths P_d to consider for each demand $d \in D$. In [KW11], a k-shortest path algorithm is used with $k = 3$. Our tests have shown that a value of $k = 7$ is required but not necessarily to all demands. The best strategy is to consider for each demand d a number of candidate paths equal to the minimum between 7 and the number of nodes in the shortest path from s_d to t_d plus one.

Algorithm C.1 RMSA

```
Initialize $n \leftarrow \max_{d \in D} n_d$
while $n \geq 1$ do
    $\bar{D} \leftarrow \{d \in D : n_d = n\}$
    while $\bar{D} \neq \emptyset$ do
        $\bar{f} \leftarrow \infty$, $\bar{l} \leftarrow \infty$, $\bar{d} \leftarrow \{\}$ and $\bar{p} \leftarrow \{\}$
        for all $p \in P_d$, $d \in \bar{D}$ do
            $f \leftarrow$ highest FS index of the lowest set of $n_p$ contiguous FSs that can be assigned
              on $p$ to $d$ without overlap with previous assignments
            if $f < \bar{f}$ or ($f = \bar{f}$ and $l_p < \bar{l}$) then
                $\bar{f} \leftarrow f$, $\bar{l} \leftarrow l_p$, $\bar{p} \leftarrow p$ and $\bar{d} \leftarrow d$
            end if
        end for
        Assign to demand $\bar{d}$ a lightpath on the candidate path $\bar{p}$ and on the FSs from $\bar{f}-n_{\bar{p}}+1$
          to $\bar{f}$
        $\bar{D} \leftarrow \bar{D} \backslash \bar{d}$
    end while
    $n \leftarrow n - 1$
end while
```

While the RMSA policy in the regular state is defined by Algorithm C.1, in a failure state a slightly different variant is used. Lightpaths not disrupted by any failure node are not changed. So, the algorithm considers the surviving network (i.e., without the failure nodes and incident links) with the FSs occupied by the non disrupted lightpaths. For the disrupted demands whose end nodes are in the same component, a new set of candidate paths and associated path lengths is computed. Then, the RMSA is similar to Algorithm C.1 but considers the demands d in increasing order of their n_d values (as opposed to the decreasing order of Algorithm C.1). Since the aim is to reassign as much as possible the disrupted lightpaths, our tests have shown that the increasing order is better, on average, since the lightpaths requiring less number of FSs can better fit in the initial fragmented spectrum.

C.3 Resilience evaluation problem

The EON resilience to multiple node failures measures their impact in the network capacity to support the estimated demands. For a given number $c \in \mathbb{N}$ of failure nodes, we adopt a worst-case approach by identifying a set of c critical nodes whose simultaneous failure maximally reduce the demand percentage that is supported.

For a given EON and a given set of lightpaths (assigned by the RMSA policy to a given set of demands), the determination of the critical nodes is a min-max bi-level optimization problem: at the bottom level, the RMSA policy aims to maximize the demand percentage that is supported by a given set of node failures; at the top level, the set of node failures aims to minimize the demand percentage that the RMSA policy is able to support. We solve the problem heuristically by computing 2 sets of failure nodes, running the RMSA policy for each set and selecting the most damaging set as the critical node set.

The first set of failure nodes is computed by solving the weighted version of the Critical Node Detection (CND) problem shown to be efficiently solved by mixed integer linear programming [SdSM18]. To compute the second set of failure nodes, we propose a *Node Demand Centrality* (NDC) metric and use it in a greedy approach to iteratively select the failure nodes. Next, we describe separately each of the two methods.

CND based method. For each node $i \in N$, consider a binary variable v_i indicating whether i is a critical node or not. For each node pair (i, j), with $i < j$, consider: (i) a weight w_{ij} given by the sum of all demands $d \in D$ whose end nodes are i and j, (ii) a set N_{ij} which is the set of adjacent nodes to i (on graph G) if the degree of node i is not higher than the degree of node j, or the set of adjacent nodes to j otherwise, and (iii) a binary variable u_{ij} which is 1 if nodes i and j are connected or 0 otherwise. For a given number c of critical nodes, the CND problem is defined as:

$$min \quad \sum_{i,j \in N: i<j} w_{ij} u_{ij} \tag{C.1}$$

$$s.t. \quad \sum_{i=1}^{n} v_i \leq c \ , \tag{C.2}$$

$$u_{ij} + v_i + v_j \geq 1 \ , \qquad (i,j) \in E, \tag{C.3}$$

$$u_{ij} \geq u_{ik} + u_{jk} - 1 + v_k, \ (i,j) \notin E, \ k \in N_{ij}, \tag{C.4}$$

$$v_i \in \{0,1\} \ , \qquad i \in N, \tag{C.5}$$

$$u_{ij} \in \{0,1\} \ , \qquad i,j \in N : i < j. \tag{C.6}$$

The objective (C.1) is to minimize the total weighted connectivity, i.e., the sum of the weights of the node pairs that remain connected when the critical nodes are removed. Constraint (C.2) ensures that at most c nodes are selected as critical nodes (in optimal solutions, c nodes are selected). Constraints (C.3) guarantee that a pair of adjacent nodes is connected if none of the two nodes is a critical node. Constraints (C.4) are an efficient generalization of constraints (C.3) for the node pairs that are not adjacent in G: node pair (i, j) is connected if there is a non-critical node $k \in N_{ij}$ such that k is connected to both i and j. Constraints (C.5-C.6) are the variable domain constraints. As noted in [SdSM18], constraints (C.6) can be replaced by $u_{ij} \geq 0$, reducing the number of binary variables.

The set of failure nodes is computed by determining an optimal solution of this model using an available ILP solver. Note that such solution is an heuristic solution for our problem since it does not take into account neither the transparent reach of lightpaths nor the spectrum capacity of fiber links.

NDC (Node Demand Centrality) based method. The proposed demand centrality of each node $k \in N$ aims to measure the impact of the node failure on the demands between all other node pairs. Let us denote as p_d the lightpath $p \in P_d$ assigned to a demand $d \in D$. The resources used by each lightpath p_d, denoted as S_d, are given by its number of FSs times the number of hops of its routing path, i.e., $S_d = n_d \times \sum_{(i,j) \in E} \alpha_{ij}^p$. Then, the node failure impact is measured as a combination of two quantities: (i) Q_1 with the total demand that can no longer be supported and (ii) Q_2 with the minimum resources increase required to reassign new lightpaths to demands that can be connected.

So, for each node $k \in N$ and for each lightpath assigned to a demand d between a pair of other nodes whose routing path includes k, we compute the candidate path $p'_d \in P_d$ that does not include k and requires the least amount of resources S'_d. If such candidate path does not exist, demand d is added to Q_1. If it exists and $S'_d > S_d$, the value $\frac{S'_d - S_d}{S_d}$ is added to Q_2, or otherwise the demand is ignored. At the end, the demand centrality r_k of node k is $r_k = (Z \times Q_1) + Q_2$. The factor Z defines the relative weight between the two quantities. Based on preliminary tests, the best results are obtained when Z is either the highest value of $\frac{S'_d - S_d}{S_d}$, if any of such values was added to Q_2, or is 1 otherwise.

The set of failure nodes C is determined with a greedy algorithm, presented in Algorithm C.2, which uses the demand centrality value of each node to select the failure nodes. The algorithm starts with graph G (representing the EON network) and set D (of all demands with lightpaths assigned by the RMSA policy) in Line 1. On each cycle, the algorithm (i) computes the demand centrality r_k of each node k (Lines 4–23), (ii) computes the node $\bar{k}$ with the highest demand centrality (Line 24), (iii) selects node $\bar{k}$ as a failure node (Line 25), (iv) the demands routed through node $\bar{k}$ are removed from D (Line 26) and (v) node $\bar{k}$ and its incident links are removed from G (Line 27). The algorithm ends when the desired number c of nodes has been determined (Line 28).

C.4 Network design problem

For the same set of demands, the same RMSA policy and a fiber budget B equal to the total fiber length of an existing EON, the design problem determines a new EON maximizing the resilience metric imposed by its critical nodes.

We have seen in the previous section that the evaluation (i.e., the determination of the resilience metric imposed by the EON critical nodes) is a min-max bi-level optimization problem. In the network design case, since we aim to compute an EON maximizing its evaluation value, this problem is a max-min-max tri-level optimization problem. To solve this problem, we use a multi-start greedy randomized heuristic similar to the one proposed in [BdSA18b] that generates multiple EONs and returns the one whose resilience metric is the highest.

First, the greedy randomized algorithm (Algorithm C.3) is used to compute each new EON. Algorithm C.3 starts with an initial graph $G = (N, E_0)$ composed by the set of nodes N of the original EON and by the set of links E_0 given by the Relative Neighbourhood Graph (RNG) [Tou80]. RNG is defined as follows: nodes $i, j \in N$ are connected by a link if and only if there is no other node $k \in N \backslash \{i, j\}$ such that $l_{ik} \leq l_{ij}$ and $l_{jk} \leq l_{ij}$. Then, the algorithm randomly selects one link (i_s, j_s) at a time until no new link can be added within the remaining budget B_R. The probability of each link being selected at each iteration is as follows. Assume E_s is the set of already selected links, δ_i is the degree of node i in $G = (N, E_s)$ and the remaining budget is $B_R = B - \sum_{(i,j) \in E_s} l_{ij}$. For all node pairs $(i, j) \notin E_s$ such that $l_{ij} \leq B_R$ and at least one of the nodes has the lowest degree in G, the probability of selecting link (i, j) is:

$$\mathrm{P}\big((i,j)\big) = \frac{1}{\left(|\delta_i - \delta_j| + 1\right)\, {l_{ij}}^2} \tag{C.7}$$

Algorithm C.2 NDC based method

```
Given $G = (N, E)$ and demand set $D$.
$C \leftarrow \emptyset$
repeat
    $Z \leftarrow 0$, $r_k \leftarrow 0$ and $c_k \leftarrow 0$, for all $k \in N \backslash C$
    for all $k \in N$ do
        for all $d \in D : s_d \neq k$ and $t_d \neq k$ do
            if $k \in p_d$ then
                Compute $p'_d \in P_d$ that does not include $k$ and requires the least amount of
                resources $S'_d$
                if $p'_d$ does not exist then
                    $c_k \leftarrow c_k + 1$
                else
                    if $S'_d > S_d$ then
                        $r_k \leftarrow r_k + \frac{S'_d - S_d}{S_d}$
                        $Z \leftarrow \max(Z, \frac{S'_d - S_d}{S_d})$
                    end if
                end if
            end if
        end for
        if $Z = 0$ then
            $Z = 1$
        end if
        $r_k \leftarrow Z \times r_k + c_k$
    end for
    $\bar{k} \leftarrow$ index $k$ such that $r_k$ is maximal
    $C \leftarrow C \cup \{\bar{k}\}$
    $D \leftarrow D \backslash \{d \in D : \bar{k} \in p_d\}$
    $N \leftarrow N \backslash \{\bar{k}\}$, $E \leftarrow E \backslash \{(i, j) \in E : i = \bar{k}$ or $j = \bar{k}\}$
until $|C| = c$
```

while for all other node pairs (i, j), $\mathrm{P}\big((i, j)\big) = 0$.

Multiple runs of Algorithm C.3 generate different EONs. So, in a multi-start greedy randomized algorithm, we run multiple times Algorithm C.3, evaluate the resilience metric of each EON and return the best generated one. The multi-start greedy randomized algorithm is presented in Algorithm C.4 with a stopping criteria given by a pre-defined number of iterations. The best EON is defined as $\bar{G}$ with a resilience metric $\bar{z}$. Algorithm C.4 starts by initializing $\bar{G} = (N, \emptyset)$ and $\bar{z} = 0$. At each iteration, Algorithm C.4 (i) generates a new EON G' (Line 3), (ii) checks if G' is valid (Line 4), (iii) computes its resilience value z_1 by the CND based method, (iv) if z_1 is better than $\bar{z}$, computes its resilience value z_2 by the NDC based method (Algorithm C.2) and the resilience value z of G' (Lines 6–8) and (v) if z is better than the resilience value $\bar{z}$ of the current best EON, $\bar{G}$ and $\bar{z}$ are updated accordingly (Lines 9–10).

Two issues require further explanation. First, a randomly generated EON G' is valid (Line

Algorithm C.3 Greedy Randomized Algorithm

```
1: Compute initial graph $G = (N, E_0)$
2: Set $B_R \leftarrow B - \sum_{(i,j) \in E_0} l_{ij}$
3: **repeat**
4:    Select a link $(i_s, j_s)$ with link probabilities given by (C.7)
5:    $E \leftarrow E \cup \{(i_s, j_s)\}$
6:    $B_R \leftarrow B_R - l_{i_s j_s}$
7: **until** $\mathrm{P}\big((i,j)\big) = 0$, for all $i, j \in N : i < j$
```

Algorithm C.4 Multi-Start Greedy Randomized Algorithm

```
1: $\bar{G} \leftarrow (N, \emptyset)$, $\bar{z} \leftarrow 0$
2: **repeat**
3:    Generate a new graph $G' = (N, E')$ using Algorithm C.3.
4:    **if** $G'$ is a valid EON **then**
5:       Compute $z_1$ using the CND based method
6:       **if** $z_1 > \bar{z}$ **then**
7:          Compute $z_2$ using Algorithm C.2
8:          $z \leftarrow \min\{z_1, z_2\}$
9:          **if** $z > \bar{z}$ **then**
10:            $\bar{G} \leftarrow G'$, $\bar{z} \leftarrow z$
11:         **end if**
12:      **end if**
13:   **end if**
14: **until** Pre-defined number of iterations reached
```

4) if it can support all demands with the RMSA policy. To validate G', we run Algorithm C.1 and check if the highest FS index is within the total number of FSs available on each fiber link. Moreover, when the topology of the original EON is 2-connected, we also require G' to be 2-connected (i.e, any single node failure still allows the establishment of a lightpath between any pair of nodes within the transparent reach $T = \max_{m \in M} T_m$).

Second, for each valid EON, Algorithm C.4 computes first its resilience value z_1 by the CND based method (Line 5). If $z_1 \leq \bar{z}$, the EON cannot be better than the best one found so far and, so, the EON can be discarded without running Algorithm C.2. The results show that z_1 is computed much faster than z_2 and, so, Algorithm C.4 is more time efficient in this way.

C.5 Computational results

The computational results are based on 3 network topologies with public available information: Germany50 [OWPT10], PalmettoNet [KNF$^+$11] and Missouri Network Alliance (MissouriNA) [KNF$^+$11]. Table C.1 presents their topology characteristics in terms of number of nodes $|N|$ and fiber links $|E|$, minimum ($\delta_{\min}$), average ($\bar{\delta}$) and maximum ($\delta_{\max}$) node degree and an indication (in column '2-C') if the topology is 2-connected. Although the geographical location of nodes is known, the geographical routes of fiber links is not.

So, to compute link lengths, we have assumed that links follow the shortest path over the Earth surface. Table C.2 presents the resulting length characteristics in terms of minimum ($l_{\min}$), average ($\bar{l}$), maximum ($l_{\max}$) and total (L) link length, and diameter, i.e., the highest length among all shortest paths adding Δ per intermediate node (the length Δ modeling the degradation suffered by a lightpath on each intermediate node was 60 Km).

Table C.1: Topology characteristics of each network.

Network	$\lvert N\rvert$	$\lvert E\rvert$	$\delta_{\min}$	$\bar{\delta}$	$\delta_{\max}$	2-C
Germany50	50	88	2	3.52	5	Yes
PalmettoNet	45	64	1	2.84	5	No
MissouriNA	64	80	1	2.50	5	No

Table C.2: Length characteristics (in km) of each network.

Network	$l_{\min}$	$\bar{l}$	$l_{\max}$	L	Diameter
Germany50	26	100.7	252	8859	1417
PalmettoNet	19	67.0	177	4286	1298
MissouriNA	7	50.0	307	4001	1301

Concerning fiber capacity, we consider each fiber with a capacity of $|F| = 320$ FSs which corresponds to a spectral grid of granularity 12.5 GHz. Concerning MF configurations (recall discussion on the Introduction), realistic transparent reach values are hard to get not only because new researches are periodically reporting reach gains (new MFs, more efficient signal processing, etc) but also because equipment vendors do not announce them in their next generation products due to market competition. So, we have considered $|M| = 4$ available MF configurations with number of FSs n_m and transparent reach T_m shown in Table C.3 which allow us to analyze the efficiency of the proposed methods. Concerning the resilience evaluation, we consider $c \in \{2, 3, 4, 5, 6\}$ as the number of critical nodes. Concerning the demand set D, we consider 4 sets with increasing number of demands for Germany50 (instances named 'Ger_a', 'Ger_b', 'Ger_c' and 'Ger_d'), 2 sets for PalmettoNet (instances named 'Pal_a' and 'Pal_b') and 2 sets for MissouriNA (instances named 'Mis_a' and 'Mis_b').

Table C.3: Modulation format configurations.

m	n_m (no. of FSs)	T_m (km)
1	1	500
2	2	1250
3	3	2000
4	4	2500

All results were obtained using the optimization software *Gurobi Optimizer* version 8.0.0, with programming language *MatLab* version 9.4.0.813654 (R2018a), running on a PC with an Intel Core i7-8700, 3.2 GHz and 16 GB RAM.

Table C.4: Resilience evaluation of existing networks.

Instance	RMSA	c	CND method		NDC method	
	Time (s)		Value	Time (s)	Value	Time (s)
Ger_a	23	2	0.8433	2	**0.8283**	12
		3	**0.5750**	1	**0.5750**	4
		4	**0.5200**	2	**0.5200**	4
		5	**0.4050**	3	0.4983	5
		6	**0.3350**	3	0.4683	9
Ger_b	50	2	0.8457	4	**0.7380**	22
		3	**0.5804**	2	**0.5804**	5
		4	**0.5224**	3	**0.5224**	6
		5	**0.4049**	5	0.5004	7
		6	**0.3388**	6	0.4727	13
Ger_c	51	2	0.8257	3	**0.7236**	23
		3	**0.5878**	2	**0.5878**	5
		4	**0.5345**	3	**0.5345**	6
		5	**0.4128**	4	0.5088	12
		6	**0.3453**	5	0.4149	8
Ger_d	52	2	0.8128	3	**0.7119**	23
		3	**0.5930**	2	**0.5930**	5
		4	**0.5252**	7	0.5426	6
		5	**0.4186**	5	0.5084	12
		6	**0.3357**	4	0.4284	9
Pal_a	19	2	**0.5165**	1	0.5496	2
		3	**0.3430**	1	0.4587	3
		4	**0.2769**	1	0.2851	3
		5	**0.1653**	1	0.2190	3
		6	**0.1116**	1	0.1632	4
Pal_b	24	2	**0.5161**	1	0.5528	2
		3	**0.3492**	1	0.4594	3
		4	**0.2833**	1	0.2925	3
		5	**0.1730**	1	0.2266	4
		6	**0.1194**	1	0.1715	4
Mis_a	51	2	**0.4657**	2	0.8770	8
		3	**0.2964**	2	0.6694	17
		4	**0.2218**	2	0.3327	11
		5	**0.1593**	2	0.2581	12
		6	**0.1169**	2	0.1734	12
Mis_b	69	2	**0.4598**	3	0.8720	9
		3	**0.3140**	3	0.6592	18
		4	**0.2366**	3	0.4271	12
		5	**0.1652**	3	0.2470	11
		6	**0.1265**	3	0.1786	12

Table C.4 presents the resilience evaluation results. Column 'RMSA' presents the runtime (in seconds) of Algorithm C.1 showing that the RMSA policy for the regular state takes a considerably large amount of the total runtime. The resilience evaluation (value and runtime) of the CND and the NDC based methods are presented separately (the best resilience values highlighted in bold). These results show that the CND based method (i.e., computing the critical nodes based on the impact of node failures on the connectivity between the other nodes) is the best heuristic for larger values of c while the NDC based method (i.e., computing the critical nodes based on the impact of the node failures on the supported demand between the other nodes) is the best heuristic for the smallest values of c and only in the Germany50 instances. Concerning runtimes, as observed in Section C.4, the CND based method is computed quicker than the NDC based method.

Tables C.5 and C.6 present the network design results (running Algorithm C.4 with 1000 iterations). Table C.5 shows the performance of the generation and validation part of the multi-start greedy randomized algorithm showing the number of valid EONs (out of the 1000), and the runtime spent in the generation, topology validation and RMSA validation. Once again, the RMSA is the part by far most time consuming. Moreover, the more supported demands, the less number of generated EONs are valid (behavior easily observed in the Germany50 instances). Table C.6 presents the results of the evaluation of the valid EONs (resilience values of the original cases repeated in column 'Original' for comparison reasons). The most important conclusion is that the resilience value of the best EONs is always much higher than the original EONs. A second conclusion is that the resilience evaluation also takes a significant amount of runtime. Note that the total runtime of the network design task is given by the sum of the 3 time values of Table C.5 and the time value of Table C.6. So, in overall, the method takes several hours to run, which is still reasonable for a network design task.

Table C.5: Network design - generation and validation.

Instance	Valid EONs	Time (hh:mm:ss)		
		Generation	Topology Val.	RMSA Val.
Ger_a	929	00:00:01	00:00:48	06:52:47
Ger_b	676	00:00:01	00:00:47	14:02:58
Ger_c	260	00:00:01	00:00:46	14:09:54
Ger_d	23	00:00:01	00:00:46	14:20:49
Pal_a	1000	00:00:01	00:00:01	04:52:14
Pal_b	999	00:00:01	00:00:01	07:10:13
Mis_a	1000	00:00:01	00:00:01	12:16:21
Mis_b	1000	00:00:01	00:00:01	18:41:03

Figure C.1 presents the original topologies and the best topologies obtained for $c = 3$ critical nodes and for the instances with more demands of each network. To understand the differences, links of the best topology not in the original topology are highlighted in dashed blue and the critical nodes of each case are represented with red squares. The number of links highlighted in blue clearly shows that the resilience improvement of the network design

Table C.6: Network design - evaluation.

Instance	c	Original	Best	Time (hh:mm:ss)
Ger_a	2	0.8283	0.9200	00:51:53
	3	0.5750	0.8067	00:51:07
	4	0.5200	0.6517	00:51:14
	5	0.4050	0.5150	00:48:57
	6	0.3350	0.4217	00:45:04
Ger_b	2	0.7380	0.8824	01:17:15
	3	0.5804	0.7624	01:17:22
	4	0.5224	0.6490	01:14:25
	5	0.4049	0.5224	01:11:58
	6	0.3388	0.4171	01:01:32
Ger_c	2	0.7236	0.8588	00:27:55
	3	0.5878	0.7500	00:31:41
	4	0.5345	0.6466	00:32:11
	5	0.4128	0.5162	00:30:02
	6	0.3453	0.4135	00:25:48
Ger_d	2	0.7119	0.8191	00:04:18
	3	0.5930	0.7246	00:03:47
	4	0.5252	0.6214	00:05:32
	5	0.4186	0.5142	00:04:04
	6	0.3357	0.3878	00:03:23
Pal_a	2	0.5165	0.8306	00:30:37
	3	0.3430	0.6488	00:28:59
	4	0.2769	0.4855	00:27:55
	5	0.1653	0.3533	00:22:56
	6	0.1116	0.2438	00:19:50
Pal_b	2	0.5161	0.8300	00:37:15
	3	0.3492	0.6493	00:33:26
	4	0.2833	0.4855	00:32:44
	5	0.1730	0.3553	00:26:36
	6	0.1194	0.2466	00:22:32
Mis_a	2	0.4657	0.8226	01:10:41
	3	0.2964	0.6935	01:40:11
	4	0.2218	0.5242	01:06:44
	5	0.1593	0.3992	01:05:17
	6	0.1169	0.3105	01:00:55
Mis_b	2	0.4598	0.8229	01:29:37
	3	0.3140	0.6979	02:03:13
	4	0.2366	0.5298	01:17:20
	5	0.1652	0.4033	01:17:49
	6	0.1265	0.3170	01:13:04

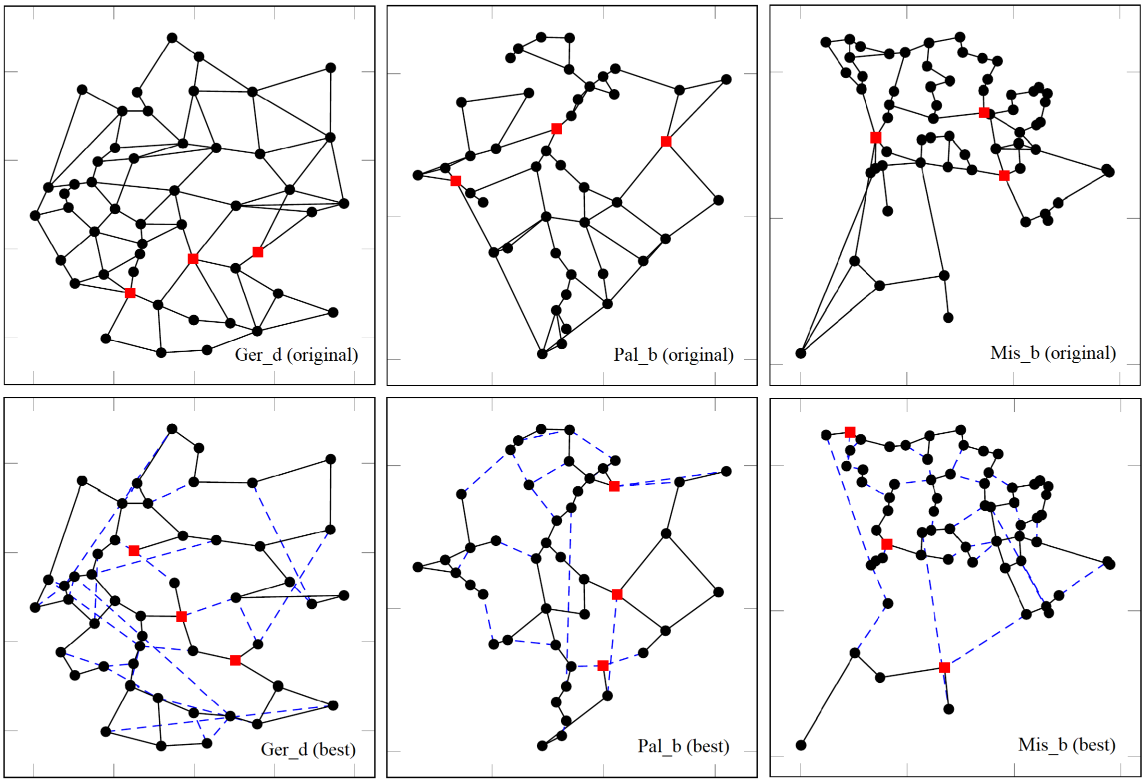


Figure C.1: Original topologies (top) and best topologies (bottom) for $c = 3$ critical nodes (in red). Links not in the original topology highlighted in dashed blue in the best topology.

solutions is obtained with topologies which are very different from the original ones.

Another interesting aspect is the comparison of the node degree distributions between the original topologies and the topologies of the best network design solutions. Figure C.2 shows these distributions for the 8 instances with the best EONs obtained for $c = 3$ critical nodes (original topologies in blue and best topologies in green). In the best solutions, there is a decrease of the number of nodes with the lowest and highest degrees and an increase of the number of nodes with degrees closer to the average. This observation also stands for the other values of c showing that EONs resilient to multiple node failures tend to have more homogeneous node degrees.

C.6 Conclusions

In this work, we have considered the evaluation and network design of EONs resilient to multiple node failures. First, we have addressed the resilience of EONs to multiple node failures by identifying the critical nodes whose simultaneous failure maximally reduce the demand percentage that is supported by the network. Then, for the same estimated demands, the same RMSA policy and a fiber budget equal to the total fiber length of an existing EON, we have addressed the design of a new EON maximizing the resilience metric imposed by its critical nodes. For both tasks, we have proposed heuristic methods that were evaluated on known network topologies.

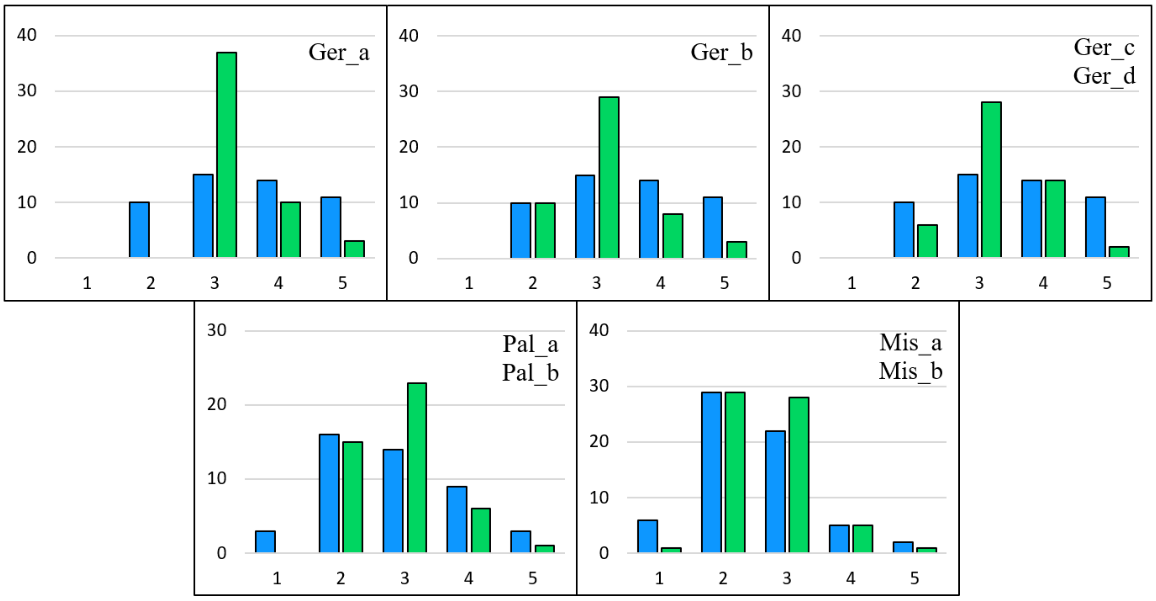


Figure C.2: Node degree histograms of original topologies (in blue) and best generated topologies (in green).

The results showed that the network design solutions are much more resilient to multiple node failures. The improvements are obtained with topologies with more homogeneous node degrees which are very different from the original ones. In computing terms, a key aspect is the RMSA which was the most computational demanding part of the proposed methods.

Note that the adopted RMSA policy assumes a restoration mechanism where disrupted demands are reassigned as much as possible with new lightpaths supporting the same line rate. A topic that deserves further study is to consider bandwidth squeezed protection/restoration mechanisms (exploiting the advanced flexibility provided by sliceable bandwidth-variable transponders) [CSO15] where the line rate supported by lightpaths is dynamically reduced so that more lightpaths can be accommodated in the case of large-scale failures.

Bibliography

[ACEP09] A. Arulselvan, C. Commander, L. Elefteriadou, and P. Pardalos. *Detecting critical nodes in sparse graphs.* Computers & Operations Research, 36(7):2193–2200, 2009.

[AdSD16] A. Agra, A. de Sousa, and M. Doostmohammadi. *The minimum cost design of transparent optical networks combining grooming, routing, and wavelength assignment.* IEEE/ACM Transactions on Networking, 24(6):3702–3713, 2016.

[AFM+18] V. Abedifar, M. Furdek, A. Muhammad, M. Eshghi, and L. Wosinska. *Routing, modulation, and spectrum assignment in programmable networks based on optical white boxes.* Journal of Optical Communications and Networking, 10(9):723–735, 2018.

[AR17] F. Abkenar and A. Rahbar. *Study and analysis of routing and spectrum allocation (RSA) and routing, modulation and spectrum allocation (RMSA) algorithms in elastic optical networks (EONs).* Optical Switching and Networking, 23:5–39, 2017.

[BdSA18a] F. Barbosa, A. de Sousa, and A. Agra. *The design of transparent optical networks minimizing the impact of critical nodes.* Electronic Notes in Discrete Mathematics, 64:165–174, 2018.

[BdSA18b] F. Barbosa, A. de Sousa, and A. Agra. *Topology design of transparent optical networks resilient to multiple node failures.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

[BGLR05] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish. *Improving network robustness by edge modification.* Physica A: Statistical Mechanics and its Applications, 357(3-4):593–612, 2005.

[CSO15] B. Chatterjee, N. Sarma, and E. Oki. *Routing and spectrum allocation in elastic optical networks: a tutorial.* IEEE Communications Surveys Tutorials, 17(3):1776–1800, 2015.

[CTV11] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos. *Elastic bandwidth allocation in flexible OFDM-based optical networks.* Journal of Lightwave Technology, 29(9):1354–1366, 2011.

[dSMS17] A. de Sousa, D. Mehta, and D. Santos. *The robust node selection problem aiming to minimize the connectivity impact of any set of p node failures.* In 13th International Conference on Design of Reliable Communication Networks (DRCN), pages 138–145, 2017.

[DTM14] F. Dikbiyik, M. Tornatore, and B. Mukherjee. *Minimizing the risk from disaster failures in optical backbone networks.* Journal of Lightwave Technology, 32(18):3175–3183, 2014.

[FWG+16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GTE+16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[GWK15] R. Goścień, K. Walkowiak, and M. Klinkowski. *Tabu search algorithm for routing, modulation and spectrum allocation in elastic optical network with anycast and unicast traffic.* Computer Networks, 79:148–165, 2015.

[GZLZ12] L. Gong, X. Zhou, W. Lu, and Z. Zhu. *A two-population based evolutionary approach for optimizing routing, modulation and spectrum assignments (RMSA) in O-OFDM networks.* IEEE Communications Letters, 16(9):1520–1523, 2012.

[JKT$^+$10] M. Jinno, B. Kozicki, H. Takara, A. Watanabe, Y. Sone, T. Tanaka, and A. Hirano. *Distance-adaptive spectrum resource allocation in spectrum-sliced elastic optical path network* [topics in optical communications]. IEEE Communications Magazine, 48(8):138–145, 2010.

[KNF$^+$11] S. Knight, H. Nguyen, N. Falkner, R. Bowden, and M. Roughan. *The internet topology zoo.* IEEE Journal on Selected Areas in Communications, 29(9):1765–1775, 2011.

[KW11] M. Klinkowski and K. Walkowiak. *Routing and Spectrum Assignment in Spectrum Sliced Elastic Optical Path Network.* IEEE Communications Letters, 15(8):884–886, 2011.

[NYWF17] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek. *Link addition framework for optical CDNs robust to targeted link cut attacks.* In 9th International Workshop on Resilient Networks Design and Modeling (RNDM). IEEE, 2017.

[NZCM11] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano. *Assessing the vulnerability of the fiber infrastructure to disasters.* IEEE/ACM Transactions on Networking, 19(6):1610–1623, 2011.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[RCM17] D. Rueda, E. Calle, and J. Marzo. *Robustness comparison of 15 real telecommunication networks: structural and centrality measurements.* Journal of Network and Systems Management, 25(2):269–289, 2017.

[RHC$^+$16] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska. *RECODIS: Resilient communication services protecting end-user applications from disaster-based failures.* In 18th International Conference on Transparent Optical Networks (ICTON). IEEE, 2016.

[SdSM18] D. Santos, A. de Sousa, and P. Monteiro. *Compact models for critical node detection in telecommunication networks.* Electronic Notes in Discrete Mathematics, 64:325–334, 2018.

[SGL12] M. Di Summa, A. Grosso, and M. Locatelli. *Branch and cut algorithms for detecting critical nodes in undirected graphs.* Computational Optimization and Applications, 53(3):649–680, 2012.

[STD15] K. Sabeh, M. Tornatore, and F. Dikbiyik. *Progressive network recovery in optical core networks.* In 7th International Workshop on Reliable Networks Design and Modeling (RNDM), pages 106–111. IEEE, 2015.

[Tou80] G. Toussaint. *The relative neighbourhood graph of a finite planar set.* Pattern Recognition, 12(4):261–268, 1980.

[TR17] S. Talebi and G. Rouskas. *On distance-adaptive routing and spectrum assignment in mesh elastic optical networks.* IEEE/OSA Journal of Optical Communications and Networking, 9(5):456–465, 2017.

[VBP14] A. Veremyev, V. Boginski, and E. Pasiliao. *Exact identification of critical nodes in sparse networks via new compact formulations.* Optimization Letters, 8(4):1245–1259, 2014.

[WCP11] Y. Wang, X. Cao, and Y. Pan. *A study of the routing and spectrum allocation in spectrum-sliced Elastic Optical Path networks.* In 2011 Proceedings IEEE INFOCOM, pages 1503–1511, 2011.

[YZZY13] Y. Yin, M. Zhang, Z. Zhu, and S. Yoo. *Fragmentation-aware routing, modulation and spectrum assignment algorithms in elastic optical networks.* In Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), pages 1–3, 2013.

[ZL12] A. Zeng and W. Liu. *Enhancing network robustness against malicious attacks.* Physical Review E, 85((6 Pt 2):066130), 2012.

[ZWA15] J. Zhao, H. Wymeersch, and E. Agrell. *Nonlinear impairment-aware static resource allocation in elastic optical networks.* Journal of Lightwave Technology, 33(22):4554–4564, 2015.

Appendix D: A RMSA Algorithm Resilient to Multiple Node Failures on Elastic Optical Networks

Abstract: An Elastic Optical Network (EON) provides a lot of flexibility on the way an optical network supports the demands of multiple services. This flexibility is given by the Routing, Modulation and Spectrum Assignment (RMSA) algorithm whose primary goal is to use the spectrum resources of the network in an efficient way. Recently, large-scale failures are becoming a concern and one source of such failures is malicious human activities. In terrorist attacks, although node shutdowns are harder to realize than link cuts, they are the most rewarding in the attackers' perspective since the shutdown of one node also shuts down all its connected links. In order to obtain a RMSA algorithm resilient to multiple node failures, we propose the use of a path disaster availability metric which measures the probability of each path not being affected by a multiple node failure. We present computational results considering a mix of unicast and anycast services in 3 well-known topologies. We assess the trade-off between spectrum usage efficiency and resilience to multiple node failures of our proposal against other previous known algorithms. The results show that the RMSA decision is always better when the disaster path availability metric is used. Moreover, the best way to use the path disaster availability metric in the RMSA decision depends on the traffic load of the EON.

Keywords: Elastic Optical Networks, RMSA, Multiple Node Failures, Disaster Resilience

F. Barbosa, A. de Sousa, A. Agra, K. Walkowiak, and R. Goścień. *A RMSA algorithm resilient to multiple node failures on elastic optical networks.* In 11th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2019.

D.1 Introduction

An Elastic Optical Network (EON) provides a lot of flexibility on the way an optical network can support the demands of multiple services. This flexibility is given by the Routing, Modulation and Spectrum Assignment (RMSA) of each demand and is used, in practice, to make the most out of the available spectrum resources of the optical network.

The primary goal of the RMSA is to use the resources in an efficient way, i.e., by keeping the spectrum resources usage low so that future demands can be accommodated as much as possible [AR17, CTV11, KW11, TR17, WK13]. Then, other goals can also be considered as transceiver costs or power consumption [CSO15, GWK15, PAK$^+$12].

One of the most relevant goals is the network resilience to failures. Network resilience is, broadly speaking, the ability of the network to keep supporting the service demands in case of network failures. Many works address this problem considering protection mechanisms to guarantee that all demands can be maintained after any single link or node failure [CZJZ15, GK19, WNG17].

Recently, large-scale failures are becoming a concern to network operators due to different causes, as natural disasters [GTE$^+$16] or human malicious activities [FWG$^+$16], which might involve a significant number of simultaneous failures. The guarantee that all demands are maintained in a large-scale failure is infeasible in practice as the required resources become too costly. In this case, the aim is to improve the network preparedness to large-scale failures by maximizing the amount of demand that can still be maintained in face of such failures. In terrorist attacks, although node shutdowns are harder to realize than link cuts, they are the most rewarding in the attackers' perspective since the shutdown of one node also shuts down all its connected links. So, in this work, we deal with the multiple node failures as they are the most harmful case.

The topology design of optical networks resilient to multiple node failures was recently addressed in [BdSA18]. In that work, the resilience is evaluated by the impact of the simultaneous failure of the critical nodes, i.e., the nodes with the highest impact on the connectivity of the network. Here, we propose a family of RMSA algorithms resilient to multiple node failures assuming that an attacker "discovers" with some probability a set of nodes to be attacked. The algorithms use a path metric, which we name *path disaster availability*, in the RMSA decision of each demand. This metric measures the probability of the path not being affected by the attacked nodes. Although the concept of path availability is commonly used to characterize the availability of networking services to unintended failures, as far as we are aware, it has never been exploited in the context of multiple node failures.

We present a set of computational results considering a mix of unicast and anycast services in 3 well-known topologies and compare the proposed RMSA algorithms with the first-fit algorithm, used in many works due to its simplicity, and with a RMSA algorithm recently used in [BdSA19] and adapted from [KW11]. All algorithms are evaluated through simulation considering a restoration mechanism where, when a multiple node failure happens, the non-affected lightpaths remain unchanged and the demands of the affected lightpaths are reassigned as much as possible in the surviving network resources.

The different RMSA algorithms are compared in terms of spectrum usage efficiency and resiliency to multiple node failures. In the latter case, the resiliency is evaluated by 2 parameters: the average non-disrupted demand (the average demand percentage that is not disrupted after a failure) and the average surviving demand (the average demand percentage that is supported after a failure). Both parameters are important in practice. Higher surviving demands are important for non-critical services as they are less penalized by short-term disruptions. Higher non-disrupted demands are important for critical services (requiring high availability) and because a lower number of lightpaths required to be reassigned minimizes the instability impact of the simultaneous reconfiguration of many lightpaths.

The paper is organized as follows. In Section D.2, the path disaster availability metric is presented, together with its determination method. Section D.3 describes the RMSA methods considered in this work. The computational results are presented and discussed in Section D.4. Finally, Section D.5 draws the main conclusions of the work.

D.2 Modeling path disaster availability for node attacks

Consider an EON topology defined by a graph $G = (N, E)$, with a set of $|N|$ nodes and a set of $|E|$ undirected links. Consider the following attack model: an attacker "discovers" with some probability a set of nodes and plans to attack them (almost) simultaneously.

Since public information might exist related to the location of each node (for example, the location of Data Centers is usually publicly known and most likely a network node is nearby), we assume that each node $i \in N$ is associated with a positive weight w_i proportional to the probability of the node being discovered by an attacker. We assume that there is no correlation between discovered nodes as, if exists, it is related to attacker's organizational issues which require insight information usually not available to the network operator. Moreover, we assume that the number of attacked nodes s is between a minimum number s_m and a maximum number s_M. Finally, we assume that the effort to attack s nodes is proportional to the number of nodes and, therefore, the probability of s nodes being attacked, with $s_m \leq s \leq s_M$, is inversely proportional to the number of attacked nodes $1/s$.

First, the path disaster availability a_p of a given path p defined by its set of nodes $i \in p$ (including the source and destination nodes) is:

$$a_p = \prod_{i \in p} (1 - p_i) \tag{D.1}$$

i.e., the probability that path p is available in the surviving network. In expression (D.1), p_i is the probability of node $i \in N$ to be attacked when a multiple node attack is realized and, by the adopted attack model, it is independent of the other attacked nodes.

Then, the probability p_i of node $i \in N$ being attacked is:

$$p_i \;=\; \frac{1}{\sigma} \sum_{s=s_m}^{s_M} p_i^s \times \frac{1}{s} \tag{D.2}$$

where $\sigma = \sum_{s=s_m}^{s_M} \frac{1}{s}$ and p_i^s is the probability of node i being attacked on an attack to s nodes.

Finally, the probability p_i^s of node i being attacked on an attack to s nodes is the sum of the probabilities of all sequences (without repetitions) of s out of n nodes that include node i, given by:

$$\begin{aligned} p_i^s &= \frac{w_i}{W_N} + \sum_{j \in N\backslash\{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N\backslash\{j\}}} \\ &+ \sum_{j \in N\backslash\{i\}} \frac{w_j}{W_N} \Big(\sum_{k \in N\backslash\{i,j\}} \frac{w_k}{W_{N\backslash\{j\}}} \times \frac{w_i}{W_{N\backslash\{j,k\}}} \Big) + ... \end{aligned} \tag{D.3}$$

where W_R denotes the sum of the weights of the nodes in set R, with $R \subset N$, i.e., $W_R = \sum_{i \in R} w_i$.

The first term $\frac{w_i}{W_N}$ in expression (D.3) is the probability of all sequences such that node i is the first node of the sequence. The second term $\sum_{j \in N\backslash\{i\}} \frac{w_j}{W_N} \times \frac{w_i}{W_{N\backslash\{j\}}}$ is the probability of all sequences such that node i is the second node of the sequence, i.e., all sequences composed by a node $j \in N\backslash\{i\}$ in the first position and node i in the second position. The third term is the generalization of the previous term for the sequences such that node i is the third node of the sequence.

The probability p_i^s given by expression (D.3) has s terms and can be computed recursively as follows. For a given set N of nodes and associated weights $w = \{w_i, i \in N\}$, a given number of attacked nodes s and a given node i, the probability p_i^s is computed as:

$$p_i^s = prob(N, w, i, 0, s) \tag{D.4}$$

where *prob*() is a recursive function defined in Algorithm D.1. The input parameters (Line 1) are a set of nodes R which were still not selected (in the first call in (D.4), this parameter is the complete node set N), the set w of node weights, the node i whose probability we want to compute, the number z of already selected nodes (in the first call in (D.4), this parameter is $z = 0$) and the number s of nodes to be selected.

Algorithm D.1 Recursive function to compute p_i^s

```
 1: function  $p = prob(R, w, i, z, s)$
 2: $z \leftarrow z + 1$
 3: $W_R \leftarrow \sum_{j \in R} w_j$
 4: $p \leftarrow \frac{w_i}{W_R}$
 5: if $z < s$ then
 6:     for all $j \in R\backslash\{i\}$ do
 7:         $p \leftarrow p + \frac{w_j}{W_R} \times prob(R\backslash\{j\}, w, i, z, s)$
 8:     end for
 9: end if
10: return  $p$
```

D.3 RMSA algorithms

Consider a given EON topology defined by graph $G = (N, E)$ and a given set D of estimated traffic demands. Each demand $d \in D$ can be of either unicast or anycast service type. In unicast services, each demand is characterized by a pair of end-nodes (s_d, t_d) and its required bit-rate b_d. In anycast services, a set S of services is provided by a set $C \subset N$ of existing Data Centers (DCs) and each anycast service $r \in S$ is provided by a DC subset $C_r \subseteq C$. Then, each anycast demand is characterized by a source node s_d, an anycast service $r_d \in S$ and a bit-rate b_d. In this case, the anycast demand can be satisfied by any of the DCs in C_{r_d}.

The RMSA algorithm determines the way lightpaths are assigned both in the regular state and in any failure state. To model the RMSA, we need additional sets and parameters. Set $F = \{1, 2, ..., |F|\}$ is the ordered set of Frequency Slots (FSs) available on each fiber link to be assigned to lightpaths. Set P_d is the set of candidate paths associated with demand $d \in D$, ordered from the shortest to the longest optical length.

The optical length of a path is the sum of its link lengths plus a given length value Δ per intermediate node (which models the optical degradation suffered by a lightpath while traversing an intermediate optical switch). Each $p \in P_d$ is defined by:

- the binary parameters α_e^p which are equal to 1 if link $e \in E$ is in p, or equal to 0 otherwise;
- the integer parameter n_p indicating the number of FSs of the most efficient modulation format whose transmission range is not lower than the optical length of p.

D.3.1 First-fit RMSA algorithm

In the First-Fit (FF) RMSA algorithm, each demand d is routed in the first candidate path with available resources. Starting from an empty network, this task is conducted for each demand by some order. Many works assume the order of the demands given by the input data file. However, the best results are obtained if we consider first the demands that require more network resources. For fairness reasons when comparing the different RMSA algorithms, in this work, we consider this “more sophisticated” FF approach.

Initially, the set of demands $d \in D$ is ordered based on the properties of the shortest path of its set of candidate paths, i.e., the first path in P_d. This order follows the next 3 hierarchical orders (from the most important to the least important):

1. decreasing order of the number of hops of the optical shortest path between the source s_d and either the destination t_d (for unicast demands) or the closest DC (for anycast demands);
2. decreasing order of the demand bit-rate b_d;
3. decreasing order of the optical shortest path length between the source s_d and either the destination t_d (for unicast demands) or the closest DC (for anycast demands).

This ordering strategy was adopted after some preliminary computational tests. Then, for each $d \in D$ (and by this order), we compute the highest FS f of the lowest set of n_p contiguous FSs that can be assigned on the shortest path $p \in P_d$ without overlap with previous assignments. If $f \in F$, a lightpath is assigned to demand d on path p and on FSs from $f - n_p + 1$ to f. Otherwise, the process is repeated for the next shortest path $p \in P_d$ until a lightpath can be assigned to demand d or all paths in P_d have been computed (in the latter case, the demand is not assigned).

D.3.2 Resilient RMSA algorithms

Recall that the required number of FSs n_p depends on the candidate path $p \in P_d$. First, consider for each demand d the parameter n_d with the minimum number of FSs required by any of its candidate paths $p \in P_d$, i.e., $n_d = \min_{p \in P_d} n_p$. Consider also P_e as the set of candidate paths of all demands that include link $e \in E$.

A RMSA algorithm for the regular state of the network is defined in Algorithm D.2, following the general approach proposed in [KW11]. In a nutshell, Algorithm D.2 is a greedy algorithm that starts with an empty network (i.e., all FSs are free in all links) and, iteratively, assigns to a demand $d \in D$, a lightpath $p \in P_d$ and a set of n_p contiguous FSs.

Algorithm D.2 starts by computing the maximum value n among the n_d values of all demands (Line 1) and initializes set $\bar{D}$ with all demands such that $n_d = n$ (Line 3). Then, for all candidate paths of all demands in $\bar{D}$ (Line 6), the algorithm computes the lowest set of n_p contiguous FSs that can be assigned without overlapping with previous assignments (Lines 7–11) and, among all, it selects the one according to a given *best assignment condition* (Lines 8–10), explained later. The selected path and associated set of FSs are used to assign the lightpath to the corresponding demand (Line 12) and the demand is removed from set $\bar{D}$ (Line 13). When $\bar{D}$ becomes empty, n is decremented (Line 15) and the algorithm continues until n reaches 0.

Algorithm D.2 Robust RMSA

```
 1: Initialize $n \leftarrow \max_{d \in D} n_d$
 2: while $n \geq 1$ do
 3:     $\bar{D} \leftarrow \{d \in D : n_d = n\}$
 4:     while $\bar{D} \neq \emptyset$ do
 5:         $\bar{f} \leftarrow \infty$, $\bar{l} \leftarrow \infty$, $\bar{d} \leftarrow \{\}$, $\bar{p} \leftarrow \{\}$ and $\bar{a} \leftarrow 0$
 6:         for all $p \in P_d$, $d \in \bar{D}$ do
 7:             $f \leftarrow$ highest FS index of the lowest set of $n_p$ contiguous FSs that can be assigned
                on $p$ to $d$ without overlap with previous assignments
 8:             if [best assignment condition] then
 9:                 $\bar{f} \leftarrow f$, $\bar{p} \leftarrow p$, $\bar{d} \leftarrow d$, $\bar{l} \leftarrow l_p$ and $\bar{a} \leftarrow a_p$
10:             end if
11:         end for
12:         Assign to demand $\bar{d}$ a lightpath on the candidate path $\bar{p}$ and on the FSs from $\bar{f}-n_{\bar{p}}+1$
            to $\bar{f}$
13:         $\bar{D} \leftarrow \bar{D} \backslash \bar{d}$
14:     end while
15:     $n \leftarrow n - 1$
16: end while
```

The *best assignment condition* (Line 8) is the step where the RMSA can be tuned according to different lightpath assignment criteria. In [KW11], a collision metric c_e is proposed for each link $e \in E$ given by $c_e = \sum_{d \in D} \sum_{p \in (P_d \cap P_e)} n_p$. Then, each candidate path $p \in \cup_{d \in D} P_d$ has an associated path collision length metric $l_p = \sum_{e \in E} \alpha_e^p c_e$ which is used in the RMSA when selecting candidate paths.

Here, we investigate how both metrics (the path collision length and the path disaster availability, as defined in (D.1)) can be combined to reach a RMSA algorithm which is more resilient to multiple node failures.

Note that in Lines 5–11 of Algorithm D.2, the selected path $\bar{p}$ is initialized empty (Line 5) and is updated (Line 9) when a new best candidate path p is found (Line 8). So, the *best assignment condition* in Line 8 is a comparison between the best path already found $\bar{p}$ (associated with demand $\bar{d}$ with the highest FS $\bar{f}$, collision length $\bar{l}$ and disaster availability $\bar{a}$) and the current candidate path p (associated with demand d with the highest FS f, collision length l_p and disaster availability a_p).

To define different *best assignment conditions*, we consider 3 measures: the best FS ("S"), the best path disaster availability ("P") and the best path collision length ("C"). Then, the following 4 different *best assignment conditions* were investigated:

SC: p is better than $\bar{p}$ if its highest FS is better ($f < \bar{f}$), or if $f = \bar{f}$ and its collision length is better ($l_p < \bar{l}$). This condition represents the strategy proposed in [KW11] where it is shown to be more efficient than other RSMA algorithms in terms of spectrum usage efficiency.

SPC: p is better than $\bar{p}$ if its highest FS is better ($f < \bar{f}$), or if $f = \bar{f}$ and its disaster availability is better ($a_p > \bar{a}$), or if $f = \bar{f}$ and $a_p = \bar{a}$ and its collision length is better ($l_p < \bar{l}$). The first preference is still to assign the lowest spectrum but, as a tie-breaker, the path disaster availability is used aiming to improve the resilience to multiple node attacks (the collision length is only used as a tie-breaker of the path disaster availability).

PSC: p is better than $\bar{p}$ if its disaster availability is better ($a_p > \bar{a}$), or $a_p = \bar{a}$ and its highest FS is better ($f < \bar{f}$), or if $a_p = \bar{a}$ and $f = \bar{f}$ and its collision length is better ($l_p < \bar{l}$). Now, the first preference is the path disaster availability even if p requires higher spectrum than $\bar{p}$ (i.e., the aim is to improve the resilience to multiple node attacks at the possible cost of a lower spectrum usage efficiency).

Mix: it is defined as **PSC** if $f \leq H$, or as **SPC** if $f > H$, where H is the highest FS already assigned to all previous lightpaths. It is a combination of the two previous cases: if the highest FS f of path p does not increase H, the first preference is to improve the disaster resilience; otherwise, the first preference is to assign the lowest spectrum.

Algorithm D.2 with the SC *best assignment condition* was recently used in [BdSA19] in the design of EONs resilient to multiple node failures. Like in here, a restoration mechanism is considered in [BdSA19] where, when a multiple node failure happens, the non-affected lightpaths remain unchanged and the affected demands are reassigned as much as possible in the surviving network. Following [BdSA19], we consider for the failure state (i.e., when multiple nodes fail), a RMSA algorithm slightly different than the RMSA algorithm used in the regular state (as presented in Algorithm D.2). The algorithm starts with the FSs occupied by the non-affected lightpaths (i.e., with a fragmented spectrum occupation). Then, the RMSA considers the demands in increasing order of their n_d values (as opposed to the decreasing order used in Algorithm D.2) as the increasing order performs better, on average (lightpaths requiring less number of FSs can better fit in the initial fragmented spectrum). Finally, the SC *best assignment condition* is used as in a failure state the aim is to reassign as much as possible the affected demands (spectrum usage efficiency is the most important aim).

D.4 Computational results

The computational results presented in this section are based on 3 network topologies with public available information [OWPT10]: Germany50, Cost266 and Janos-US. Table D.1 presents their topology characteristics in terms of number of nodes $|N|$ and fiber links $|E|$, average node degree $\bar{\delta}$, average link length $\bar{l}$ and diameter, i.e., the highest length among all shortest paths adding Δ per intermediate node (the length Δ modeling the degradation suffered by a lightpath on each intermediate node was set to 60 km). The last column presents the number of DC nodes considered on each topology. The network topologies are shown in Fig. D.1 with DC node locations (highlighted in large circles) selected among the nodes with largest node degree.

Table D.1: Topology characteristics of each network.

Network	$\|N\|$	$\|E\|$	$\bar{\delta}$	$\bar{l}$	Diameter	$\|C\|$
Germany50	50	88	3.52	100.7	1417	11
Cost266	37	57	3.08	438.1	4574	9
Janos-US	26	42	3.23	600.6	5094	7

The candidate paths associated to each demand were computed with a k-shortest path algorithm considering $k = 5$ in all cases. For anycast demands, we have considered 5 shortest paths between the source node and each DC node of its anycast service, and then excluded the paths that have DC nodes of the same service as intermediate nodes.

For each fiber, we have considered a capacity of $|F| = 320$ FSs which corresponds to a spectral grid of granularity 12.5 GHz. The number of FSs n_p required by each candidate path $p \in P_d$ of each demand d was computed as follows. Based on the distance-adaptive transmission (DAT) rule, we first select the highest bit-rate MF whose transmission reach is not lower than the optical length of p (the assumptions are that transceivers support polarization division multiplexing, operate at a fixed baud rate of 28 Gbaud, and transmit/receive on an optical channel occupying 37.5 GHz). If the bit-rate b_d of demand d is not higher than the selected MF bit-rate, one single transceiver is required. Otherwise, multiple optical channels (each one used by one transceiver with the previous selected MF) are grouped in a single spectral super-channel (SCh). We assume that lightpaths require a 12.5 GHz guard-band. So, the required number of contiguous FSs is $n_d = 3t + 1$, where t denotes the minimum number of transceivers with a total bit-rate not lower than b_d. The transmission reach and bit-rate of all considered MFs are presented in Table D.2 (transceiver model based on [KRS+16] and transmission reaches based on [RBMT17]).

Table D.2: Transmission reach and bit-rate of each MF.

Modulation Format (MF)	BPSK	QPSK	8-QAM	16-QAM
Transmission reach (km)	6300	3500	1200	600
Bit-rate (Gbps)	50	100	150	200

Concerning the estimated demand set D, we have considered 5 sets for each topology

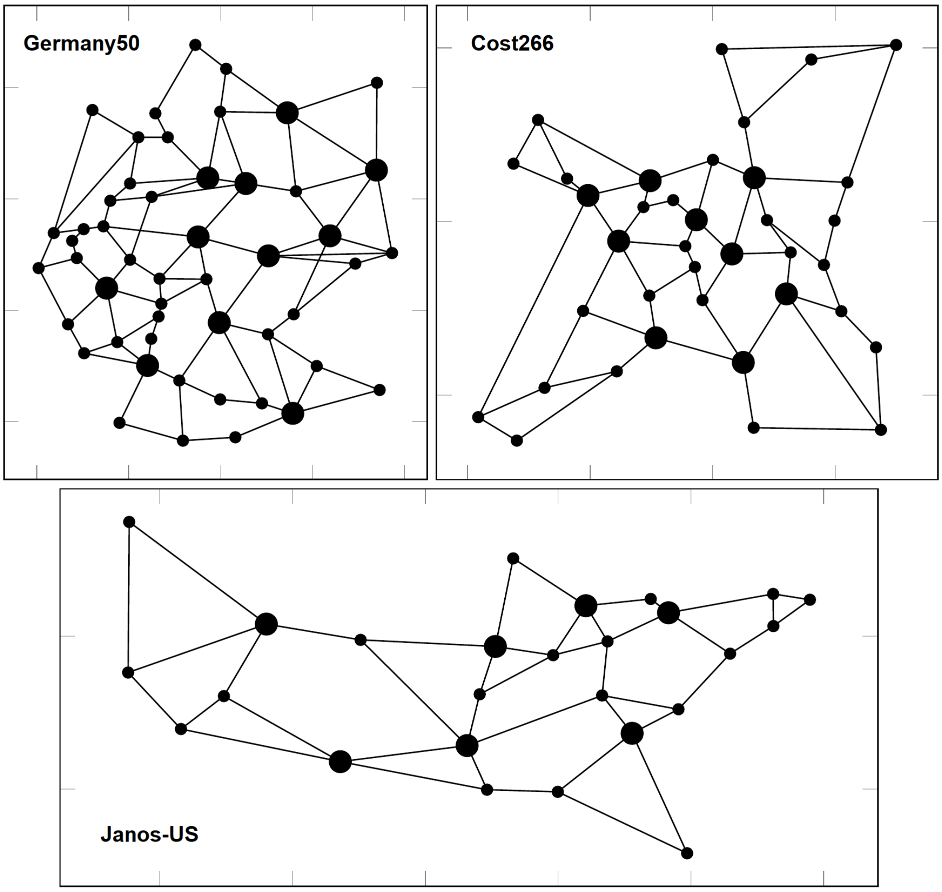


Figure D.1: Network topologies.

with an increasing amount of traffic where each set considers the traffic equally divided into unicast and anycast traffic.

Regarding the unicast traffic, each unicast demand $d \in D$ has its end-nodes (s_d, t_d) randomly generated without replacement (with a uniform distribution among all nodes) and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set $\{50, 100, 150, 200\}$.

Regarding the anycast traffic, a set of five anycast services ($|S| = 5$) is considered in all cases and each service $r \in S$ is served by five randomly selected DCs from C (i.e., the DC subset C_r of anycast service $r \in S$ is randomly selected with a uniform distribution from the set of all DC nodes C). Then, each anycast demand $d \in D$ has its source node s_d randomly generated with a uniform distribution among all nodes, its anycast service $r_d \in S$ randomly generated with a uniform distribution between all services and its bit-rate b_d (in Gbps) randomly generated with a uniform distribution in the set $\{50k \colon k \in \mathbb{N},\ 1 \leq k \leq 20\} = \{50, 100, ..., 1000\}$. The s_d and r_d values are generated without repetition (i.e., we guarantee at most one demand from each source node s_d to each anycast service $r \in S$).

Concerning the multiple node attacks, we have considered that the number of attacked nodes s is between $s_m = 2$ and $s_M = 6$ (we have excluded $s = 1$ since typical topologies are already resilient to single node failures). Moreover, the node weights (defining the probability of the nodes being discovered by the attacker), were assumed to be $w_i = 5$ for the DC nodes (set C) and $w_i = 1$ for all other nodes (set $N\backslash C$).

Recall that the aim is to determine the trade-off between spectrum usage efficiency and resiliency to multiple node failures among the different RMSA algorithms. Note that all RMSA algorithms described in section III assign lightpaths in the lowest possible spectrum available in the routing path selected to each demand. So, the spectrum usage efficiency can be evaluated by the highest FS allocated at the end of the algorithm and a better algorithm is one whose highest allocated FS is lower.

Table D.3 presents the highest allocated FS obtained by each RMSA algorithm on each problem instance in the regular state (T is the total bit-rate, in Tbps, of the instance, i.e., $T = \sum_{d \in D} b_d$). The lowest value among all algorithms is highlighted in bold for each problem instance and the absence of a value means that the RMSA algorithm was not able to assign lightpaths to all demands.

Table D.3: Highest FS allocated by each RMSA method.

Network	T (Tbps)	FF	SC	SPC	PSC	Mix
Germany50	20	90	**62**	65	108	72
	45	177	119	**113**	199	146
	70	282	**172**	179	318	235
	95	320	227	**221**	–	304
	135	–	320	**319**	–	–
Cost266	15	122	65	**64**	91	83
	30	218	138	**133**	199	171
	45	275	**181**	185	258	238
	60	320	**250**	251	–	292
	80	–	**300**	310	–	–
Janos-US	15	113	**73**	76	89	80
	30	226	**155**	156	191	175
	45	317	**211**	214	276	258
	55	–	254	**248**	–	299
	65	–	294	**288**	–	–

Table D.3 results show that, concerning spectrum usage efficiency, both SC and SPC based RMSA algorithms present very similar results and are much more efficient than the others. This is a direct consequence of both using the highest FS as the first measure in the *best assignment condition.* The PSC based RMSA strongly penalizes the spectrum usage efficiency (even worst than FF in the Germany50) while the Mix (being a combination of the SPC and PSC) presents intermediate penalty results.

In order to assess the resilience of each RMSA algorithm to multiple node attacks, we have generated 500 random attacks for each problem instance (after some preliminary testing, this value was shown to be good enough as larger values do not significantly change the average results).

Each attack was implemented as follows. First, the number of attacked nodes s is randomly generated in $\{s_m, ..., s_M\}$ with probabilities proportional to $1/s$. Then, s network nodes are randomly sampled without repetition with probabilities proportional to the weights w_i. For each attack, we run the RMSA algorithm variant for the failure state and we compute the total non-disrupted demand (the sum of the demands whose lightpaths were not disrupted) and the total surviving demand (the sum of the demands whose lightpaths were not disrupted plus the sum of the demands that were assigned with new lightpaths). Finally, the resiliency of each RSMA algorithm is evaluated by 2 parameters: the Average Non-Disrupted Demand (the average bit-rate percentage that is not disrupted among all 500 attacks) and the Average Surviving Demand (the average bit-rate percentage that is supported after the attack among all 500 attacks).

Table D.4 presents the average results of the resilience evaluation of each RSMA algorithm on each problem instance (once again, best values among all RMSA algorithms highlighted in bold for each problem instance).

First, note that when multiple nodes are shut down, there are some demands that cannot survive whatever RMSA is adopted. The obvious ones are the demands such that at least one of its end-nodes is a shutdown node. Then, in multiple node shutdowns that separate the network in different components: (i) unicast demands with end-nodes in different components cannot survive and (ii) anycast demands whose source node is in a network component without any of the DC nodes of its anycast service also cannot survive. So, on each random attack, the total demand that can survive is also computed and both evaluation parameters are determined as percentages of this total survivable demand. The last column "Surv. D." of Table D.4 presents the average total bit-rate that can survive among all 500 random attacks.

Table D.4: Resilience evaluation results.

N.	T	Average Non-Disrupted Demand (%)					Average Surviving Demand (%)					Surv. D.
		FF	SC	SPC	PSC	Mix	FF	SC	SPC	PSC	Mix	
Germany50	20	75.444	74.503	75.884	**77.491**	76.827	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	18.2
	45	76.520	75.149	75.867	**78.230**	77.320	99.694	99.790	**99.794**	99.751	99.780	40.7
	70	76.193	73.953	75.134	**78.014**	77.324	97.776	**98.626**	98.608	97.696	98.374	63.4
	95	75.360	74.217	75.273	–	**76.895**	93.972	95.614	**95.807**	–	94.344	85.9
	135	–	73.847	**74.689**	–	–	–	87.118	**87.205**	–	–	121.9
Cost266	15	71.751	72.998	73.309	73.829	**74.032**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	12.6
	30	71.135	71.335	71.361	**73.494**	73.180	97.657	**97.778**	97.758	97.568	97.690	25.3
	45	71.780	72.359	71.229	**73.801**	73.690	94.264	**95.035**	94.958	94.447	94.530	38.1
	60	71.193	71.520	71.695	–	**72.984**	89.430	89.684	**90.161**	–	89.279	50.9
	80	–	71.696	**71.903**	–	–	–	84.925	**85.063**	–	–	67.8
Janos-US	15	72.650	72.034	72.862	**73.945**	73.452	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	11.6
	30	70.973	69.104	69.611	**71.929**	71.187	98.538	**98.650**	98.516	98.346	98.496	23.3
	45	70.517	68.928	68.797	**71.562**	71.106	91.457	91.488	**91.726**	91.318	91.125	35.1
	55	–	68.988	69.376	–	**71.183**	–	88.086	**88.668**	–	88.011	43.0
	65	–	68.444	**69.458**	–	–	–	84.613	**85.306**	–	–	50.5

Regarding the Average Non-Disrupted Demand, the best results are provided, on average, by the PSC based RMSA (i.e., using the path disaster availability metric as the first measure in the *best assignment condition*). However, due to its low spectrum usage efficiency (already seen in the results of Table D.3), it can be used in practice only for light to medium loaded EONs. The Mix based RMSA is, on average, the second best algorithm and, as it can accommodate more total traffic demand, it becomes the best algorithm for the demand sets D that cannot be accommodated by the previous PSC based RMSA. Finally, for the demand sets D with the highest traffic, the SPC based RMSA provides the best results although closely followed by the SC based RMSA. Note that there is no case where either the FF or the SC based RMSA algorithms are better than all RMSA algorithms using the path disaster availability metric.

Regarding the Average Surviving Demand, all RSMA algorithms present similar results for the demand sets D of lower traffic (in fact, for the smallest traffic values considered in each topology, all RMSA algorithms were able to maintain 100% of all survivable demand). When the total demand becomes higher, then the SPC based RMSA becomes the best, on average, although closely followed by the SC based RMSA. Again, there is no case where the FF RMSA is better than all other algorithms.

Finally, it should be pointed out that, for a given problem instance, the percentage difference across all RMSA algorithms is never higher than 3% in Table D.4. The next tables show the resilient evaluation of the different RMSA algorithms in a different way by presenting the number (in percentage) of the 500 random attacks such that each RMSA algorithm (excluding the FF based RMSA) has provided the best resiliency value. Table D.5 presents the results for the Average Non-Disrupted Demand while Table D.6 presents the results for the Average Surviving Demand. In both cases, when a best value is given by multiple algorithms, it is accounted in the percentage of all of them (once again, best values highlighted in bold).

Table D.5: Percentage number of attacks such that each RMSA provides the best Average Non-Disrupted Demand value.

Network	T	SC	SPC	PSC	Mix
Germany50	20	22.8	13.0	**56.6**	17.0
	45	11.0	10.6	**54.4**	27.4
	70	10.4	2.8	**57.2**	31.6
	95	13.8	6.0	–	**81.0**
	135	27.4	**73.4**	–	–
Cost266	15	17.8	23.8	**43.6**	32.8
	30	26.4	9.2	**49.2**	22.8
	45	28.2	7.6	**43.0**	23.8
	60	25.6	11.0	–	**65.4**
	80	48.2	**52.8**	–	–
Janos-US	15	27.0	9.6	**54.0**	24.8
	30	7.6	20.0	**53.8**	26.6
	45	11.0	5.2	**58.6**	34.8
	55	18.4	13.0	–	**72.8**
	65	30.0	**72.2**	–	–

Regarding the Average Non-Disrupted Demand, the results in Table D.5 highlight the conclusions taken from Table D.4. For the three lowest traffic instances of all topologies, the PSC based RMSA is the best algorithm on 52.3% of the attacks (among 4 algorithms); then, for the fourth traffic instance of all topologies, the Mix based RMSA becomes the best algorithm on 73.1% of the attacks (among 3 algorithms); finally, for the highest traffic instance of all topologies, the SPC based RMSA is the best algorithm on 66.1% of the attacks (among

Table D.6: Percentage number of attacks such that each RMSA provides the best Average Surviving Demand value.

Network	T	SC	SPC	PSC	Mix
Germany50	20	**100.0**	**100.0**	**100.0**	**100.0**
	45	**98.2**	98.0	96.2	97.0
	70	**89.8**	87.2	58.6	75.8
	95	64.0	**74.8**	–	21.4
	135	27.4	**73.4**	–	–
Cost266	15	**100.0**	**100.0**	**100.0**	**100.0**
	30	**89.0**	**89.0**	82.6	86.2
	45	**78.4**	73.2	58.2	59.4
	60	46.4	**58.2**	–	27.4
	80	52.0	**54.0**	–	–
Janos-US	15	**100.0**	**100.0**	**100.0**	**100.0**
	30	**93.4**	90.4	83.6	86.2
	45	51.0	**61.0**	45.6	37.4
	55	40.6	**65.4**	–	33.4
	65	40.4	**73.2**	–	–

2 algorithms).

Regarding the Average Surviving Demand, again the results in Table D.6 confirm the conclusions taken from Table D.4. For the lowest traffic instance of each topology, all RSMA algorithms were able to maintain 100% of all demand that can survive. For the problem instances with growing traffic demand, the SPC based RMSA becomes the best, on average, and the SC based RMSA becomes the second best algorithm.

In the overall, the trade-off analysis between spectrum usage efficiency (Table D.3) and resiliency to multiple node failures (Tables D.4, D.5 and D.6) among the different RMSA algorithms is as follows. First, the FF RMSA is worst than all other algorithms, on average, as it is one of the algorithms with the lowest spectrum usage efficiency and, for all cases, it never provides the best resilience to multiple node failures. This comes without surprise, although we have adopted a "more sophisticated" variant, as described in Section III.

Then, comparing the RMSA algorithms using the disaster path availability metric (SPC, PSC and Mix) with the previously known SC based RMSA, we can conclude that the 3 alternatives provide 3 different trade-offs. The PSC alternative provides significant better resiliency at the cost of a significantly lower spectrum usage efficiency. The SPC alternative provides slightly better resiliency with the same spectrum usage efficiency. Finally, the Mix alternative is a trade-off between the two previous ones providing an intermediate level of resiliency gain at the cost of an intermediate penalty of spectrum usage efficiency.

As a consequence, the best RMSA algorithm depends on the traffic load of the EON. For lightly loaded networks, since spectrum resources are abundant, the PSC based RMSA is the best alternative as an higher percentage of non-disrupted demand can be provided. For medium loaded networks, the Mix based RMSA is the best alternative for the cases such that the previous algorithm cannot accommodate all the traffic. For heavily loaded networks, the

SPC based RMSA is still better than the previous known SC based RMSA as it has the same spectrum usage efficiency and it is better (at least slightly) in both the non-disrupted demand percentage and surviving demand percentage.

Table D.7 presents the total running time, in seconds, of the k-shortest paths algorithm (column "k-SP"), which is common to all algorithms, and of each RSMA algorithm on the highest demand problem instance of each network such that the algorithm has accommodated all the traffic (i.e, the RMSA algorithm was able to assign lightpaths to all demands). For each algorithm, the total running time is the sum of its runtime with the k-shortest paths algorithm runtime.

Table D.7: Running time (in seconds) of each RMSA algorithm in the regular state.

Network	T	k-SP	FF	SC	SPC	PSC	Mix
Germany50	70	14.7	1.2	0.8	0.9	0.9	0.9
Cost266	45	4.9	0.5	0.2	0.2	0.3	0.3
Janos-US	45	1.7	0.5	0.2	0.2	0.2	0.2

Table D.7 shows that the pre-computation of the set of candidate paths for all demands is much more time-consuming than the RMSA itself. Moreover, because the FF strategy requires ordering the set of demands, it presents a higher runtime than all other RMSA algorithms. Finally, and more importantly, the disaster path availability metric does not impose any runtime penalty in the RMSA decision, when compared with the previously known SC based RMSA algorithm.

Finally, Table D.8 presents the average running time per attack (among all 500 attacks), in seconds, of each RSMA algorithm on the same problem instances used in the previous table. In this case, the values include the computation of the k-shortest paths for all demands with disrupted lightpaths as these demand sets vary between the different cases.

Table D.8: Average running time (in seconds) of each RMSA algorithm per attack.

Network	T	FF	SC	SPC	PSC	Mix
Germany50	70	4.237	4.644	4.361	3.958	3.991
Cost266	45	1.598	1.624	1.645	1.527	1.538
Janos-US	45	0.548	0.568	0.572	0.531	0.537

Table D.8 shows that the running times are very similar among all algorithms but the RMSA algorithms that prioritize the path disaster availability metric (PSC and Mix) are slightly faster, on average, than the others. Since these algorithms provide better average non-disrupted demand, the total number of demands whose lightpaths are disrupted is lower, on average, and so these RMSA algorithms have a lower number of demands for lightpath reassignment.

D.5 Conclusions

In this work, we have proposed a family of RMSA algorithms resilient to multiple node failures due to malicious human activities. First, we have assumed that an attacker “discovers” with some estimated probabilities a set of nodes to be attacked and we have proposed a path disaster availability metric that measures the probability of each path not being affected by the attacked nodes. Then, the path disaster availability metric was included in the RMSA decision in three different alternative ways (SPC, PSC and Mix).

The resulting algorithms were compared with the simplest first-fit algorithm and with a previously known RMSA algorithm in terms of spectrum usage efficiency, average non-disrupted demand and the average surviving demand.

The results have shown that the RMSA decision is always better when the disaster path availability metric is included but the best algorithm depends on the traffic load of the EON. For lightly loaded networks, the PSC based RMSA is the best alternative as an higher percentage of non-disrupted demand can be provided. For medium loaded networks, the Mix based RMSA is the best alternative for the cases such that the previous algorithm cannot accommodate all the traffic. For heavily loaded networks, the SPC based RMSA is still better than the previous known algorithm as it has the same spectrum usage efficiency and it is better (at least slightly) in both the non-disrupted demand percentage and surviving demand percentage.

Finally, the computational results have also shown that the use of the disaster path availability metric in the RMSA decision does not impose any runtime penalty in any of the 3 proposed alternatives.

Bibliography

[AR17] F. Abkenar and A. Rahbar. *Study and analysis of routing and spectrum allocation (RSA) and routing, modulation and spectrum allocation (RMSA) algorithms in elastic optical networks (EONs).* Optical Switching and Networking, 23:5–39, 2017.

[BdSA18] F. Barbosa, A. de Sousa, and A. Agra. *Topology design of transparent optical networks resilient to multiple node failures.* In 10th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 1–8, 2018.

[BdSA19] F. Barbosa, A. de Sousa, and A. Agra. *Evaluation and design of elastic optical networks resilient to multiple node failures.* In 15th International Conference on the Design of Reliable Communication Networks (DRCN), pages 154–161, 2019.

[CSO15] B. Chatterjee, N. Sarma, and E. Oki. *Routing and spectrum allocation in elastic optical networks: a tutorial.* IEEE Communications Surveys Tutorials, 17(3):1776–1800, 2015.

[CTV11] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos. *Elastic bandwidth allocation in flexible OFDM-based optical networks.* Journal of Lightwave Technology, 29(9):1354–1366, 2011.

[CZJZ15] X. Chen, S. Zhu, L. Jiang, and Z. Zhu. *On spectrum efficient failure-independent path protection p-cycle design in elastic optical networks.* Journal of Lightwave Technology, 33(17):3719–3729, 2015.

[FWG⁺16] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, M. Gushev, and J. Marzo. *An overview of security challenges in communication networks.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 43–50. IEEE, 2016.

[GK19] R. Goścień and M. Kucharzak. *On the efficient optimization of unicast, anycast and multicast flows in survivable elastic optical networks.* Optical Switching and Networking, 31:114–126, 2019.

[GTE⁺16] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore. *A survey of strategies for communication networks to protect against large-scale natural disasters.* In 8th International Workshop on Resilient Networks Design and Modeling (RNDM), pages 11–22, 2016.

[GWK15] R. Goścień, K. Walkowiak, and M. Klinkowski. *Tabu search algorithm for routing, modulation and spectrum allocation in elastic optical network with anycast and unicast traffic.* Computer Networks, 79:148–165, 2015.

[KRS⁺16] P. Khodashenas, J. Rivas-Moscoso, D. Siracusa, F. Pederzolli, B. Shariati, D. Klonidis, E. Salvadori, and I. Tomkos. *Comparison of spectral and spatial superchannel allocation shemes for SDM networks.* Journal of Lightwave Technology, 34(11):2710–2716, 2016.

[KW11] M. Klinkowski and K. Walkowiak. *Routing and Spectrum Assignment in Spectrum Sliced Elastic Optical Path Network.* IEEE Communications Letters, 15(8):884–886, 2011.

[OWPT10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski. *SNDlib 1.0 - survivable network design library.* Networks, 55(3):276–286, 2010.

[PAK⁺12] E. Palkopoulou, M. Angelou, D. Klonidis, K. Christodoulopoulos, A. Klekamp, F. Buchali, E. Varvarigos, and I. Tomkos. *Quantifying spectrum, cost, and energy efficiency in fixed-grid and flex-grid networks* [invited]. IEEE/OSA Journal of Optical Communications and Networking, 4(11):B42–B51, 2012.

[RBMT17] C. Rottondi, P. Boffi, P. Martelli, and M. Tornatore. *Routing, modulation format, baud rate and spectrum allocation in optical metro rings with flexible grid and few-mode transmission.* Journal of Lightwave Technology, 35(1):61–70, 2017.

[TR17] S. Talebi and G. Rouskas. *On distance-adaptive routing and spectrum assignment in mesh elastic optical networks.* IEEE/OSA Journal of Optical Communications and Networking, 9(5):456–465, 2017.

[WK13] K. Walkowiak and M. Klinkowski. *Joint anycast and unicast routing for elastic optical networks: Modeling and optimization.* In IEEE International Conference on Communications (ICC), pages 3909–3914, 2013.

[WNG17] J. Wu, Z. Ning, and L. Guo. *Energy-efficient survivable grooming in software-defined elastic optical networks.* IEEE Access, 5:6454–6463, 2017.