

Técnicas para Compartilhamento de Proteção Multicaminho em Redes de Comunicação de Alta Capacidade

Trabalho de Conclusão de Curso

Engenharia de Computação

Michael Matheus de Lima Cavalcanti
Orientador: Daniel Augusto Ribeiro Chaves

**Universidade de Pernambuco
Escola Politécnica de Pernambuco
Graduação em Engenharia de Computação**

Michael Matheus de Lima Cavalcanti

**Técnicas para Compartilhamento de
Proteção Multicaminho em Redes de
Comunicação de Alta Capacidade**

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia de Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, outubro de 2022.

Cavalcanti, Michael Matheus de Lima

Técnicas para compartilhamento de proteção multicaminho em redes de comunicação de alta capacidade / Michael Matheus de Lima Cavalcanti. – Recife - PE, 2022.

xiv, 41 f. : il. ; 29 cm.

Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) Universidade de Pernambuco, Escola Politécnica de Pernambuco, Recife, 2022.

Orientador: Prof. Dr. Daniel Augusto Ribeiro Chaves.

Inclui referências.

1. Redes ópticas elásticas. 2. Provisionamento multicaminho. 3. Largura de Banda Espremida. I. Título. II. Chaves, Daniel Augusto Ribeiro. III. Universidade de Pernambuco.

MONOGRAFIA DE FINAL DE CURSO

Avaliação Final (para o presidente da banca)*

No dia 31/10/2022, às 15h00min, reuniu-se para deliberar sobre a defesa da monografia de conclusão de curso do(a) discente **MICHAEL MATHEUS DE LIMA CAVALCANTI**, orientado(a) pelo(a) professor(a) **DANIEL AUGUSTO RIBEIRO CHAVES**, sob título Técnicas para Compartilhamento de Proteção Multicaminho em Redes de Comunicação de Alta Capacidade, a banca composta pelos professores:

CARMELO JOSE ALBANEZ BASTOS FILHO (PRESIDENTE)

DANIEL AUGUSTO RIBEIRO CHAVES (ORIENTADOR)

Após a apresentação da monografia e discussão entre os membros da Banca, a mesma foi considerada:

Aprovada Aprovada com Restrições* Reprovada

e foi-lhe atribuída nota: 10,0 (Dez)

*(Obrigatório o preenchimento do campo abaixo com comentários para o autor)

O(A) discente terá sete dias para entrega da versão final da monografia a contar da data deste documento.



AVALIADOR 1: Prof (a) **CARMELO JOSE ALBANEZ BASTOS FILHO**



AVALIADOR 2: Prof (a) **DANIEL AUGUSTO RIBEIRO CHAVES**

AVALIADOR 3: Prof (a)

* Este documento deverá ser encadernado juntamente com a monografia em versão final.

Este trabalho é dedicado à minha mãe, namorada e todos os meus amigos que de alguma forma me apoiaram e contribuíram com minha evolução.

Agradecimentos

Primeiramente gostaria de agradecer à minha família, em especial a minha mãe por todo apoio durante os anos de dedicação ao curso. A minha namorada Ingrid Alves pelo apoio e paciência durante os anos de dedicação ao curso. Aos amigos que fiz Matheus Albert, Matheus Alves, Murilo Stodolni, Nilton Vieira e Richard Jeremias que compartilharam comigo várias horas de estudo e confecção de atividades acadêmicas.

Gostaria de agradecer também a mestrandas Gabriela Teixeira e o professor Henrique Dinarte por compartilharem seus conhecimentos e me ajudarem com a confecção deste trabalho.

E por fim, gostaria de agradecer ao meu orientador, o professor Daniel Chaves, por me aceitar como orientando e compartilhar seus conhecimentos e experiências acadêmicas.

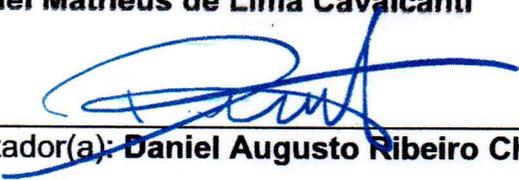
Autorização de publicação de PFC

Eu, **Michael Matheus de Lima Cavalcanti** autor(a) do projeto de final de curso intitulado: **Técnicas para Compartilhamento de Proteção Multicaminho em Redes de Comunicação de Alta Capacidade**; autorizo a publicação de seu conteúdo na internet nos portais da Escola Politécnica de Pernambuco e Universidade de Pernambuco.

O conteúdo do projeto de final de curso é de responsabilidade do autor.

Michael Matheus de Lima Cavalcanti

Michael Matheus de Lima Cavalcanti


Orientador(a): Daniel Augusto Ribeiro Chaves

Coorientador(a):



Prof, de TCC: **Daniel Augusto Ribeiro Chaves**

Data: 31/10/2022

Resumo

Devido ao crescimento nas demandas de transmissão de dados, as redes ópticas por possuírem a capacidade de prover altas taxas de transmissão têm sido bastante utilizadas no atendimento dessa demanda. As redes ópticas elásticas têm sido adotadas devido às suas características mais flexíveis. No entanto, essas redes também estão sujeitas a falha. A ocorrência de falhas pode gerar uma grande perda de dados e conseqüentemente gerar um impacto na receita dos fornecedores e de seus clientes. Portanto, a resiliência é um requisito essencial para essas redes. A sobrevivência é uma estratégia de resiliência. Vários mecanismos de sobrevivência podem ser aplicados para promover resiliência para as redes. Um desses mecanismos são os esquemas de proteção. Entre os esquemas de proteção o provisionamento multicaminho é uma técnica que permite dividir a taxa de transmissão requisitada em partições que são transmitidas por caminhos ópticos disjuntos. A técnica largura de banda espremida permite uma redução da largura de banda requisitada durante a ocorrência de uma falha. A associação entre essas duas técnicas pode promover uma melhoria no desempenho da rede. Porém a combinação desses mecanismos ainda pode gerar um consumo ineficiente de recursos. Além disso, é sabido que em uma rede real há tantos clientes e serviços que demandam alta disponibilidade quanto clientes e serviços que não demandam tal exigência. Esse tráfego heterogêneo em termos de demanda de resiliência pode gerar oportunidades para melhorar a eficiência do uso dos recursos de rede. Este trabalho propõe um algoritmo para otimizar a alocação de recursos utilizados pela combinação dessas duas técnicas em uma rede real sujeita a tráfego heterogêneo. É proposta uma estratégia com o objetivo de reutilizar os recursos ociosos devido a combinação das técnicas durante a operação normal da rede para atendimento de requisições de dois tipos: as que solicitam e as que não solicitam mecanismos de sobrevivência. Os resultados obtidos nas simulações mostram uma melhoria acima de 40% nos cenários para as cargas mais baixas, porém com o aumento progressivo de cargas essa melhoria vai diminuindo ficando abaixo de 10% para cargas mais altas.

Palavras-chave: Redes ópticas elásticas, provisionamento multicaminho, largura de banda espremida, reutilização, recursos ociosos.

Abstract

Due to the growth in data transmission demands, optical networks, for having the ability to provide high transmission rates, have been widely used to meet this demand. Elastic optical networks have been adopted due to their more flexible characteristics. However, these networks are also prone to failure. The occurrence of failures can generate a great loss of data and consequently generate an impact on the revenue of suppliers and their customers. Therefore, resilience is an essential requirement for these networks. Survival is a resilience strategy. Several survivability mechanisms can be applied to promote resilience to networks. One such mechanism is protection schemes. Among the protection schemes, multipath provisioning is a technique that allows dividing the requested transmission rate into partitions that are transmitted by disjoint optical paths. The bandwidth squeezed technique allows a reduction in the bandwidth requested during the occurrence of a failure. The association between these two techniques can promote an improvement in network performance. However, the combination of these mechanisms can still generate an inefficient consumption of resources. Furthermore, it is known that in a real network there are as many clients and services that demand high availability as clients and services that do not. This heterogeneous traffic in terms of resilience demand can generate opportunities to improve the efficiency of the use of network resources. This work proposes an algorithm to optimize the allocation of resources used by the combination of these two techniques in a real network subject to heterogeneous traffic. A strategy is proposed with the objective of reusing idle resources due to the combination of techniques during the normal operation of the network to attend to requests of two types: those that request and those that do not request survival mechanisms. The results obtained in the simulations show an improvement above 40% in the scenarios for the lowest loads, but with the progressive increase in loads, this improvement decreases, being below 10% for higher loads.

Keywords: Elastic optical network, multipath provisioning, bandwidth squeezed restoration, reutilization, idle resources.

Lista de ilustrações

Figura 1 – Cabos Ópticos.....	17
Figura 2 – WDM.....	18
Figura 3 – Alocação de Sinais em uma Rede WDM.....	18
Figura 4 – Alocação WDM e EON.....	19
Figura 5 – Restrição de Continuidade e Contiguidade no Espectro Óptico	20
Figura 6 – Representações de um Grafo	21
Figura 7 – Topologia NsfNet	21
Figura 8 – NsfNet - Topologia com Custos Definidos.....	22
Figura 9 – Fluxograma do Algoritmo First Fit.....	24
Figura 10 – Rompimento de Fibra Óptica por Escavação	25
Figura 11 – Caminhão Preso em Cabos Ópticos	25
Figura 12 – Resiliência em Redes de Comunicações	26
Figura 13 – Mecanismos de Sobrevivência.....	27
Figura 14 – Proteção Dedicada 1+1.....	30
Figura 15 – Proteção Dedicada 1:1.....	30
Figura 16 – Proteção Compartilhada.....	31
Figura 17 – Ferramenta CLion	32
Figura 18 – Provisionamento Multicaminho.....	33
Figura 19 – MPP e BSR.....	34
Figura 20 – Funcionamento do Algoritmo IBR.....	36
Figura 21 – Pseudocódigo do IBR.....	37
Figura 22 – Pseudocódigo Requisição Protegida.....	39
Figura 23 – Pseudocódigo Requisição Não Protegida	40
Figura 24 – Pseudocódigo Requisição Normal.....	41
Figura 25 – Topologias: (a) NsfNet, (b) Germany e (c) European	43
Figura 26 – Probabilidade de Bloqueio em Função da Carga para NsfNet.....	44
Figura 27 – Variação da Probabilidade de Bloqueio Para NsfNet	45
Figura 28 – Probabilidade de Bloqueio em Função da Carga para Germany	46
Figura 29 – Variação da Probabilidade de Bloqueio para Germany	47

Figura 30 – Probabilidade de Bloqueio em Função da Carga para European	48
Figura 31 – Variação da Probabilidade de Bloqueio para European	49
Figura 32 – Abordagem para Trabalhos Futuros.....	51

Lista de tabelas

Tabela 1 – Parâmetros Usados nas Simulações.....	42
Tabela 2 – Resultados de Probabilidade de Bloqueio para NsfNet	44
Tabela 3 – Resultados da Variação da Probabilidade de Bloqueio para NsfNet	45
Tabela 4 – Resultados de Probabilidade de Bloqueio para Germany.....	46
Tabela 5 – Resultados da Variação da Probabilidade de Bloqueio para Germany ...	47
Tabela 6 – Resultados de Probabilidade de Bloqueio para European.....	48
Tabela 7 – Resultados da Variação da Probabilidade de Bloqueio para European ..	49

Lista de abreviaturas e siglas

BSR – Bandwidth Squeezed Restoration

DPP – Dedicated Path Protection

EON – Elastic Optical Network

IBR – Idle Bandwidth Reuse

MPP – Multipath Provisioning

MPR – Multipath Routing

RSA – Routing and Spectrum Allocation

RWA – Routing and Wavelength Assignment

SLA – Service Level Agreement

SBPP – Shared Backup Path Protection

ScRG – Serviços com Resiliência Garantida

SsRG – Serviços sem Resiliência Garantida

SPP – Single Path Provisioning

WDM – Wavelength Multiplexing Division

Sumário

CAPÍTULO 1 INTRODUÇÃO.....	14
1.1 MOTIVAÇÃO	14
1.2 OBJETIVOS.....	16
1.2.1 Objetivo Geral	16
1.2.2 Objetivos Específicos	16
1.3 ESTRUTURA DO DOCUMENTO.....	16
CAPÍTULO 2 FUNDAMENTAÇÃO TEÓRICA	17
2.1 REDES ÓPTICAS	17
2.1.1 Multiplexação por Comprimento de Onda	18
2.1.2 Redes Ópticas Elásticas.....	19
2.1.3 Roteamento e Alocação de Espectro	20
2.2 TOPOLOGIA	21
2.2.1 Grafos	21
2.2.2 Backbone	21
2.3 ALGORITMOS DE ROTEAMENTO	22
2.3.1 Roteamento Multicaminho.....	23
2.4 ALGORITMOS DE ALOCAÇÃO ESPECTRAL	23
2.4.1 First Fit	24
2.5 FALHAS.....	24
2.6 RESILIÊNCIA.....	25
2.6.1 Sobrevivência.....	27
2.7 ESQUEMAS DE RESTAURAÇÃO	28
2.7.1 Restauração por Enlace	28
2.7.2 Restauração por Subcaminho	28
2.7.3 Restauração por Caminho.....	28
2.8 ESQUEMAS DE PROTEÇÃO.....	29
2.8.1 Proteção de Caminho Dedicado.....	29
2.8.2 Proteção de Caminho Compartilhado.....	31
2.9 PROTEÇÃO COM BANDA ESPREMIDA.....	31

CAPÍTULO 3 METODOLOGIA.....	32
3.1 SIMEON.....	32
3.2 MÉTRICAS DE DESEMPENHO.....	33
3.3 PROTEÇÃO COM MPP.....	33
3.4 TRÁFEGO COM DEMANDAS HETEROGÊNEAS DE RESILIÊNCIA.....	35
CAPÍTULO 4 ALGORITMO PARA REUTILIZAÇÃO DE BANDA OCIOSA	36
CAPÍTULO 5 RESULTADOS	42
5.1 PREMISSAS DE SIMULAÇÃO.....	42
5.2 RESULTADOS DAS SIMULAÇÕES	44
5.2.1 Resultados para a Topologia NsfNet.....	44
5.2.2 Resultados para a Topologia Germany	46
5.2.3 Resultados para a Topologia European	48
CAPÍTULO 6 CONCLUSÃO.....	50
6.1 CONCLUSÃO.....	50
6.2 TRABALHOS FUTUROS.....	51
REFERÊNCIAS	52

Capítulo 1 Introdução

Este capítulo é dedicado à apresentação da monografia. Inicialmente é descrito a motivação pela qual o tema proposto foi escolhido. Em segundo, são retratados os objetivos traçados para com a finalização do projeto. E por fim, o detalhamento da estruturação dos demais capítulos desta monografia.

1.1 Motivação

Com o avanço tecnológico o mundo encontra-se cada vez mais conectado à internet, segundo pesquisa TIC Domicílios (RODRIGUES, 2022), em 2021 aproximadamente 82% dos domicílios brasileiros possuem acesso à internet. Com mais acesso à internet, conseqüentemente têm-se um maior tráfego de internet. Um estudo feito pela SimilarWeb (CARNEIRO, 2020) aponta o Brasil como o 4º país com maior tráfego de internet do mundo. E a tendência é de aumento no tráfego. O Brasil Internet Exchange (IX.br), projeto do Comitê Gestor da Internet no Brasil (CGI.br) que promove e cria a infraestrutura necessária para a interconexão direta entre as redes que compõem a Internet Brasileira, alcançou uma marca histórica no dia 6/12/2021 e atingiu o pico de 20 Tbits/s de troca de tráfego na internet, 43% a mais do que o registrado no mesmo mês de 2020 (TELE.SINTESE, 2021).

A base infraestrutural que permite que a internet funcione são chamadas de redes *backbones*. Os *backbones* são compostos por cabos de fibra ótica, de longa distância e alta capacidade de transmissão (MOTTA, 2012). São responsáveis pelo envio e recebimento dos dados entre diferentes localidades (NASCIMENTO, 2012).

As redes ópticas também estão sujeitas a falhas, as causas mais comuns são:

- Interrupção de linha: É causada por uma fibra ótica danificada ou rompida, que pode ser ocasionada por escavações sem supervisão, quedas de árvores, incêndios, terremotos, entre outros. (SOUZA, 2006);
- Falhas de hardware: Falhas nos circuitos eletrônicos de transmissores ou receptores (RAMASWAMI, 2009);

Sobrevivência é a capacidade de um sistema em absorver e contornar os efeitos de uma falha de forma que não haja interrupção dos serviços (FREITAS, 2012).

Mecanismos podem ser utilizados para promover sobrevivência em redes ópticas, os mecanismos de sobrevivência podem ser classificados em esquemas de restauração e esquemas de proteção (XAVIER, 2016).

A restauração de rede é o processo de rearranjar as rotas através dos recursos disponíveis distribuídos por toda a rede (LOURENÇO, 2015). Os Esquemas de restauração são baseados na descoberta dinâmica de recursos após a ocorrência da falha (XAVIER, 2016).

A proteção de rede consiste em reservar recursos para o uso dedicado na transmissão do tráfego afetado por uma falha na rede. A proteção é um mecanismo proativo, pois os recursos são reservados no momento do estabelecimento da conexão, antes da ocorrência de qualquer falha (LOURENÇO, 2015).

Os esquemas de proteção, comumente, utilizam dois tipos de provisionamento: o provisionamento de caminho único (*Single Path Provisioning* - SPP) e o provisionamento multicaminho (*Multipath Provisioning* - MPP). No SPP, um caminho óptico de trabalho é protegido com um ou mais caminhos de proteção disjuntos. Entretanto, a taxa de transmissão requisitada não é particionada entre os caminhos. O segundo tipo, o MPP, propõe o particionamento da taxa de transmissão requisitada em múltiplas parcelas de menores taxas de transmissão, e a sua transmissão é feita de forma simultânea por múltiplos caminhos disjuntos (DINARTE, 2021).

Proteção com largura de banda espremida (*Bandwidth Squeezed Restoration* – BSR) é um conceito onde é possível atribuir aos caminhos ópticos atingidos por uma falha uma largura de banda mais estreita do que sua largura de banda original. A largura de banda pós falha para cada caminho óptico é determinada por um acordo de nível de serviço (*Service Level Agreement* – SLA) realizado entre cliente e fornecedor (ASSIS, 2012).

Nesse contexto, é proposto para este trabalho uma estratégia combinando os conceitos de MPP com BSR. Durante a operação normal do tráfego, o esquema realiza o particionamento da taxa de transmissão considerando a reserva de recursos de forma que em caso de falha de uma das rotas a taxa de transmissão ainda respeita o nível de SLA acordado. A taxa de transmissão necessária para operação normal é ocupada e a taxa de transmissão excedente é reservada. Enquanto a taxa reservada estiver ociosa pode ser utilizada por serviços que, segundo o SLA, não demandam esquema de proteção. O intuito é promover economia nos recursos disponíveis e diminuir a probabilidade de bloqueio de novas requisições.

1.2 Objetivos

1.2.1 Objetivo Geral

Este trabalho tem como objetivo principal definir uma estratégia e desenvolver um algoritmo com o intuito de utilizar os recursos de rede ociosos reservados para serviços de rede que utilizam provisionamento multicaminho combinado com o conceito de proteção com largura de banda espremida, por tráfego de serviços de rede de baixa prioridade que não demandem ou não necessitam de proteção, promovendo a redução e/ou otimização na utilização dos recursos de rede respeitando os acordos de nível de serviço.

1.2.2 Objetivos Específicos

Como objetivos específicos para o desenvolvimento deste trabalho, têm -se:

- Estudar e compreender a problemática dos mecanismos de sobrevivência;
- Implementar o conceito proposto;
- Avaliar os resultados obtidos utilizando o conceito proposto.

1.3 Estrutura do Documento

Este documento está dividido em cinco capítulos: Introdução, Fundamentação Teórica, Metodologia, Resultados e Conclusão. Este primeiro capítulo, contém as informações introdutórias sobre o trabalho onde foi descrito a motivação e objetivos para com a conclusão do trabalho além da estrutura do documento. No segundo capítulo, está exposta a fundamentação teórica que contém os conceitos necessário para a resolução do problema ao qual este trabalho se propõe. No capítulo seguinte, o terceiro, toda a metodologia necessária para a realização do trabalho e os experimentos realizados. O quarto capítulo concentra os resultados obtidos com a conclusão dos objetivos deste trabalho. Por fim, o quinto e último capítulo, contém as considerações finais sobre o desenvolvimento desta monografia e dos resultados que foram alcançados com a sua conclusão além de levantar possíveis pontos abordados em trabalhos futuros.

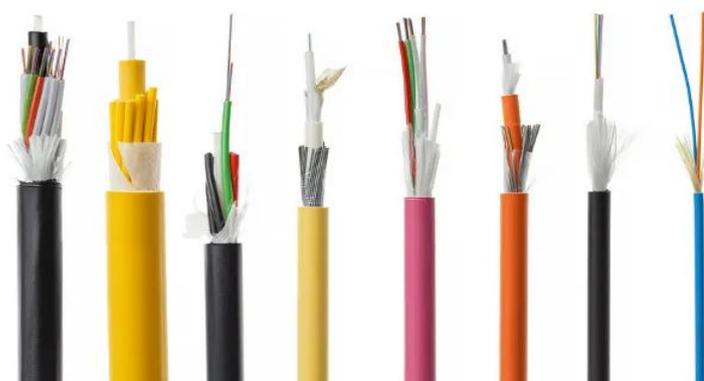
Capítulo 2 Fundamentação Teórica

Este capítulo tem como objetivo fundamentar os conceitos teóricos dos principais temas de estudo que foram alvo de estudo para o desenvolvimento desta monografia. Inicialmente são vistos os conceitos relacionados as redes ópticas e os mecanismos utilizados que propõe uma resolução para o problema citado.

2.1 Redes Ópticas

As fibras ópticas são filamentos flexíveis fabricados em materiais transparentes como fibras de vidro ou plástico e que são utilizadas como meio de propagação da luz. As fibras ópticas são geralmente muito finas, mas podem ter vários quilômetros de comprimento. Fibras ópticas têm diversas aplicações, sendo a transmissão de dados uma das mais comuns. As fibras ópticas também podem propagar mais de uma cor, ou comprimento de onda, em seu interior, permitindo que mais informações sejam transmitidas simultaneamente ao longo de uma única fibra óptica, esse processo é chamado de multiplexação (HELERBROCK, 2022).

Figura 1 – Cabos Ópticos



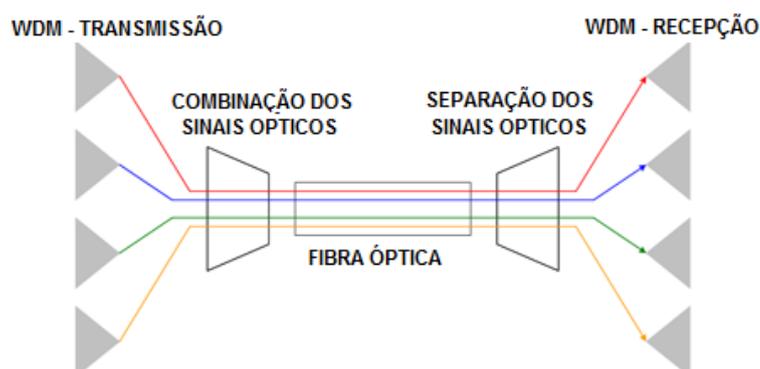
Fonte: Adaptado de (HELERBROCK, 2022).

A Figura 1 ilustra os vários tipos de cabos ópticos disponíveis. Uma rede óptica é um tipo de rede de comunicação de dados criada com a tecnologia de fibra óptica. Utiliza cabos de fibra óptica como principal meio de comunicação para converter e transmitir dados como pulsos de luz entre os nós emissores e receptores (TECHOPEDIA, 2022).

2.1.1 Multiplexação por Comprimento de Onda

A Multiplexação por Divisão do Comprimento de Onda (*Wavelength Multiplexing Division* – WDM) é a técnica de transmitir vários sinais simultaneamente em frequências diferentes por meio de uma única fibra óptica. É uma técnica para a utilização de uma fibra para transportar diversos canais ópticos separados e independentes, portanto, sem interferência. Os sinais são transmitidos em diferentes comprimentos de onda e transportam a informação por meio de uma única fibra com o objetivo de aumentar a capacidade de transmissão e, conseqüentemente, usar a largura de banda de maneira mais eficiente (MAURÍCIO, 2020).

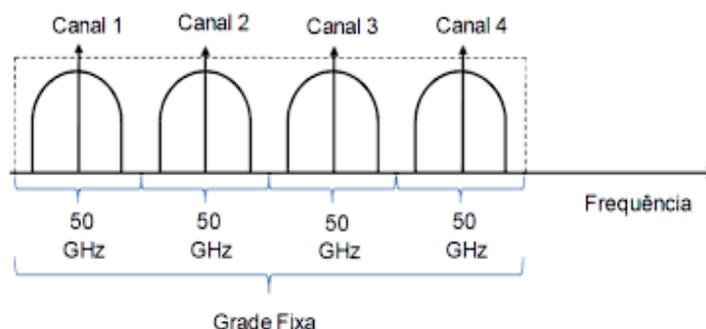
Figura 2 – WDM



Fonte: Adaptado de (MAURÍCIO, 2020).

A Figura 2 ilustra a técnica WDM. O uso da tecnologia WDM divide o espectro em faixas de largura de banda fixas, tornando a taxa de transmissão para cada comprimento de onda mais rígida. A Figura 3 ilustra a alocação de sinais em uma rede WDM, com grade fixa de 50 GHz (LIRA, 2016).

Figura 3 – Alocação de Sinais em uma Rede WDM

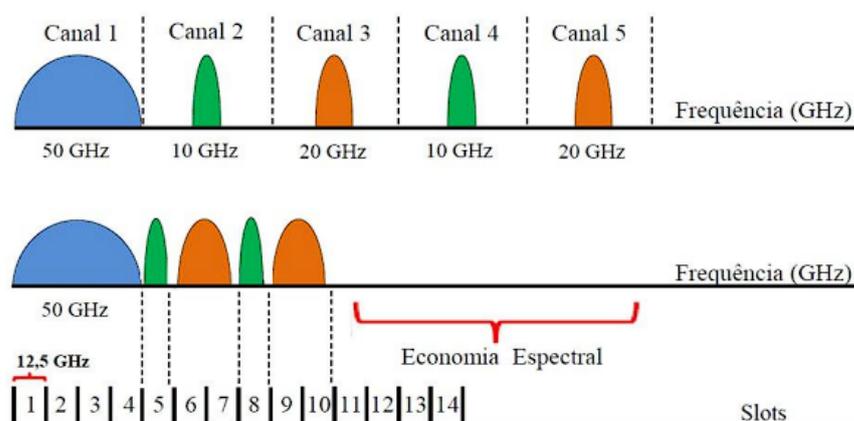


Fonte: Adaptado de (LIRA, 2016).

2.1.2 Redes Ópticas Elásticas

Diferentemente do que acontece nas redes WDM, as redes ópticas elásticas (*Elastic Optical Network – EON*) são capazes de fornecer um caminho óptico com largura de banda variável e, portanto, capaz de se adaptar às demandas de acordo com a taxa de dados a ser transmitida. O formato de modulação a ser escolhido para o estabelecimento da conexão pode depender da distância entre os nós de origem e destino, podendo coexistir nesse tipo de rede diversos formatos de modulação distintos. De maneira geral, nas EON, a largura de banda total de uma requisição será alocada com a utilização de uma determinada quantidade de *slots* na rede, fazendo com que o número de *slots* requisitados quantifique a demanda por largura de banda da requisição. Na Figura 4 compara-se a economia de espectro com a utilização da rede EON quando comparada com a tecnologia WDM (LIRA, 2016).

Figura 4 – Alocação WDM e EON



Fonte: Adaptado de (LIRA, 2016).

Observa-se na Figura 4 a economia espectral alcançada com a Rede EON. Ao se usar a tecnologia WDM um canal de largura fixa deve ser ocupado, no exemplo da Figura 4 a largura fixa do canal foi definida em 50 GHz e deve ser ocupada independentemente do tamanho da requisição. Por outro lado, na rede EON é possível selecionar apenas a quantidade de *slots* necessária para cada requisição. É importante também destacar o fato de que os filtros de largura fixada usados para delimitar os canais em uma rede WDM, não permitem requisições com largura maior que a de um canal. Essa limitação não ocorre nas EONS por possuírem filtros com larguras variáveis (LIRA, 2016).

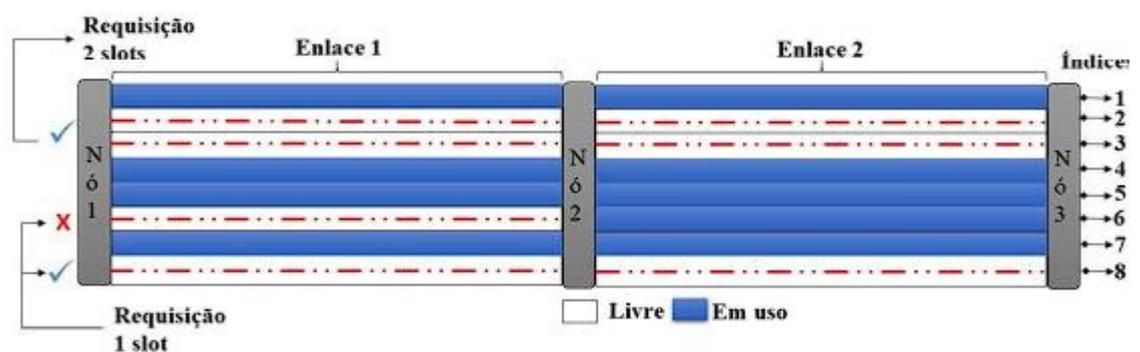
2.1.3 Roteamento e Alocação de Espectro

No estabelecimento das conexões em redes ópticas, um dos problemas fundamentais é rotear e alocar os recursos de espectro para acomodar as demandas de tráfego. Dessa forma, o tradicional problema de roteamento e atribuição de um comprimento de onda (*Routing and Wavelength Assignment – RWA*) aplicado em redes WDM é redefinido para redes ópticas elásticas como problema de roteamento e alocação de espectro (*Routing and Spectrum Allocation – RSA*) (CANDIA, 2014).

O RSA em EONs determina uma rota possível entre um determinado par origem/destino, posteriormente aloca o espectro necessário para a conexão ao longo da rota selecionada. O processo de estabelecer conexões dinamicamente cria fragmentação no espectro na rede, resultando na fragmentação da largura de banda e em seu desperdício (LIRA, 2020).

Para preservar a transmissão das informações nos enlaces é importante atender alguns requisitos do meio óptico denominados restrições de continuidade e contiguidade espectral (CORREIA, 2018). Na restrição de continuidade os *slots* escolhidos para alocação devem estar livres em todos os enlaces da rota, e para a restrição de contiguidade os *slots* devem estar adjacentes para serem alocados em requisições que necessitem de mais de dois para serem atendidas (CORREIA, 2018).

Figura 5 – Restrição de Continuidade e Contiguidade no Espectro Óptico



Fonte: Adaptado de (CORREIA, 2018).

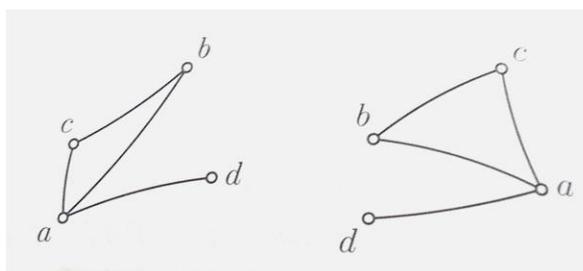
Na Figura 5 é possível observar que a requisição de 2 *slots* no índice 2 e 3 foi estabelecida devido aos *slots* disponíveis estarem adjacentes respeitando a restrição de contiguidade e livres em todos os enlaces respeitando a restrição de continuidade. O mesmo acontece para a requisição de 1 *slot* no índice 8, porém é possível observar que na requisição de 1 *slot* no índice 6 a requisição não possui disponibilidade no *slot* escolhido em um dos enlaces, desrespeitando a restrição de continuidade e consequentemente sendo bloqueada (CORREIA, 2018).

2.2 Topologia

2.2.1 Grafos

Graficamente uma rede óptica é representada por um grafo. Um grafo G consiste de um conjunto finito e não vazio $V(G)$ de objetos chamados vértices, juntamente com um conjunto $E(G)$ de pares não ordenados de vértices, os elementos de $E(G)$ são chamados de arestas. Podemos representá-lo por $G = (V; E)$, onde $V = V(G)$ e $E = E(G)$ (MELO, 2014).

Figura 6 – Representações de um Grafo



Fonte: Adaptado de (MELO, 2014).

Na Figura 6 observa-se duas formas de representação de um grafo. Nas redes ópticas os equipamentos transmissores e/ou receptores podem ser modelados por vértices de um grafo, enquanto as fibras ópticas que conectam esses equipamentos podem ser modeladas pelas arestas do mesmo grafo.

2.2.2 Backbone

A base infraestrutural que permite que a internet funcione são chamadas de redes *backbones*. Os *backbones* são compostos por cabos de fibra ótica, de longa distância e alta capacidade de transmissão (MOTTA, 2012). São responsáveis pelo envio e recebimento dos dados entre diferentes localidades (NASCIMENTO, 2012).

Figura 7 – Topologia NsfNet



Fonte: Adaptado de (SILVA, J. 2016).

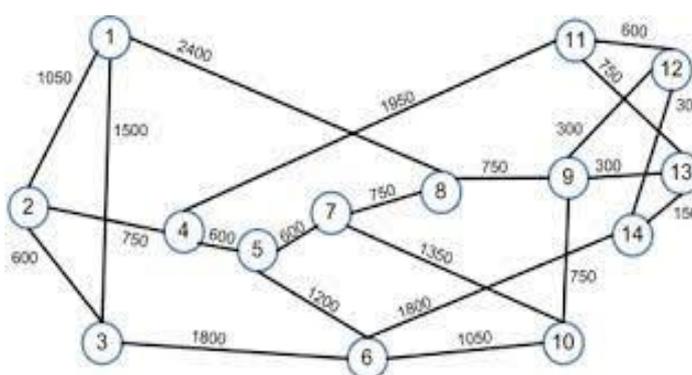
Na figura 7 está a representação da topologia do *backbone* NsfNet.

2.3 Algoritmos de Roteamento

Como mencionado anteriormente, é possível representar topologias de redes ópticas por meio de grafos.

Para que seja possível definir um ou mais caminhos ópticos entre um nó de origem e um nó de destino, é preciso atribuir valores às arestas. A expressão “custo” pode ser usada para referir estes valores, e estes valores podem ser definidos por parâmetros como a distância entre os nós, a capacidade de transmissão do enlace e etc. (JURKIEWICZ, 2009).

Figura 8 – NsfNet - Topologia com Custos Definidos



Fonte: Adaptado de (ZHU, 2015).

A Figura 8 ilustra a topologia NsfNet com custos definidos em suas arestas. Foram desenvolvidos vários algoritmos com o intuito de definir caminhos e minimizar custos, alguns dos algoritmos utilizados para definição de caminhos ópticos são:

- Dijkstra: É um algoritmo que calcula o caminho de custo mínimo entre dois nós (DIAS, 2022);
- Yen: É um algoritmo que calcula um número “n” de caminhos de custo mínimo entre dois nós, onde para $n = 1$ o algoritmo se comporta exatamente como o algoritmo de Dijkstra (NEO4J, 2022);
- BSR: É um algoritmo que calcula as rotas de menor caminho, e ao mesmo tempo, busca um melhor balanceamento de carga entre os enlaces de rede (SANTOS 2013);
- Roteamento Multicaminho: É um algoritmo que separa “k” grupos de “n” rotas disjuntas para dividir o tráfego entre eles (SANTI, 2011).

O algoritmo de roteamento utilizado neste trabalho é o Roteamento Multicaminho.

2.3.1 Roteamento Multicaminho

Devido ao crescimento no volume de transmissões, são pequenas as chances de encontrar um número suficiente de comprimento de onda no mesmo enlace de fibra óptica em uma única rota (SANTI, 2011).

O roteamento multicaminho tem como objetivo utilizar os recursos da rede através da utilização de múltiplos caminhos entre os pares origem-destino. O roteamento multicaminho tem potencial de agregar a banda passante de vários caminhos, permitindo a rede suportar taxas de transferência de dados maiores que o um roteamento por um único caminho (SANTI, 2015).

Primeiramente é necessário calcular um conjunto de caminhos para prover comunicação entre um par origem-destino. Duas características podem ser consideradas para determinar um conjunto de caminhos, a quantidade de caminhos e a independência entre caminhos. A quantidade de caminhos é o número de caminhos disponíveis entre os nós de origem e destino. Quanto maior este número, maiores são as chances de distribuição de carga. A independência entre caminhos considera os enlaces compartilhados entre os caminhos, caminhos independentes, ou seja, caminhos que não compartilham enlaces em comum, levam a melhor utilização dos recursos e menor probabilidade de congestionamento (SANTI, 2015).

O MPR é um algoritmo que separa uma quantidade “K” de grupos com uma quantidade “N” de rotas disjuntas, com o objetivo de realizar a divisão do tráfego entre essas rotas, buscando entre os grupos um grupo que possua capacidade de alocar a requisição solicitada.

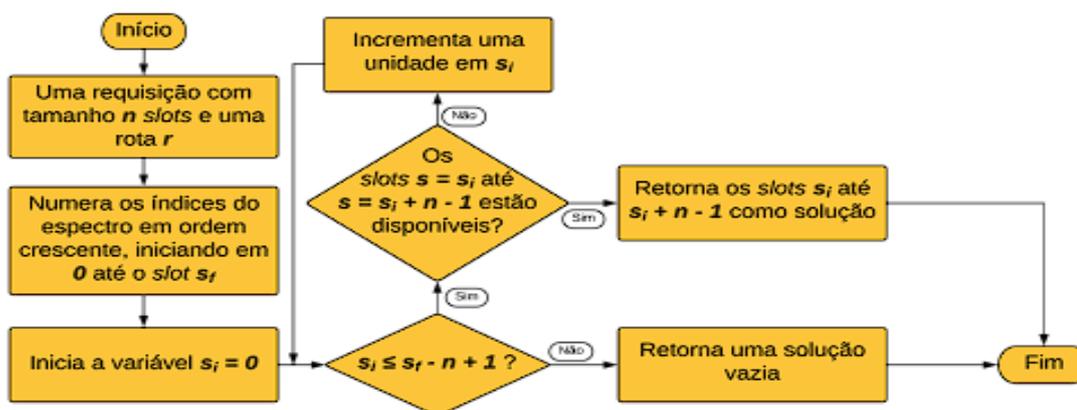
2.4 Algoritmos de Alocação Espectral

O algoritmo de alocação de espectro é o responsável por escolher a faixa de slots adequada para o estabelecimento do circuito óptico requisitado (FONTINELE, 2018). Dentre os métodos de alocação de espectro de fácil implementação e com baixa complexidade computacional têm-se o *first fit*, *random fit*, *last fit*, *best fit* e *exact fit* (FONTINELE, 2018). O algoritmo *First Fit* é o algoritmo escolhido para ser utilizado neste trabalho.

2.4.1 First Fit

O método *First Fit* é o mais utilizado na literatura. Nele, os *slots* são indexados e mantidos em uma lista com os *slots* disponíveis. No momento do estabelecimento de um circuito é escolhida uma faixa de *slots* disponíveis com os menores índices presentes na lista (FONTINELE, 2018).

Figura 9 – Fluxograma do Algoritmo First Fit



Fonte: Adaptado de (SANTOS, M. 2021).

A Figura 10 mostra o passo a passo de execução do método *First Fit*. O algoritmo ao receber uma requisição com tamanho “*n*” *slots* e uma rota “*r*”, numera os índices do espectro em ordem crescente, iniciando a variável de busca em zero e faz uma comparação. Se todos os *slots* já foram verificados levando em consideração o tamanho de *slots* da requisição recebida o algoritmo retorna uma solução vazia. Se houver *slots* para verificar que sejam suficientes para alocar a requisição, o algoritmo verifica se os *slots* estão disponíveis para alocação. Se os *slots* estiverem disponíveis o algoritmo retorna os *slots* necessários para alocação como solução, caso contrário o algoritmo incrementa em uma unidade a variável de busca e compara se todos os *slots* já foram verificados novamente.

2.5 Falhas

A ocorrência de falhas em nós ou em enlaces principalmente de *backbones* podem causar uma perda de uma enorme quantidade de dados devido ao potencial de transmissão de dados dessas redes. A falha na transmissão de dados pode gerar perda de receita para usuários e por consequência gerar prejuízos a operadoras de redes ópticas devido a multas contratuais relacionadas ao SLA (SILVA, R. 2014).

As causas mais comuns de falhas em redes ópticas são:

- Interrupção de linha: É causada por uma fibra ótica danificada ou rompida, que pode ser ocasionada por escavações sem supervisão, quedas de árvores, incêndios, terremotos, entre outros. (SOUZA, 2006);
- Falhas de *hardware*: Falhas nos circuitos eletrônicos de transmissores ou receptores ópticos (RAMASWAMI, 2009);

Figura 10 – Rompimento de Fibra Óptica por Escavação



Fonte: Adaptado de (SILVA, R. 2014).

Figura 11 – Caminhão Preso em Cabos Ópticos



Fonte: Adaptado de (SILVA, R. 2014).

A Figura 10 mostra um rompimento de fibra causado por escavação e a Figura 11 mostra cabos danificados por causa de um veículo preso entre eles.

2.6 Resiliência

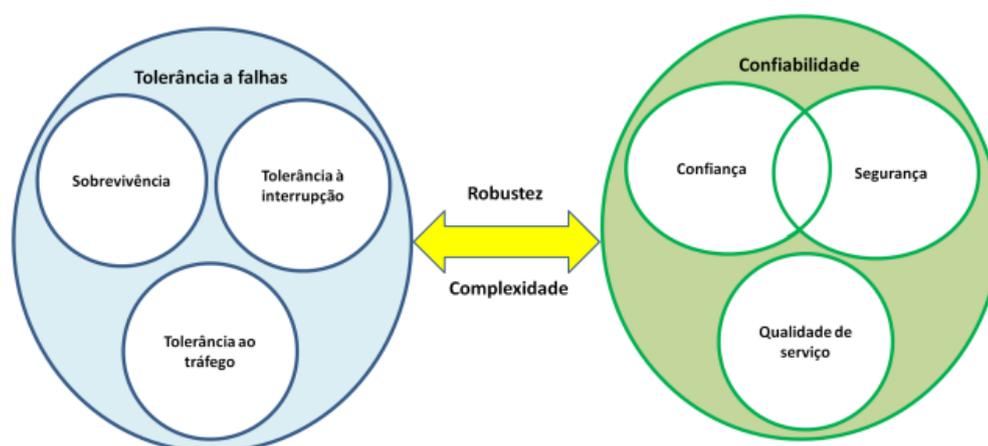
A resiliência é a habilidade de um sistema de manter-se operacional em um nível aceitável de funcionamento após a ocorrência de uma falha (SMITH, 2011).

Prover resiliência contra falhas em redes ópticas é um requisito importante e fundamental, pois como já mencionado, estas redes são responsáveis por transmitir um grande volume de dados e caso algum problema ocorra, uma perda volumosa de informação é inevitável, provocando diversos transtornos (FREITAS, 2018).

O escopo de pesquisa da resiliência pode ser dividido em duas categorias:

- Tolerância a falhas: Contempla as estratégias que possibilitam que as redes de comunicações possam continuar a prover serviços na ocorrência de falhas (FREITAS, 2018).
- Confiabilidade: Descreve os aspectos de confiabilidade dos serviços providos pelos sistemas de comunicações (FREITAS, 2018).

Figura 12 – Resiliência em Redes de Comunicações



Fonte: Adaptado de (Freitas, 2012).

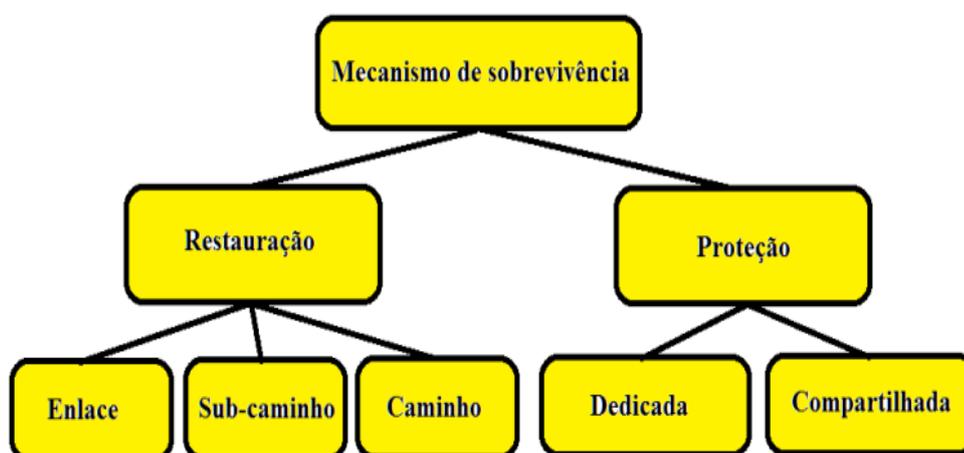
A Figura 12 mostra a divisão das categorias da resiliência.

- Sobrevivência: É a capacidade de um sistema em absorver e contornar efeitos de um eventual problema, de modo que não haja interrupção dos serviços (FREITAS, 2018).
- Tolerância à interrupção: É a capacidade que um sistema possui de lidar com a mobilidade dos dispositivos, com os atrasos longos na transmissão e com a restrição de energia (FREITAS, 2018).
- Tolerância a tráfego: Garante resiliência à rede na ocorrência de um tráfego inesperado (FREITAS, 2018).
- Confiança: Quantifica o grau de confiança que um serviço pode oferecer e consiste em dois principais aspectos: disponibilidade e confiabilidade (FREITAS, 2018).
- Segurança: É a propriedade de um sistema tomar medidas de precaução que garantam sua proteção contra acessos não autorizados (FREITAS, 2018).
- Qualidade de serviço: É a propriedade que avalia o desempenho especificado para um serviço (FREITAS, 2018).

2.6.1 Sobrevivência

Mecanismos podem ser utilizados para promover sobrevivência em redes ópticas, os mecanismos de sobrevivência podem ser classificados em esquemas de proteção e esquemas de restauração (XAVIER, 2016).

Figura 13 – Mecanismos de Sobrevivência



Fonte: Adaptado de (XAVIER, 2016).

A Figura 13 mostra como são divididos os mecanismos de sobrevivência. Os esquemas de proteção e restauração podem atuar com dois tipos de abordagens:

- Enlace: É reservado um ou mais enlaces redundantes para cada enlace que compõe o caminho óptico. Em caso de falha, somente o enlace em específico é protegido ou recuperado sendo realizada a comutação para seu respectivo enlace de proteção (SILVA, T. 2022).
- Caminho: É reservado um caminho óptico disjunto do caminho óptico principal. Em caso de alguma falha, é realizada a comutação do tráfego para o caminho óptico reservado (SILVA, T. 2022).

Os caminhos ópticos podem ser disjuntos em enlace ou nó. Um caminho disjunto em enlace é aquele em que não há enlaces em comum entre o caminho primário e o caminho secundário, mas pode conter nós em comum. Por outro lado, em um caminho disjunto em nó não existem intersecções entre os conjuntos de nós entre o caminho principal e o secundário (LOURENÇO, 2015).

2.7 Esquemas de Restauração

A restauração de rede é o processo de rearranjar as rotas através dos recursos disponíveis distribuídos por toda a rede (LOURENÇO, 2015). Os Esquemas de restauração são baseados na descoberta dinâmica de recursos após a ocorrência da falha (XAVIER, 2016). Os esquemas de restauração podem ser reativos ou proativos. No caso da restauração reativa após a ocorrência e detecção da falha, o algoritmo de restauração tenta encontrar um novo caminho óptico para restabelecer a conexão. No caso da restauração proativa é calculado um caminho de backup antes da falha, mas a reserva de recursos não é realizada (LOURENÇO, 2015).

A restauração é mais eficiente em termos de utilização dos recursos de rede, mas esse mecanismo não pode garantir um caminho óptico disponível para estabelecer as conexões afetadas, pois depende dos recursos disponíveis na rede no momento da ocorrência da falha, e o seu tempo de reestabelecimento da conexão é mais longo em comparação aos mecanismos de proteção (LOURENÇO, 2015).

As estratégias de restauração são classificadas em: restauração por enlace, restauração por subcaminho e restauração por caminho (LIRA, 2014).

2.7.1 Restauração por Enlace

Na restauração por enlace, os nós adjacentes a falha são os responsáveis pela busca da rota alternativa. Logo, neste tipo de restauração é encontrado um novo caminho óptico entre o nó antecessor e predecessor a falha (LIRA, 2014).

2.7.2 Restauração por Subcaminho

Na restauração por subcaminho, o nó origem da chamada não é envolvido no processo de restauração após o acontecimento da falha. Nesse tipo de restauração é encontrado uma rota alternativa que interligue o nó predecessor a falha ao nó de destino da chamada (LIRA, 2014).

2.7.3 Restauração por Caminho

Na restauração por caminho, os nós adjacentes à falha enviam mensagens de falha aos nós origem e destino do caminho óptico. Em seguida, os recursos que eram utilizados são liberados e inicia-se uma busca por um novo caminho óptico para a chamada. Uma das características dessa restauração é que os nós de origem e destino participam do processo de restauração (LIRA, 2014).

2.8 Esquemas de Proteção

A proteção de rede consiste em reservar recursos para o uso dedicado na transmissão do tráfego afetado por uma falha na rede. A proteção é um mecanismo proativo, pois os recursos são reservados no momento do estabelecimento da conexão, antes da ocorrência de qualquer falha (LOURENÇO, 2015).

Os esquemas de proteção por serem baseados nas reservas de recursos acabam gerando uma grande demanda de recursos dedicados, onde na maior parte do tempo esse recurso estará ocioso, aguardando a ocorrência de uma falha para que sejam utilizados, em compensação a sua principal vantagem é a rápida recuperação das conexões (XAVIER, 2016).

Os esquemas de proteção, comumente, utilizam dois tipos de provisionamento: o provisionamento de caminho único (*Single Path Provisioning* – SPP) e o provisionamento multicaminho (*Multipath Provisioning* – MPP). No primeiro, um caminho óptico de trabalho é protegido com um ou mais caminhos de proteção disjuntos. Entretanto, a taxa de transmissão requisitada não é particionada entre os caminhos. Assim, cada caminho de proteção possui uma taxa de transmissão para prover a proteção igual à taxa de transmissão requisitada. O segundo tipo propõe o particionamento da taxa de transmissão requisitada em múltiplas parcelas de menores taxas de transmissão, e a sua transmissão é feita de forma simultânea por múltiplos caminhos disjuntos. Diferentemente do SPP, no MPP não há distinção entre caminho óptico de trabalho e de proteção, visto que todos os caminhos ópticos envolvidos podem ser usados para transmissão de dados da conexão, seja na operação normal da rede ou sob falha em um dos enlaces das rotas (DINARTE, 2021).

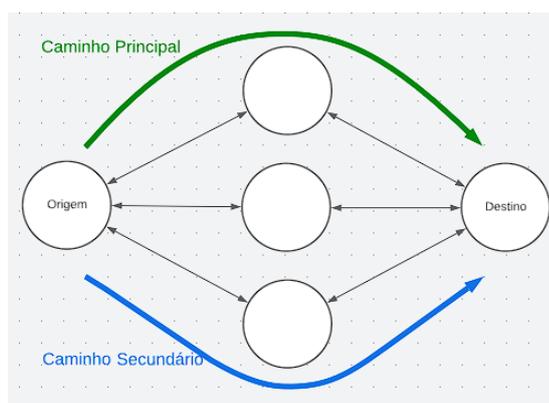
2.8.1 Proteção de Caminho Dedicado

A proteção de caminho dedicado (*Dedicated Path Protection* – DPP) é um esquema de proteção baseado em caminho em que dois caminhos ópticos disjuntos são reservados no momento do estabelecimento da conexão, sendo um o caminho primário e o outro o caminho de proteção (LOURENÇO, 2015). Para cada caminho principal existe um caminho de proteção disjunto dedicado (SILVA, T. 2022). O DPP é um esquema do tipo SPP (DINARTE, 2021). Neste esquema de proteção, duas configurações são possíveis: DPP 1+1 e DPP 1:1 (LOURENÇO, 2015).

A) Proteção de Caminho Dedicado 1+1

Neste tipo de proteção, o tráfego é transmitido simultaneamente por dois caminhos ópticos disjuntos em enlace, entre o nó-origem e o nó-destino. Durante a operação normal da rede, o receptor seleciona o tráfego da fibra que apresenta melhor sinal. Em caso de falha em uma das rotas, a rede fica indiferente a este evento, pois o receptor continua recebendo tráfego da outra rota (FREITAS, 2012). Na figura 14, é representada a proteção dedicada 1+1.

Figura 14 – Proteção Dedicada 1+1

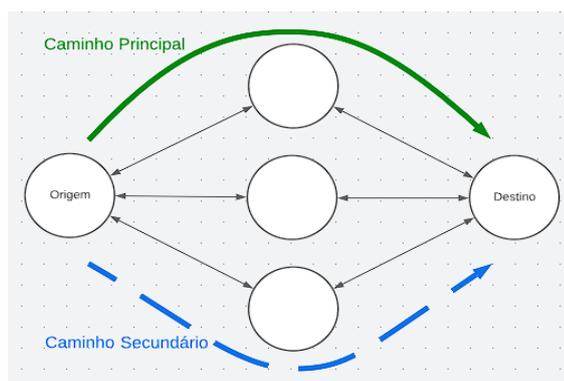


Fonte: O autor.

B) Proteção de Caminho Dedicado 1:1

Neste tipo de proteção, são definidos dois caminhos ópticos disjuntos em enlace, um principal e um secundário. Durante a operação normal da rede, o tráfego é transmitido apenas por um caminho óptico, o caminho principal, entre o nó-origem e o nó-destino. Apenas em caso de falha do caminho principal é que o tráfego será transferido para o caminho secundário (FREITAS, 2012). Na figura 15, é representada a proteção dedicada 1:1.

Figura 15 – Proteção Dedicada 1:1

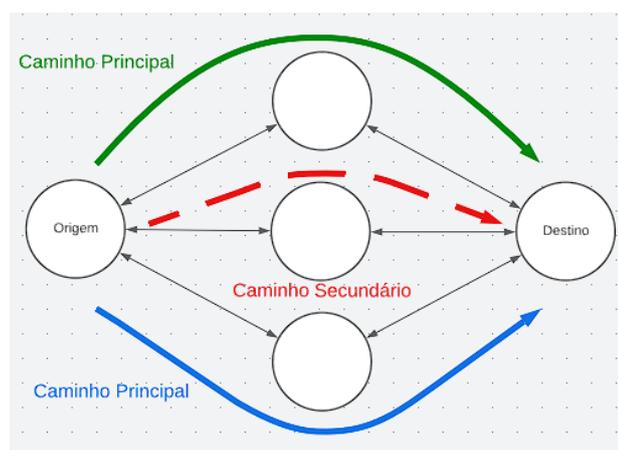


Fonte: O autor.

2.8.2 Proteção de Caminho Compartilhado

A proteção de caminho compartilhado (*Shared Backup Path Protection – SBPP*) corresponde a um esquema de proteção onde um caminho de proteção é compartilhado entre vários caminhos primários. Durante a operação normal da rede, o tráfego é transportado apenas pelos caminhos primários. Em caso de falha de um dos caminhos primários é que o tráfego será transferido para o caminho secundário (FREITAS, 2012). Na figura 16, é representada a proteção compartilhada.

Figura 16 – Proteção Compartilhada



Fonte: O autor.

O esquema SBPP é mais complexo de implementar do que o DPP, porém ele oferece vantagem de melhorar a utilização dos recursos de rede, oferecendo o mesmo nível de proteção que o DPP no caso de uma única falha, mas para isso é preciso que todos os caminhos, tanto os primários quanto o de proteção sejam disjuntos em enlace (FREITAS, 2012).

2.9 Proteção com Banda Espremida

É um conceito de esquema de proteção que admite uma redução na largura de banda disponível para um serviço no caso de ocorrência de uma falha. É possível atribuir aos caminhos ópticos atingidos por uma falha, uma largura de banda menor do que a sua largura de banda original. Consequentemente, mais caminhos ópticos podem ser protegidos na rede usando os mesmos recursos físicos. Isso implica em uma proteção econômica em termos de utilização de recursos espectrais, o que melhora a capacidade de proteção e desempenho da rede. A largura de banda pós falha para cada caminho óptico é determinada por um SLA realizado entre o cliente e o operador da rede (ASSIS, 2012).

Capítulo 3 Metodologia

Neste capítulo é descrita a metodologia utilizada no desenvolvimento desta monografia. No tópico 3.1 são descritas as ferramentas de simulação utilizadas para desenvolvimento do conceito proposto. No tópico 3.2 descrita a métrica utilizada para avaliação de desempenho de uma rede óptica. No tópico 3.3 é descrito como a proteção MPP é aplicada neste trabalho e na seção 3.4 é descrito o tráfego heterogêneo considerado na monografia.

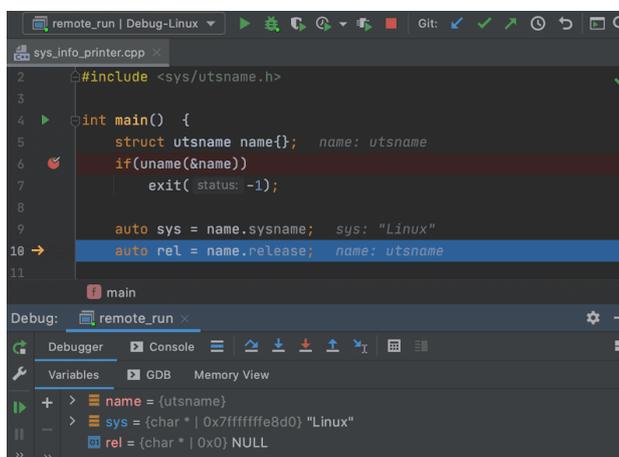
3.1 SimEON

Um simulador desenvolvido a partir do SimEON (CAVALCANTE, 2017) é utilizado para o desenvolvimento e simulação do conceito proposto.

O SimEON é um software de simulação construído na linguagem C++. C++ é uma linguagem de programação open source orientada a objetos, utilizada tanto como linguagem de máquina quanto para softwares. Essas características permitem que seja considerada uma linguagem tanto de alto quanto de baixo nível, o que permite que sistemas desenvolvidos sejam de alto desempenho e estáveis (NOLETO, 2021).

A IDE utilizada para manipulação do SimEON é o CLion. O CLion é um ambiente de desenvolvimento multiplataforma construído exclusivamente para manipulação de códigos nas linguagens C e C++. A IDE possui licenças educacionais gratuitas (JETBRAINS, 2022).

Figura 17 – Ferramenta CLion



Fonte: Adaptado de (JETBRAINS, 2012)

A Figura 17 ilustra a ferramenta utilizada neste trabalho.

3.2 Métricas de Desempenho

A principal métrica de avaliação de uma rede óptica é a probabilidade de bloqueio (Blocking Probability) (CANDIA, 2014).

A probabilidade de bloqueio é obtida pela razão do número de requisições bloqueadas (não atendidas) pelo número total de requisições de conexão. É uma medida de desempenho global da rede, onde quanto mais elevado for o valor da probabilidade de bloqueio pior será o desempenho da rede. Para estimar a probabilidade de bloqueio, é comum simular um grande número de requisições de conexão à rede óptica e contabilizar a quantidade de requisições bloqueadas. A probabilidade de bloqueio é definida pela equação 1:

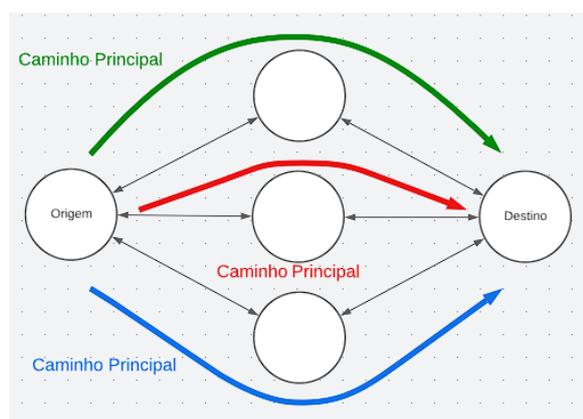
$$\text{Probabilidade de bloqueio} = R_b/R_t \quad (1)$$

em que R_b é a quantidade de requisições bloqueadas e R_t é a quantidade total de requisições de conexão ofertadas à rede. As requisições bloqueadas podem ocorrer devido à falta de recursos, seja por indisponibilidade de comprimentos de onda em redes ópticas WDM ou *slots* de frequência em EONs (XAVIER, 2016).

3.3 Proteção com MPP

Como já mencionado anteriormente, o provisionamento multicaminho (MPP) é um esquema de proteção que permite o particionamento da banda de transmissão em múltiplas parcelas. A transmissão dessas parcelas é feita de forma simultânea por múltiplos caminhos disjuntos, ou seja, todos os caminhos ópticos envolvidos são utilizados para a transmissão de dados, seja na operação normal ou sob falha.

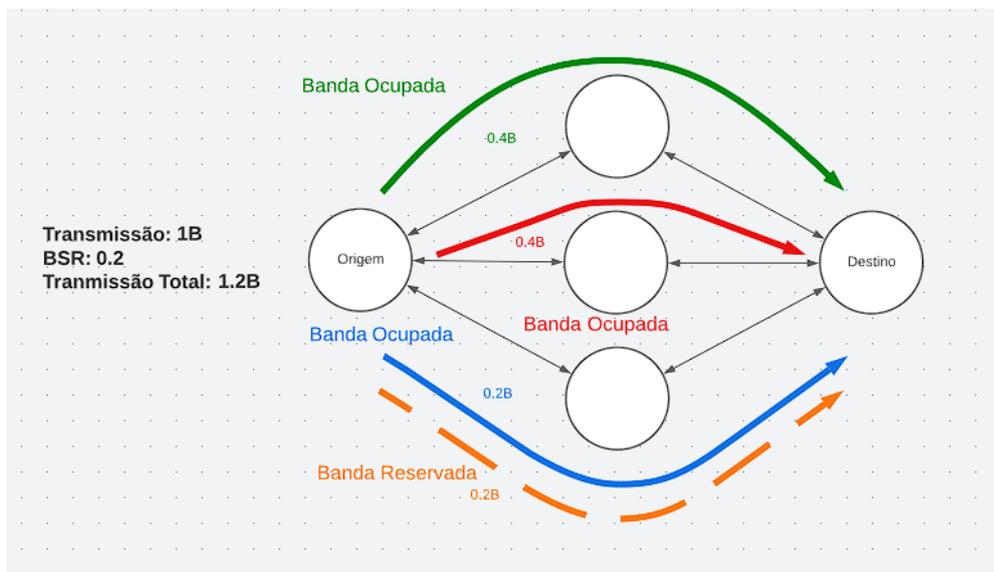
Figura 18 – Provisionamento Multicaminho



Fonte: O autor.

A Figura 18 ilustra o conceito do MPP. É possível adicionar ao MPP o conceito de largura de banda espremida. Ao realizar o particionamento da taxa de transmissão é adicionada uma taxa extra de transmissão. Em caso de uma falha simples em exatamente uma das rotas utilizadas na transmissão, a soma da banda restante das rotas remanescentes ainda é suficiente considerando o SLA definido e a banda espremida acorda. Em caso de operação normal, a taxa de transmissão extra não será ocupada, mas sim reservada para ser utilizada em caso de falhas.

Figura 19 – MPP e BSR



Fonte: O autor.

A Equação 2 (DINARTE, 2021) mostra como a divisão da taxa total de transmissão é realizada:

$$Taxa\ por\ Rota = \frac{(1 - \beta) * B}{N - 1} \tag{2}$$

em que β é o espremeimento de banda e N é o número de rotas.

Como é possível observar na Figura 19. Uma taxa de transmissão de 1B considerando um espremeimento de banda máximo de 0.2B, aplicando esses valores na Equação 2, têm-se como resultado:

$$Taxa\ por\ Rota = \frac{(1 - 0.2) * B}{3 - 1} = \frac{0.8B}{2} = 0.4B \tag{3}$$

Para esse cenário cada rota possui 0.4B de taxa de transmissão. Nessa abordagem, parte da banda reservada na terceira rota é usada durante a transmissão durante a operação normal da rede e parte é mantida ociosa, sendo a banda de reserva necessária para respeitar o SLA em ocorrência de falhas.

3.4 Tráfego com Demandas Heterogêneas de Resiliência

Como discutido no final da seção anterior, em operação normal sem falhas ativas na rede, há slots de frequência na terceira rota que estão ociosos, ocupando um recurso que não será utilizado enquanto não houver falha, gerando desperdício espectral. Esse recurso ocioso pode ser utilizado de alguma forma.

As operadoras de telecomunicações podem vender serviços diferenciados de acordo com a demanda do cliente. Neste trabalho são assumidos dois tipos de tráfego:

- Serviços que demandam alta disponibilidade – são serviços que necessitam de um esquema de proteção. Neste trabalho esse requisito é implementado usando MPP combinado com BSR;
- Serviços que não demandam alta disponibilidade – são serviços que podem ser implementados sem nenhum esquema de proteção. Neste trabalho esses serviços são implementados preferencialmente usando um caminho único aproveitando a banda ociosa dos caminhos protegidos já alocados. Caso não estejam disponíveis, o serviço é implementado usando o MPP sem BSR e com dois caminhos sem buscar o aproveitamento da banda ociosa.

Os primeiros são denominados nesta monografia como serviços com resiliência garantida (ScRG) e serviços sem resiliência garantida (SsRG).

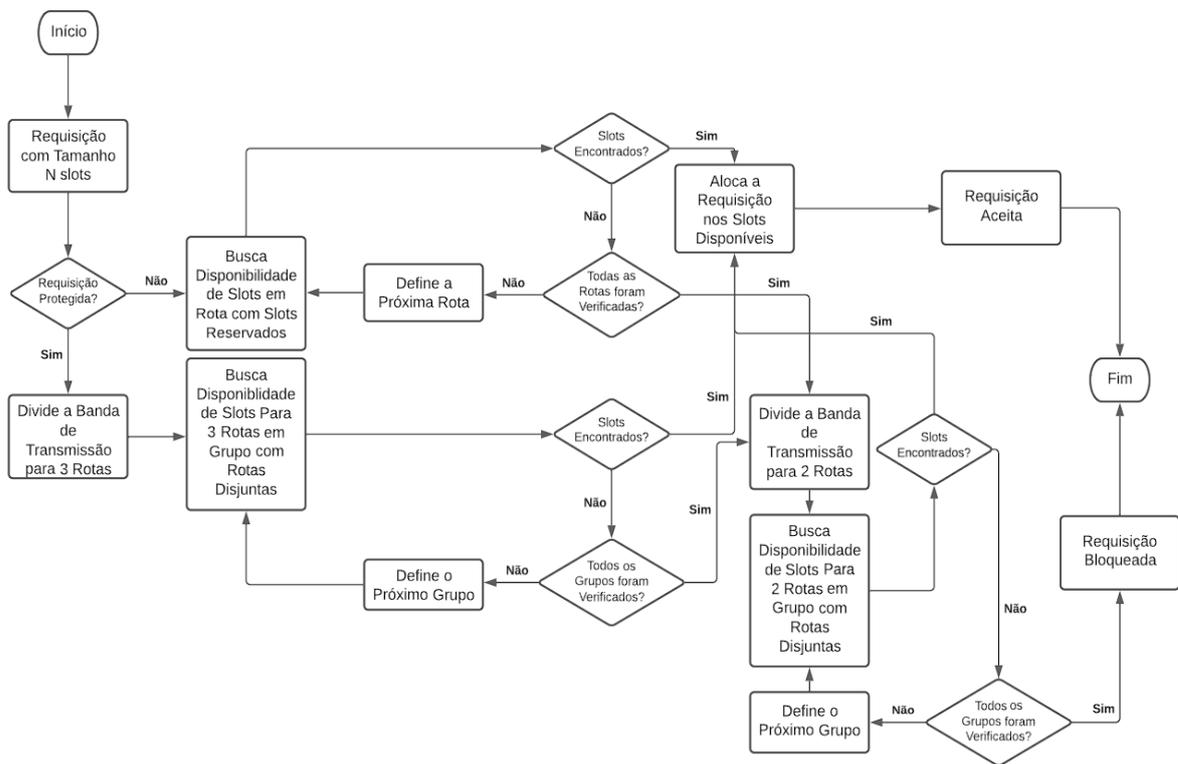
Com essa perspectiva, buscando potencializar a gestão dos recursos de banda, uma estratégia a ser adotada é de utilizar os recursos ociosos do tráfego protegido para atender o tráfego não protegido. Essa é a proposta investigada nesta monografia.

Capítulo 4 Algoritmo para Reutilização de Banda Ociosa de Banda Ociosa

O algoritmo proposto nesta monografia recebe o nome de reutilização de banda ociosa (*Idle Bandwidth Reuse – IBR*).

O IBR é um algoritmo que tem como objetivo buscar a reutilização dos recursos ociosos gerados pela implementação do MPP com BSR. Nesse contexto, os slots de frequência alocados, mas deixados ociosos pelo tráfego do tipo ScRG, podem ser reutilizados pelo tráfego do tipo SsRG.

Figura 20 – Funcionamento do Algoritmo IBR



Fonte: O autor.

A Figura 20 ilustra um fluxograma que descreve o funcionamento do algoritmo IBR.

Figura 21 – Pseudocódigo do IBR

Algorithm 1 Idle Bandwidth Reuse

```

1: procedure RECEBE UMA REQUISIÇÃO
2:   Verifica os nós origem(S) e destino(D);
3:   Armazena os N grupos encontrados no conjunto  $R = [r1, r2, \dots, rN]$ 
   com 3 rotas disjuntas entre os nós S e D;
4:   if requisição == protegida, do tipo ScRG then
5:     varAlocação = requisiçãoProtegida;
6:     if varAlocação == true then
7:       requisição = aceita;
8:     else varAlocação == false
9:       varAlocação = requisiçãoNormal;
10:    if varAlocação == true then
11:      requisição = aceita;
12:    else
13:      requisição = bloqueada;
14:    end if
15:  end if
16:  else requisição == nãoProtegida, do tipo SsRG
17:    varAlocação = requisiçãoNãoProtegida;
18:    if varAlocação == true then
19:      requisição = aceita;
20:    else varAlocação == false
21:      varAlocação = requisiçãoNormal;
22:      if varAlocação == true then
23:        requisição = aceita;
24:      else
25:        requisição = bloqueada;
26:      end if
27:    end if
28:  end if
29: end procedure

```

Fonte: O autor.

Na Figura 21 observa-se o pseudocódigo que descreve o funcionamento do algoritmo do IBR. Ao receber uma requisição com tamanho “S” *slots*, o algoritmo verifica primeiramente os nós de origem e destino, e de acordo com a quantidade definida de grupos o algoritmo MPR irá definir as três rotas disjuntas que compõem cada grupo. Posteriormente é verificada se a requisição é protegida ou não.

Se a requisição for protegida, ou seja, do tipo ScRG o algoritmo executa a função Requisição Protegida, o pseudocódigo que descreve o funcionamento da função Requisição Protegida está ilustrado na Figura 22. Essa função tenta particionar a requisição em três caminhos disjuntos. Se essa função retornar sucesso na alocação da requisição, a requisição é aceita, caso contrário o algoritmo desiste de alocar a requisição no formato ScRG e executa outra função que busca alocar a requisição com uma estratégia diferente, essa função está nomeada como Requisição Normal, o pseudocódigo que descreve o funcionamento da Requisição Normal está ilustrado na Figura 24. Essa função tenta particionar a requisição em dois caminhos disjuntos ainda considerando a estratégia de espremimento de banda adotada para prover proteção. Se essa função retornar sucesso na alocação da requisição, a requisição é aceita, caso contrário, a requisição é bloqueada.

Se a requisição for não protegida, ou seja, uma requisição do tipo SsRG, o algoritmo executa a função Requisição Não Protegida, o pseudocódigo que descreve o funcionamento da Requisição Não Protegida está ilustrado na Figura 23. Essa função tenta reutilizar slots alocados para prover proteção para chamadas do tipo ScRG, mas que não estão sendo usados efetivamente para transmissão (recursos alocados para serem usados apenas durante uma falha. Se essa função retornar sucesso na alocação da requisição, a requisição é aceita, caso contrário o algoritmo busca alocar a requisição com uma estratégia diferente, essa função está nomeada como Requisição Normal. Essa função é a mesma citada no parágrafo anterior, ela divide a taxa requerida pela chamada em duas partes e tenta aloca-las em dois caminhos disjuntos. A diferença é que para uma chamada do tipo SsRG não são alocados slots extras para prover proteção. Se essa função retornar sucesso na alocação da requisição, a requisição é aceita, caso contrário, a requisição é bloqueada.

Figura 22 – Pseudocódigo Requisição Protegida

Algorithm 2 Requisição Protegida

```
1: procedure REQUISIÇÃOPROTEGIDA(R)
2:   Particiona a taxa total requisitada em 3 considerando o espremi-
   mento de banda;
3:   varAlocação = false;
4:   for i = 1 até N do
5:     Encontre o grupo r[i] do conjunto R;
6:     Busca slots com status livre nas 3 rotas do grupo r[i];
7:     if Slots Livres Encontrados then
8:       Aloca a requisição nos slots livres;
9:       Os slots de 2 rotas são alocados com o status ocupado;
10:      Os slots de 1 rota são alocados como parte ocupado e parte
   reservado;
11:      varAlocação = true;
12:      break;
13:     end if
14:   end for
15:   Retorna varAlocação;
16: end procedure
```

Fonte: O autor.

Na Figura 22 observa-se o pseudocódigo que descreve o funcionamento da função para requisição protegida. Quando uma requisição protegida é solicitada à rede o algoritmo particiona igualmente a taxa de transmissão total demandada em três requisições considerando a estratégia de espremeimento de banda adotada e então cria uma variável para verificação do sucesso ou não da alocação. Em cada um dos “ N ” grupos de “ K ” rotas disjuntas ($k=3$) o algoritmo busca *slots* disponíveis para as três requisições nas três rotas de cada grupo. Se *slots* livres utilizando o algoritmo *first fit* forem encontrados para alocar as três partes da requisição, elas são alocadas. Todos os *slots* da primeira e da segunda rota são ocupados, enquanto na terceira rota, parte dos *slots* encontrados são efetivamente usados na transmissão e parte permanece ociosa e somente são efetivamente usados na transmissão em caso de ocorrência de uma falha na rede, a variável de alocação recebe o valor *true* e o laço de busca é encerrado. Se *slots* livres não forem encontrados e todos os grupos já foram analisados, o laço de busca é encerrado e a variável de alocação permanece com o valor *false*. No final a variável de alocação é retornada contendo a informação se a requisição foi alocada com sucesso ou não.

Figura 23 – Pseudocódigo Requisição Não Protegida

Algorithm 3 Requisição Não Protegida

```
1: procedure REQUISICÃO NÃO PROTEGIDA(R)
2:   varAlocação = false;
3:   for i = 1 até N do
4:     Encontre a terceira rota  $p_i$  do grupo  $r[i]$  do conjunto R;
5:     Busca slots com status reservado na rota  $p_i$  encontrada;
6:     if Slots Reservados Encontrados then
7:       Aloca a requisição nos slots reservados;
8:       Os slots são alocados com o status reutilizado;
9:       varAlocação = true;
10:      break;
11:    end if
12:  end for
13:  Retorna varAlocação;
14: end procedure
```

Fonte: O autor.

Na Figura 23 observa-se o pseudocódigo que descreve o funcionamento da função para requisição não protegida. Quando uma requisição não protegida é solicitada à rede o algoritmo não particiona a requisição, o algoritmo busca alocar a requisição inteiramente em uma única rota e então cria uma variável para verificação do sucesso ou não da alocação. Para os “ N ” grupos de rotas com três rotas disjuntas o algoritmo busca slots disponíveis nas terceiras rotas de cada grupo, visto que a função de requisição protegida sempre reserva slots nas terceiras rotas. Se *slots* com status de reservado utilizando o algoritmo *first fit* forem encontrados para alocar a requisição, a requisição será alocada com os slots recebendo o status reutilizado, a variável de alocação recebe o valor *true* e o laço de busca é encerrado. Se slots com status de reservado não forem encontrados e todos os grupos já foram analisados, o laço de busca é encerrado e a variável de alocação permanece com valor *false*. No final a variável de alocação é retornada contendo a informação se a requisição foi alocada com sucesso ou não.

Figura 24 – Pseudocódigo Requisição Normal

Algorithm 4 Requisição Normal

```

1: procedure REQUISICÃO NORMAL(R)
2:   if requisição == protegida, do tipo ScRG then
3:     Particiona a taxa total requisitada em 2 considerando o espremi-
       mento de banda;
4:   else requisição == nãoProtegida, do tipo SsRG
5:     Particiona a taxa total requisitada em 2;
6:   end if
7:   varAlocação = false;
8:   for i = 1 até N do
9:     Busca slots com status livre para 2 rotas de r[i];
10:    if Slots Livres Encontrados then
11:      Aloca a requisição nos slots livres;
12:      Os Slots são alocados com o status ocupado;
13:      varAlocação = true;
14:      break;
15:    end if
16:  end for
17:  Retorna varAlocação;
18: end procedure

```

Fonte: O autor.

Na Figura 24 observa-se o pseudocódigo que descreve o funcionamento da função para requisição normal. A requisição normal é utilizada quando o algoritmo não consegue alocar a requisição na primeira tentativa, seja do tipo ScRG usando três rotas disjuntas ou SsRG usando slots ociosos alocados para prover proteção para chamadas do tipo ScRG. A função requisição normal particiona igualmente a requisição em duas. Para requisições do tipo ScRG. Já para requisições do tipo SsRG a taxa total requerida pela chamada é simplesmente dividida em duas. Posteriormente ao particionamento o algoritmo cria uma variável para verificação da do sucesso ou não da alocação. Para os “N” grupos de rotas com três rotas disjuntas o algoritmo busca *slots* livres para duas rotas de cada grupo. Se *slots* livres utilizando o algoritmo *first fit* forem encontrados para alocar as duas partes da requisição, elas são alocadas com os *slots* sendo ocupados. A variável de alocação recebe o valor *true* e o laço de busca é encerrado. Se *slots* livres não forem encontrados e todos os grupos já foram analisados, o laço de busca é encerrado e a variável de alocação permanece com o valor *false*. No final a variável de alocação é retornada contendo a informação se a requisição foi alocada com sucesso ou não.

Capítulo 5 Resultados

Este capítulo apresenta as premissas de simulação definidas e os seus resultados. No tópico 5.1 as premissas referentes as simulações. No tópico 5.2 os resultados obtidos das simulações.

5.1 Premissas de Simulação

Para avaliação das propostas deste trabalho, o simulador foi configurado com os parâmetros mostrados na Tabela 1.

Tabela 1 – Parâmetros Usados nas Simulações

Descrição	Valor
Quantidade de <i>slots</i> por enlace	320
Tamanho do Slot (GHz)	12,5
Número de requisições	10^6
BSR	0.2
Algoritmo de Roteamento	MPR
Quantidade de Rotas Disjuntas	3
Quantidade de Grupos de Rotas	10
Algoritmo de Alocação de Espectro	<i>First Fit</i>

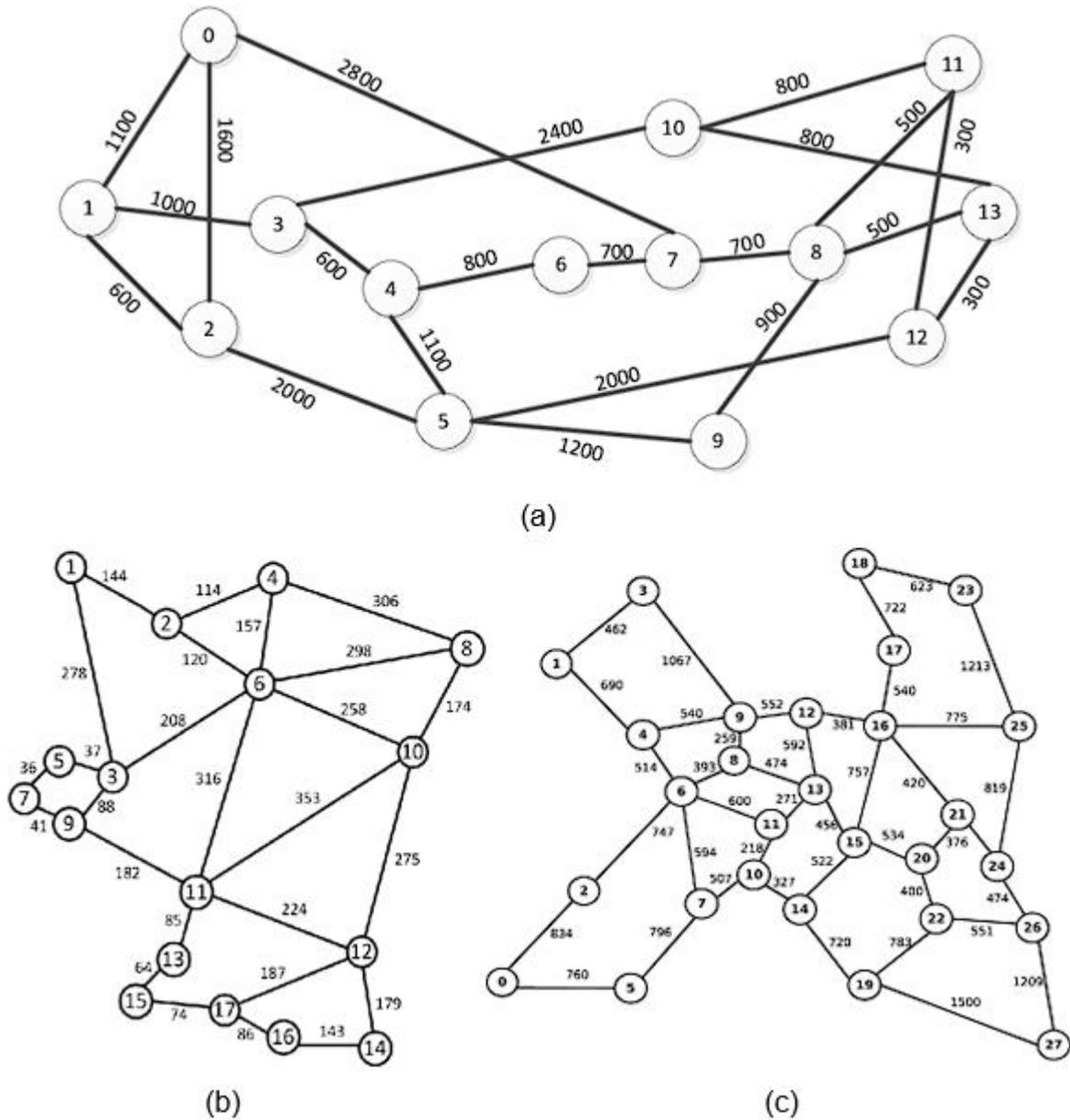
Fonte: O autor.

A quantidade de *slots* por enlace definida é de 320. Cada *slot* ocupa uma frequência de 12, 5 GHz. Para cada simulação são utilizadas 10^6 requisições. As requisições são definidas de forma aleatória como protegidas ou não protegidas com distribuição uniforme de 70% para protegidas e 30% para desprotegidas. As taxas de transmissão são sorteadas a cada requisição. Essas taxas podem assumir os seguintes valores: 100, 200 e 400 Gbits/s uniformemente distribuídas. As cargas Erlang definidas variam de acordo com a topologia. Erlang é uma medida de intensidade de tráfego utilizada em telecomunicações. A largura de banda espremida definida em 20%. O algoritmo de roteamento escolhido é o MPR. A quantidade de rotas disjuntas é de três. A quantidade de grupos com três rotas disjuntas é de dez. O algoritmo de alocação espectral escolhido é o *First Fit*. Três topologias diferentes foram simuladas: NsfNet, Germany e European. Elas estão mostradas na Figura 27. A métrica utilizada para avaliação do conceito proposto é a probabilidade de bloqueio.

Com o objetivo de avaliar o impacto que a estratégia proposta tem na reutilização dos slots da rede, ela é comparada com outra estratégia que não realiza a reutilização de *slots* ociosos. A estratégia proposta neste trabalho é mostrada nos resultados sob o nome de “com reuso”. A estratégia de comparação, sob o nome de

“sem reuso”, não executa a busca por *slots* ociosos, o algoritmo 4 (Figura 25) realiza a busca e alocação apenas em *slots* livres.

Figura 25 – Topologias: (a) NsfNet, (b) Germany e (c) European



Fonte: O autor.

Na Figura 25 as topologias estão com os nós numerados e os enlaces com pesos definidos. A topologia NfsNet possui 14 nós e 42 enlaces, a topologia Germany possui 17 nós e 52 enlaces e a topologia European possui 28 nós e 82 enlaces.

5.2 Resultados das Simulações

Esta seção apresenta os resultados obtidos para as simulações definidas na seção 4.1 e suas respectivas análises. No tópico 4.2.1 os resultados referentes as simulações realizadas na topologia NsfNet. No tópico 4.2.2 os resultados referentes as simulações realizadas na topologia Germany. No tópico 4.2.3 os resultados referentes as simulações realizadas na topologia European.

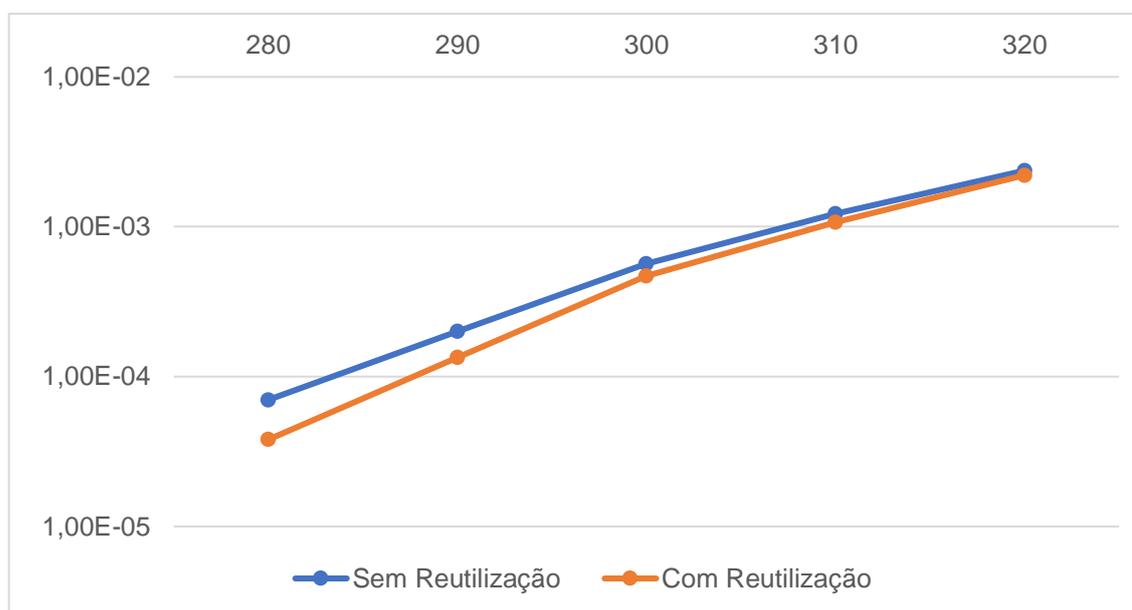
5.2.1 Resultados para a Topologia NsfNet

Tabela 2 – Resultados de Probabilidade de Bloqueio para NsfNet

Probabilidade de Bloqueio	Erlang				
	280	290	300	310	320
Sem Reutilização	7,00E-05	2,01E-04	5,66E-04	1,22E-03	2,37E-03
Com Reutilização	3,80E-05	1,34E-04	4,68E-04	1,08E-03	2,21E-03
Diferença	84,21%	50,00%	20,94%	13,12%	7,29%

Fonte: O autor.

Figura 26 – Probabilidade de Bloqueio em Função da Carga para NsfNet



Fonte: O autor.

A Figura 26 mostra a probabilidade de bloqueio obtida pelas simulações de cada carga erlang na topologia NsfNet com o algoritmo buscando reutilizar ou não os *slots* reservados. Com os resultados é possível observar que para a topologia NsfNet houve uma diminuição acima de 50% na probabilidade de bloqueio para cargas mais baixas, porém com o aumento progressivo de carga, essa diminuição vai se tornando menos significativa, chegando a ficar abaixo de 10%, de forma que quase não há impacto na probabilidade de bloqueio para as cargas mais altas.

Para verificar se os resultados possuíam significância estatística, ou seja, se a diferença do resultado entre os métodos é significativa, foram calculadas as margens de erro para um intervalo de confiança de 95% considerando dez simulações independentes, usando a fórmula:

$$CI = x \pm z \frac{s}{\sqrt{n}} \quad (4)$$

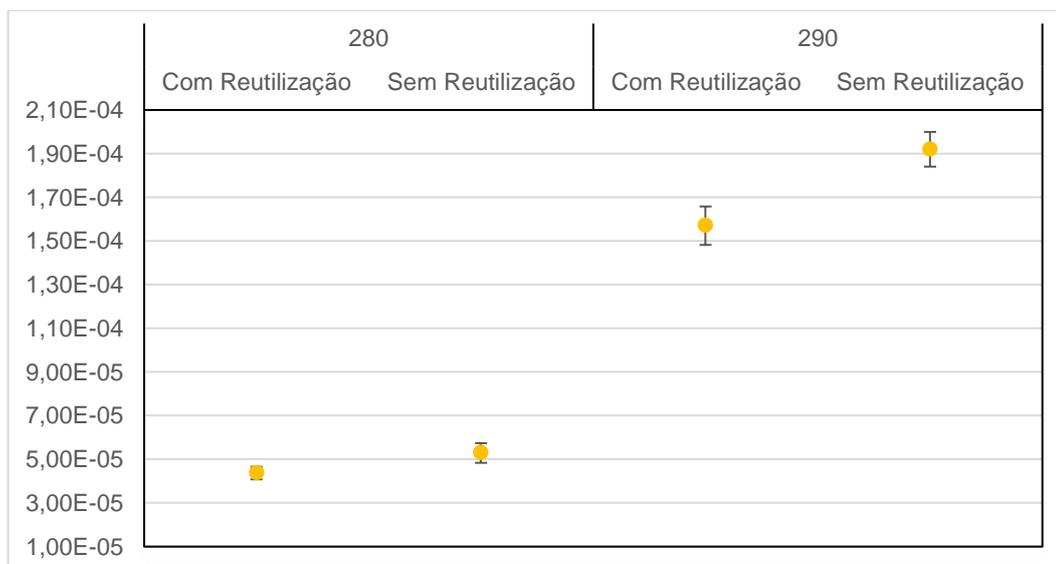
em que CI é o intervalo de confiança, x é a média da amostra, z é o valor do nível de confiança, s é o desvio padrão da amostra e n é o tamanho da amostra. Apenas as cargas mais baixas foram selecionadas por possuírem um resultado de melhoria significativo. Os resultados estão mostrados na Tabela 3.

Tabela 3 – Resultados da Variação da Probabilidade de Bloqueio para NsfNet

Intervalo de Confiança				
	280		290	
	Com Reutilização	Sem Reutilização	Com Reutilização	Sem Reutilização
Desvio Padrão	4,64E-06	7,28E-06	1,42E-05	1,28E-05
Margem de Erro	2,88E-06	4,51E-06	8,80E-06	7,93E-06
Limite Inferior	4,08E-05	4,84E-05	1,48E-04	1,84E-04
Média	4,37E-05	5,29E-05	1,57E-04	1,92E-04
Limite Superior	4,66E-05	5,74E-05	1,66E-04	2,00E-04

Fonte: O autor.

Figura 27 – Variação da Probabilidade de Bloqueio Para NsfNet



Fonte: O autor.

A Figura 27 mostra um gráfico para as cargas de 280 e 290 erlangs na topologia NsfNet que mostra o valor médio e as margens de erro de probabilidade de bloqueio para um nível de confiança de 95% obtidos para as dez simulações independentes mencionadas anteriormente. É possível observar que para todos os resultados não há superposição dos limites inferior e superior das margens de erro, sugerindo significância estatística nos resultados obtidos.

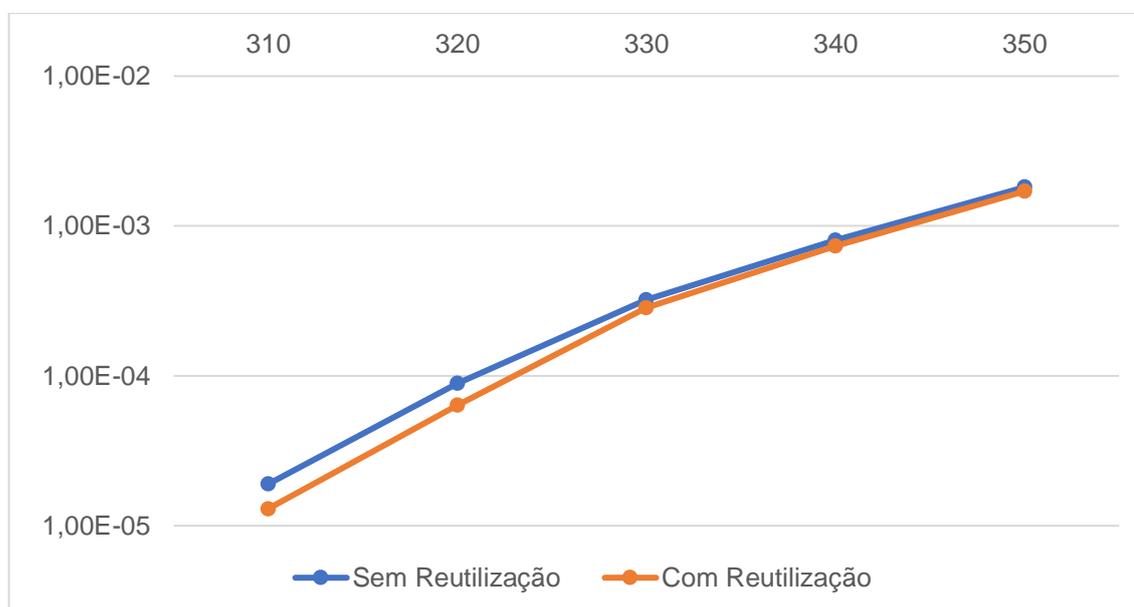
5.2.2 Resultados para a Topologia Germany

Tabela 4 – Resultados de Probabilidade de Bloqueio para Germany

Probabilidade de Bloqueio	Erlang				
	310	320	330	340	350
Sem Reutilização	1,90E-05	8,90E-05	3,21E-04	8,03E-04	1,82E-03
Com Reutilização	1,30E-05	6,40E-05	2,84E-04	7,38E-04	1,70E-03
Diferença	46,15%	39,06%	13,03%	8,81%	6,51%

Fonte: O autor.

Figura 28 – Probabilidade de Bloqueio em Função da Carga para Germany



Fonte: O autor.

A Figura 28 mostra a probabilidade de bloqueio obtida pelas simulações de cada carga erlang na topologia Germany com o algoritmo buscando reutilizar ou não os *slots* reservados. Com os resultados é possível observar que para a topologia Germany houve uma diminuição de pelo menos 39% na probabilidade de bloqueio para cargas baixas, porém com o aumento progressivo de carga, essa diminuição vai se tornando menos significativa, chegando a ficar abaixo de 10%, de forma que quase não há impacto na probabilidade de bloqueio para as cargas mais altas.

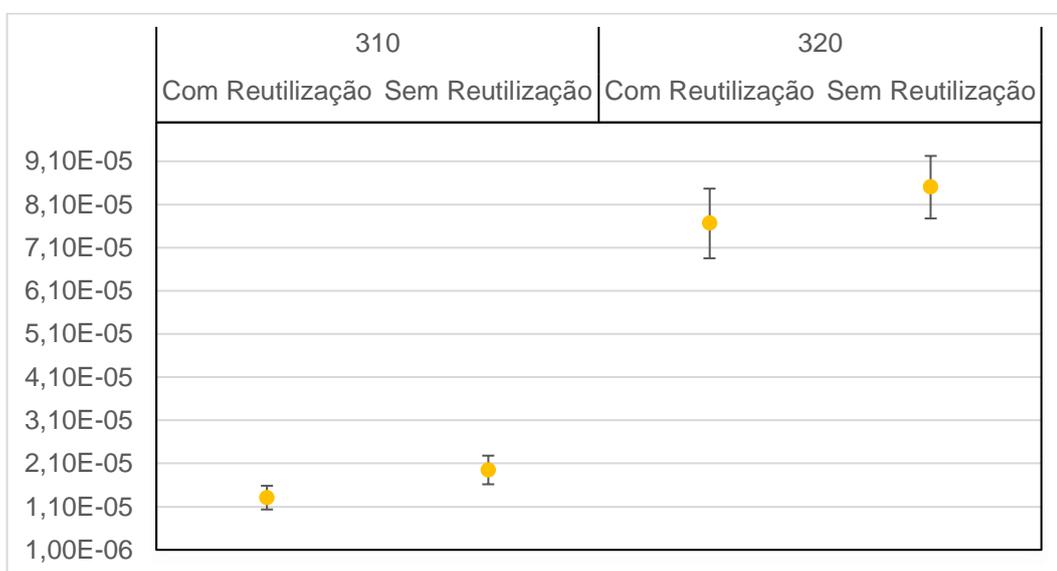
O mesmo cálculo de intervalo de confiança realizado para obtenção da Tabela 3 e Figura 27 é repetido para a topologia Germany. Novamente, apenas as cargas mais baixas foram selecionadas por possuírem um resultado de melhoria significativo. Os resultados estão mostrados na Tabela 5.

Tabela 5 – Resultados da Variação da Probabilidade de Bloqueio para Germany

Intervalo de Confiança				
	310		320	
	Com Reutilização	Sem Reutilização	Com Reutilização	Sem Reutilização
Desvio Padrão	4,43E-06	5,36E-06	1,30E-05	1,17E-05
Margem de Erro	2,75E-06	3,32E-06	8,07E-06	7,24E-06
Limite Inferior	1,04E-05	1,62E-05	6,85E-05	7,78E-05
Média	1,31E-05	1,95E-05	7,66E-05	8,50E-05
Limite Superior	1,58E-05	2,28E-05	8,47E-05	9,22E-05

Fonte: O autor.

Figura 29 – Variação da Probabilidade de Bloqueio para Germany



Fonte: O autor.

A Figura 29 mostra um gráfico para as cargas de 310 e 320 erlangs na topologia Germany que mostra o valor médio e as margens de erro de probabilidade de bloqueio para um nível de confiança de 95% obtidos para as dez simulações independentes mencionadas anteriormente. É possível observar que para a carga de 310 erlangs não há superposição dos limites inferior e superior das margens de erro, sugerindo significância estatística nos resultados obtidos. Para a carga de 320 erlangs apesar da média de probabilidade de bloqueio da estratégia sem reuso ser maior que com reuso, há uma superposição das margens de erro o que indica uma incerteza acerca da melhora da estratégia com reuso nessa carga específica.

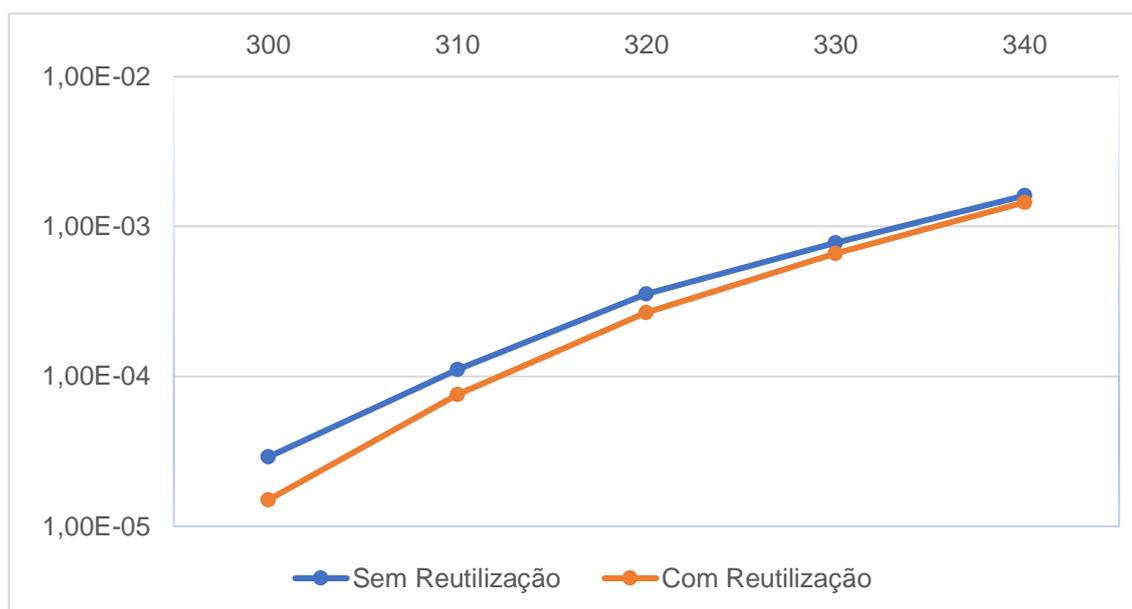
5.2.3 Resultados para a Topologia European

Tabela 6 – Resultados de Probabilidade de Bloqueio para European

Probabilidade de Bloqueio	Erlang				
	300	310	320	330	340
Sem Reutilização	2,90E-05	1,11E-04	3,54E-04	7,77E-04	1,61E-03
Com Reutilização	1,50E-05	7,60E-05	2,67E-04	6,59E-04	1,45E-03
Diferença	93,33%	46,05%	32,58%	17,91%	10,84%

Fonte: O autor.

Figura 30 – Probabilidade de Bloqueio em Função da Carga para European



Fonte: O autor.

A Figura 30 mostra a probabilidade de bloqueio obtida pelas simulações de cada carga erlang na topologia European com o algoritmo buscando reutilizar ou não os *slots* reservados. Com os resultados é possível observar que para a topologia European houve uma diminuição acima de 45% na probabilidade de bloqueio para cargas baixas, porém com o aumento progressivo de carga, essa diminuição vai se tornando menos significativa, atingindo em torno de 10%, de forma que quase não há impacto na probabilidade de bloqueio para as cargas mais altas.

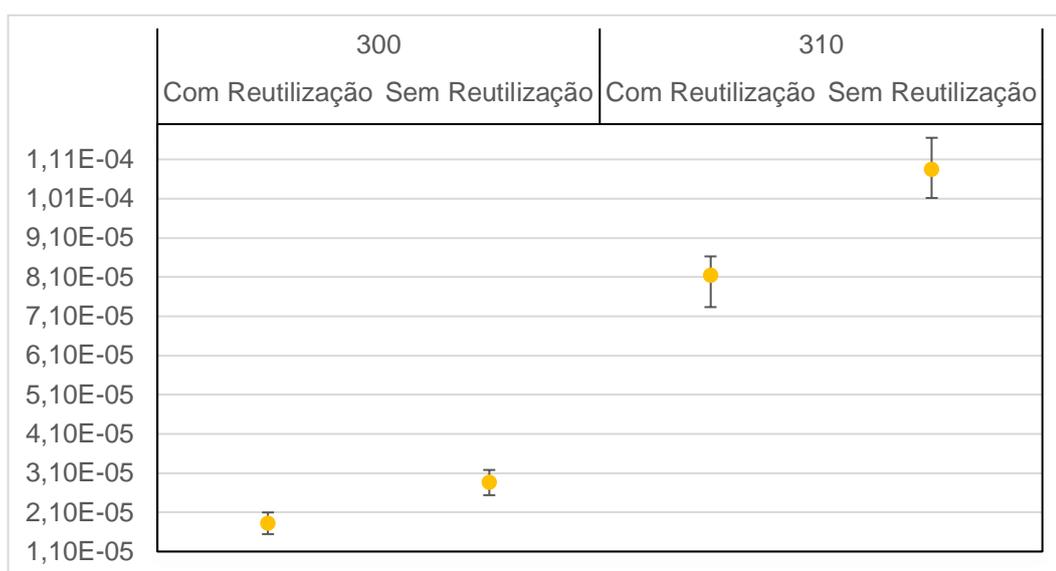
O mesmo cálculo de intervalo de confiança realizado para obtenção das Tabelas 5 e 6 e Figuras 27 e 29 é repetido para a topologia European. Novamente, apenas as cargas mais baixas foram selecionadas por possuírem um resultado de melhoria significativo. Os resultados estão mostrados na Tabela 7.

Tabela 7 – Resultados da Variação da Probabilidade de Bloqueio para European

Intervalo de Confiança				
	300		310	
	Com Reutilização	Sem Reutilização	Com Reutilização	Sem Reutilização
Desvio Padrão	4,47E-06	5,01E-06	7,86E-06	1,31E-05
Margem de Erro	2,77E-06	3,11E-06	4,87E-06	8,11E-06
Limite Inferior	1,54E-05	2,56E-05	7,65E-05	1,00E-04
Média	1,82E-05	2,87E-05	8,14E-05	1,08E-04
Limite Superior	2,10E-05	3,18E-05	8,63E-05	1,17E-04

Fonte: O autor.

Figura 31 – Variação da Probabilidade de Bloqueio para European



Fonte: O autor.

A Figura 31 mostra um gráfico para as cargas de 300 e 310 erlangs na topologia European que mostra o valor médio e as margens de erro de probabilidade de bloqueio para um nível de confiança de 95% obtidos para as dez simulações independentes mencionadas anteriormente. É possível observar que para todos os resultados não há superposição dos limites inferior e superior das margens de erro, sugerindo significância estatística nos resultados obtidos.

Capítulo 6 Conclusão

6.1 Conclusão

Com a necessidade de utilização de redes ópticas para atendimento da crescente demanda de utilização de internet no Brasil e no mundo, os mecanismos de proteção se mostraram bastante úteis para promoção de resiliência para as redes ópticas contra os diversos tipos variados de falhas, porém a promoção de resiliência nem sempre é acompanhada de uma gestão eficiente de recursos.

Esta monografia propôs o uso de um algoritmo com o objetivo de reutilizar os recursos ociosos oriundos da aplicação do provisionamento multicaminho combinado com a técnica de largura de banda espremida como mecanismo de proteção no atendimento de serviços que solicitam resiliência, para atendimento de serviços que não necessitam ou solicitam resiliência.

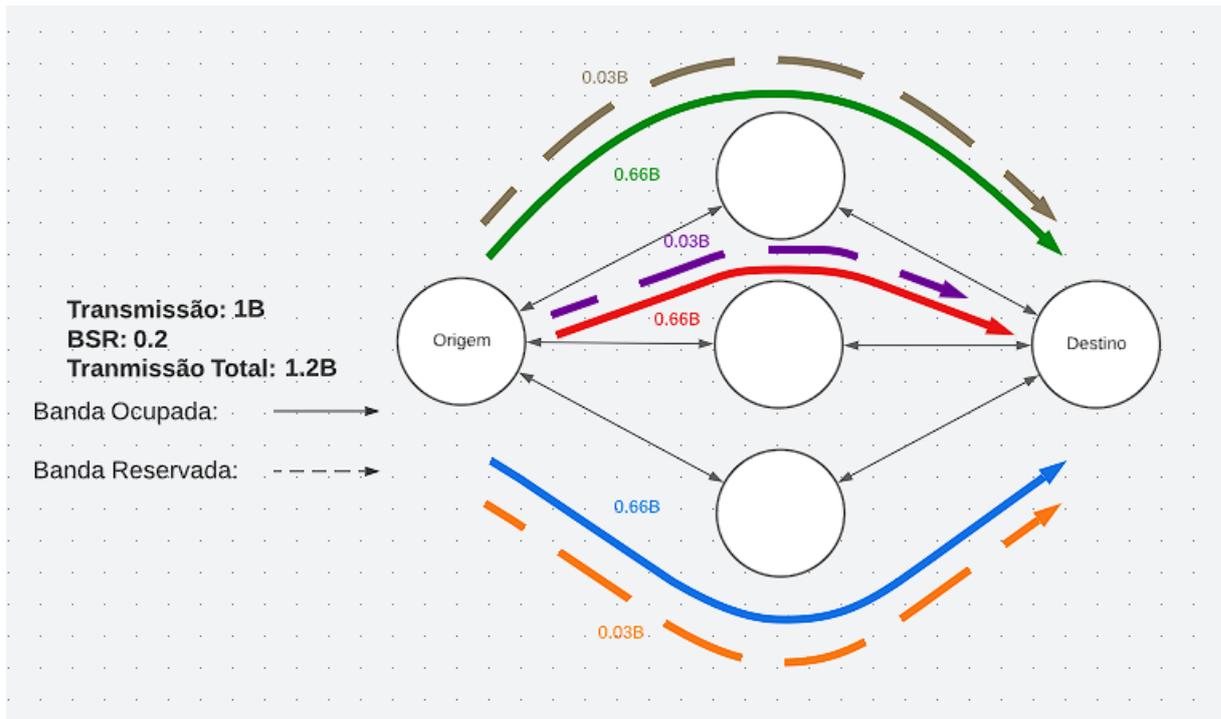
As simulações realizadas foram aplicadas em três topologias *backbone* diferentes, NsfNet, Germany e European, aplicando ou não a tentativa de reutilização dos slots reservados enquanto ociosos pelo mecanismo de proteção adotado, sendo configuradas cargas progressivas com o intuito de diversificar os experimentos e utilizando os algoritmos MPR para roteamento e *First Fit* para alocação espectral.

O algoritmo proposto nesta monografia possui uma lógica bastante simples, porém mesmo assim conseguiu contribuir com a diminuição na probabilidade de bloqueio, essa diminuição sendo mais considerável para cargas mais baixas em relação as mais altas. A aplicação de algoritmos mais sofisticados pode trazer resultados mais impactantes em todos os cenários. Com isso é possível afirmar que foi possível desenvolver novos conceitos relacionados a mecanismos de sobrevivência com o objetivo de buscar melhores estratégias na alocação de recursos requisitados, buscando promover economia e resiliência.

6.2 Trabalhos Futuros

Os possíveis trabalhos futuros consistem em buscar outras abordagens no particionamento do MPP e BSR, bem como outras estratégias para a reserva de *slots* e sua reutilização. Implementar o conceito de banda de guarda para diminuir a probabilidade de interferências entre requisições nas alocações dos *slots*.

Figura 32 – Abordagem para Trabalhos Futuros



Fonte: O autor.

Na Figura 29 é possível observar um outro tipo de abordagem na divisão total de banda para transmissão, onde todas as rotas ocupam e reservam parte de seus *slots*.

Referências

ASSIS, K. et al. Um Novo Esquema de Proteção com Economia de Banda em Redes Ópticas Elásticas. **SBrt**, Brasília, 13-16 set. 2012.

CANDIA, M. **Heurística para Alocação de Espectro em Redes Ópticas Elásticas Baseada em Medidas de Fragmentação**. 2014. Dissertação (Mestrado em Computação Aplicada) – INPE, São Paulo, 2014. Disponível em: <http://urlib.net/8JMKD3MGP7W/3FMFJ4S>. Acesso em: 25 set. 2022.

CARNEIRO, I. A. Brasil tem 4º maior tráfego de internet do mundo, segundo estudo. **Tecmundo**. 2020. Disponível em: <https://www.tecmundo.com.br/internet/150501-brasil-tem-4-maior-trafegointernet-mundo-segundo-estudo.htm?f>. Acesso em: 15 ago. 2022.

CAVALCANTE, M. A. et al. SimeEON: an open-source elastic optical network simulator for academic and industrial purposes. **Photonic Network Communications**, v. 34, n. 2, p. 193-201, 2017.

CORREIA, B. **Heurísticas e Meta-Heurísticas para Eficiente Alocação e Uso de Unidades de Desfragmentação Espectral em Redes Ópticas Elásticas**. 2018. Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal De Pernambuco, Pernambuco, 2018.

DIAS, C. Algoritmo de caminho de custo mínimo de Dijkstra - uma introdução detalhada e visual. **freeCodeCamp**. 2022. Disponível em: <https://www.freecodecamp.org/portuguese/news/algoritmo-de-caminho-de-custo-minimo-de-dijkstra-uma-introducao-detalhada-e-visual/>. Acesso em: 25 set. 2022.

NEO4J, Yen's algorithm Shortest Path. **neo4j**. 2022. Disponível em: <https://neo4j.com/docs/graph-data-science/current/algorithms/yens/>. Acesso em: 25 set. 2022.

DINARTE, H A. et al. Provisionamento Multicaminho com Otimização de Particionamento de Taxa de Transmissão para Proteção Dedicada em Redes Ópticas Elásticas. **SBrt**, Fortaleza, 26-29 set. 2021.

FONTINELE, A. et al. Alocação de Espectro com Redução de Interferências entre Circuitos em Redes Ópticas Elásticas. **SRBC**, Campos do Jordão, p. 561-574, 2018.

FREITAS, R. **Estratégia para Sobrevivência em Redes Ópticas Considerando Penalidades da Camada Física**. 2012. Tese (Doutorado) – Engenharia Elétrica, Universidade Federal de Pernambuco, Pernambuco, 2012.

FREITAS, R. et al. Sobrevivência em Redes Ópticas: Análise Comparativa entre Redes Transparentes e Redes Translúcidas. **SBrt**, Campina Grande, 16-19 set. 2018.

HELERBROCK, R. Fibra óptica. **Brasil Escola**. 2022. Disponível em: <https://brasilecola.uol.com.br/fisica/fibra-optica.htm>. Acesso em: 21 set. 2022.

JETBRAINS. CLion Um IDE multiplataforma para C e C++, 2022. Página inicial. Disponível em: <https://www.jetbrains.com/pt-br/clion/>. Acesso em: 01 out. 2022

JURKIEWICZ, Samuel. Grafos—uma introdução. São Paulo: **OBMEP**, 2009.

LIRA, C. et al. Estratégias de RSA Utilizando Split Spectrum e o algoritmo MSCL em EONS. **SBrT**, Florianópolis, 13-16 set. 2020.

LIRA, C. **Utilização de meta-heurística e de divisão espectral para alocação eficiente de espectro em redes ópticas elásticas**. 2016. Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal de Pernambuco, Pernambuco, 2016. Disponível em: https://www.ufpe.br/documents/39830/1359036/284_ClaytonLira. Acesso em: 23 set. 2022

LOURENÇO, A. **Técnicas de proteção e restauração em redes ópticas elásticas**. 2015. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de São Paulo, São Paulo, 2015.

MAURÍCIO, J. Redes Ópticas Densas. **Ispblog**. 2020. Disponível em: <https://www.ispblog.com.br/2020/08/10/redes-opticas-densas/>. Acesso em: 23 set. 2022.

MOTTA, M. P. da. Topologia dos backbones de internet no Brasil. **Soc. & Nat.**, Uberlândia, ano 24, n.1, p. 21-36, jan/abr. 2012.

MELO, G. S. de. **Introdução à teoria dos grafos**. 2014. Dissertação (Mestrado em Matemática) – Universidade Federal da Paraíba, Paraíba, 2014. Disponível em: <https://repositorio.ufpb.br/jspui/bitstream/tede/7549/5/arquivototal.pdf>. Acesso em: 23 set. 2022.

NASCIMENTO, A. O que é backbone?. **Canaltech**. 2014. Disponível em: <https://canaltech.com.br/telecom/o-que-e-backbone/>. Acesso em: 15 ago. 2022.

Noletto, C. C++: o que é, porque usar e quais as diferenças com C. **Trybe**. 2021. Disponível em: <https://blog.betrybe.com/linguagem-de-programacao/cpp/> Acesso em: 15 ago. 2022.

RAMASWAMI, Rajiv; SIVARAJAN, Kumar; SASAKI, Galen. **Optical networks: a practical perspective**. Morgan Kaufmann, 2009.

RODRIGUES, A. Em 2021, 82% dos domicílios brasileiros tinham acesso à internet. **AgênciaBrasil**. 2022. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2022-06/em-2021-82-dosdomicilios-brasileiros-tinham-acesso-internet>. Acesso em: 15 ago. 2022.

SANTI, J. de. et al. Roteamento em Múltiplas Rotas com Agregação Dinâmica de Fluxos com Duração Conhecida em Rede WDM. 2011. **CSBC**, 2011

SANTI, J. Agregação Dinâmica de Tráfego com Especificações de Tempo e Roteamento Multicaminho em Redes Ópticas WDM. 2015. Tese (Doutorado) – Ciência da Computação, Universidade Estadual de Campinas, São Paulo, 2015.

SANTOS, A. F. et al. Adaptação do Algoritmo BSR para Redes Ópticas Slice. **SBRC**, ano 31, p. 512-525, 2013.

SANTOS, M. **Abordagens para Atribuição de Espectro em Redes Ópticas Elásticas Baseadas em Perda de Capacidade Sob Múltiplas Rotas**. Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal de Pernambuco, Pernambuco, 2021.

SILVA, J. et al. 2016. **Um Algoritmo Eficiente de Roteamento Considerando Risco Compartilhado em Grupos de Enlaces**. 10.14209/sbrt.2016.224.

SILVA, R. C. L. Um algoritmo adaptativo alternativo para restauração em redes ópticas transparentes. 2014. Dissertação (Mestrado em Engenharia da Computação) – Universidade de Pernambuco, Pernambuco, 2014.

SILVA, T. Estratégia Híbrida de proteção dedicada e restauração dirigida por conexões de baixa prioridade com degradação diferenciada em redes EON para recuperação de desastres. 2022. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal da Bahia, Bahia, 2022.

SMITH, P. et al. **Network resilience: a systematic approach**. Communications Magazine, IEEE, vol. 49, p.88-97, jul. 2011.

SOUZA, J. V. de. **Tolerância a falha em redes ópticas de nova geração**. 2006. Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal do Pará, Pará, 2006.

TECHOPEDIA. O que é uma rede óptica?. **Techopedia**. 2022. Disponível em: <https://pt.theastrologypage.com/optical-network>. Acesso em: 21 set. 2022.

TELE.SINTESE. IX.br chega a 20 Tbitps de pico de tráfego, nova marca histórica. **Tele.síntese**. 2021. Disponível em: <https://www.telesintese.com.br/ix-br-chega-a-20-tbit-s-depico-de-trafego-nova-marca-historica/>. Acesso em: 15 ago. 2022.

UFSC. Algoritmo de Dijkstra para cálculo do Caminho de Custo Mínimo. **UFSC**. 2022. Disponível em: <https://www.inf.ufsc.br/grafos/temas/custo-minimo/dijkstra.html>. Acesso em: 25 set. 2022.

XAVIER, A. V. S. **Roteamento e proteção dedicada em redes ópticas usando inteligência computacional**. 2016. Tese (Doutorado) – Engenharia Elétrica, Universidade Federal de Pernambuco, Pernambuco, 2016.

ZHU, Z. et al. OpenFlow-Assisted Online Defragmentation in Single-/Multi-Domain Software-Defined Elastic Optical Networks. **J. Opt. Commun. Netw.** Vol. 7, p. A7-A15, jan. 2015.