Algoritmos RWA para Redes Ópticas Transparentes considerando Limitações da Camada Física

Este exemplar corresponde à redação final da Dissertação devidamente corrigida e defendida por Sávio Rodrigo Antunes dos Santos Rosa e aprovada pela Banca Examinadora.

Campinas, 07 de Maio de 2010.

Nelson Luis Saldanha da Fonseca
(Orientador)

Dissertação apresentada ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Rosa, Sávio Rodrigo Antunes dos Santos

R71a Algoritmos RWA para redes ópticas transparentes considerando limitações na camada física/Sávio Rodrigo Antunes dos Santos Rosa-- Campinas, [S.P. : s.n.], 2010.

Orientador : Nelson Luis Saldanha da Fonseca.

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Computação.

1.Redes de computadores. 2.Comunições oticas. 3.Confiabilidade (Engenharia). I. Fonseca, Nelson Luis Saldanha da. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Título em inglês: RWA algorithms for optical transparent networks considering physical impairments

Palavras-chave em inglês (Keywords): 1.Computer networks.. 2.Optical comunications. 3.Reability (Engineering).

Área de concentração: Sistemas de Computação

Titulação: Mestre em Ciência da Computação

Banca examinadora: Prof. Dr. Nelson Luis Saldanha da Fonseca (IC-UNICAMP)
Prof. Dr. Marcelo Luís Francisco Abbade (PUC-Campinas)
Prof. Dr. Edmundo Roberto Mauro Madeira (IC-UNICAMP)

Data da defesa: 07/05/2010

Programa de Pós-Graduação: Mestrado em Ciência da Computação

TERMO DE APROVAÇÃO

Dissertação Defendida e Aprovada em 07 de maio de 2010, pela Banca examinadora composta pelos Professores Doutores:

Prof. Dr. Marcelo Luís Francisco Abbade
PUC / Campinas

Prof. Dr. Edmundo Roberto Mauro Madeira
IC / UNICAMP

Prof. Dr. Nelson Luis Saldanha da Fonseca
IC / UNICAMP

Instituto de Computação
Universidade Estadual de Campinas

Algoritmos RWA para Redes Ópticas Transparentes considerando Limitações da Camada Física

Sávio Rodrigo Antunes dos Santos Rosa[1]

Maio de 2010

Banca Examinadora:

- Nelson Luis Saldanha da Fonseca (Orientador)
- Marcelo Luís Francisco Abbade PUC-Campinas
- Edmundo Roberto Mauro Madeira IC- UNICAMP
- Maurício Ferreira Magalhães FEEC-UNICAMP (Suplente)
- Flávio Keidi Miyazawa IC-UNICAMP (Suplente)

[1]Suporte financeiro de: FAPESP (processo 07/53604-0) 2007–2009

Resumo

Com a proliferação de novos serviços multimídia, tais como VoIP e IP-TV existe uma demanda crescente por altas taxas de transferência de dados. O núcleo da rede, por outro lado, deve ter sua capacidade continuamente dimensionada para para prover um serviço confiável aos usuários finais.

Nas Redes WDM, os caminhos ópticos consistem em circuitos ópticos fim-a-fim estabelecidos por meio da alocação de comprimento de onda em cada enlace de fibra óptica da rota origem-destino. Nas redes WDM transparentes, o sinal óptico pode trafegar sem sofrer conversão opto-eletro-óptica (O-E-O), minimizando o custo da rede, pois os equipamentos de comutação O-E-O são elementos de alto custo. Entretanto, apesar da vantagem na diminuição do custo, essas redes são mais susceptíveis às restrições de camada física, uma vez que o sinal não é regenerado a cada nó. Efeitos como Emissão Espontânea Amplificada (ASE), Dispersão de Modo de Polarização (PMD), entre outros, degradam a relação sinal-ruído óptica (OSNR) na recepção, podendo levar a taxas de erro de bits (BER) elevadas.

Além dos efeitos degradantes do sinal, uma outra grande questão em redes ópticas é a proteção. Mecanismos devem ser desenvolvidos para aumentar a confiabilidade dos serviços que fazem uso da rede. Dessa forma, quando uma fibra óptica sofre um corte, as chamadas que faziam uso dessa fibra devem ser reroteadas, a fim de que a duração da interrupção do sinal seja a menor possível.

Este trabalho apresenta um estudo das limitações da camada física no contexto de proteção em redes ópticas transparentes. Pela primeira vez os efeitos limitantes foram avaliados sobre redes com proteção por caminho compartilhado, e um novo algoritmo mais eficiente neste contexto foi desenvolvido. O estudo de confiabilidade diferenciada em redes submetidas a limitações físicas foi também analisado de forma inovadora.

Abstract

With the proliferation of new multimedia services such as VoIP and IP-TV, an increasing demand for high rates of data transfer is being seen. Thus, the demand on the core of the network is continuously growing, so its capacity must increase in the same ratio to provide a reliable service to end users. The Transparent Optical Networks with WDM appears as a solution to this problem. In this new technology, the channel of transmission of data is called the optical path, which consists of an end-to-end optical circuit established through the assignment of a wavelength on every link of fiber optic route of origin-destination. The optical signal can travel by the nodes of a totally transparent network without suffering conversion opto-electro-optical (OEO), minimizing the cost of the network, whose most expensive elements are the devices that perform OEO switching. However, despite the advantage to reduce the cost, it is observed that these networks are more susceptible to the restrictions of the physical layer, because the signal is not regenerated at each node. Amplified Spontaneous Emission (ASE), Polarization Mode Dispersion (PMD), among others, degrade the optical signal to noise ratio (OSNR) in reception, which could lead to a high bit error rate (BER).

Besides the degrading effects of the signal, another relevant issue in optical networks is protection. When the dependence on network resources is considerable, it is necessary to develop mechanisms to increase the reliability on services provided by the network. Thus, when a fiber optic is cut, the calls that did use this fiber need to be rerouted, so that the interruption of the signal has the smallest impact possible.

This thesis presents a study of the limitations of the physical layer protection in the context of transparent optical networks. For the first time, theses effects were studied over protected networks with shared path protection, and a more efficient novel algorithm has been developed. Differentiated reliability has also been analyzed.

Agradecimentos

Eu gostaria de agradecer ao meu orientador, Dr. Nelson Fonseca, por toda atenção e auxílio dispensados.

Ao colega André Costa Drummond pelo apoio e suporte desde o início com todo seu conhecimento a respeito de Redes Ópticas.

À agência financiadora FAPESP.

A Deus, que, de fato, tornou essa pesquisa possível.

Lista de Acrônimos

WDM Wavelength Division Multiplexing

ASE Amplified Spontaneous Emission

PMD Polarization Mode Dispersion

OSNR Optical Signal-to-Noise Ratio

BER Bit Error Rate

OEO Opto-Eletro-Óptica (Conversão)

ARPA Advanced Research Project Agency

SONET Synchronous Optical Network

SADM SONET Add-Drop-Multiplexers

DXC Digital Cross Connect

ADM Add-Drop-Multiplexers

OADM Optical Add-Drop-Multiplexers

ROADM Reconfigurable Add-Drop-Multiplexers

OADX Optical Add-Drop Switches

OXC Optical Cross Connect

FXC Fiber Switch Cross-Connects

WSXC Wavelength Selective Cross-Connect

WIXC Wavelength Interchanging Cross-Connect

RWA Routing and Wavelength Assignment

SLE Static Lightpath Establishment

DLE Dynamic Lightpath Establishment

PLI Programação Linear Inteira

SPM Self Phase Modulation

XPM Cross Phase Modulation

FWM Four Wave Mixing

IETF Internet Engineering Task Force

SSMF Standard Single Mode Fiber

DCF Dispersion Compensation Fiber

PDL Polarization Dependent Loss

SBS Stimulated Brillouin Scattering

SRS Stimulated Raman Scattering

SRLG Shared Risk Link Group

NSFNET National Science Foundation Network

CAC Controle de Acesso de Chamadas

SPPIAFF Shared Path Protection Impairment Aware First Fit

SPPIARP Shared Path Protection Impairment Aware Random Pick

Sumário

Lista de Tabelas

Lista de Figuras

Capítulo 1

Introdução

Com o aparecimento das redes de computadores, ocorrido na década de 60, possível graças ao financiamento da agência ARPA, novas aplicações, interessantes para a época, foram viabilizadas. Dentre elas, as mais importantes foram o correio eletrônico (e-mail) e o *login* remoto.

Desde então, após quase 50 anos de desenvolvimento uma séria de novas aplicações, antes inimagináveis, se tornaram viáveis. Hoje além de dados, as redes de computadores, sobretudo a Internet, são usadas para transmissão de imagem, áudio e vídeo. Essa evolução só foi possível graças a dois aspectos fundamentais:

- Desenvolvimento de hardware: processadores, memória, disco rígido e outros equipamentos mais rápidos possibilitaram um aumento na capacidade computacional disponível para os aplicativos desenvolvidos.

- Desenvolvimento da infra-estrutura de rede, possibilitando um maior volume de tráfego entre os terminais.

Com estas novas facilidades foi possível o desenvolvimento de um grande número de novas aplicações, muitas das quais passaram a exigir velocidades cada vez mais altas da rede. Dentre as principais aplicações que fazem grande uso de largura de banda, podem-se citar:

- VoIP: Os serviços de voz sobre IP, tem como principal finalidade a transmissão e roteamento de conversação humana pela Internet ou qualquer outra rede de computadores IP, e desse modo são capazes de prover telefonia de alta qualidade por meio de uma conexão de banda larga. Ano a ano, este serviço impõe uma competição cada vez maior com a telefonia convencional.

- Internet TV: sites de armazenamento e distribuição de vídeos, exemplificados por YouTube e Google Videos, foram amplamente difundidos nos últimos 5 anos, e hoje são conhecidos por todos, e largamente utilizados. Neste caso, a demanda por largura de banda é ainda maior, porque os vídeos são transmitidos em baixa definição, uma vez que as redes ainda não comportam a transmissão de vídeos de alta definição.

- IPTV: A transmissão de TV digital por meio de redes IP está começando a aparecer nos países desenvolvidos, e espera-se que, em poucos anos, torne-se popular o suficiente para competir com os atuais métodos de transmissão de TV, como TV a cabo e TV via satélite. Diferentemente da Internet TV, que é assistida pelo computador, a IPTV deve ser assistida na televisão. Espera-se que grandes redes privadas de alta velocidade sejam construídas para essa nova forma de transmissão.

- Jogos *on-line*: Jogos interativos on-line multi-usuários são largamente utilizados desde a década de 90. Esses jogos estão se tornando cada vez mais complexos, e por esse motivo, os requisitos de banda crescem continuamente.

A Figura 1.1 [4] apresenta o crescimento do uso de banda larga nos países com maior número de usuários de internet no mundo, o que evidencia a demanda dos consumidores por maiores velocidades na taxa de transmissão de bits, a fim de suprir a exigência das novas aplicações.

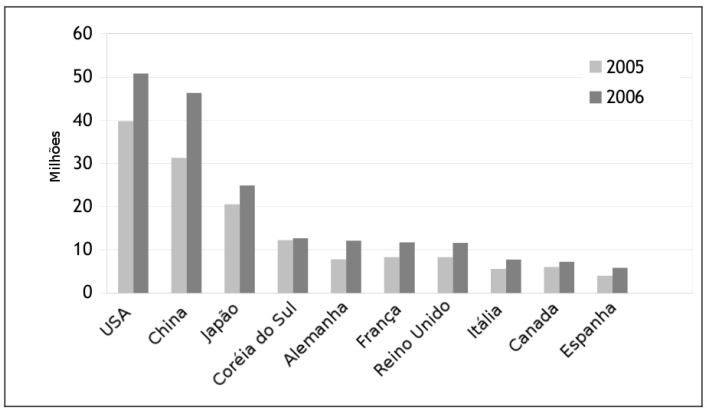


Figura 1.1: Evolução do uso de banda larga entre 2005 e 2006

Como se pode ver a demanda por altas velocidades é iminente, e sem dúvida, o método de transmissão mais veloz conhecido, nos dias de hoje, é dado pelas redes ópticas, que são capazes de prover as taxas de transmissão necessárias para atender à essa demanda, pelo

menos em nível das redes de núcleo, e em alguns casos até mesmo nas redes de acesso, como no caso da técnica *Fiber to the Home* (FTTH).

A tecnologia que permite as redes ópticas prover altas de transmissão é a Multiplexação por Comprimento de Onda (WDM). Esta técnica permite que sinais com comprimentos de onda diferentes, sejam multiplexados em uma única fibra, possibilitando a existência de diversos canais de transmissão em cada guia óptico. Equipamentos comerciais são capazes de transmitir cinquenta canais, cada um com uma taxa de transmissão de 40 Gbps, o que totaliza 2 TBps. Essa taxa é capaz de prover recursos suficientes para transmissão de todo tráfico de telefonia do planeta [29], em apenas uma fibra. Com um feixe de algumas centenas de fibras, como apresentado na Figura 1.2, é possível alcançar taxas que totalizam a demanda global atual de transmissão.

Figura 1.2: Feixe de fibras atinge transmissão superior ao tráfego do planeta

Apesar das vantagens das redes ópticas, estas possuem limitações. Uma delas é a atenuação inerente às fibras, que limita a distância máxima entre a origem e o destino, já que na ponta final, o sinal precisa ter energia suficiente para ser detectado por um receptor. Em geral, a distância máxima alcançada é de 100 km, o que é muito curto para possibilitar ligações intercontinentais. Existem, felizmente, amplificadores capazes solucionar esse problema. Dessa forma, para ligar distâncias maiores, basta projetar a rede de tal forma que o sinal seja amplificado sempre que estiver com energia inferior ao limite aceito pelos receptores.

Apesar dos amplificadores amenizarem a restrição da atenuação do sinal óptico, eles são responsáveis pela inserção de ruído. O método de amplificação consiste em aplicar energia sobre o sistema. A maior parte dessa energia é transferida para o sinal, entretanto uma pequena margem dela é transformada em ruído, através do processo chamado de emissão espontânea amplificada (ASE).

O ruído ASE é só um exemplo dos diversos efeitos degradantes do sinal, que são gerados pela interação entre os sinais na fibra, ou pelos equipamentos nos quais o sinal passa no

seu caminho entre a origem e o destino. Um estudo sobre esses efeitos será apresentado no Capítulo 4.

As redes ópticas são usadas principalmente nas redes de núcleo, que têm como objetivo a interligação de grandes áreas, podendo ser comparadas a *highways* ligando grandes cidades. Desse modo, uma falha nessas redes pode deixar grandes regiões sem transmissão, causando prejuízos catastróficos para as empresas que fazem uso do trecho da rede com falha.

Por esse motivo o estudo de proteção a falhas é muito importante. Uma vez que as falhas são inevitáveis, o gerente da rede deve desenvolver políticas para que as chamadas possam ser restauradas na eventualidade de um acidente. Ao mesmo tempo, a restauração deve ocorrer da forma mais rápida possível, de forma que a interrupção no serviço seja transparente ao usuário.

Este trabalho investiga os efeitos limitantes da camada física no oferencimento de proteção a falhas em redes ópticas transparentes. As principais contribuições apresentadas são:

- Desenvolvimento de dois novos algoritmos de proteção por caminho compartilhado que levam em consideração os efeitos degradantes do sinal, capazes de produzir resultados mais eficientes que os algoritmos tradicionais, tanto em relação ao aproveitamento de recursos como a confiabilidade oferecida
- Desenvolvimento de uma técnica de proteção com confiabilidade diferenciada, capaz de atender demandas com diferentes requisitos.

Esta dissertação está organizada da seguinte forma: o Capítulo 2 apresenta o estado da arte das redes ópticas, e o Capítulo 3, dos métodos de proteção, atualmente. O Capítulo 4 descreve os principais efeitos degradantes do sinal, e o Capítulo 5 estuda seus impactos sobre as transmissões ópticas. O Capítulo 6 apresenta dois novos algoritmos de proteção que levam em consideração tais efeitos e são capazes de produzir resultados mais eficientes que os algoritmos tradicionais. Por fim, o Capítulo 7 apresenta uma nova técnica de proteção com confiabilidade diferenciada.

Capítulo 2

Redes Ópticas

Como introduzido no capítulo anterior, as redes ópticas são largamente adotadas para a provisão de altas taxas de transmissão de bits aos usuários. Dois são os principais motivadores dessa adoção:

- **Banda passante**: A transmissão de dados pode ser realizada sobre comprimentos de onda muito pequenos (em geral, 1400nm 1600nm), o que permite uma largura de banda extremamente grande (ordem de grandeza de Terahertz). Com a disponibilidade de grande banda passante, pode-se obter taxas de transmissão muito maiores do que se obtém ao se utilizar outros meios.

- **Atenuação**: As fibras ópticas possuem pequenas taxas de atenuação. Quando utilizada na faixa de comprimentos de onda entre 1400nm e 1600nm, pode-se obter uma atenuação de apenas 0,2 db/km, o que permite o seu uso na interligação de pontos muito distantes, uma vez que, mesmo viajando grandes distâncias, o sinal ainda é capaz de chegar ao receptor com potência suficiente para ser entendido.

Outra fator que tornou ainda mais vantajosa a utilização de redes ópticas foi o desenvolvimento da tecnologia de multiplexação por comprimento de onda (*Wavelength Division Multiplexing* - WDM). Antes dessa técnica, transmitia-se apenas um sinal por fibra, geralmente de baixa capacidade (menos de 10 Gbps). Após o desenvolvimento da tecnologia WDM, tornou-se possível transmitir uma grande quantidade de sinais em apenas uma fibra, cada um deles em um comprimento de onda que ocupa uma pequena faixa de freqüência. Desta forma, passou-se a utilizar a banda passante disponível, de forma muito mais eficiente, dividindo-a em diversos canais, que são transmitidos, simultaneamente, sobre uma mesma fibra.

2.1 Arquiteturas de Nós Ópticos

O tráfego que passa por um equipamento em um nó pode ser representado, de forma geral, por uma *tupla* (fibra óptica, comprimento de onda, fatia de tempo). Um nó ideal seria capaz de efetuar a comutação entre todos estes níveis. No entanto, devido a questões de custo e escalabilidade, arquiteturas de nós com diferentes capacidades, em geral inferiores, são adotadas.

Em anéis SONET, as fibras são interconectadas por SONET *Add-Drop-Multiplexers* (SADM), que possuem a capacidade de comutar o tráfego no nível de fatia de tempo. Em redes SONET em malha, as fibras são interconectadas por *Digital Cross Connects* (DXCs), que, diferentemente dos ADMs, possuem várias fibras de entrada e de saída. Em anéis WDM, ao invés de serem utilizados um SADM por comprimento de onda, ADMs Ópticos (OADMs) são empregados (Figura 2.1). Um OADM permite que caminhos ópticos passem diretamente sem sofrer conversão opto-elétrica, bem como permite a iniciação e o término de caminhos ópticos. Por não efetuar conversão de comprimento de onda, caminhos ópticos que atravessam OADMs devem satisfazer a restrição de continuidade de comprimento de onda (*wavelength-continuity constraint*), ou seja, o mesmo comprimento de onda deve ser utilizado em todos os enlaces nos quais o caminhos óptico passar. Para cada comprimento de onda que é adicionado, utiliza-se um SADM para processar eletronicamente o tráfego carregado pelo comprimento de onda. É sabido que o custo dos equipamentos de conversão O-E-O são os principais responsáveis pelo custo da rede, portanto, o número de SADMs disponíveis em um OADM é normalmente o objetivo a ser minimizado, ou a restrição a qual um problema de otimização está sujeito.

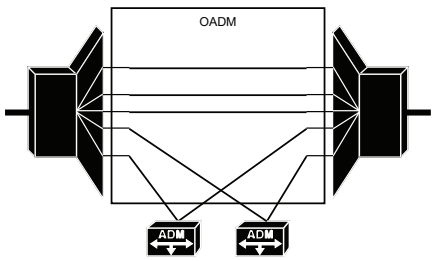


Figura 2.1: OADM - Optical Add-Drop Multiplexer

Em contraste aos OADMs, que em geral possuem SADM dedicados para alguns comprimentos de onda, OADMs Reconfiguráveis (ROADMs) podem adicionar ou descartar comprimentos de onda de forma seletiva (Figura 2.2). Além dos OADMs, *Optical Add-Drop Switches* (OADX) são produzidos comercialmente. Um OADX é a integração de um OADM e um DXC, logo OADX podem ser utilizados em redes de malha. De uma

forma geral, OADX podem ser vistos como um caso especial dos *Optical Cross Connects* (OXCs), que são a tecnologia a ser empregada nas redes em malha no futuro.

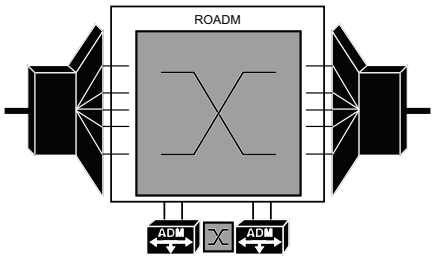


Figura 2.2: ROADM - Reconfigurable Optical Add-Drop Multiplexer

Três classes de OXC foram definidas:

- *Fiber Switch Cross-Connects* (FXC);
- *Wavelength Selective Cross-Connect* (WSXC): comuta um subconjunto de comprimentos de onda de uma fibra de entrada para uma fibra de saída;
- *Wavelength Interchanging Cross-Connect* (WIXC): são WSXC com capacidade de conversão de comprimento de onda.

Um OXC é similar a um ROADM, exceto pelo fato de que eles permitem múltiplas fibras de entrada e saída. O número de fibras de entrada, normalmente, é igual ao número de fibras de saída, porém em [27] o projeto OXCs com um número diferente de fibras de entrada e saída é apresentado. Um OXC, em geral, possui duas matrizes de comutação (switching fabrics) e uma matriz de comutação de comprimentos de onda, que efetua a comutação no nível do comprimento de onda. [37] (Figura 2.3).

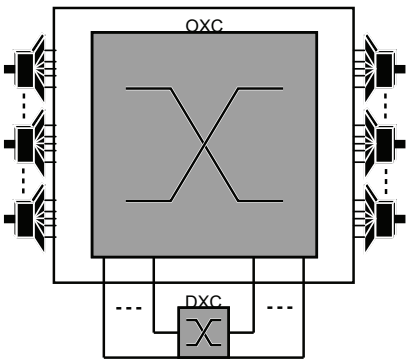


Figura 2.3: OXC - Optical Cross-Connect

Como foi mostrado, dependendo da arquitetura do nó, o nó pode trabalhar no nível da fibra, comprimento de onda ou fatia de tempo, e em cada um desses níveis ele pode ter uma funcionalidade completa ou limitada.

2.2 Regeneração do Sinal

Cada nó em uma rede óptica é responsável por efetuar a comutação dos sinais que recebe. A tecnologia tradicional, ainda largamente utilizada, requer que o sinal seja totalmente convertido do domínio óptico para domínio eletrônico para poder ser comutado. Depois de passar pela fase de comutação, o sinal precisa novamente ser convertido, dessa vez para o domínio óptico, para que então possa ser transmitido pela próxima fibra. Essa conversão do sinal é conhecida como regeneração opto-eletro-óptica (O-E-O), e apresenta um custo muito alto, uma vez que cada nó passa a necessitar de um número muito grande de receptores e transmissores, equipamentos que ainda são muito caros.

Há ainda a possibilidade de que a comutação em um nó seja feita exclusivamente em domínio óptico. Isso só foi possível graças ao desenvolvimento dos OXCs (*Optical Cross Connects*), equipamentos que substituem os comutadores eletrônicos. Nos OXCs, receptores e transmissores são necessários apenas para os sinais que têm, respectivamente, o dispositivo como nó destino ou origem. Sinais que tratam um OXC como nó intermediário podem sofrer comutação sem que sejam necessários receptores ou transmissores. Esta diminuição no uso de tais equipamentos faz com que o custo de um nó seja muito menor, o que torna muito vantajoso o uso deste dispositivo.

As redes ópticas podem ser classificadas segundo o nível de regeneração de sinal que apresentam. As seguintes três classificações são possíveis:

- Opacas, nas quais todos os nós efetuam comutação em nível eletrônico.
- Transparentes, nas quais todos os nós são capazes de efetuar comutação do sinal apenas no domínio óptico.
- Translúcidas, nas quais parte dos nós efetuam comutação em domínio eletrônico (opacos) e parte exclusivamente em domínio óptico (transparentes).

2.2.1 Redes Ópticas Transparentes

Uma rede óptica pode ser classificada quanto sua transparência em opaca e transparente. Redes ópticas opacas efetuam conversões (O-E-O) nos nós de um caminho, nos quais o sinal é regenerado em sua forma elétrica e pode ser comutado neste nível, para depois ser novamente convertido na forma óptica e transmitido. [14] Como em cada nó, o sinal

é regenerado, as restrições da camada física são menos evidentes em redes opacas, entretanto, apresenta desvantagem do alto custo, já que os conversores O-E-O são os elementos mais caros de uma rede óptica. Com o objetivo de minimizar o custo, nas redes transparentes, o sinal é comutado sem precisar sofrer regeneração para o domínio elétrico, sendo transportado por em um caminho óptico ou *lightpath*.

O caminho óptico representa uma conexão direta entre dois nós terminais e deve ser estabelecido antes que a transmissão possa iniciar. Para estabelecer o caminho óptico e respeitar a "restrição de continuidade do comprimento de onda", é necessário que o mesmo comprimento de onda esteja alocado em cada enlace que participa do caminho escolhido entre dois pontos. Tal propriedade torna a modelagem das redes ópticas diferente das tradicionais redes de comutação de circuitos da telefonia fixa [5].

Em uma rede óptica, pedidos de estabelecimento de caminhos ópticos entre dois pontos quaisquer são feitos sob demanda, e são estabelecidos sobre uma "camada virtual". Mesmo que um link não esteja disponível na topologia física para ligação entre estes dois pontos, ele pode ser estabelecido na camada virtual, e corresponderá a uma rota passando por nós intermediários na topologia física. A Figura 2.4 ilustra a relação entre essas duas camadas. O link "a-c" virtualmente alocado, pode corresponder, por exemplo, a rota que passa pelos nós físicos A, B e C. O problema de encontrar uma rota para as demandas da camada virtual, e alocar um comprimento de onda para cada pedido é chamado de RWA (*routing and wavelength assignment*).

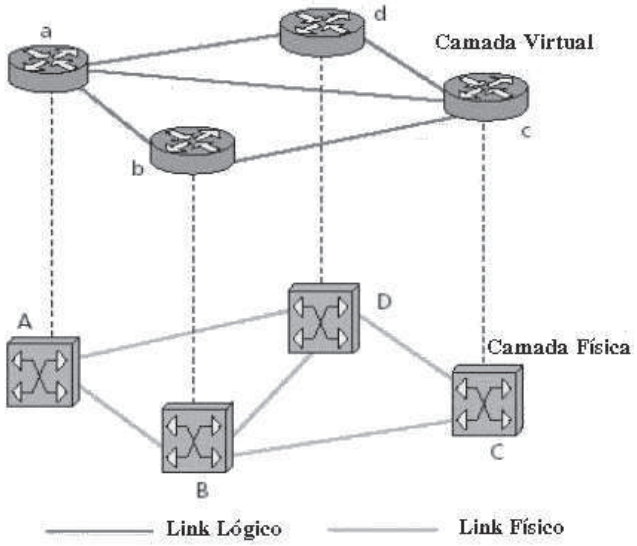


Figura 2.4: Relação entre camadas virtual e física

Uma vez que um pedido é atendido e o caminho foi estabelecido, este permanece

ativo por um período de tempo determinado. Enquanto o caminho óptico está ativo, ele ocupa um comprimento de onda específico de cada enlace da rota origem-destino, e este comprimento de onda é liberado quando o caminho é desfeito. Claramente, o mesmo comprimento de onda não poderá ser alocado a mais de um caminho óptico no mesmo enlace da rede. Dessa forma, quanto mais caminhos forem alocados sobre a rede óptica, menor é o número de comprimentos de onda disponíveis e, portanto, maior é a probabilidade de que um novo caminho não possa ser alocado por falta de recursos. [5]

2.3 Algoritmos RWA

As redes WDM têm sido utilizadas como tecnologia *de facto* nas transmissões ópticas. Em tais redes, para que se possa transmitir dados entre origem e destino, é necessário que exita uma conexão entre esses dois pontos, assim como acontece nas redes comutadas por circuitos. Tal tarefa pode ser realizada encontrando-se um caminho entre os dois nós e reservando um comprimento de onda livre em todas as fibras ao longo do caminho. No jargão de redes ópticas, tal caminho é chamado de *lightpath* e pode conter muitos nós intermediários transparentes, alocando-se um canal WDM em cada um dos links componentes. Durante todo o tempo de conexão a largura de banda de um *lightpath* permanece reservada, e quando o *lightpath* for desfeito, os comprimentos de onda que o compunham tornam-se disponíveis.

Quando a rede não apresenta conversão de comprimento de onda, é necessário que um *lightpath* utilize o mesmo comprimento de onda em todas as fibras que o compõem, o que é conhecido como restrição de continuidade de comprimento de onda. Tal restrição pode ser responsável por uma grande ineficiência na utilização dos canais WDM. Para superar esse entrave, muitas vezes o que se faz é prover uma conversão limitada, na qual apenas parte dos comprimentos de onda podem ser convertidos.

Para que se faça uma utilização eficiente dos canais WDM disponíveis, o principal ponto a ser otimizado é o estabelecimento de *lightpaths*. Dessa forma, é necessário que o ato de prover uma rota a um *lightpath* e alocar comprimentos de onda a essa rota seja otimizado. Este problema é conhecido como **Roteamento e Alocação de Comprimento de Onda** (*Routing and Wavelength Assignment* - RWA). A alocação de comprimento de onda deve proceder de forma que dois *lightpaths* que compartilham um mesmo link não usem o mesmo comprimento de onda. Além disso, deve respeitar a restrição de continuidade, ou seja, a todos os links de um *lightpath* deve ser alocado um mesmo comprimento de onda.

O problema RWA é de grande importância. Uma boa solução permite que os recursos sejam utilizados, de tal forma que mais conexões possam ser aceitas, e um número menor delas sejam rejeitadas em momentos de grande utilização.

Um grande número de técnicas existe para resolver este importante problema. Em geral, estas técnicas podem ser classificadas em duas grandes categorias:

- **Estabelecimento estático de caminhos ópticos (*Static Lightpath Establishment* - SLE)**: Assume-se que a demanda é fixa e previamente conhecida, dessa forma, todos os pedidos de conexão que precisam ser estabelecido são conhecidos desde o princípio. Almeja-se, portanto, atender a demanda requisitada, otimizando a utilização de recursos da rede.

- **Estabelecimento dinâmico de caminhos ópticos (*Dynamic Lightpath Establishment* - DLE)**: As requisições de conexão são feitas assim que necessárias e não são conhecidas previamente. Um pedido de estabelecimento de caminho óptico é efetuado em determinado instante, utilizando os recursos da rede por um período de tempo. Quando o caminho óptico é encerrado, os recursos utilizados são liberados para uso por outras conexões.

Tanto o problema estático como o dinâmico esbarram na complexidade da busca por uma solução ótima. Provou-se em [3] que o estabelecimento estático de caminhos ópticos é NP-completo, reduzindo o problema ao problema coloração de grafos. Em geral, a solução pode ser encontrada através da formulação das restrições em programação linear inteira (PLI), entretanto a complexidade de uma PLI não permite que se obtenha uma solução escalável. Para superar este entrave, desenvolvem-se heurísticas que tornam possível a resolução do problema, embora os resultados obtidos não sejam ótimos. Um exemplo muito comum é a divisão do algoritmo em duas sub-partes: na primeira, trabalha-se para obter uma rota que seja capaz de interligar origem a destino, enquanto na segunda trata-se de encontrar um comprimento de onda livre em todos os enlaces que compõem a rota. Em outras palavras, faz-se a divisão do problema em um sub-problema de roteamento e outro de alocação de comprimento de onda. A forma como as heurísticas são utilizadas na resolução destas sub-partes pode ter grande impacto na utilização dos recursos da rede e na taxa de pedidos de estabelecimento de conexões aceitas.

Na próxima subseção, apresenta-se uma formulação do problema, representando suas restrições por meio de programação linear inteira, e nas duas subseções subsequentes apresentam-se heurísticas para resolução dos sub-problemas de roteamento e de alocação de comprimento de onda.

2.3.1 Formulação do Problema

Quando se deseja obter uma solução ótima para o problema de roteamento e alocação de comprimento de onda, o uso da programação linear inteira é o mais aconselhado.

Embora computacionalmente essa solução não seja escalável, quando a rede sobre a qual se pretende resolver o problema é de pequeno porte, o que acontece na maioria dos casos, a PLI apresenta bons resultados.

Nesta subseção, introduz-se uma formulação do problema RWA utilizando PLI, apresentada em [19] e proposta em [23]. O objetivo desta formulação é a maximização do número de caminhos ópticos, a fim de atender o maior número possível de conexões requisitadas.

Considere-se uma topologia de rede representada pelo grafo $G = (V, E)$, na qual V é um conjunto de nós $\{v_1, v_2, v3, ..., v_n\}$ e E é um conjunto de enlaces $\{e_1, e_2, e_3, ..., e_m\}$, sendo que cada e_a representa uma fibra interligando dois nós v_b a v_c. A matriz de tráfego T, previamente conhecida, é dada por elementos $T_{i,j}$ que representam o número de conexões requisitadas para interligação do nó v_i ao nó v_j. O conjunto de todos os requisitos de conexões é dado por K, na qual cada conexão k tem como origem s_k e destino d_k e ocupa exatamente a capacidade de um canal WDM. Cada um dos canais WDM é representado por um comprimento de onda λ_i. O conjunto $\{\lambda_1, \lambda_2, \lambda_3, ..., \lambda_W\}$ de comprimentos de onda disponíveis em cada fibra é dado por L, sendo que cada λ_i possui a mesma capacidade de transmissão.

A partir do que foi exposto, o roteamento e alocação de comprimento de onda pode ser formalmente descrito como o problema de se encontrar uma rota p e um comprimento de onda λ disponíveis de forma que dois caminhos ópticos distintos que compartilham um enlace na rede óptica não tenham um comprimento de onda em comum.

Para representação matemática do PLI, considera-se um conjunto de variáveis preliminares que são úteis na formulação:

$$x_k = \begin{cases} 1 \text{ se a conexão } k \text{ é aceita} \\ 0 \text{ caso contrário} \end{cases} \tag{2.1}$$

$$x_k^\lambda = \begin{cases} 1 \text{ se o comprimento de onda } \lambda \text{ está livre para a conexão } k \\ 0 \text{ caso contrário} \end{cases} \tag{2.2}$$

$$x_{ke}^\lambda = \begin{cases} 1 \text{ se o comprimento de onda } \lambda \text{ está livre para a conexão } k \text{ no enlace } e \\ 0 \text{ caso contrário} \end{cases} \tag{2.3}$$

$$x_p^\lambda = \begin{cases} 1 \text{ se existe um caminho óptico definido com rota } p \text{ e comprimento de onda } \lambda \\ 0 \text{ caso contrário} \end{cases} \tag{2.4}$$

$$\omega^{+}(v_i) = \text{conjunto de enlaces que saem do nó } v_i \tag{2.5}$$

$$\omega^{-}(v_i) = \text{conjunto de enlaces que entram no nó } v_i \tag{2.6}$$

A partir dessas variáveis, apresenta-se o seguinte PLI:

$$\max z_{KS1}(x) = \sum_{k \epsilon K} x_k \tag{2.7}$$

sujeito a:

$$\sum_{e \epsilon \omega^{+}(v_i)} x_{ke}^{\lambda} = \sum_{e \epsilon \omega^{-}(v_i)} x_{ke}^{\lambda} \;\; k \epsilon K, \; \lambda \epsilon L, \; v_i \epsilon V \tag{2.8}$$

$$\sum_{e \epsilon \omega^{+}(s_k)} x_{ke}^{\lambda} - \sum_{e \epsilon \omega^{+}(s_k)} x_{ke}^{\lambda} = x_k^{\lambda} \;\; k \epsilon K, \; \lambda \epsilon L \tag{2.9}$$

$$\sum_{e \epsilon \omega^{+}(d_k)} x_{ke}^{\lambda} - \sum_{e \epsilon \omega^{+}(d_k)} x_{ke}^{\lambda} = x_k^{\lambda} \;\; k \epsilon K, \; \lambda \epsilon L \tag{2.10}$$

$$\sum_{k \epsilon K} x_{ke}^{\lambda} \leq 1 \;\; e \epsilon E, \; \lambda \epsilon L \tag{2.11}$$

$$\sum_{\lambda \epsilon L} x_k^{\lambda} = x_k \;\; k \epsilon K \tag{2.12}$$

$$x_{ke}^{\lambda} \leq x_k^{\lambda} \;\; k \epsilon K, \; e \epsilon E, \; \lambda \epsilon L \tag{2.13}$$

$$x_k, x_k^{\lambda}, x_{ke}^{\lambda} \;\; k \epsilon K, \; e \epsilon E, \; \lambda \epsilon L \tag{2.14}$$

As equações 2.8 a 2.10 têm como objetivo a garantia da restrição de continuidade de comprimento de onda. A equação 2.11 garante que não seja possível a atribuição de um mesmo comprimento de onda a dois caminhos ópticos que compartilham um mesmo comprimento de onda. A equação 2.12 faz com que seja atribuído um, e somente um comprimento de onda a todo caminho óptico, e, por fim, as equações 2.13 e 2.14 tem como objetivo a garantia da consistência do PLI.

2.3.2 Roteamento

Embora a formulação do problema RWA através de um PLI garanta soluções ótimas, a obtenção da solução demanda complexidade computacional alta, uma vez que a programação linear inteira é um problema NP-Completo, que é ainda mais problemático no caso de estabelecimento dinâmico de caminhos ópticos, pois a cada novo pedido de conexão, deseja-se que a resposta ao pedido seja a mais rápida possível. Nesses casos,

permite-se que heurísticas que levam a soluções sub-ótimas sejam adotadas em troca de uma menor complexidade computacional.

São apresentadas a seguir três heurísticas conhecidas na literatura para o sub-problema de roteamento. São elas:

Roteamento Fixo

A técnica conhecida como *Fixed Routing* é a mais simples. Dada uma topologia, e um par origem-destino, a resposta de um algoritmo que utilize a abordagem de roteamento fixo será sempre a mesma rota, não importando qual seja o estado da rede. O algoritmo de Dijkstra é o exemplo mais comum de utilização desta abordagem: cada par origem-destino será sempre mapeado na mesma rota (a menor possível).

Apesar da simplicidade, a técnica, muitas vezes, não leva a bons resultados, dado que nem sempre será possível encontrar um comprimento de onda disponível para uma rota fixa, enquanto que uma rota alternativa pode acolher o caminho óptico. A abordagem de roteamento fixo pode levar, consequentemente, a uma probabilidade de bloqueio de conexões muito alta.

Roteamento Fixo e Alternativo

Na abordagem conhecida como *Fixed-Alternate Routing*, além de uma rota fixa, o algoritmo deve retornar um conjunto de rotas alternativas. Chama-se primária a primeira rota retornada pelo algoritmo. Para que uma rota seja classificada como alternativa, deve ser disjunta a rota primaria. Em um exemplo que segue, inicialmente aplica-se o algoritmo de Dijkstra a uma topologia T, e o resultado será considerado a rota primária P. A partir daí, retira-se da topologia T todos os links de P, gerando a topologia T', sobre a qual se aplica novamente o algoritmo de Dijkstra, gerando uma rota alternativa A. Esse procedimento pode ser repetido a fim de se encontrar tantas rotas alternativas quanto seja necessário (e quanto a rede seja capaz de fornecer).

No contexto de RWA, os resultados gerados por essa técnica são muito melhores que os obtidos para a anterior. Assim que um novo pedido de conexão é feito, executa-se a busca por rotas que são temporariamente armazenadas. A rota primária é então submetida a alocação de comprimento de onda, e em caso de sucesso, a conexão é aceita, mas em caso de fracasso a conexão não é bloqueada, como aconteceria no caso anterior. Ao invés disso, submete-se a primeira rota alternativa a alocação de comprimento de onda, e em caso de fracasso, submete-se a segunda alternativa. A conexão será bloqueada somente se não for possível alocar um comprimento de onda a nenhuma das rotas. Com isso a probabilidade de bloqueio diminui quando comparada a utilização de roteamento fixo.

Roteamento Adaptativo

O roteamento adaptativo deve produzir rotas diferentes, de acordo com o estado da rede. Em outras palavras, nessa abordagem é possível adaptar o roteamento à utilização da rede, de forma a encontrar rotas que englobam somente os recursos disponíveis, o que não é possível em uma abordagem de roteamento fixo ou fixo e alternativo.

Para exemplificar o roteamento adaptativo, considera-se um algoritmo que funciona da seguinte forma: dada uma topologia baseada em camadas, na qual cada uma delas representa um comprimento de onda quando uma nova conexão for requisitada e estabelecida na rota p e no comprimento de onda λ, deve-se anular ou mudar para ∞ os pesos dos enlaces da topologia representante do comprimento de onda λ. Dessa forma, a busca por uma rota não considera os enlaces que não estão disponíveis, tornando a busca por rotas muito mais eficiente do que nas outras abordagens de roteamento. Tem-se, portanto, a vantagem de que a probabilidade de bloqueio produzida por algoritmos de roteamento adaptativo é mais baixa. Entretanto, existe uma desvantagem do ponto de vista computacional, uma vez que a técnica requer que seja mantido o estado da rede para cada comprimento de onda, aumentando o uso de memória, além da necessidade de se efetuar a busca por rotas em cada uma das camadas, aumentando-se o esforço computacional necessário.

2.3.3 Alocação de comprimento de onda

Existe na literatura um número muito grande de heurísticas para resolução do problema de alocação de comprimento de onda. Dependendo do objetivo, cada uma delas pode oferecer um resultado melhor. Nesta subseção, apresentam-se algumas das heurísticas mais conhecidas, que quando utilizadas, em conjunto, com um algoritmo de roteamento eficiente podem produzir bons resultados para o problema RWA. São elas:

First-Fit :

Busca-se fazer uma alocação ordenada dos comprimentos de onda para uma rota p. Inicia-se verificando se o primeiro comprimento de onda (λ_1) está disponível em todos os enlaces da rota p. Em caso positivo, aceita-se o caminho óptico com rota p e λ_1. Em caso negativo, executa-se o mesmo procedimento para $\lambda_2, \lambda_3, ..., \lambda_n$, até que algum comprimento de onda seja encontrado ou a rota não possa ser aceita. Esse método mantém os primeiros comprimentos de onda muito mais carregados que os últimos, já que aqueles são preferidos a estes.

Random-Pick :

Nesta técnica, a busca por um comprimento de onda disponível é forma aleatória.

Dado que se tem uma rota p, obtém-se um inteiro aleatório k_1 e verifica-se se o comprimento de onda λ_{k_1} está disponível em todas os enlaces da rota p. Em caso positivo, pode-se aceitar a conexão e estabelecer o caminho óptico. Em caso negativo, executa-se a mesma verificação para $\lambda_{k_2}, \lambda_{k_3}, ..., \lambda_{k_n}$ até que se encontre um comprimento de onda ou a rota seja rejeitada. Com essa abordagem, ocorre uma distribuição da carga, uma vez que cada um dos comprimentos de onda pode ser igualmente escolhido.

Menos Usado (*Least-Used*) :

Em *Least-Used* tem-se como objetivo a distribuição da carga, buscando-se alocar primeiro os comprimentos de onda menos utilizados. Dado que k_1 é o índice do comprimento de onda menos usado, k_2 do segundo menos usado até k_n, a verificação por um λ que esteja disponível em todos os enlaces de uma determinada rota deve seguir a ordem $\lambda_{k_2}, \lambda_{k_2}, ..., \lambda_{k_n}$. Este método tem funcionamento bastante semelhante a Random-Pick, uma vez que ambos distribuem a carga, mas seu desempenho computacional é inferior, já que é necessário manter uma ordem de utilização dos comprimentos de onda.

Mais Usado (*Most-Used*) :

Na abordagem *Most-Used*, busca-se alocar primeiro os comprimentos de onda mais utilizados, levando a uma concentração da carga. Por esse motivo, seu comportamento é bastante semelhante ao de First-Fit, mas o desempenho computacional é pior, pela necessidade de se manter a ordem de utilização dos comprimentos de onda.

Produto Mínimo (*Min-Product*) :

Este método é utilizado no contexto de múltiplas fibras, no qual cada enlace é constituído por duas ou mais fibras. Supondo que se tem uma rota p, e dado que em cada enlace l e cada comprimento de onda w, D_{lw} fibras são utilizadas, calcula-se o seguinte produtório para cada w:

$$F(w) = \prod_{l \epsilon p} D_{lw}$$

O menor produto obtido revela o comprimento de onda no qual as fibras são menos utilizadas e, para minimizar o número de fibras, deve-se alocá-lo para o novo caminho óptico.

Menos Carregado (*Least-Loaded*) :

Este mecanismo também foi projetado para um contexto de múltiplas fibras por

enlace. Considera-se que a alocação de um comprimento de onda para uma rota p. L_w é o número de fibras usadas pelo enlace mais carregado da rota p no comprimento de onda w. O objetivo é encontrar o valor w tal que L_w seja o menor possível. Busca-se, portanto, diminuir o uso de enlaces muito carregados, levando a uma distribuição mais uniforme da carga pelos comprimentos de onda possíveis. Isto faz com que *Least-Loaded* produza resultados eficazes em termos de probabilidade de bloqueio.

Capítulo 3

Sobrevivência em Redes Ópticas

Com a difusão da Internet, a adoção de uma série de novos serviços tornam a humanidade cada vez mais dependente dessa rede. Quando se trata de um *backbone*, a dependência é ainda maior, uma vez que estas redes interligam grandes regiões, transmitindo os dados de uma quantidade enorme de usuários finais. Nessas redes, o corte de uma fibra leva à interrupção de serviço de toda uma região, produzindo efeitos negativos e, por conseqüência, gerando prejuízos.

Em outras situações a tolerância a falhas é ainda mais importante. Imagine o caso de um hospital que utiliza um sistema de monitoramento a distância, mantendo informações biofísicas de seus pacientes, tais como número de batimentos cardíacos, pressão sangüínea, dentre outras características que são importantes para a identificação de possíveis problemas. Para que o sistema seja eficiente, as variáveis de cada paciente devem ser atualizadas com freqüência. Falhas na rede que transmite esses dados podem ter sérias consequencias, sob risco de interrupção do monitoramento e ocorrência de potenciais danos a saúde dos pacientes.

A sobrevivência em redes ópticas tem como objetivo o pronto reestabelecimento de conexões que tenham sofrido algum tipo de falha. Dois tipos de falhas podem acontecer em uma rede óptica:

- **Falha de um Nó:** um nó em uma rede óptica é constituído por uma série de equipamentos: multiplexadores, demultiplexadores, comutadores, entre outros. Uma falha em qualquer um desses equipamentos pode levar à interrupção na transmissão do sinal. Felizmente, os equipamentos modernos possuem redundância integrada. Com isso, o problema de falha em um nó tem sido menos comum.

- **Falha de um Enlace:** duas são as possibilidades de ocorrência de falha em um enlace: corte de uma fibra ou mal-funcionamento de amplificadores ao longo do

caminho. Os cortes de fibras são, em geral, muito comuns, e por esse motivo a falha de um enlace precisa ser levada em consideração.

Em linhas gerais, o procedimento para se prover sobrevivência recupera a transmissão de uma conexão transmitindo os dados por uma rota alternativa àquela que sofreu uma falha. Duas etapas são utilizadas na execução desse mecanismo:

Proteção :
Para que se tenha uma rota alternativa para transmitir os dados em caso de falha, é necessário que se reserve recursos exclusivamente para esse fim. A etapa de proteção realiza essa tarefa. Assim que um novo pedido de conexão é feito, o Controle de Acesso de Chamadas deve alocar um caminho óptico para transmissão de dados, chamado de caminho primário; e ao mesmo tempo deve reservar uma rota alternativa para o caso de uma falha, chamado de caminho de *backup*.

Restauração :
Na etapa de restauração, busca-se encontrar um método eficiente na realização da transição do caminho primário para o caminho de backup.

Na Seção 3.1, estudam-se diferentes abordagens existentes na literatura para se prover proteção em uma rede, e, na Seção 3.2, são apresentados importantes aspectos na restauração de conexões.

3.1 Proteção

Existem diferentes métodos de se prover proteção em redes ópticas. O que estes tem em comum é que se deve reservar recursos para que se possa recuperar uma conexão no caso de uma falha. Os métodos de proteção podem ser classificados da seguinte forma:

Proteção de Enlaces :
Cada um dos enlaces utilizados por caminhos primários em uma rede é protegido de forma independente. Na Figura 3.1, vemos como funciona esse mecanismo. O caminho primário $1-6-5-4$ sofreu falha em um de seus enlaces $(6-5)$, que tinha como rota alternativa $6-2-3-5$. A partir do momento em que ocorrer a restauração, a conexão terá seus dados transmitidos por um novo caminho: a rota $1-6-2-3-5-4$.

Proteção de Caminhos :
Nesta abordagem, cada um dos caminhos tem sua própria rota de proteção. Sendo assim, na ocorrência de uma falha em um enlace, não temos uma proteção exclusiva

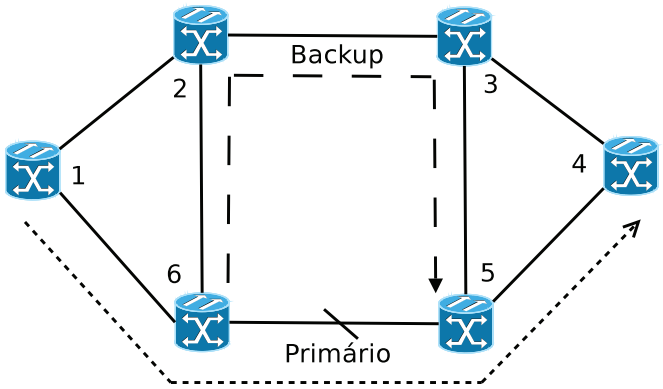


Figura 3.1: Proteção de Enlaces

para o enlace falho, mas para toda a rota que teve interrupção em seu serviço. A Figura 3.2 ilustra esse tipo de proteção: o caminho primário $1-6-5-4$ sofreu uma falha no mesmo enlace $6-5$. Todo o caminho estava protegido pelo backup $1-2-3-4$, sendo assim, após a restauração a conexão cessa sua transmissão pelos enlaces do caminho anterior e passa a ser transmitida pela nova rota.

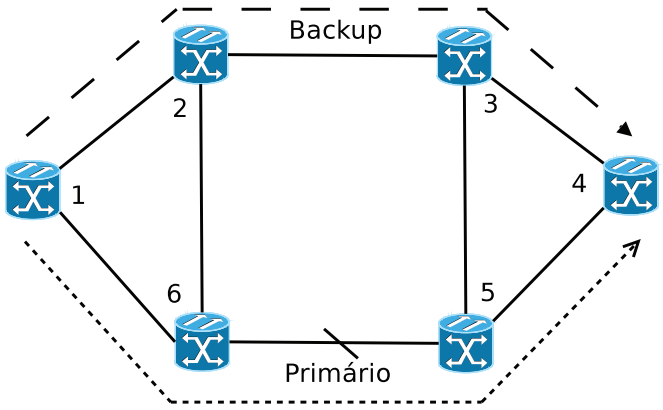


Figura 3.2: Proteção de Caminhos

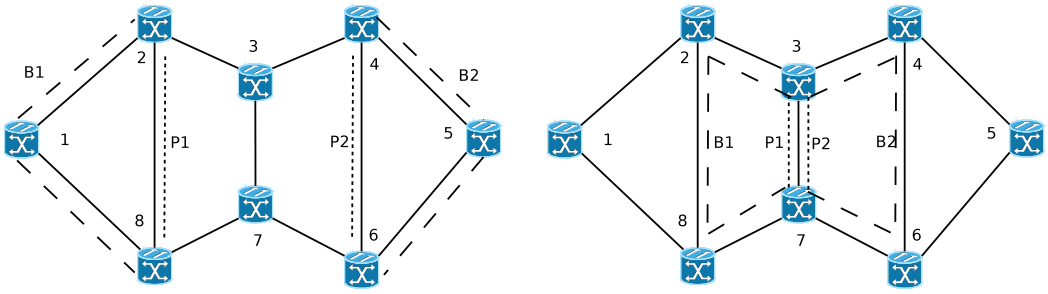
Pelos exemplos mostrados, vemos que após a restauração, no caso de proteção de enlaces, a conexão passou a usar uma rota de 5 enlaces, enquanto que na proteção de caminhos continuou usando apenas 3. Por esse motivo, a proteção de caminhos apresenta resultados melhores que a proteção de enlaces, como demonstrado em [18].

3.1.1 Esquemas de proteção de caminhos

Existem três formas de se realizar proteção de caminhos. São elas:

Caminho Dedicado :

Nesta técnica, cada caminho primário possui um caminho de backup reservado exclusivamente para sua conexão. Isto significa que o comprimento de onda utilizado nos enlaces do caminho de backup dedicado não poderá ser usado até que a conexão deixe de existir. A abordagem leva a uma redundância total de cada conexão, aumentando muito o gasto de recursos da rede. A Figura 3.3 ilustra a proteção por caminho dedicado. As rotas P1 e P2 referem-se a caminhos primários, enquanto B1 e B2 referem-se a caminhos de backup.



(a) Caminhos primários sem enlace comum (b) Caminhos primários com enlace comum

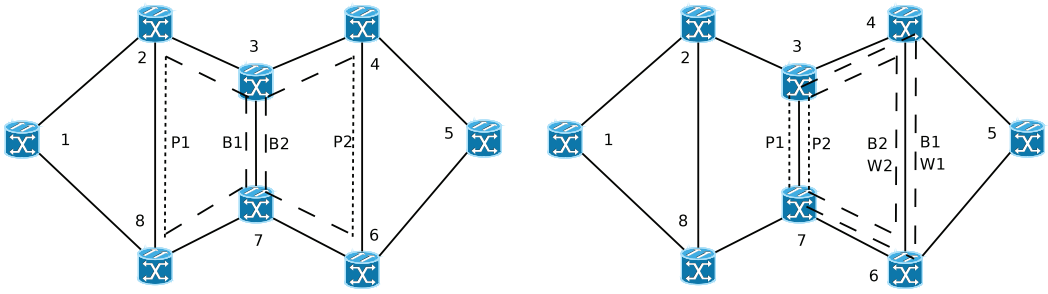
Figura 3.3: Exemplos de aplicação do caminho dedicado

Caminho Compartilhado :

Na proteção por caminho compartilhado, cada caminho primário também possui um caminho de backup reservado para sua conexão, entretanto, nesse caso, a reserva não é exclusiva. Isso significa que o comprimento de onda utilizado nos enlaces do caminho de backup compartilhado poderá ser usado por outro caminho de backup, desde que não exista a possibilidade de que ambos sejam ativados ao mesmo tempo, ou seja, desde que não seja possível que seus caminhos primários sofram falhas simultaneamente. Assim, cada um dos canais pode ser melhor utilizado, o que diminui a redundância e aumenta a eficiência no uso de recursos da rede. A Figura 3.4 apresenta exemplos da aplicação do caminho compartilhado. A mesma notação do exemplo anterior é usada nesse caso.

Caminho Compartilhado com restrição SRLG :

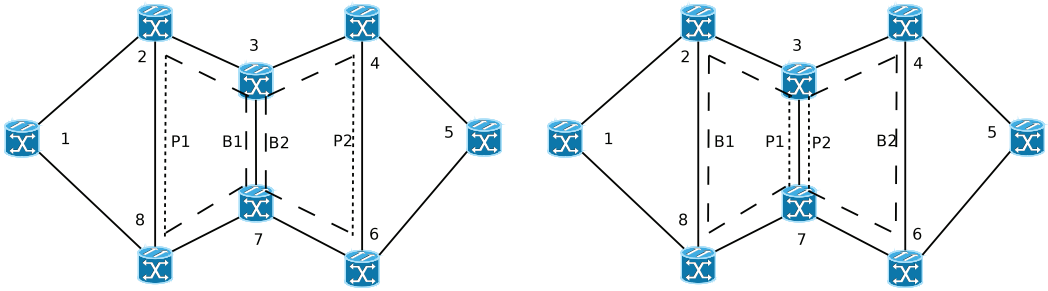
No esquema de proteção com restrição de grupos de enlace de risco compartilhado



(a) Caminhos primários sem enlace comum (b) Caminhos primários com enlace comum

Figura 3.4: Exemplos de aplicação do caminho compartilhado

(*Shared-Risk Link Group*), tem-se uma situação intermediária entre caminho compartilhado e dedicado. Apesar do compartilhamento ser permitido, quando dois caminhos primários estão no mesmo grupo de risco (ambos dividem um mesmo enlace), o compartilhamento não é aceito. Isto acontece pois quando um enlace é dividido por dois caminhos primários, no caso de uma falha, ambos precisarão ser recuperados. A restrição SRLG leva isso em consideração, a fim de produzir melhores resultados. A Figura 3.5 ilustra a restrição SRLG.



(a) Caminhos primários sem enlace comum (b) Caminhos primários com enlace comum

Figura 3.5: Exemplos de aplicação de caminho compartilhado com restrição SRLG

Assim como o problema RWA, prover proteção para uma rede óptica WDM é um problema NP-Completo. A solução ótima pode ser encontrada por meio de Programação Linear Inteira (PLI), ou por meio de heurísticas, que, embora produzam soluções sub-ótimas,

apresentam menor complexidade e são escaláveis. A fim de se exemplificar uma solução para os problemas de caminho dedicado e compartilhado, apresentam-se nas próximas Subseções formulações PLI para ambos, que foram propostas em [25].

A notação usada no PLI é a seguinte: considere-se uma rede óptica WDM cuja topologia é representada pelo grafo $G = (N, E)$, onde N é o conjunto de nós e E o conjunto de enlaces. As seguintes variáveis são definidas:

- W: Número de comprimentos de onda por enlace
- R^i: Rotas alternativas ao par de nós i
- M^i: Número de rotas alternativas ao par de nós i
- R^i_j: Rotas alternativas permitidas para o par de nós i após a falha do enlace j
- $EN(j)$: Rotas alternativas ao par de nós adjacente ao enlace j
- d^i: Conexões requisitadas para o par de nós i
- w_j: Número de comprimentos de onda usados pelo caminho primário no enlace j
- s_j: Número de comprimentos de onda reservados para proteção no enlace j
- $\gamma_w^{i,r} = \begin{cases} 1 \text{ se a rota } r \text{ entre o par de nós } i \text{ usa o comprimento de onda } w \\ \quad \text{antes de qualquer falha} \\ 0 \text{ caso contrário} \end{cases}$
- $\alpha_{w,p}^{i,b} = \begin{cases} 1 \text{ se o caminho dedicado } b \text{ com comprimento de onda } w \text{ protege a} \\ \quad \text{rota } p \text{ entre o par de nós } i \text{ antes de qualquer falha} \\ 0 \text{ caso contrário} \end{cases}$
- $\delta_{w,p}^{i,b} = \begin{cases} 1 \text{ se o caminho compartilhado } b \text{ com comprimento de onda } w \text{ protege a} \\ \quad \text{rota } p \text{ entre o par de nós } i \text{ antes de qualquer falha} \\ 0 \text{ caso contrário} \end{cases}$
- $m_w^j = \begin{cases} 1 \text{ se o comprimento de onda } w \text{ é usado por qualquer rota de restau-} \\ \quad \text{ração que tenha } j \text{ como enlace integrante} \\ 0 \text{ caso contrário} \end{cases}$

3.1.2 Caminho Dedicado - Formulação PLI

A formulação PLI proposta em [25] tem como objetivo a minimização da capacidade total usada:

$$MIN \sum_{j=1}^{E} (w_j + s_j) \tag{3.1}$$

As restrições da PLI são as seguintes:

$$(w_j + s_j) \leq W \qquad 1 \leq j \leq E \tag{3.2}$$

$$d^i = \sum_{r=1}^{M_1} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1) \tag{3.3}$$

$$w_j = \sum_{i=1}^{N(N-1)} \sum_{r \epsilon R^i, j \epsilon r} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq j \leq E \tag{3.4}$$

$$s_j = \sum_{i=1}^{N(N-1)} \sum_{b \epsilon R^i, j \epsilon b} \sum_{p \epsilon R^i, p \neq b} \sum_{w=1}^{W} \alpha_{w,p}^{i,b} \qquad 1 \leq j \leq E \tag{3.5}$$

$$\sum_{i=1}^{N(N-1)} \sum_{r \epsilon R^i : j \epsilon r} \gamma_w^{i,r} + \sum_{i=1}^{N(N-1)} \sum_{b \epsilon R^i : j \epsilon b} \sum_{p \epsilon R^i, p \neq b} \alpha_{w,p}^{i,b} \leq 1 \qquad 1 \leq w \leq W, 1 \leq j \leq E \tag{3.6}$$

$$\sum_{w=1}^{W} \gamma_w^{i,p} = \sum_{b \epsilon R^i, b \neq p} \sum_{w=1}^{W} \alpha_{w,p}^{i,b} \qquad p \epsilon R^i, 1 \leq i \leq N(N-1) \tag{3.7}$$

A equação 3.2 limita o número de caminhos ópticos por fibra, e a equação 3.3 garante que cada demanda seja atendida. O número de caminhos ópticos que usam o enlace j é descrito pela restrição 3.4. Similarmente o número de canais reservados para backup que usam o enlace j é descrito em 3.5. Por fim, a equação 3.6 garante a restrição de continuidade de comprimento de onda, e a equação 3.7 garante que o caminho primário seja protegido.

3.1.3 Caminho Compartilhado - Formulação PLI

O problema PLI proposto em [25] para resolução da proteção por caminho compartilhado tem como objetivo a minimização da capacidade total utilizada, expressa por:

$$MIN \sum_{j=1}^{E} (w_j + s_j) \tag{3.8}$$

E a resolução está sujeita às seguintes restrições:

$$(w_j + s_j) \leq W \qquad 1 \leq j \leq E \qquad (3.9)$$

$$d^i = \sum_{r=1}^{M_i} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq i \leq N(N-1) \qquad (3.10)$$

$$w_j = \sum_{i=1}^{N(N-1)} \sum_{r \epsilon R^i, j \epsilon r} \sum_{w=1}^{W} \gamma_w^{i,r} \qquad 1 \leq j \leq E \qquad (3.11)$$

$$s_k = \sum_{w=1}^{W} m_w^k \qquad 1 \leq k \leq E \qquad (3.12)$$

$$m_k^w \leq \sum_{i=1}^{N(N-1)} \sum_{p,b \epsilon R^i, k \epsilon b} \delta_{w,p}^{i,b} \qquad 1 \leq k \leq E, 1 \leq w \leq W \qquad (3.13)$$

$$N(N-1) \times E \times M \times m_k^w \geq \sum_{i=1}^{N(N-1)} \sum_{p,b \epsilon R^i, k \epsilon b} \delta_{w,p}^{i,b} \qquad 1 \leq k \leq E, 1 \leq w \leq W \qquad (3.14)$$

$$\sum_{i=1}^{N(N-1)} \sum_{r \epsilon R^i : j \epsilon r} \gamma_w^{i,r} + m_w^j \leq 1 \qquad 1 \leq j \leq E, 1 \leq w \leq W \qquad (3.15)$$

$$\sum_{i=1}^{N(N-1)} \sum_{p \epsilon R^i : f \epsilon p} \sum_{b \epsilon R^i : k \epsilon b} \delta_{w,p}^{i,b} \leq 1 \qquad 1 \leq f \leq E, 1 \leq k \leq E, 1 \leq w \leq W \qquad (3.16)$$

$$\sum_{w=1}^{W} \gamma_w^{i,p} = \sum_{b \epsilon R^i, b \neq p} \sum_{w=1}^{W} \alpha_{w,p}^{i,b} \qquad 1 \leq w \leq W, \forall p \epsilon R^i, 1 \leq i \leq N(N-1) \qquad (3.17)$$

As equações 3.9, 3.10 e 3.11 são idênticas àquelas do PLI para caminho dedicado, seguidas pelas restrições 3.12, 3.13 e 3.14, as quais se referem a capacidade de proteção que deve ser reservada. A equação 3.15 trata da restrição de continuidade de comprimento de onda e a restrição 3.16 trata da requisição de que um comprimento de onda só pode ser compartilhado por dois caminhos de backup se os caminhos primários a que se referem forem disjuntos. Por fim, a equação 3.17 requer que todo caminho primário seja protegido.

3.2 Restauração

A restauração é o objetivo em si da sobrevivência em redes ópticas, ou seja, é a recuperação de uma chamada na ocorrência de uma falha. Em geral, o processo de restauração está associado a algum método de proteção. Isto acontece pois o mecanismo de se encontrar um

caminho óptico alternativo a rota principal que sofreu falha é bastante custoso e demorado. Para que a transição do caminho primário ao de backup seja o mais transparente possível, diminui-se o tempo necessário alocando-se o caminho óptico alternativo no momento em que a chamada é aceita. Apesar do ganho em transparência no caso de uma falha, o associação entre proteção e restauração aumenta os gastos de recursos, já que é preciso manter redundância dos caminhos. Com isso, quando se deseja minimizar o uso de recursos da rede, o processo de alocar um caminho alternativo é feito somente na ocorrência de uma falha, num processo chamado restauração dinâmica.

3.2.1 Tempo de transição

Quando se trata de restauração, uma das principais preocupações de todo processo é o tempo de transição do caminho primário ao caminho de backup, ou seja, o tempo decorrido entre o instante em que uma falha ocorre até o momento em que o caminho de backup referente a rota que contém o enlace falho é ativado. A seguir, apresentam-se alguns importantes elementos que devem ser considerados no tempo de transição e sua estimativas, que foram propostos em [25]:

- **Detecção da falha:** A detecção de uma falha geralmente é feita pelos nós adjacentes ao enlace falho. Todo sinal óptico transmitido por uma fibra, sempre se dá de um nó origem s a um nó destino d. Assim que o nó d detecta uma interrupção no sinal que recebia, pode considerar que o enlace sobre o qual ocorria a transmissão falhou. No pior dos casos, a falha pode ocorrer próxima ao nó s, e a detecção só ocorrerá após todo um período de propagação pela fibra. Considerando uma rede na qual o tamanho de um enlace seja de 80 km, o tempo de detecção de uma falha pode ser estimado em $500\mu s$

- **Processamento de mensagens:** Assim que um nó detecta uma falha, deve informar aos nós interessados da ocorrência deste evento. Nós interessados são aqueles que devem ser configurados para que o caminho de backup seja ativado. Na transmissão dessa mensagem, cada nó possui um tempo de processamento da mensagem, assim como ocorre em um roteador IP. Este tempo pode ser estimado em 10 μs

- **Propagação de mensagens:** Além do tempo de processamento, cada mensagem precisa ser propagada por um conjunto de enlaces até chegar aos nós interessados. Este tempo está diretamente associado ao diâmetro da rede. Considerando enlaces de 80 km, o intervalo de propagação pode ser estimado em 400 μs

- **Configuração de OXCs:** Assim que todos os nós interessados foram informados que precisam ser configurados para ativação do caminho de backup, torna-se

necessário configurar os OXCs a fim de que a comutação do novo caminho óptico se dê corretamente. Não se possui uma boa estimativa para esta variável, mas pode-se considerar que seu valor esteja entre 10 μs e 500 μs

A partir das variáveis expostas, pode-se concluir que o tempo gasto na transição é da ordem de alguns milissegundos. Este tempo pode variar conforme a técnica utilizada para restauração, pois quanto menor o número de enlaces nos quais as mensagens devem se propagar, menor o tempo de transição.

3.2.2 Restauração e Proteção Compartilhada

A proteção compartilhada é o mecanismo que torna o processo de restauração o mais lento, quando comparada a proteção dedicada 1:1 e 1+1. O diferencial para isso é o fato de que um comprimento de onda pode ser usado por mais de um caminho de backup. Com isso, os OXCs que se localizam ao longo do caminho não podem ser pré-configurados, já que sua utilização não é dedicada. A configuração só será feita no momento em que uma falha ocorrer e, como este é um procedimento que pode ser demorado, a restauração torna-se menos eficiente. A Figura 3.6 apresenta este método.

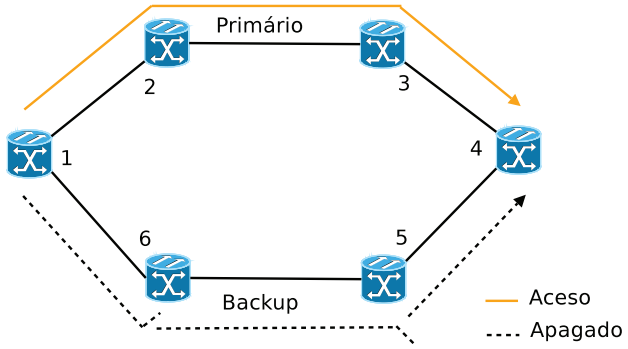


Figura 3.6: Restauração e Proteção Compartilhada

3.2.3 Restauração e Proteção Dedicada 1:1

Com a proteção dedicada 1:1 o tempo de transição é sensivelmente diminuído quando comparado a proteção compartilhada. Isso por que o caminho de backup pode ser pré-configurado, ou seja, a configuração dos OXCs ao longo do caminho pode ser feita de modo que, quando o laser no nó origem for ligado (aceso), o nó destino poderá receber o sinal transmitido. Isso torna o processo de restauração mais rápido, e é importante,

sobretudo, quando a configuração dos dispositivos OXCs é muito lenta. A Figura 3.7 ilustra este mecanismo.

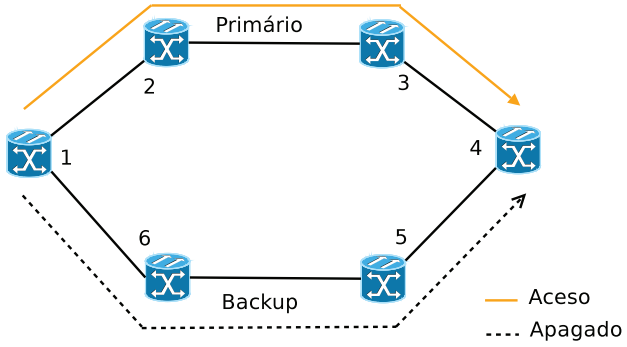


Figura 3.7: Restauração e Proteção Dedicada 1:1

3.2.4 Restauração e Proteção Dedicada 1+1

A proteção dedicada 1+1 apresenta o menor tempo de restauração quando comparada com as técnicas anteriores. Além de utilizar a pré-configuração dos OXCs, este mecanismo mantém o caminho de backup transmitindo (aceso) simultaneamente e de forma redundante ao caminho primário. Assim, o tempo de transição entre os caminhos é significativamente diminuído, pois além de não ser necessário configurar os OXCs, também não será necessária a propagação de mensagens para a recuperação da chamada. Basta que o nó destino detecte a falha e passe a receber o sinal transmitido pelo caminho de backup. A Figura 3.8 ilustra a proteção dedicada 1+1.

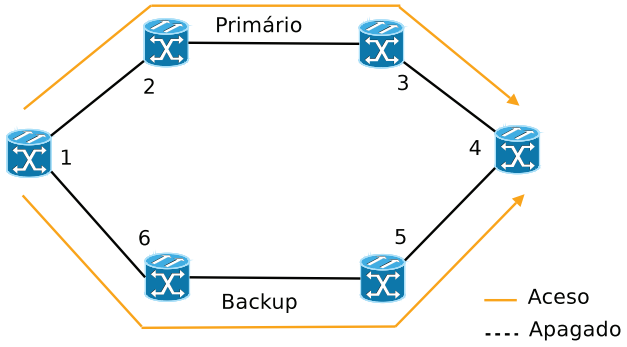


Figura 3.8: Restauração e Proteção Dedicada 1+1

Capítulo 4

Limitações da Camada Física

Com a crescente demanda por altas taxas de transmissão de dados, esforços têm sido empreendidos a fim de aumentar a eficiência das transmissões ópticas. Entretanto, os avanços que permitiam o aumento contínuo na taxa de bits transmitida, têm agora encontrado barreiras para a obtenção de taxas ainda maiores. Tais barreiras se devem às limitações da camada física, que podem ser definidas como efeitos eletromagnéticos inerentes às fibras e aos equipamentos ópticos, capazes de degradar o sinal óptico a níveis que podem ser produzidos resultados inaceitáveis na recepção.

A degradação do sinal pode estar relacionada a potência, ao comprimento de onda, ao tempo ou a uma combinação destes fatores. A Figura 4.1 ilustra o grande número de efeitos conhecidos e a que fatores estão relacionados. Boa parte desses efeitos interferem muito pouco na transmissão do sinal, e podem ser desconsiderados.

Os efeitos limitantes da camada física podem ser classificados em lineares e não-lineares, de acordo com a equação que os regem. Pertencem a classe dos lineares aqueles que dependem apenas das propriedades físicas constantes inerentes às fibras e aos equipamentos ópticos, ou seja, propriedades que não variam com a passagem do sinal pela fibra. Ao contrário, os efeitos não-lineares possuem em suas equações elementos cujo valor varia de acordo com o sinal transmitido na fibra. São exemplos de efeitos lineares a dispersão cromática, a dispersão por modo de polarização (PMD) e a emissão espontânea amplificada (ASE). Exemplos de efeitos não-lineares são a auto-modulação de fase (SPM), modulação de fase cruzada (XPM) e a mistura de quatro ondas (FWM).

A origem dos principais efeitos está relacionada à:

- **Fibra**: Tratam-se dos efeitos decorrentes da propagação do sinal pela fibra. São exemplos deste grupo as dispersões cromática e PMD, e os efeitos não-lineares.

- **Equipamentos Ópticos**: A passagem do sinal pelos equipamentos ópticos inflige danos sobre o sinal. Quando passa por um amplificador, por exemplo, está sujeito

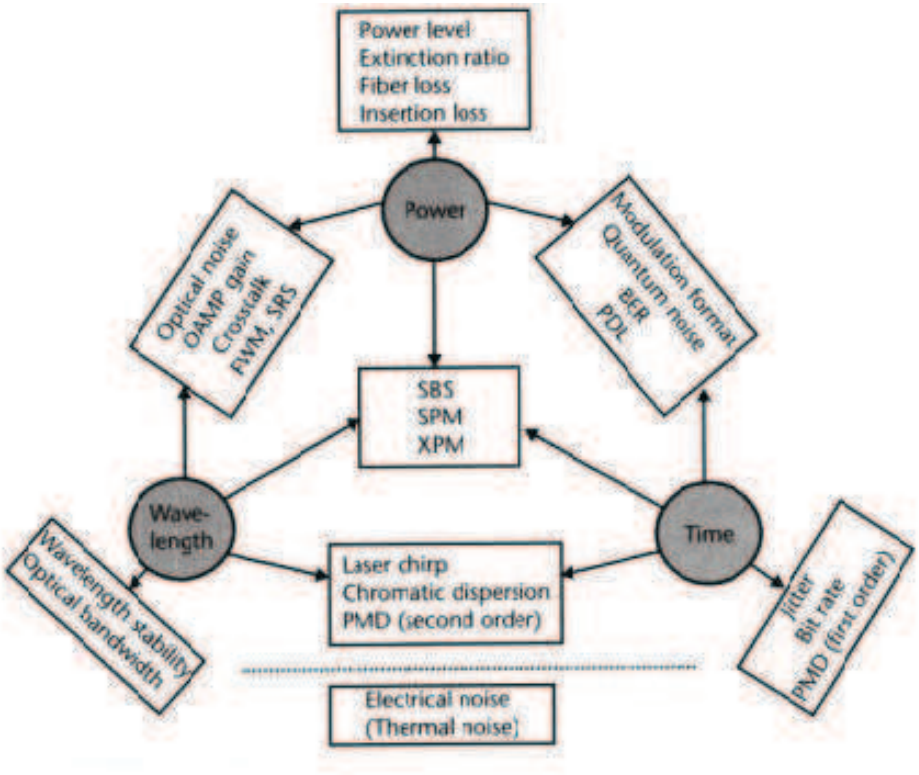


Figura 4.1: Efeitos degradantes do sinal

à adição do ruído ASE. Já quando efetua sua passagem por um demultiplexador ou comutador, está sujeito a uma série de efeitos, tais como crosstalk e PDL.

Este capítulo é constituído da seção 4.1, na qual são apresentados os efeitos lineares mais importantes; e da seção **??**, a qual descreve os efeitos não-lineares mais conhecidos.

4.1 Efeitos Lineares

Os efeitos lineares são extremamente importantes, uma vez que a degradação do sinal que provocam é bastante grave, e por esse motivo são amplamente estudados na literatura. As referências [24, 2, 17], dedicam-se ao estudo das limitações da camada física levando exclusivamente os efeitos lineares em consideração. Mesmo os trabalhos que consideram os efeitos não-lineares [14, 16], também tratam dos lineares, devido a sua grande relevância. Além disso, cabe salientar que o RFC proposto pela IETF [31], considera dois efeitos lineares como os mais importantes (ASE e PMD).

Nas próximas subseções, apresenta-se uma descrição dos cinco efeitos lineares mais relevantes.

4.1.1 Dispersão Cromática

O conceito de dispersão é de grande importância no contexto das limitações da camada física, e ocorre quando um sinal é constituído de dois ou mais componentes que viajam em velocidades diferentes sobre uma fibra, chegando ao receptor em instantes distintos. Tal fenômeno faz com que se tenha um alargamento do pulso, o que leva à uma interferência entre pulsos adjacentes.

Sabe-se que qualquer transmissão de dados precisa de uma faixa de freqüências $f_1..f_2$ para que seja capaz de transmitir dados binários, e o número máximo de bits transmitidos será dado pela critério de Nyquist: $2\Delta f$. Sabe-se, também, que em qualquer sistema óptico, freqüências diferentes viajam em velocidades diferentes. Desta forma, a componente de menor freqüência f_1 de um sinal, viajará em uma velocidade diferente da componente de maior freqüência f_2, levando à ocorrência do fenômeno de dispersão. Quando se deve a esta diferença de velocidade entre as componentes espectrais do sinal, o fenômeno é denominado **dispersão cromática**.

A pesquisa em tecnologia óptica permitiu o desenvolvimento de fibras capazes de compensar a dispersão cromática. Em termos gerais, o funcionamento dessas fibras inverte a ordem de velocidade das freqüências. Dado que a freqüência f_1 é mais rápida em uma fibra padrão SSMF (*Standard Single Mode Fiber*), sua velocidade será menor em uma fibra compensadora DCF (*Dispersion Compensation Fiber*). Ao contrário, uma freqüência f_2, mais lenta em uma fibra SSMF, terá sua velocidade aumentada em uma fibra DCF.

4.1.2 Dispersão por Modo de Polarização (PMD)

A dispersão PMD está diretamente relacionada aos conceitos de modo e polarização.

Um modo de propagação pode ser entendido como um possível caminho de transmissão. Em uma fibra multimodo, portanto, tem-se dois ou mais possíveis caminhos, enquanto que em uma fibra monomodo apenas um caminho é possível, o qual é chamado de modo fundamental. Atualmente, apenas fibras monomodos são usadas, pois permitem uma utilização muito mais eficiente da banda passante. O campo elétrico que descreve o caminho de uma fibra monomodo é dado pela equação $E(r,\omega) = E_x e_x + E_y e_y + E_z e_z$, onde e_x, e_y e e_z são os vetores unitários ao longo dos eixos x, y e z. Tomando z como direção de propagação, e considerando as equações de onda de Maxwell, encontramos duas soluções linearmente independentes para o modo fundamental. Uma delas possui $E_x = 0$ e $E_y, E_z \neq 0$, enquanto a outra apresenta $E_y = 0$ e $E_x, E_z \neq 0$. A direção de propagação z é chamada de longitudinal, enquanto os eixos x e y são denominados transversais. [26]

Um campo elétrico varia no tempo, tanto em magnitude como em direção. Entretanto, quando polarizado, tem-se que a direção é sempre constante, independente do tempo. Apenas a magnitude varia. Além disso, um campo elétrico é dito transverso quando não possui componentes na direção de propagação. É o caso do modo fundamental, que só possui componentes E_x e E_y. Pode-se concluir, portanto, que seu campo elétrico é polarizado nos eixos x e y. Qualquer combinação linear dos dois campos polarizados é, também, uma solução para o modo fundamental, chamando-se Estado de Polarização, a distribuição de energia entre esses duas direções diferentes, denominadas modos de polarização. Embora existam dois modos distintos, a fibra é denominada monomodo pois a constante de propagação de ambos é idêntica, ao menos quando se trate de uma fibra ideal. Sendo assim, embora a energia seja dividida em dois modos de polarização, estes são transmitidos em conjuntos, como se fossem um só, o que evita a ocorrência de dispersão. [26]

As fibras do mundo real não possuem, infelizmente, esse propriedade. Imperfeições na fabricação não permitem que a constante de propagação seja a mesma para os dois modos de polarização. Com isso, um dos modos viaja em velocidade superior ao outro, alargando o pulso e levando a ocorrência do fenômeno de dispersão. A Figura 4.2 ilustra a dispersão PMD.

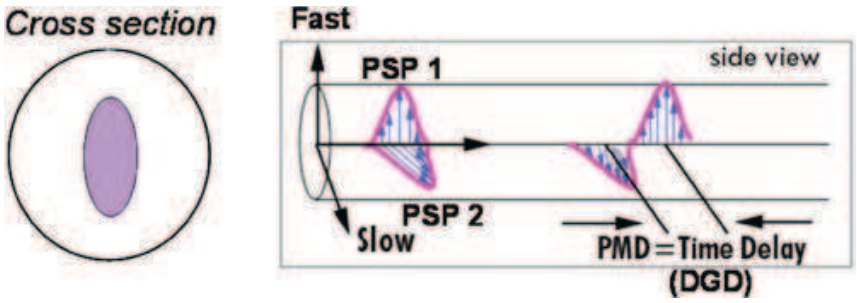


Figura 4.2: Alargamento de pulso devido a dispersão PMD

4.1.3 Atenuação Dependente da Polarização (PDL)

Um outro fenômeno associado a polarização é a PDL. Assim como diferentes constantes de propagação podem ocorrer para cada um dos modos, podem também existir diferentes taxas de atenuação associadas a ambos, o que pode levar a problemas na recepção do sinal. A atenuação dependente da polarização é ilustrada na Figura 4.3.

Em geral, a PDL está associada muito mais aos componentes ópticos localizados ao longo da rede do que a transmissão pela fibra. Alguns dispositivos respondem de forma diferente para cada um dos dois modos. Circuladores e isoladores são exemplos desses

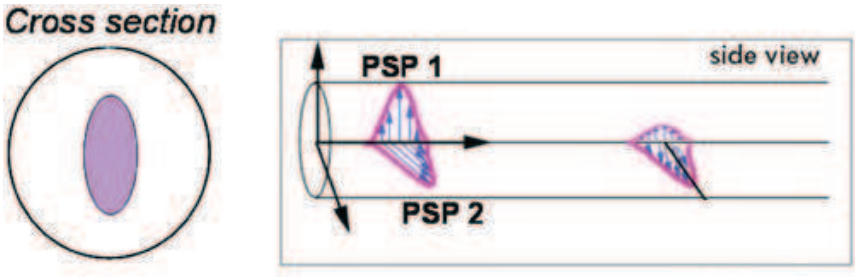


Figura 4.3: Atenuação Dependente da Polarização

componentes. Associado a essa diferente resposta observa-se, também, taxas de atenuação distintas.

4.1.4 *Crosstalk*

O efeito *crosstalk* ocorre sempre que dois sinais interagem entre si, levando à interferência de um sobre o outro, que, quando indesejada, provoca alterações nos sinais que podem ser mal interpretados na recepção.

Tanto as fibras, como a maior parte dos dispositivos ópticos provocam crosstalk sobre o sinal. Os componentes que infligem crosstalk com maior intensidade são os multiplexadores, demultiplixadores e comutadores.

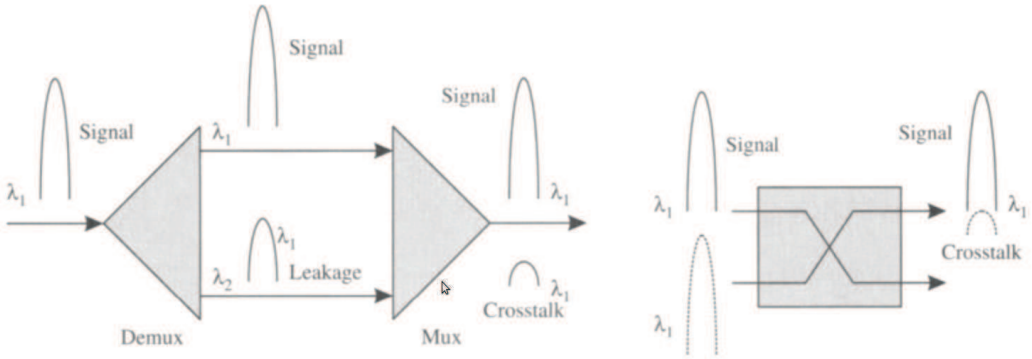
O efeito pode ser classificado em crosstalk intra-canal e crosstalk inter-canal. A seguir, descreve-se cada uma dessas classificações.

Crosstalk Intra-Canal

Quando dois sinais de mesmo comprimento de onda interagem entre si, chama-se a esse efeito de crosstalk intra-canal, ou crosstalk coerente.

A Figura 4.4 apresenta dois exemplos de ocorrência deste efeito. Na Figura 4.4(a), observa-se um demultiplexador seguido de um multiplexador. Na primeira parte do sistema, um sinal constituído apenas do comprimento de onda λ_1 é demultiplexado. Num cenário ideal, o sinal deveria ser totalmente transferido para a fibra superior, entretanto, em um demultiplexador real isso não acontece, e uma porção residual do sinal é transferida para a fibra inferior. Na segunda parte do sistema, quando o sinal é multiplexado, observa-se a composição do sinal original de comprimento de onda λ_1 com a porção residual de mesmo comprimento de onda, o que origina o efeito crosstalk inter-canal. Na Figura 4.4(b) o exemplo é de um comutador. Neste equipamento, sinais de mesmo comprimento de onda chegam pelas portas de entrada do lado esquerdo e partem pelas portas de saída do lado direito. Cabe ao dispositivo decidir qual o destino de cada um dos sinais. Uma vez

que o isolamento do comutador não é perfeito, e os sinais operam de forma tão próxima, ocorre interação indesejada entre os canais.



(a) Crosstalk em Multiplexadores/Demultiplexadores (b) Crosstalk em Comutadores

Figura 4.4: Crosstalk Intra-Canal [26]

Crosstalk Inter-Canal

O efeito crosstalk inter-canal ou incoerente ocorre quando dois sinais de comprimentos de onda diferentes interferem entre si.

A Figura 4.5 apresenta um exemplo deste efeito, bastante semelhante ao que ocorre na Figura 4.4(a). Neste caso, temos um demultiplexador que, como descrito anteriormente, não opera de forma ideal. Porções residuais do sinal interferem com outros sinais de comprimentos de onda próximos, dando origem ao efeito apresentado na figura.

4.1.5 Emissão Espontânea Amplificada (ASE)

O princípio básico de funcionamento de um amplificador óptico é a emissão de fótons, regida pelas leis da mecânica quântica. Tais leis consideram que um átomo é constituído por diversos níveis discretos de energia, e a cada instante, encontra-se em apenas um desses níveis. Quando ocorre uma transição de um nível de maior energia para outro de energia mais baixa, observa-se a emissão de um fóton. A amplificação do sinal utiliza-se desse processo estimulando a emissão de fótons.

A Figura 4.6 apresenta o princípio de funcionamento do amplificador: dado que o átomo a constitui um amplificador hipotético G. Em equilíbrio, a encontra-se no nível de energia E_1. Para que a emissão possa ocorrer, é preciso que o átomo mude de estado, elevando seu nível de energia a E_2. Isto é feito através da absorção de um campo eletromagnético de freqüência f_c, com $hf_c = E_2 - E_1$, onde h é a constante de Planck. Uma

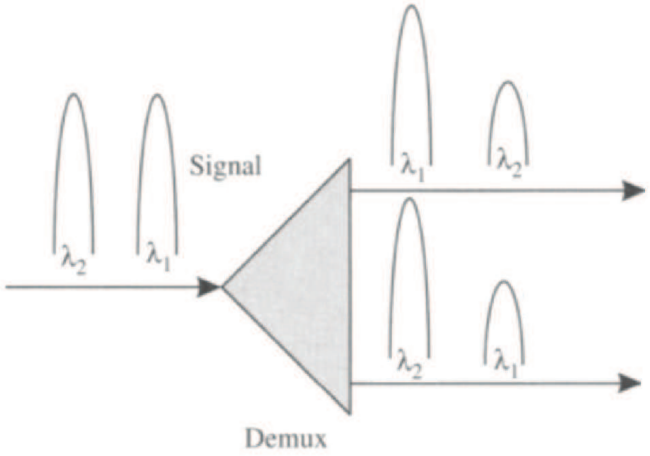


Figura 4.5: Crosstalk Inter-Canal

vez no nível E_2, o sinal incidente faz o átomo retornar ao equilíbrio, o que é feito com a emissão de um fóton que realiza a amplificação.

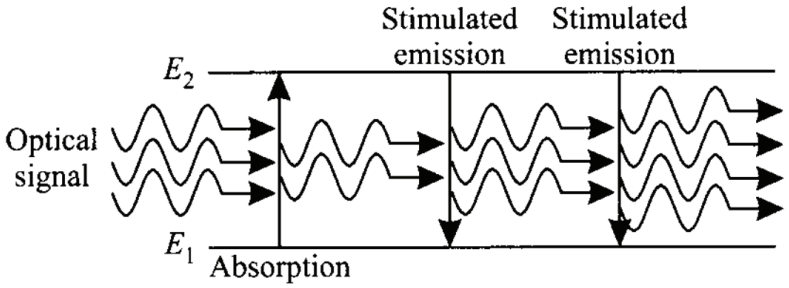


Figura 4.6: Principio de funcionamento do amplificador [26]

O processo de emissão estimulada não acontece,infelizmente, sozinho, sendo acompanhado de uma emissão espontânea. A tendência de todo sistema de energia mais alta é retornar ao equilíbrio. Quando o átomo está no nível E_2, este, espontaneamente, tende a voltar ao nível E_1, emitindo um fóton, que se comportará como ruído. Este fenômeno é conhecido como Emissão Espontânea Amplificada (*Amplified Sponteous Emission* - ASE), e é um dos ruídos que infligem maior dano às transmissões ópticas.

Capítulo 5

Impacto das Limitações da Camada Física em Redes com Proteção

O Capítulo 4 fez um estudo dos efeitos limitantes da camada física em redes ópticas, enquanto o Capítulo 3 apresentou os principais pontos a respeito de proteção. Este Capítulo pretende verificar como se comportam as redes com proteção quando sujeitas aos efeitos degradantes do sinal.

Vários artigos abordam a sobrevivência em redes ópticas [25, 35, 13, 15, 32], outros os efeitos limitantes da camada física [24, 17, 16, 2, 31, 20, 1, 14]. Entretanto, poucas foram as investigações de proteção em redes WDM considerando as limitações do meio físico. Existem, porém, alguns trabalhos tratam deste assunto. Em [34], considera-se a colocação de equipamentos de conversão O-E-O na rede, a fim de se prover regeneração do sinal, tratando-se, portanto, de rede translúcida. Em [22], leva-se em conta, também, uma rede translúcida, entretanto, o tráfego é dinâmico, diferentemente do artigo anterior, cujo tráfego é estático. Em [36], a rede em consideração é transparente, com tráfego dinâmico, e a técnica de proteção é o caminho dedicado. O trabalho em [33] difere daquele em [36], pois considera proteção do tipo SRLG.

O trabalho descrito neste capítulo compara a abordagem de proteção por caminho compartilhado em redes ópticas WDM transparentes com limitações na camada física a um cenário de redes ideais, ou seja, livres de erros devido a degradação do sinal. A verificação da qualidade do sinal é importante no fornecimento de garantias de Qualidade de Transmissão (QoT) mínima às chamadas, sem a qual a perda de pacotes pode ser muito elevada. O efeito das limitações da camada física deve ser levado em consideração, também, quando se emprega proteção, pois a transição para o caminho de backup deve ser transparente ao usuário, e, dessa forma, o serviço prestado deve permanecer com boa qualidade mesmo na ocorrência de uma falha.

Faz-se, também, neste capítulo, uma comparação das principais políticas de alocação

de comprimento de onda quando se levam em consideração os efeitos da camada física e proteção por caminho compartilhado. Dessa forma, mostra-se qual dessas políticas oferece um desempenho melhor neste contexto.

Este capítulo contém duas seções: a seção 5.1 especifica o cenário para examinar o comportamento dos algoritmos, e a seção 5.2 apresenta os resultados numéricos encontrados através de simulação.

5.1 Proteção de Caminho Compartilhado e Limitações Físicas

Nesta seção, apresenta-se o contexto para o qual os algoritmos foram examinados, explicitando tópicos importantes, como o modelo de rede na Subseção 5.1.1, o modelo de camada física na Subseção 5.1.2, e por fim uma breve descrição do funcionamento dos algoritmos na Subseção 5.1.3.

5.1.1 Modelo de Rede

Em redes de longa distância são necessários amplificadores ao longo dos caminhos a fim de que o sinal chegue ao seu destino com uma potência mínima capaz de excitar o receptor. Sendo assim, divide-se a rede em trechos, de tal forma que, ao fim de cada um destes, seja posicionado um amplificador. Optou-se pelo uso de amplificadores EDFA, mas os resultados são extensíveis a amplificadores de Raman.

Cada um dos trechos é composto por 70 Km de Fibra Monomodo Padrão (SSMF) e 12 Km de Fibra Compensadora de Dispersão (DCF), capaz de compensar a totalidade da dispersão imposta ao sinal. A Figura 5.1 ilustra esse modelo.

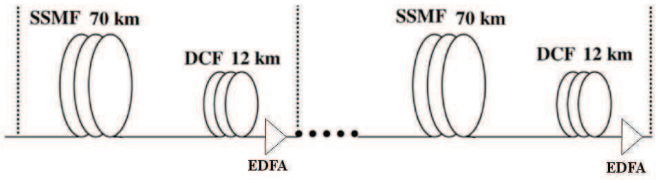


Figura 5.1: Ilustração do modelo de amplificação e compensação de dispersão

As fibras SSMF possuem uma atenuação de 0.2 dB/Km, fazendo com que a potência do sinal seja 14 dB menor ao seu final. As fibras DCF têm uma atenuação de 0.5 dB/Km,

levando a uma diminuição de 6 dB na potência. O EDFA deve ser capaz de restaurar a potência do sinal ao seu valor inicial, portanto o ganho de cada amplificador é de 20 dB.

Outro ponto importante no projeto de rede é a estrutura do nós WDM. A Figura 5.2 mostra a arquitetura de um nó típico em redes ópticas, apresentada pela primeira vez em [24].

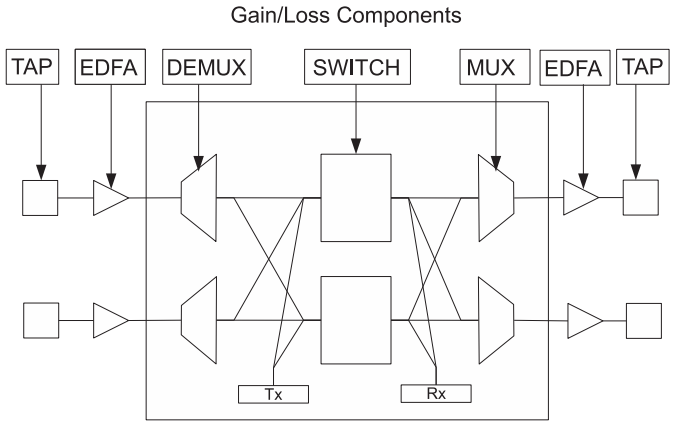


Figura 5.2: Estrutura de um nó WDM [24]

Como se pode ver, o nó é formado por diversos componentes, alguns dos quais impõem atenuação sobre o sinal (multiplexador, demultiplexador, comutador). Para contornar esse problema, são colocados amplificadores na entrada e na saída, a fim de que a atenuação seja compensada.

Esse modelo de rede foi baseado no proposto em [17], exceto pelos amplificadores *in-line*, que neste modelo são EDFAs, como descrito anteriormente.

5.1.2 Modelo de Camada Física

O modelo de camada física foi projetado de tal forma que duas etapas fossem consideradas. Em um primeiro momento, calcula-se a Dispersão por Modo de Polarização (PMD), efeito gerado pela diferença de velocidade existente entre os modos constituintes de um sinal. Em seguida, calcula-se a razão sinal ruído óptica (OSNR). Duas são as fontes de ruído na rede: a Emissão Espontânea Amplificada (ASE), gerada no processo de amplificação ocorrido nos EDFAs; e o crosstalk, produzido pela interação entre sinais de mesmo comprimento de onda nos OXCs.

Para a primeira etapa procede-se da seguinte forma: dado um caminho óptico com M enlaces intermediários, a dispersão PMD segue a equação [17]:

$$B * \sqrt{\sum_{k=1}^{M} D_{PMD}^2(k) * L(k)} \leq \delta \tag{5.1}$$

na qual B é a taxa de dados transmitidas, $D_{PMD}(k)$ é o parâmetro PMD da fibra k, e $L(k)$ é o seu comprimento. O valor calculado para a dispersão PMD deve ser inferior ao valor de um parâmetro δ, conhecido como alargamento de pulso (*pulse broadening*), cujo valor aceitável deve ser inferior a 10% do slot de tempo de um bit.

Tendo verificado a validade do caminho óptico quanto à dispersão PMD, calcula-se o valor da OSNR. A potência do ruído ASE é dada pela seguinte equação [2]:

$$P_{ASE} = 2 * \eta_{sp} * (G - 1) * h * f \tag{5.2}$$

na qual η_{sp} é o fator de emissão espontânea do EDFA, G é o seu ganho, h é a constante de Planck, e f é a freqüência de operação.

Já o *crosstalk* observado nos OXCs, de forma simplificada, segue a equação [24]:

$$P_{xt} = \sum_{j=1}^{J} X_{sw} * P_{in}(j) \tag{5.3}$$

na qual X_{sw} é a razão de crosstalk e $P_{in}(j)$ é a potência dos sinais de entrada do switch que compartilham o mesmo comprimento de onda.

Tendo em mãos as equações para cálculo das duas fontes de ruído pode-se derivar a OSNR. Para que o sinal chegue ao seu destino com uma qualidade mínima aceitável, é necessário limitar o valor encontrado para este parâmetro. Permite-se que o valor mínimo assumido pela OSNR seja de 7.4 dB, o que equivaleria a uma BER de 10^{-9}. Este valor, bem como outras constantes utilizadas para definir o cenário, encontram-se sumarizados na Tabela 5.1, na qual apresenta-se, também, a atenuação e o ganho de todos os equipamentos da rede. Os valores dispostos na tabela são comumente usados na literatura, e podem ser encontrados em [24, 17].

5.1.3 Algoritmos RWA

Os algoritmos de Roteamento e Alocação de Comprimento de Onda devem cuidar de prover proteção e considerar a qualidade do sinal, a fim de aceitar ou não um caminho óptico.

A fim de verificar a influência da degradação do sinal no desempenho dos algoritmos foram considerados dois tipos de rede [17]:

Parâmetro	**Valor**
Taxa de Bits por Canal	10 Gbps
Largura de Banda	70 GHz
Comprimentos de onda	Centrado em 1548 nm, separação de 0.8 nm
Número de canais na fibra	16
Potência do Sinal por Canal	1 mW
Razão de Crosstalk do Switch	-25 dB
Atenuação do Multiplexador	-4 dB
Atenuação do Demultiplexador	-4 dB
Atenuação do Switch	-8 dB
Atenuação da Junção	-1 dB
Ganho do EDFA de entrada nos OXCs	12 dB
Ganho do EDFA de saída nos OXCs	6 dB
Ganho dos EDFAs inline	20 dB
Parâmetro PMD	0.1 $ps/(km)^{1/2}$
Fator ASE η_{sp}	1.2
OSNR mínimo	7.4 dB

Tabela 5.1: Parâmetros usados na simulação

- Rede Ideal: Ignora a existência dos efeitos degradantes do sinal no controle de acesso de chamadas (CAC), ou seja, são livre de erros, na medida em que os equipamentos ao longo de um caminho óptico são considerados ideais.

- Rede Realista: Os componentes de rede infligem ruído sobre o sinal, causando sua degradação, que é levada em consideração pelo CAC na aceitação de chamadas.

Sendo assim, foram desenvolvidos algoritmos capazes de simular redes ideais e realistas. A versão para redes realistas pode ser brevemente descrita pelo fluxograma da Figura 5.3.

Neste algoritmo, busca-se, inicialmente, dois caminhos disjuntos, um primário e outro de backup, e, posteriormente, testa-se se eles podem oferecer uma qualidade de transmissão adequada. Caso seja possível encontrar os caminhos e o teste tenha retorno positivo, a chamada é aceita; caso contrário a chamada é bloqueada. Para as redes ideais, tem-se apenas a fase de busca dos caminhos disjuntos, e não é feito o teste das limitações da camada física.

Foram avaliadas três políticas de alocação de comprimento de onda: *First-Fit*, *Random-Pick*, e *Best-Path*. Na primeira delas, a busca por um caminho interligando a origem e o destino é realizada de forma ordenada entre as camadas, enquanto que na segunda é feita de forma aleatória. Na terceira política, a ordenação é feita segundo o menor caminho,

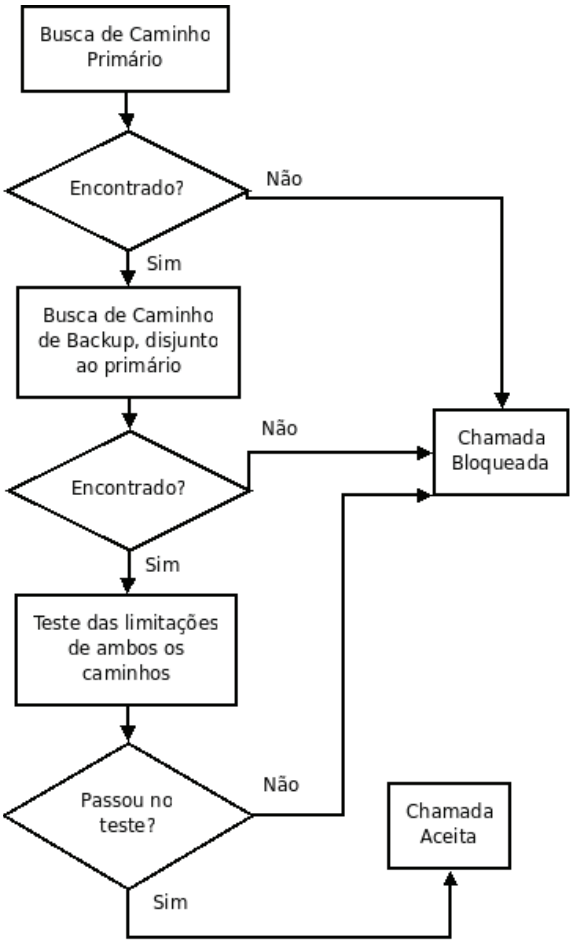


Figura 5.3: Descrição do algoritmo

optando-se primeiro pela camada que possuir o caminho de menor distância.

5.2 Resultados Numéricos

Nos experimento de simulação, verificou-se o comportamento da probabilidade de bloqueio com o aumento da carga, bem como da probabilidade de que um caminho óptico não seja recuperado em caso de falha, denominada de razão de vulnerabilidade.

Considera-se, nos cenários de simulação, que o tráfego é dinâmico e que a chegada de chamadas é regida por uma distribuição de Poisson, enquanto que período de duração de uma chamada (*holding time*) é regido por uma distribuição exponencial com média 1. Dessa forma, a carga de rede é descrita pela taxa de chegadas em Erlangs. Considera-se, também, modelo de falhas de enlace único, ou seja, em qualquer momento da vida de uma rede, a falha de apenas um enlace é aceita, e a ocorrência de uma nova falha só é possível quando o conserto da anterior já houver ocorrido[36]. Para cada valor de carga, foram realizadas 10^6 chamadas, de modo que, estatisticamente, os erros fossem minimizados a ponto de poderem ser considerados insignificantes.

A topologia de rede usada para fins de simulação está apresentada na Figura 5.4. Nela, cada nó e cada enlace seguem as especificações dadas na Tabela 5.1.

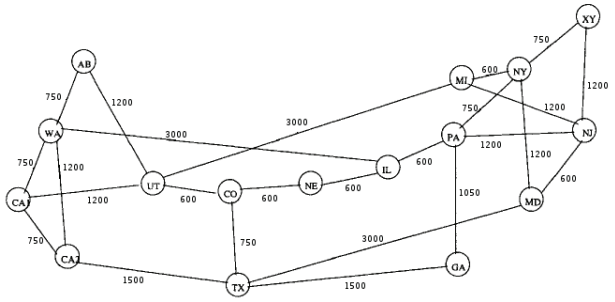
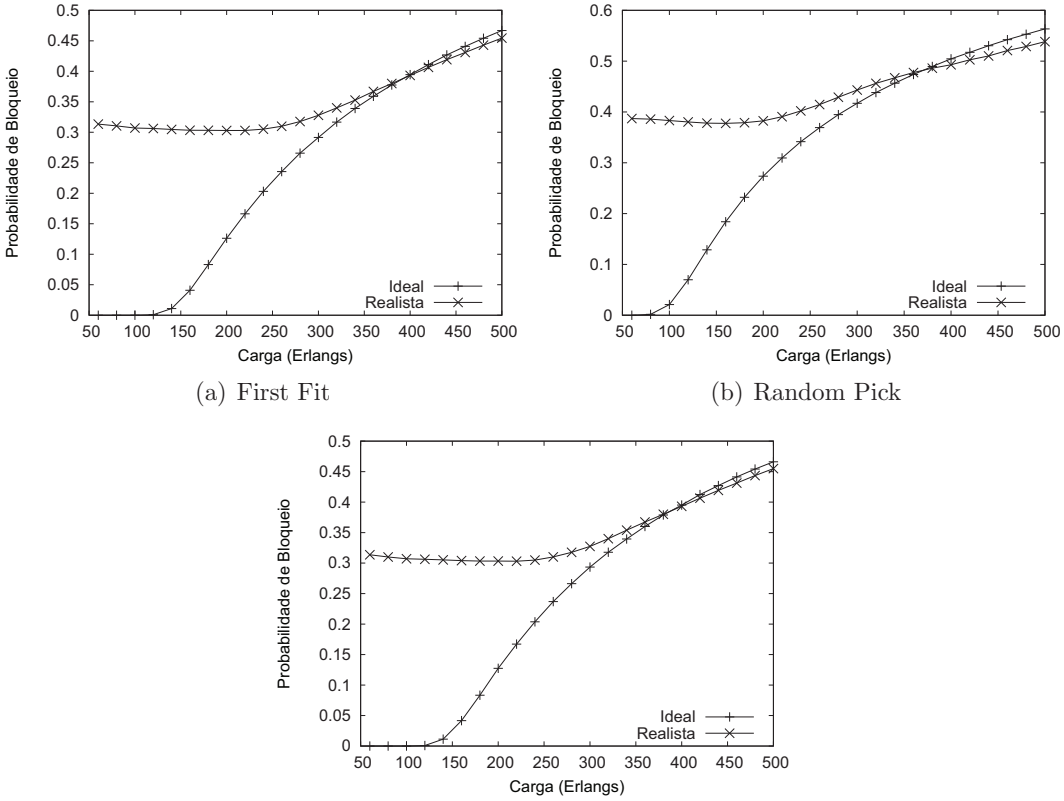


Figura 5.4: NSFNET

5.2.1 Probabilidade de Bloqueio

Mostra-se, inicialmente, o efeito das limitações físicas sobre a probabilidade de bloqueio, em função da variação da carga (Figura 5.5). No primeiro gráfico, utiliza-se o algoritmo First-Fit para alocação de comprimento de onda. Nota-se que o bloqueio para redes ideais acontece a partir de uma carga superior a 150 Erlangs, enquanto que em redes reais, esse

bloqueio já é visível, mesmo a partir de cargas muito baixas. Isso acontece porque mesmo com cargas baixas, as limitações da camada física são bastante relevantes, fazendo com que algumas chamadas não consigam atingir o limite máximo aceito para degradação do sinal. A partir de um valor de carga aproximadamente igual a 370 Erlangs, as curvas se juntam, o que significa que nesse ponto a escassez de recursos é muito mais importante na causa de bloqueios do que a degradação do sinal.



(a) First Fit

(b) Random Pick

(c) Best Path

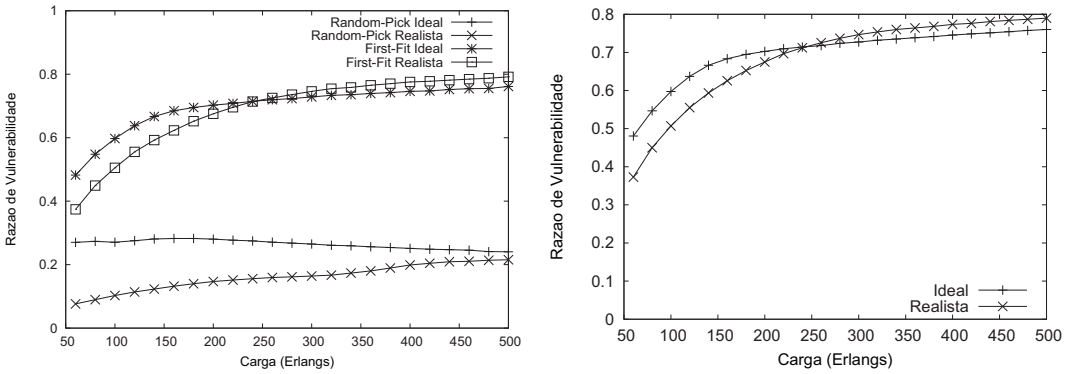
Figura 5.5: Comparação da probabilidade de bloqueio para redes reais e ideais segundo 3 algoritmos alocações de comprimento de onda

Para o algoritmo Best-Path, o bloqueio é muito parecido com aquele obtido para o First-Fit, dado que as distâncias obtidas para cada uma das camadas são quase sempre iguais, fazendo com que o ganho não seja significante, e que o algoritmo tenha um comportamento muito próximo ao First-Fit. No gráfico do Random-Pick, o bloqueio em redes ideais passa a acontecer, a partir de 100 Erlangs, e o comportamento para redes reais é

ligeiramente diferente dos anteriores, com uma pequena diminuição no desempenho, que é explicada pelo aumento na fragmentação da utilização dos recursos, uma vez que a busca por caminhos viáveis não se dá de forma tão organizada quanto para o algoritmo First-Fit.

5.2.2 Razão de Vulnerabilidade

Outro ponto de investigação foi a razão de vulnerabilidade. Pretende-se verificar qual a proporção de caminhos que não podem ser recuperados na eventualidade de um falha. A Figura 5.6 apresenta a comparação da razão de vulneravilidade em redes reais e em redes ideais, para os três algoritmos de alocação de comprimento de onda. O gráfico relativo aos resultados para Best-Path foi separado apenas para aumentar sua legibilidade.



(a) First Fit e Random Pick (b) Best Path

Figura 5.6: Comparação da razão de vulnerabilidade para redes reais e ideais segundo 3 algoritmos alocações de comprimento de onda

Uma das informações que os dois gráficos revelam é que o desempenho de qualquer algoritmo para redes ideais é pior em reação às redes reais quando a carga é muito baixa, e que essa diferença diminui com o aumento da carga. Isso acontece porque as redes ideais aceitam um número muito maior de chamadas, e quanto maior a utilização de recursos, maior também é a probabilidade de que um caminho óptico, ao sofrer uma falha, não encontre um caminho para ser restaurado.

Nota-se, também, o desempenho muito melhor oferecido pelo algoritmo Random-Pick (Figura 5.6(a)). Comparando as taxas de bloqueio (Figuras 5.5(a) e 5.5(b)), nota-se que o desempenho deste algoritmo é um pouco inferior, mas quando se trata da razão de vulnerabilidade, este é capaz de oferecer uma taxa cerca de 160% menor, tanto para redes reais quanto para redes ideais. Pode-se concluir que o algoritmo mais indicado

a ser utilizado para proteção com limitações da camada física é o Random-Pick, pois oferece um custo-benefício maior. A razão para a melhoria no desempenho reside na busca por caminhos ópticos que não se dá de forma tão organizada, como ocorre com o First-Fit, uma vez que a alocação de comprimentos de onda é aleatória. Com isso, a taxa de compartilhamento dos caminhos de backup é menor, e, por conseqüência, a razão de vulnerabilidade, também, é menor.

O algoritmo Best-Path não apresenta nenhuma melhoria em relação ao First-Fit, uma vez que ambos se comportam de maneira muito semelhante, como explicado na Seção 5.2.1.

5.2.3 Lightpaths BER Acima da BER Máxima em Redes Ideais

Mediu-se também a proporção de caminhos ópticos alocados em redes ideais que tenham qualidade abaixo da mínima proposta, bem como a proporção das falhas recuperadas que também não ofereçam uma taxa de erro de bits aceitável. Pode-se verificar quantas das chamadas sofreram perdas de pacote elevadas o suficiente para causar prejuízos à transmissão de dados. Os resultados obtidos para esse estudo podem ser observados na Figura 5.7.

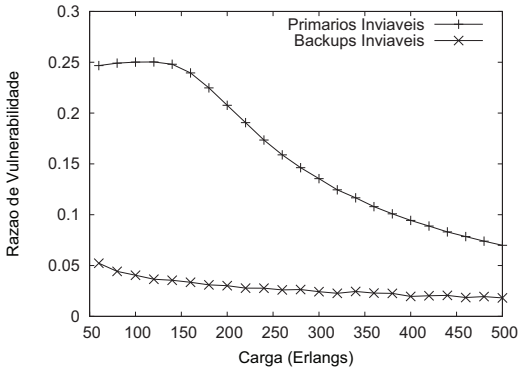
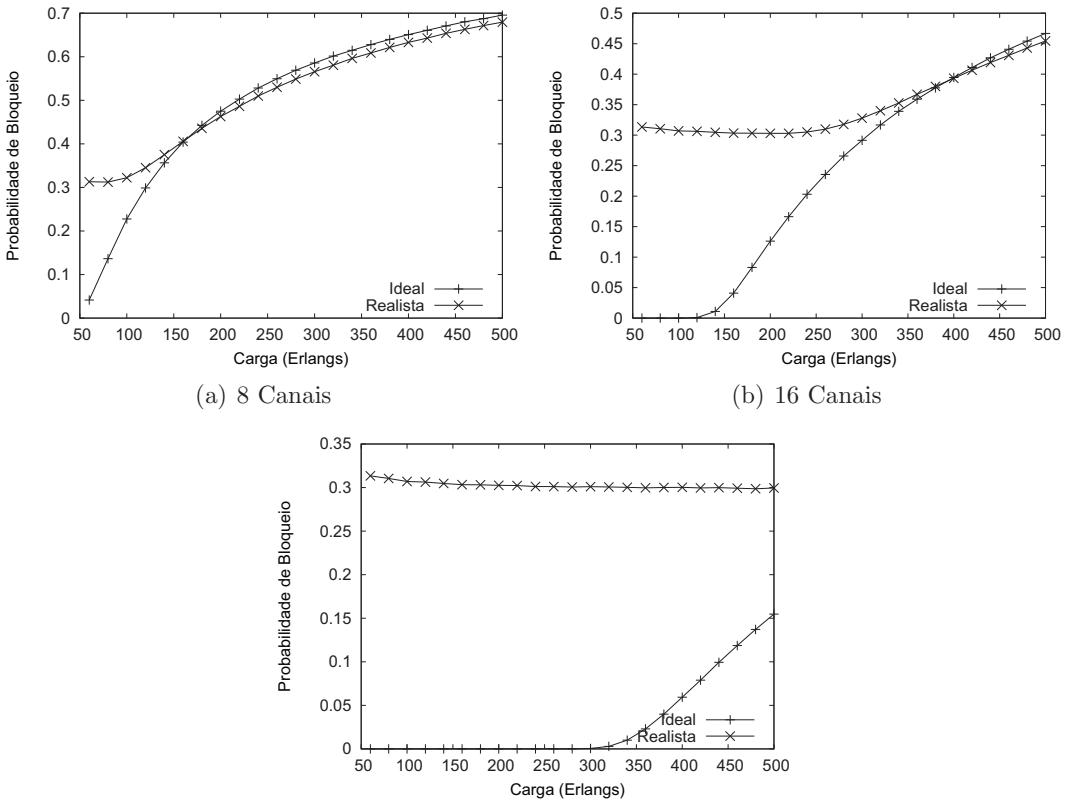


Figura 5.7: Comparação entre caminhos ópticos e falhas recuperadas abaixo da qualidade mínima em redes ideais

A diminuição mais acentuada na curva de caminhos ópticos inviáveis em função da carga justifica-se pelo fato de que foi medido o número de caminhos ópticos sem qualidade em relação ao total de chamadas e não apenas o número das chamadas aceitas. Dessa forma, o aumento do bloqueio ocasiona uma diminuição desta curva. Nota-se que os efeitos degradantes são muito mais relevantes para os caminhos primários do que para os caminhos de backup, o que é observado pela grande distância entre as curvas.

5.2.4 Efeito do Número de Canais

A Figura 5.8 compara o efeito do número de canais na eficiência dos algoritmos. Utiliza-se o algoritmo First-Fit apenas para fins ilustrativos. A conclusão é a mesma para outros algoritmos.



(a) 8 Canais

(b) 16 Canais

(c) 32 Canais

Figura 5.8: Verificação do efeito do número de canais na taxa de bloqueio para redes reais e ideais utilizando-se First-Fit

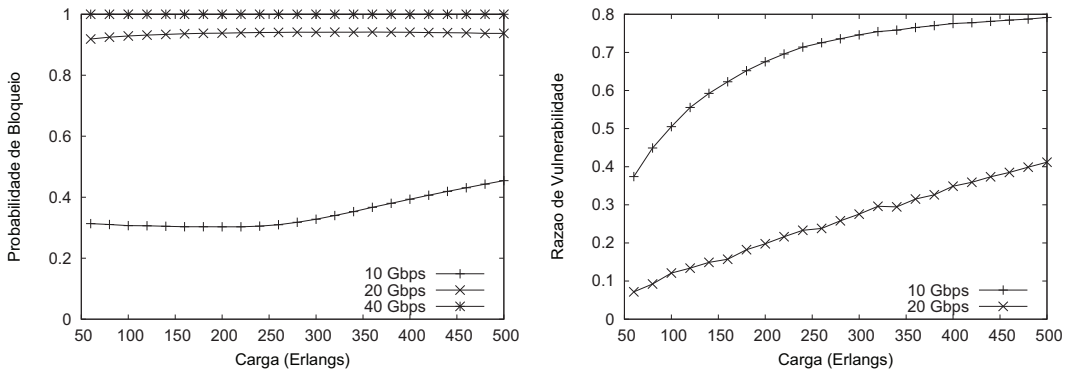
Pode-se ver que o aumento da quantidade de recursos da rede não afeta o desempenho do algoritmo para redes reais sob cargas baixas, pois não foram levadas em consideração interações inter-canais. Caso fossem levados em consideração alguns efeitos não-lineares, como FWM e XPM, que possuem essa característica de interação inter-canal, poderia ser observado um aumento na taxa de bloqueio das redes com maior número de canais.

Sob cargas altas, o aumento observado na taxa de bloqueio, cuja ocorrência se dá principalmente para redes com menos canais, deve-se essencialmente à escassez de recursos.

Mais uma vez, observa-se que quando existe essa escassez, o comportamento observado para redes reais e ideais é, praticamente, o mesmo.

5.2.5 Comparação para Diversas Capacidades

Pode-se ver, na Figura, 5.9 o efeito da taxa de bits no bloqueio em redes reais. Utiliza-se o algoritmo First-Fit, devido ao seu menor bloqueio.



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

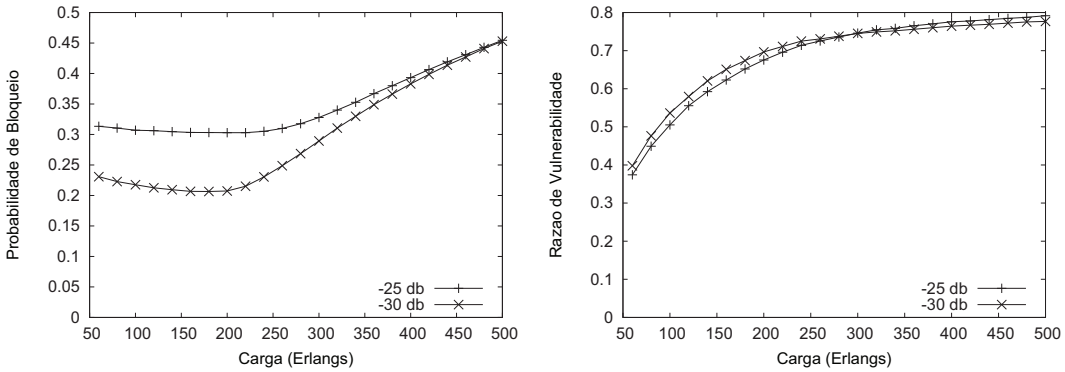
Figura 5.9: Verificação do efeito da taxa de bits no bloqueio para redes reais usando First-fit

Pode-se ver neste gráfico quão grave são os efeitos limitantes da camada física sob altas velocidades. Enquanto uma rede com 10 Gbps apresenta uma taxa de bloqueio que ainda pode ser aceita, para redes com 20 Gbps essa taxa já passa a ser proibitiva, atingindo mais de 90%. A taxas de 40 GBps o transporte torna-se ineficiente, uma vez que nenhum caminho na rede é capaz de oferecer uma qualidade de transmissão aceitável, nem mesmo os mais curtos. No gráfico da razão de vulnerabilidade, nota-se que o aumento na velocidade faz com que a razão seja menor, o que só aconteceu porque houve uma diminuição drástica da utilização de recursos, que não foi acompanhada por uma diminuição de mesma magnitude na razão de vulnerabilidade. Para taxas de transmissão de 40 Gbps, a curva não foi mostrada pois não faz sentido fazer essa medição quando nenhuma chamada é aceita.

Pode-se concluir então que, para redes com alta velocidades, não é possível a implementação de redes transparentes de longa distância com proteção, uma vez que os efeitos da camada física não permitem o atendimento de chamadas com qualidade.

5.2.6 Resultado da Variação no Nível de Crosstalk

Na Figura 5.10, investiga-se o efeito do *crosstalk* no bloqueio e na razão de vulnerabilidade. O algoritmo First-Fit foi usado devido ao seu menor bloqueio.



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

Figura 5.10: Variação do crosstalk e seu impacto na probabilidade de bloqueio e razão de vulnerabilidade para redes reais e ideais usando First-Fit

Na Figura 5.10(a), vê-se que para um valor menor de crosstalk (-30 dB) a probabilidade de bloqueio é ligeiramente menor. Entretanto, essa diminuição é muito pequena, mostrando que o crosstalk não é o efeito preponderante. Na verdade, a maior fonte de ruídos na rede é, de fato, a emissão ASE. Para valores maires que 300 Erlangs, a razão principal de bloqueio passa a ser a escassez de recursos, portanto, a alteração na tendência entre as duas curvas não é significativa.

Com relação a razão de vulnerabilidade, apresentada na Figura 5.10(b), observa-se que as duas curvas seguem praticamente juntas; conclui-se, portanto, que o crosstalk não afeta essa variável.

5.2.7 USA Network

De forma a confirmar os resultados encontrados, considerou-se, também, a topologia USA Network (Figura 5.11).

Os resultados de simulação encontrados para essa nova topologia são apresentados na Figura 5.12.

Na Figura 5.12(a), nota-se que para essa rede a probabilidade de bloqueio é um pouco maior que a anterior para o cenário real, pois permite que um número muito maior de

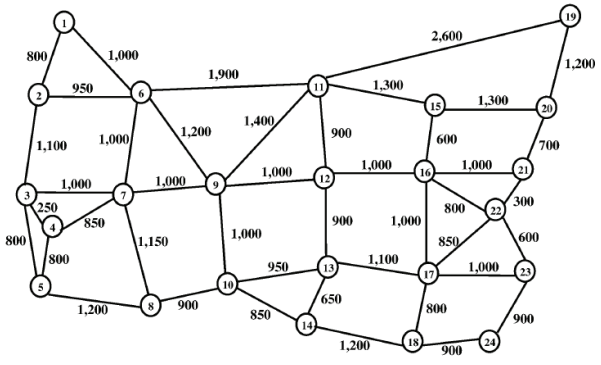


Figura 5.11: USA Network

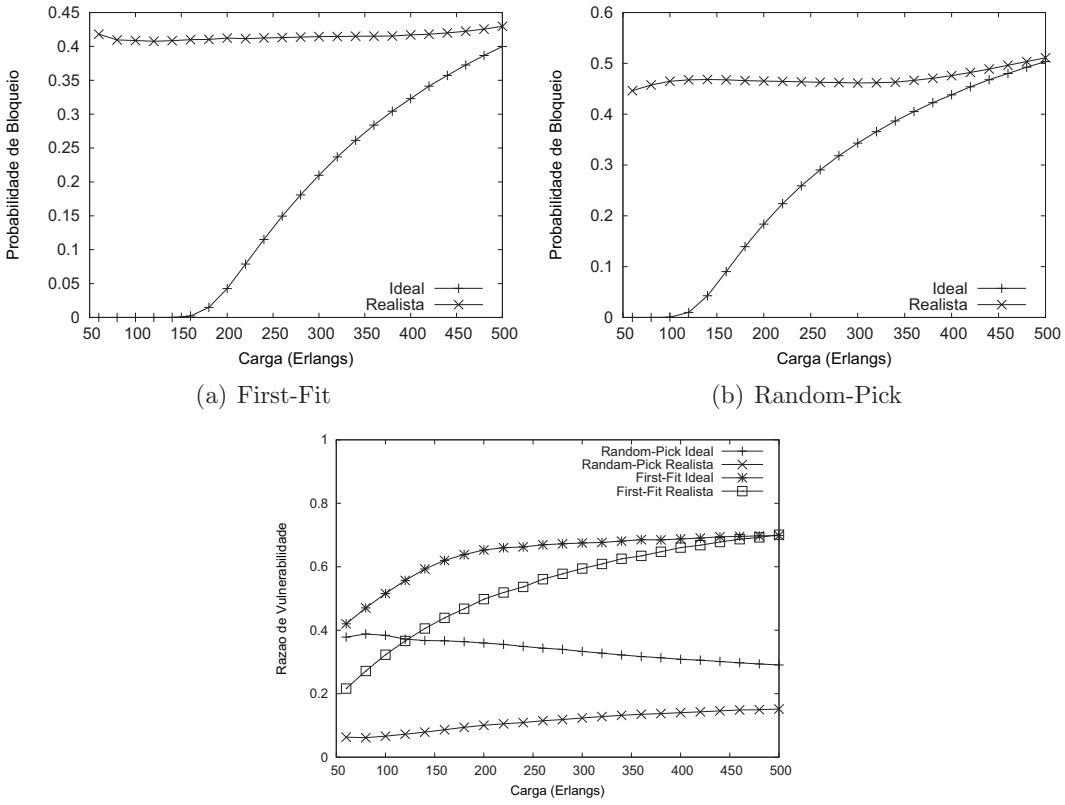
pares tenham distância grandes o suficiente para que o sinal seja degradado a ponto de que a qualidade não atinja o valor mínimo necessário. Observa-se o mesmo fenômeno na Figura 5.12(b), que também teve um aumento no bloqueio. Com relação a escassez de recursos, é muito menos influente neste caso, uma vez que essa topologia apresenta um número muito maior de enlaces, e conseqüentemente de recursos.

Por fim, na Figura 5.12(c) confirma-se que o algoritmo Random-Pick apresenta o melhor custo benefício, uma vez que gera uma diminuição muito grande da razão de vulnerabilidade a custo de um aumento muito pequeno na probabilidade de bloqueio.

As duas principais constatações são, portanto, confirmadas: os efeitos limitantes da camada física são muito importantes e devem ser levados em consideração, e o algoritmo de alocação de comprimento de onda que oferece melhor desempenho é o Random-Pick.

5.3 Considerações Parciais

A partir dos resultados encontrados, pode-se concluir alguns pontos importantes a respeito das limitações da camada física para o oferecimento de proteção por caminho compartilhado. Verifica-se que, sob altas taxas de transmissão, a utilização da rede é inviável, uma vez que não se consegue encontrar pares de caminhos primário-backup que satisfaçam uma qualidade mínima aceitável de sinal. Verifica-se, também, que o crosstalk não é o efeito preponderante de ruídos, mas sim a emissão ASE. Por fim, conclui-se que os dois pontos mais importantes referem-se a importância dos efeitos degradantes do sinal, e a escolha adequada do algoritmo de alocação de comprimento de onda. Em relação ao primeiro ponto, verifica-se que a probabilidade de bloqueio aumenta muito quando se leva em conta a qualidade do sinal, e, dessa forma, a análise dos efeitos degradantes deve sempre



(a) First-Fit

(b) Random-Pick

(c) Razão de Vulnerabilidade

Figura 5.12: Confirmação dos resultados para USA Network

ser observada para redes ópticas transparentes. Conclui-se, também, que o desempenho do algoritmo Random-Pick oferece o melhor custo-benefício, e por isso é o mais indicado para alocação de comprimento de onda.

Uma comparação com os resultados obtidos em [17] permite concluir que é muito importante levar em consideração os efeitos limitantes da camada física em redes com proteção, pois o aumento no bloqueio é ainda maior. Isso ocorre pois, nesse caso, torna-se necessário obter um par de caminhos disjuntos com qualidade aceitável, diferentemente daquele, onde apenas um caminho é necessário.

Dessa forma, a verificação feita e a comparação com a literatura apontam a importância de se considerar as limitações da camada física em redes ópticas transparentes com proteção por caminho compartilhado.

Capítulo 6

Proteção Sensível às Limitações da Camada Física

Conforme visto no Capítulo anterior, as limitações da camada física em redes com proteção são de grande importância. Apresentou-se naquele Capítulo uma abordagem de um algoritmo RWA tradicional com proteção compartilhada por melhor esforço que considera os efeitos degradantes do sinal no Controle de Acesso de Chamadas (CAC). Nessa abordagem, um caminho primário e um caminho de backup são escolhidos, aloca-se um comprimento de onda para ambos, e somente após este processo a qualidade do sinal é avaliada. Em nenhum momento, as limitações da camada física são consideradas pelo algoritmo RWA. Este procedimento resulta em um bloqueio muito alto, e uma nova técnica é necessária, a fim de produzir resultados mais eficientes.

Sendo assim, desenvolveram-se dois novos algoritmos de roteamento e alocação de comprimento de onda, para redes ópticas WDM transparentes com limitações na camada física, que adotam proteção por caminho compartilhado. Os novos algoritmos são sensíveis à essas limitações, ou seja, levam em consideração os efeitos degradantes do sinal no momento da escolha de um caminho óptico, a fim de produzir um melhor desempenho.

Para que a comparação do desempenho possa ser feita de forma mais evidente, utilizou-se o mesmo modelo de rede e de camada física projetado para o trabalho anterior, bem como as mesmas topologias adotadas na realização de simulações. O modelo de rede e da camada física estão descritos, respectivamente, nas Seções 5.1.1 e 5.1.2.

Este capítulo está, assim, organizado: na seção 6.1, são descritos os novos algoritmos RWA com proteção por melhor esforço sensíveis às limitações da camada física. Na seção 6.2, os resultados obtidos pela avaliação dos algoritmos propostos são apresentados. Por fim, na seção 6.3, conclui-se o capítulo.

6.1 Proteção por caminho compartilhado sensível às limitações da camada física

Nesta seção, são introduzidos dois novos algoritmos para estabelecimento de caminhos ópticos que utilizam um esquema de proteção por caminho compartilhado e que considera as limitações produzidas em virtude de efeitos degradantes do sinal. PMD, ASE e crosstalk são os efeitos considerados. O caminho escolhido é tal que seu comprimento permite níveis de PMD e OSNR aceitáveis no nó destino. O estabelecimento de um caminho óptico muda o estado da rede pois pode aumentar a razão de bits errados (bit error rate, BER), assim como o término de uma conexão pode diminuir o valor da BER.

Os algoritmos seguem a abordagem introduzida em [17], que adota um modelo de RWA hierárquico. De maneira geral, estes algoritmos consistem de duas etapas distintas: na primeira, busca-se um caminho óptico na camada de rede, da mesma forma que se faz em algoritmos tradicionais insensíveis às limitações da camada física; na segunda, faz-se a verificação da qualidade de transmissão deste caminho óptico. No processo de verificação, obtém-se, inicialmente, uma estimativa da qualidade do sinal. Caso o valor obtido para a qualidade estimada seja aceitável, o caminho óptico pode ser estabelecido; caso contrário uma nova rota deve ser calculada. Se, após uma busca exaustiva, nenhuma rota for encontrada, a conexão é bloqueada.

Os algoritmos assumem uma proteção por caminho compartilhado com uma confiabilidade do tipo melhor esforço [28, 15]. Nesta metodologia, dois caminhos primários podem compartilhar um caminho de backup sem restrição. Esta é uma abordagem diferente da proteção por caminho compartilhado tradicional, na qual dois caminhos primários com um enlace em comum não podem compartilhar um outro enlace no caminho de backup. O relaxamento desta restrição é realista, uma vez que no cenário em que se consideram as limitações da camada física, alguma falhas não podem ser recuperadas.

Os dois algoritmos propostos diferem pelo critério usado na alocação de comprimento de onda. O primeiro algoritmo é o SPPIAFF (acrônimo para *Shared Path Protection Impairment Aware First Fit*) e o segundo é o SPPIARP (acrônimo para *Shared Path Protection Impairment Aware Random Pick*). O primeiro usa o critério de alocação de comprimento de onda First-Fit, ou seja, aloca o primeiro comprimento de onda disponível. O segundo usa o critério randômico, ou seja, escolhe um comprimento de onda de forma aleatória.

Adota-se a notação usada em [17]. Considera-se uma topologia baseada em camadas $W_w(N, L)$, onde cada uma das camadas representa um comprimento de onda w, $w = 1, 2, ..., W$ em uma topologia física $T(N, L)$, onde N é o conjunto de nós, e L o conjunto de enlaces. Todas as camadas da topologia $W_w(N, L)$ assumem, inicialmente, o mesmo valor da topologia física $T(N, L)$, e o roteamento é baseado nestes grafos auxiliares. A

seguir os dois algoritmos são apresentados. Indica-se, também, as linhas do pseudocódigo correspondente ao passo do algoritmo.

6.1.1 SPPIAFF

Entrada: A topologia $T(N, L)$, o estado da rede $Ww(N, L)$, $w = 1, 2, ..., W$ e uma requisição de conexão $R(origem, destino)$:

1. Inicialize o procedimento pelo primeiro comprimento de onda, $w = 1$(linha 1 do Algoritmo 1);

2. Aplique o algoritmo do menor caminho, a fim de se achar um caminho primário Pw em $Ww(N, L)$. Se nenhum caminho for encontrado, faça $w = w + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 8 (linha 2 do Algoritmo 1);

3. Obtenha uma estimativa da qualidade do caminho $P\lambda$. Caso o lightpath não seja viável volte ao passo 2 (linha 3 do Algoritmo 1);

4. Faça $T'(N, L) = T(N, L) - Pw$, produzindo um novo conjunto de camadas $W'w'(N, L)$ derivado de $T'(N, L)$ (linha 5 do Algoritmo 1);

5. Inicialize $w' = 1$ (linha 4 do Algoritmo 1);

6. Aplique o algoritmo do menor caminho a fim de achar um caminho de backup compartilhado Bw' em $W'w'(N, L)$. Se nenhum caminho for encontrado, faça $w' = w' + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2 (linha 6 do Algoritmo 1);

7. Obtenha uma estimativa da qualidade do caminho $B\lambda'$. Caso o lightpath seja viável, aceite a chamada, atualize $W\lambda$ (colocando os enlaces de $P\lambda$ em modo ocupado), atualize $W\lambda'$ (colocando os enlaces de $B\lambda'$ em modo backup), e, por fim, atualize os ruídos gerados por $P\lambda$; caso contrário volte ao passo 6 (linhas 7 e 8 do Algoritmo 1);

8. Pare o procedimento

O pseudocódigo do algoritmo SPPIAFF é apresentado no Algoritmo 1.

O procedimento executado pela camada de rede é identificado pelas linhas 2 e 6 do pseudocódigo. O resultado obtido é entregue a camada física nas linhas 3 e 7. Deve-se

Algorithm 1 SPPIAFF

```
1: for w = 1 até W do
2:   Pw ⇐ shortestPath(T, w)
3:   if temQualidadeMinima(Pw) then
4:     for w' = 1 até W do
5:       T' ⇐ topologiaDisjunta(T, Pw)
6:       P'w' ⇐ shortestPath(T', w')
7:       if temQualidadeMinima(P'w') then
8:         setupLightpath(Pw, P'w')
9:       end if
10:    end for
11:  end if
12: end for
```

notar também que nas linhas 1 a 3 efetua-se a busca por caminhos primários, enquanto que nas linhas 4 a 7 busca-se um caminho de backup.

6.1.2 SPPIARP

O algoritmo SPPIARP difere pela forma que se dá a iteração entre as camadas. Em SPPIAFF, a iteração é feita ordenadamente, começando pela primeira camada e terminando na última. No SPPIARP, a busca é aleatória. Visita-se cada uma das camadas sem uma ordem pré-definida, sendo que o único requisito necessário é que todas as camadas sejam visitadas. Entretanto, a forma como se encontra o par de seguimentos é a mesma: busca-se, inicialmente, um caminho primário com qualidade mínima, e em seguida encontra-se um caminho disjunto a esse primário. Caso este também ofereça uma qualidade mínima, a chamada pode, então, ser aceita.

A seguir, descreve-se o SPPIARP:

Entrada: A topologia $T(N, L)$, o estado da rede $Ww(N, L)$, $w = 1, 2, ..., W$ e uma requisição de conexão $R(origem, destino)$:

1. Inicialize w com um inteiro aleatório no intervalo $[1, W]$;

2. Aplique o algoritmo do menor caminho, a fim de achar um caminho primário Pw em $Ww(N, L)$. Se nenhum caminho for encontrado, atribua a w o próximo inteiro aleatório não repetido no intervalo $[1, W]$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 8;

3. Obtenha uma estimativa da qualidade do caminho $P\lambda$. Caso o lightpath não seja viável volte ao passo 2;

4. Faça $T'(N, L) = T(N, L) - Pw$, produzindo um novo conjunto de camadas $W'w'(N, L)$ derivado de $T'(N, L)$;

5. Inicialize w' com um inteiro aleatório no intervalo $[1, W]$;

6. Aplique o algoritmo do menor caminho, a fim de achar um caminho de backup compartilhado Bw' em $W'w'(N, L)$. Se nenhum caminho for encontrado, atribua a w' um próximo valor aleatório diferente dos anteriores no intervalo $[1, W]$. Repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2;

7. Obtenha uma estimativa da qualidade do caminho $B\lambda'$. Caso o lightpath seja viável, aceite a chamada, atualize $W\lambda$ (colocando os enlaces de $P\lambda$ em modo ocupado), atualize $W\lambda'$ (colocando os enlaces de $B\lambda'$ em modo backup), e, por fim, atualize os ruídos gerados por $P\lambda$. Caso contrário, volte ao passo 6;

8. Pare o procedimento

O Algoritmo 2 apresenta o pseudocódigo do algoritmo SPPIARP.

Algorithm 2 SPPIARP

```
1:  for i = 1 até W do
2:    w ⇐ random(1, W)
3:    Pw ⇐ shortestPath(T, w)
4:    if temQualidadeMinima(Pw) then
5:      for j = 1 até W do
6:        w' ⇐ random(1, W)
7:        T' ⇐ topologiaDisjunta(T, Pw)
8:        P'w' ⇐ shortestPath(T', w')
9:        if temQualidadeMinima(P'w') then
10:         setupLightpath(Pw, P'w')
11:       end if
12:     end for
13:   end if
14: end for
```

Nota-se que antes de partir para a busca do menor caminho, atribui-se a w um inteiro aleatório (Linhas 2 e 6), e sobre a camada representada por w busca-se o caminho. Utiliza-se a função *random* de tal forma que esta retorne apenas inteiros não repetidos, a fim de que todas as camadas possam ser testadas.

6.2 Avaliação dos Algoritmos Propostos

Nesta Seção, a eficácia dos algoritmos propostos é verificada por meio de simulação. Os resultados produzidos por eles são comparados aos resultados produzidos por algoritmos tradicionais para redes realistas. Nestes, os componentes de rede inflingem ruído sobre o sinal, causando sua degradação, que é levada em consideração pelo CAC na aceitação de chamadas. Note que nos algoritmos propostos, o problema RWA leva em consideração as limitações da camada física, a fim de encontrar um caminho com qualidade aceitável, ao contrário dos algoritmos tradicionais para redes realistas, que levam em consideração a degradação do sinal apenas na decisão do controle e admissão de chamadas.

O bloqueio de caminhos com baixa qualidade de sinal ocorre tanto para os algoritmos sensíveis como para os algoritmos tradicionais aos efeitos degradantes do sinal. Duas topologias são usadas para ilustrar o desempenho dos algoritmos: a topologia da rede NSFNET, com 16 nós e 25 enlaces; e a topologia da *USA Network*, com 24 nós e 43 enlaces, ambas apresentadas no capítulo anterior.

Duas medidas foram aferidas: a taxa de bloqueio e a razão de vulnerabilidade. A primeira contabiliza as chamadas bloqueadas, seja por falta de recurso, ou por falta de caminhos que ofereçam uma qualidade mínima; e a segunda mede a probabilidade de que, na ocorrência de uma falha, uma chamada não encontre um caminho de backup disponível (devido ao compartilhamento) e com qualidade adequada para ser restabelecida. Sendo assim, a razão de vulnerabilidade P pode ser definida como $P = \frac{D}{T}$, onde D é o número de conexões que não puderam ser recuperadas, e T designa o número de chamadas afetadas por uma falha, sejam elas recuperadas ou não-recuperadas.

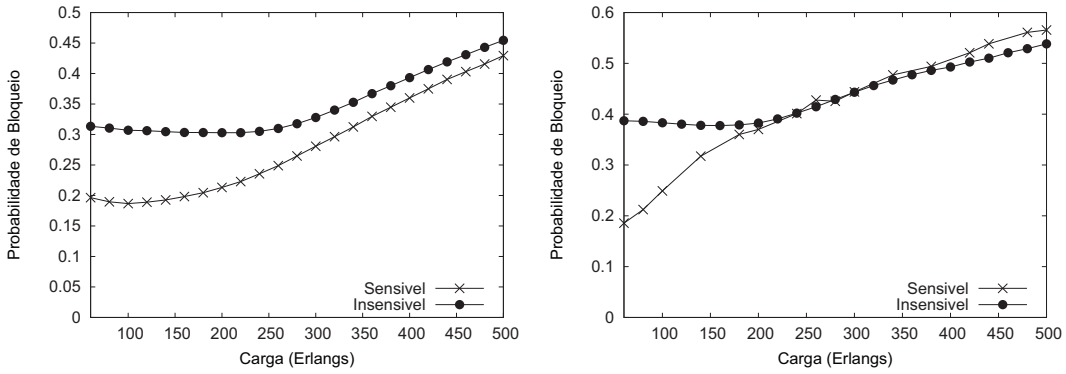
Nas simulações, considerou-se que o tráfego é dinâmico e que a chegada de chamadas segue um processo de Poisson, enquanto que período de duração de uma chamada (*holding time*) é dado por uma distribuição exponencial com média 1, de modo que a carga da rede seja dada pela taxa de chegada. O modelo de falhas adotado é o de enlace único, ou seja, em qualquer momento existe apenas a falha de um enlace, e a ocorrência de uma nova falha só é possível quando o conserto da anterior já houver ocorrido[36].

A largura do intervalo de confiança para nível de significância igual a 95% é inferior a 1% do valor medido. Foram realizadas 10^6 requisições de conexão para cada simulação.

6.2.1 Bloqueio

A Figura 6.1 apresenta a probabilidade de bloqueio encontrada em função da carga da rede. Compara-se a execução de um algoritmo insensível às limitações da camada física com os algoritmos propostos na Subseção 6.1.

Pode-se notar que o algoritmo proposto apresenta uma melhora significativa, para as duas técnicas de alocação de comprimento de onda diferentes. Na primeira delas, para



(a) SPPIAFF (b) SPPIARP

Figura 6.1: Comparação da taxa de bloqueio para algoritmo tradicional e aware segundo 3 algoritmos alocações de comprimento de onda

uma carga de 100 Erlangs, o novo algoritmo foi capaz de diminuir a taxa de bloqueio de 0,3 para 0,18, ou seja, uma melhora de 66%. Com o aumento da carga, esse desempenho diminui. Mesmo sob cargas altas, o algoritmo SPPIAFF apresenta sempre resultados superiores.

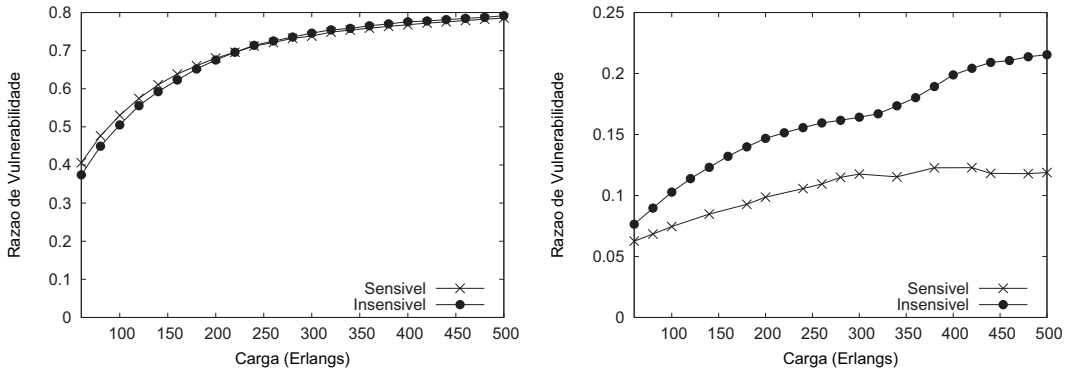
Além disso, a melhora é muito grande para cargas baixas. Sob carga de 50 Erlangs, ocorre uma diminuição de 0,38 para 0,17, ou seja, uma melhoria de 123%. Entretanto, com o aumento da carga, a diminuição no desempenho é muito maior do que para o algoritmo SPPIAFF, e a partir de 220 Erlangs, o desempenho do SPPIABP já é muito semelhante à sua versão insensível aos limites da camada física.

6.2.2 Razão de Vulnerabilidade

Verificou-se, também, a razão de vulnerabilidade produzida pelos algoritmos (Figura 6.2).

Na Figura 6.2(a), pode-se observar que a melhoria obtida para a probabilidade de bloqueio não implicou em uma diminuição no desempenho. Apesar de haver uma utilização muito maior dos recursos (mais chamadas aceitas), o algoritmo SPPIAFF apresentou um comportamento praticamente igual à sua versão insensível aos limites da camada física, o que comprova a eficácia do algoritmo proposto.

Analisando o SPPIARP, a partir do gráfico da Figura 6.2(b), observa-se uma melhoria muito grande da razão de vulnerabilidade, principalmente para cargas muito altas. Quando a carga é de 500 Erlangs, o novo algoritmo foi capaz de realizar uma diminuição de 0,22 para 0,12, uma melhoria de 83%. Além disso, os algoritmos Random-Pick apresentam



(a) SPPIAFF (b) SPPIARP

Figura 6.2: Comparação da razão de vulnerabilidade para algoritmo tradicional e aware segundo 3 algoritmos alocações de comprimento de onda

resultados superiores ao do First-Fit, tornando seu uso aconselhável para a diminuição da razão de vulnerabilidade.

6.2.3 Efeito do Número de Canais

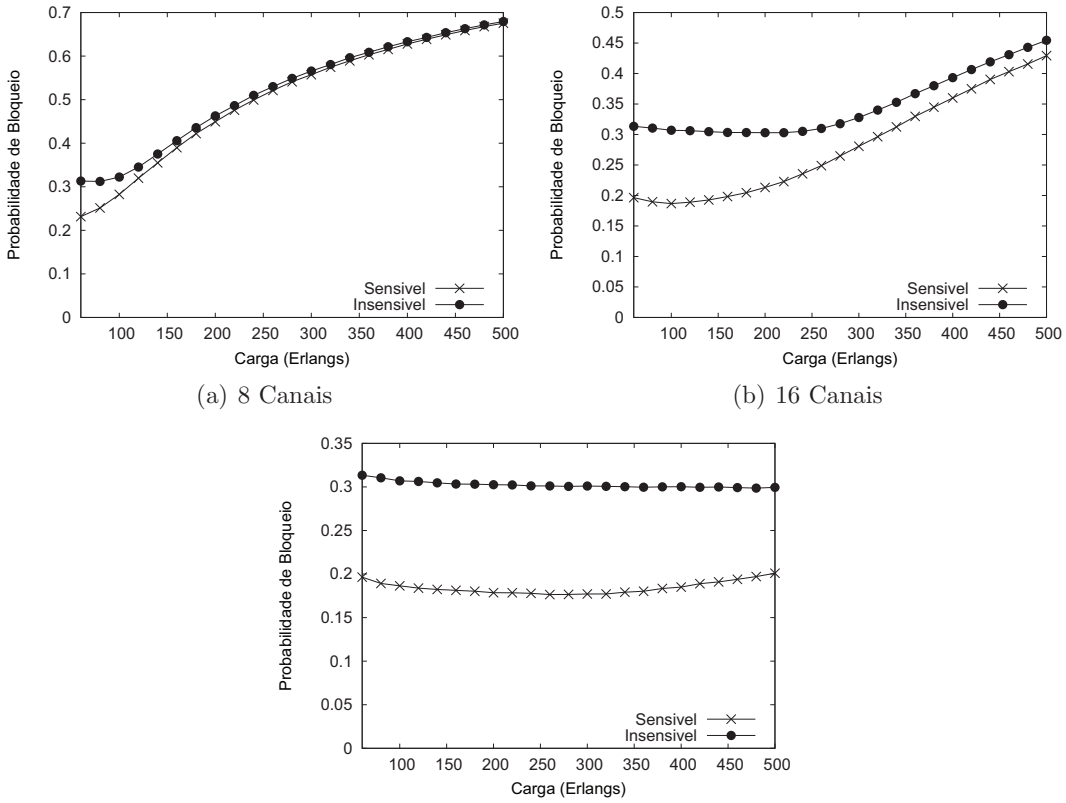
A fim de se verificar a eficiência de nosso algoritmo em função da variação do número de canais, plotam-se, na Figura 6.3, os resultados de simulação para redes com 8, 16 e 32 canais.

Na Figura 6.3(a), pode-se ver que, a partir de 110 Erlangs, a eficiência do algoritmo diminui muito, dado que a rede possui muito menos recursos. Como o objetivo do algoritmo é diminuir o bloqueio devido a ausência de qualidade mínima de um caminho óptico, é esperado que em um ambiente com escassez de recursos o desempenho do algoritmo não seja muito melhor que o obtido com um algoritmo tradicional.

Nota-se que, para redes com 16 canais, o desempenho é menor sob cargas a partir de 300 Erlangs. Esse aumento deve-se ao fato de a rede possuir muito mais recursos. Observa-se, também, que mesmo a partir desse valor de carga, o algoritmo apresenta desempenho melhor que o algoritmo tradicional.

O novo algoritmo apresenta bom desempenho para redes com 32 canais, uma vez que a disponibilidade de recursos é maior.

Observa-se que no melhor caso, o ganho de desempenho é de cerca de 63%, ou seja, a probabilidade de bloqueio cai de 0,3 para 0,18%. Essa ganho é válido para os três cenários, e não é conseqüência da disponibilidade de recursos, portanto, esta variável não



(a) 8 Canais

(b) 16 Canais

(c) 32 Canais

Figura 6.3: Verificação do efeito do número de canais na taxa de bloqueio para algoritmos tradicional e aware usando First-Fit para alocar comprimentos de onda

afeta o desempenho do novo algoritmo.

6.2.4 Eficácia para Velocidades Diferentes

A Figura 6.4 mostra a probabilidade de bloqueio do algoritmo quando a rede opera a 20 Gbps.

Não é possível verificar a diferenciação entre o algoritmo sensível aos efeitos limitantes da camada física e o tradicional, dado a coincidência das curvas, o que revela que para altas velocidades o desempenho do novo algoritmo é igual ao do tradicional. Isso acontece porque o melhor desempenho apresentado deve-se, principalmente, à exploração dos efeitos do crosstalk. Entretanto, com altas taxas de banda passante, o efeito preponder-

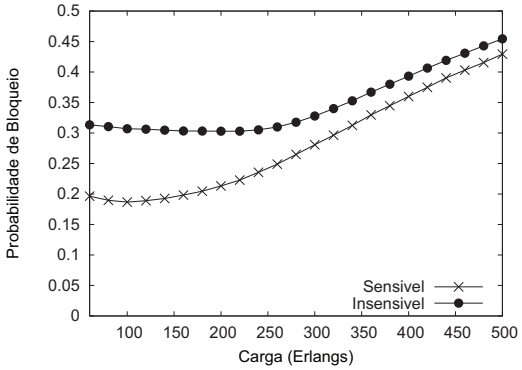


Figura 6.4: Verificação do efeito da taxa de bits no bloqueio para algoritmo tradicional e aware usando First-Fit para alocar comprimentos e onda

ante na diminuição da qualidade de um caminho óptico é a dispersão PMD, efeito sobre o qual o algoritmo nada pode fazer para obter um melhor desempenho, uma vez que depende apenas da distância e não da intereção entre os sinais.

Observa-se, também, que para altas taxas, a dispersão PMD é devastadora, levando a probabilidades de bloqueio superiores a 0,9, o que torna a rede praticamente inoperante. Simulações realizadas com taxa de 40 Gbps, mostram que a taxa de bloqueio é invariavelmente 1,0, tanto para o algoritmo tradicional, quando para o sensível aos efeitos limitantes da camada física, mostrando mais uma vez como os efeitos PMD podem ser desastrosos.

6.2.5 Comportamento com Variação no Nível de *Crosstalk*

A Figura 6.5 apresenta a eficiência do algoritmo para uma taxa menor de *crosstalk*. Para este caso diminuiu-se a razão de crosstalk, de -25db para -30db.

Pode-se ver que com um nível de *crosstalk* menor, o ganho de desempenho do algoritmo é inferior; enquanto que com o cenário padrão obteve-se uma melhoria de 63% na probabilidade de bloqueio, para este cenário a melhoria foi de apenas 33%. A razão para essa queda, é o fato de o novo algoritmo considerar principalmente os efeitos do *crosstalk* na obtenção de um melhor desempenho. Dessa forma, pode-se concluir que o algoritmo tem desempenho superior em ambientes onde os OXCs inserem grande quantidade de ruído no sinal devido ao crosstalk.

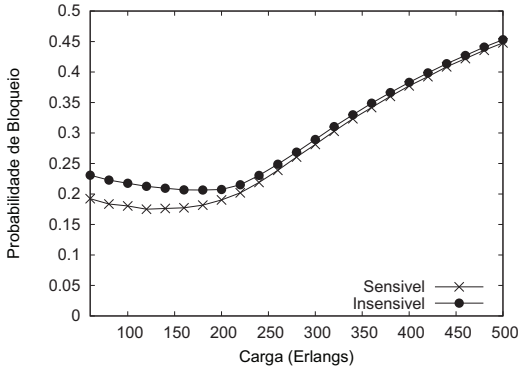


Figura 6.5: Verificação do efeito do nível de crosstalk no bloqueio em algoritmos tradicionais e sensíveis

6.2.6 USA Network

Foram, também, realizadas simulações com a topologia USA Network. O grau de conectividade, bem como o diâmetro dessa topologia são maiores do que os mesmos parâmetros na NSFNET. Se, por um lado, as distâncias entre origem e destino são maiores, e consequentemente, a intensidade dos efeitos degradantes do sinal; por outro lado, as possibilidades de caminhos alternativos são muito maiores, devido ao maior número de nós e enlaces, tornando mais fácil a busca por caminhos com qualidade de sinal aceitável. A Figura 6.6 mostra a probabilidade de bloqueio em função da carga usando First-Fit como técnica de alocação de comprimento de onda. Comparando-se os resultados apresentados com os obtidos para a NSFNET, houve um aumento de 0.1 na probabilidade de bloqueio tanto para o algoritmo proposto como para o algoritmo tradicional em redes realistas, tendo como causa a maior degradação do sinal devido ao aumento no diâmetro da rede. Além disso, a topologia da *USA Network* permite um maior número de caminhos alternativos, e mesmo sob cargas altas a escassez de recursos não é um fator preponderante para o aumento de bloqueio nas redes não ideais. A razão de vulnerabilidade, entretanto, teve um pequeno aumento. Além disso, o algoritmo SPPIAFF reduziu aproximadamente 0.15 e 0.1 sob baixas e altas cargas, respectivamente, a probabilidade de fracasso ao se tentar restaurar uma conexão. Nota-se que o SPPIAFF reduz cerca de 0.11 a probabilidade de bloqueio quando comparado ao algoritmo tradicional realista, que bloqueia caminhos sem QoT porém que não considera a QoT, na escolha do caminho. Nota-se, também, que sob cargas de 160 Erlangs 30% das chamadas seriam aceitas inadequadamente ao se ignorar a QoT, e que esta tendência errônea aceitaria cerca de 10% das chamadas inadequadamente sob cargas de 300 Erlangs, valor que seria 0.2, caso uma abordagem realista fosse adotada.

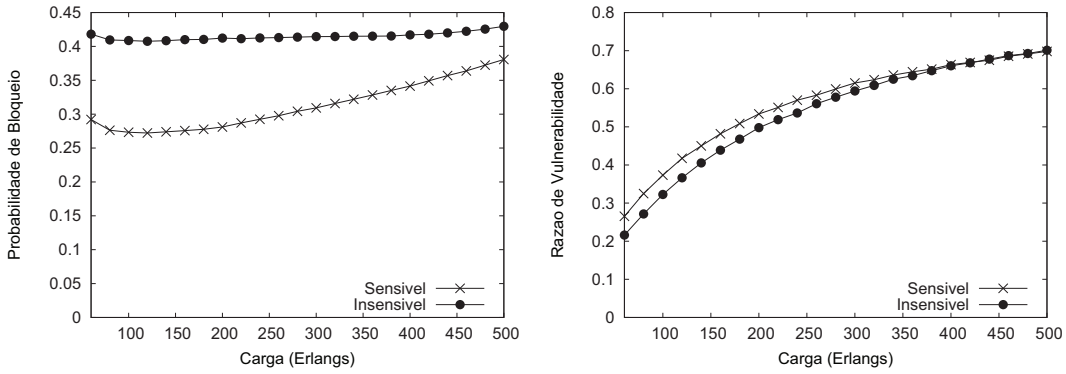


Figura 6.6: Avaliação do algoritmo SPPIAFF para a topologia USA Network

A Figura 6.7 apresenta os resultados obtidos para a avaliação do algoritmo SPPIARP para a topologia USA Network. Sob cargas baixas, o algoritmo produz uma diminuição significativa da probabilidade de bloqueio (Figura 6.7(a)) quando comparado com a versão insensível às limitações da camada física. Sob 50 Erlangs, observa-se uma queda de 0,45 a 0,28. Com o aumento da carga, a escassez de recursos passa a ser o fator preponderante, e SPPIARP passa a ter um desempenho semelhante ao outro algoritmo. A diminuição no ganho de desempenho é progressiva, e a partir de 400 Erlangs ambos passam a ter o mesmo desempenho. A razão de vulnerabilidade apresenta um padrão inverso ao do bloqueio. Sob cargas baixas, o desempenho dos algoritmos sensível e insensível é muito semelhante, e até 220 Erlangs as curvas que representam cada um dos algoritmos seguem praticamente juntas. A partir dessa carga, no entanto, ocorre uma distanciação entre as curvas, e o algoritmo SPPIARP passa a oferecer um desempenho melhor. O ganho aumenta progressivamente, e sob 500 Erlangs o vulnerabilidade cai de 15% para o algoritmo insensível e de 10% para o novo algoritmo. Observa-se, desse modo, que tanto para cargas altas como para cargas baixas o uso do novo algoritmo é vantajoso. Para cargas baixas é capaz de diminuir o bloqueio mantendo a mesma confiabilidade na recuperação de chamadas, e para cargas altas mantém a mesma probabilidade de bloqueio diminuindo a vulnerabilidade no caso de falhas.

6.3 Considerações Parciais

Em redes WDM, a regeneração do sinal resultante da conversão opto-eletro-óptica (O-E-O) tem um custo muito alto, e, por este motivo, manter o sinal no domínio óptico é preferível. Com isso, a comutação do sinal é, muitas vezes, feita de modo transparente,

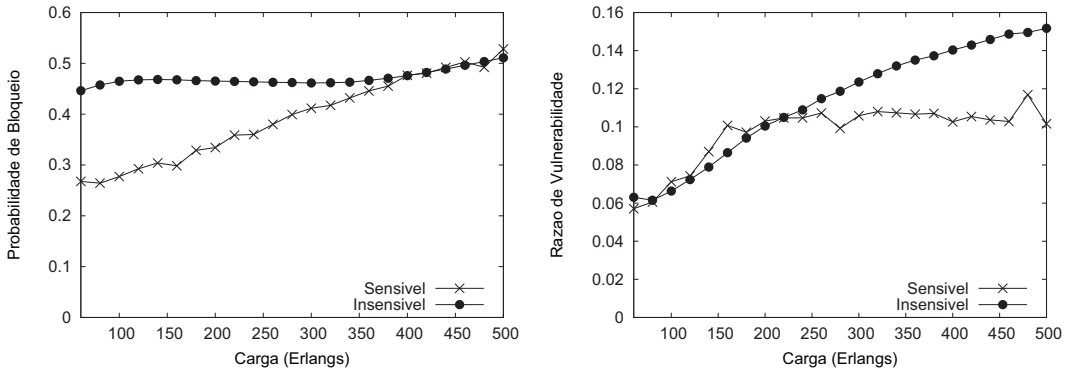


Figura 6.7: Avaliação do algoritmo SPPIARP para a topologia USA Network

o que leva a um aumento progressivo das deficiências nas transmissões. As limitações da camada física podem deteriorar o sinal até níveis inaceitáveis causando o bloqueio dos pedidos de estabelecimento de caminhos ópticos. Deixar de considerar os efeitos degradantes do sinal no processo de roteamento e alocação de comprimento de onda pode levar a um bloqueio demasiadamente alto (Capítulo 5), justificando a necessidade por algoritmos sensíveis a esses efeitos limitantes.

Neste capítulo, apresentaram-se dois novos algoritmos, capazes de oferecer um melhor desempenho no contexto de redes ópticas transparentes com proteção por caminho compartilhado segundo o melhor esforço. Resultados derivados via simulação, apontaram que os algoritmos são capazes de diminuir consideravelmente o bloqueio devido a degradação da qualidade do sinal, principalmente quando a técnica de alocação de comprimento de onda é aquela utilizada em SPPIAFF. Em relação ao algoritmo SPPIARP, observa-se um ganho menor em relação ao bloqueio, e uma diminuição muito grande da razão de vulnerabilidade.

Observou-se, também, que os algoritmos são eficientes apenas em ambientes com taxa de dispersão PMD moderada, e que quanto maior o ruído gerado por crosstalk, melhores os desempenho dos algoritmos sensíveis às limitações da camada física.

Capítulo 7

Proteção por Caminho Compartilhado com Diferentes Níveis de Confiabilidade

O surgimento da tecnologia WDM permitiu um aumento muito grande da taxa de bits transmitida sobre uma fibra. Com isso a ocorrência de falhas pode ser ainda mais catastrófica, uma vez que perda de dados é muito grande, o que tornou ainda mais evidente a necessidade por técnicas de proteção. Os métodos tradicionais para se prover proteção têm como requisito 100% de confiabilidade, no caso de falhas únicas de enlace, ou seja, todas as conexões prejudicadas por uma falha devem ser recuperadas. Esta técnica apresenta um custo muito alto, pois, em geral, pelo menos o dobro de recursos são necessários para este grau de confiabilidade. Apesar de ser um caso importante, existem situações onde o custo-benefício permitido por estes métodos não é interessante, por exemplo: um consumidor doméstico pode julgar que não é necessário pagar o dobro pelo serviço de proteção quando as falhas são raras. Ao contrário, para um banco ou um hospital a confiabilidade é imprescindível, e o custo-benefício é compensado. Situações intermediárias nas quais a confiabilidade é maior do que a fornecida pelo serviço sem proteção, e mais barata que a permitida pela proteção total também são interessantes.

Trabalhos anteriores iniciaram o estudo deste tipo de proteção. Nos capítulos anteriores [7, 8], propos-se um mecanismo de proteção por caminho compartilhado do tipo melhor esforço. Nesta técnica, permite-se que um comprimento de onda seja compartilhado por dois caminhos primários diferentes, e, na ocorrência de uma falha, recuperam-se tantos caminhos primários quanto forem possíveis. Em [28], a idéia é semelhante, entretanto, a proteção possui restrições do tipo SRLG (*Shared-Risk Link Group*). Em [15, 32] propõe-se algoritmos de proteção com confiabilidade diferenciada (*Differentiated in Reliability* - DiR). Nesta abordagem, permite-se que conexões não sejam 100% protegidas,

considerando-se a valor da probabilidade de falha de cada enlace da rede.

Além da confiabilidade obtida com mecanismos de proteção, deve-se levar em consideração a degradação do sinal, a fim de se prover serviços de qualidade. Como mostrado no Capítulo 5, o impacto dos efeitos degradantes do sinal sobre transmissões ópticas é significativo, e deixar de levá-lo em consideração pode levar a conclusões errôneas.

Neste capítulo, propõe-se um novo algoritmo de proteção por caminho compartilhado com diferentes níveis de confiabilidade, a fim de que se possa atender tanto os requisitos de clientes para os quais a confiabilidade é imprescindível, quanto a clientes para os quais a confiabilidade não é fundamental. O algoritmo considera as limitações da camada física, a fim de que as transmissões possuam boa qualidade de sinal. Considera-se os efeitos degradantes geradas pelos efeitos de Emissão Espontânea Amplificada (*Amplified Spontaneous Emission* - ASE), Dispersão por Modo de Polarização (*Polarization Mode Dispersion* - PMD) e Crosstalk intracanal. Estes efeitos foram considerados pois apresentam degradação de maior intensidade, de acordo com o que foi sugerido em RFC pelo IETF [31].

O trabalho está organizado da seguinte forma: na Seção 7.1, o novo algoritmo é introduzido. Na Seção 7.2, seu desempenho é avaliado. Por fim, na Seção 7.3 apresentam-se as considerações parciais. O modelo de rede usado nas simulações, bem como o modelo de camada física utilizado na proposição do algoritmo sensível às limitações da camada física são os mesmos introduzidos nos Capítulos 5 e 6.

7.1 Algoritmo de Proteção com Diferentes Níveis de Confiabilidade

Nesta Seção, introduz-se um novo algoritmo para estabelecimento de caminhos ópticos em redes com proteção com diferentes níveis de confiabilidade. São apresentadas duas versões: uma para redes ideais, nas quais as limitações da camada física são desconsideradas; e uma versão sensível aos efeitos degradantes.

O algoritmo é baseado na abordagem de melhor esforço, introduzida no Capítulo 6. Nesta técnica, dois caminhos primários não-disjuntos podem compartilhar comprimentos de onda de backup. No momento em que uma falha ocorre, é recuperado o maior número de chamadas possível. Assim, ao final do processo de restauração, parte das chamadas que sofreram com a falha é recuperada, e outra parte permanece com seus serviços interrompidos. A razão entre caminhos não recuperados e o total de chamadas pertencentes a um enlace falho é denominada razão de vulnerabilidade.

O novo algoritmo de proteção proposto busca limitar o compartilhamento de comprimentos de onda introduzido pela abordagem do melhor esforço. Na técnica apresentada

no Capítulo 6, um comprimento de onda pode ser compartilhado por tantos caminhos primários quanto se queira, o que leva a uma razão de vulnerabilidade alta. Em um algoritmo de proteção por caminho compartilhado tradicional, a razão de vulnerabilidade é zero, uma vez que em caso de falha todas as chamadas são recuperadas. O novo algoritmo busca uma alternativa a estas duas propostas. Limitando-se o compartilhamento dos comprimentos de onda, consegue-se razões de vulnerabilidade nem tão altas quando a abordagem do Capítulo 6, e nem tão baixa quando a obtida por algoritmos tradicionais, o que permite atender a clientes com diferentes necessidades.

Leva-se, adicionalmente, em consideração, as limitações da camada física, a fim de que se possa comparar o desempenho do algoritmos em redes nas quais os efeitos degradantes do sinal sejam relevantes. Adota-se, também, a abordagem apresentada no Capítulo 6, que faz uso de um modelo de RWA hierárquico. Os algoritmos consistem de duas etapas distintas: na primeira, busca-se um caminho óptico na camada de rede, da mesma forma que fazem os algoritmos tradicionais insensíveis às limitações da camada física; na segunda, verifica-se a qualidade de transmissão deste caminho óptico. No processo de verificação, obtém-se, inicialmente, uma estimativa da qualidade do sinal. Caso o valor obtido para a qualidade estimada seja aceitável, o caminho óptico pode ser estabelecido; caso contrário uma nova rota deve ser calculada. Se, após uma busca exaustiva, nenhuma rota for encontrada, a conexão é bloqueada.

Nas próximas subseções, descreve-se o novo algoritmo. Na Subseção 7.1.1 o algoritmo é descrito para redes ideais, insensíveis as limitações da camada física, e na Subseção 7.1.2 os efeitos degradantes do sinal são considerados. Ambos utilizam First Fit como critério para alocação de comprimento de onda. Nas Subseções 7.1.3 e 7.1.4, tanto a versão sensível quanto a versão insensível às limitações da camada física do algoritmo utilizando a política de alocação de comprimento de onda Random Pick são apresentadas.

O formalismo adotado na descrição considera a seguinte notação: dada uma topologia baseada em camadas $W_w(N, L)$, onde cada uma das camadas representa um comprimento de onda w, $w = 1, 2, ..., W$ em uma topologia física $T(N, L)$. N é o conjunto de nós, e L o conjunto de enlaces. Todas as camadas da topologia $W_w(N, L)$ assumem, inicialmente, o mesmo valor da topologia física $T(N, L)$, e o roteamento é baseado nestes grafos auxiliares. O algoritmo opera sobre um nível de confiabilidade constante C. Comprimentos de onda utilizados como caminho de backup estão associados a um nível de compartilhamento S, correspondente ao número de caminhos primários que utilizam o canal para proteção.

7.1.1 Novo SPP - First Fit

A descrição formal do novo algoritmo é a seguinte:

Entrada: A topologia $T(N, L)$, o estado da rede $Ww(N, L)$, $w = 1, 2, ..., W$, o nível

de confiabilidade C e uma requisição de conexão $R(origem, destino)$:

1. Inicializar o procedimento pelo primeiro comprimento de onda, $w = 1$;
2. Aplicar o algoritmo do menor caminho, a fim de se achar um caminho primário Pw em $Ww(N, L)$. Se nenhum caminho for encontrado, faça $w = w + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 7;
3. Faça $T'(N, L) = T(N, L) - Pw$, produzindo um novo conjunto de camadas $W'w'(N, L)$ derivado de $T'(N, L)$;
4. Inicializar $w' = 1$;
5. Aplicar o algoritmo do menor caminho, a fim de achar um caminho de backup compartilhado Bw' em $W'w'(N, L)$, tal que todos os enlaces ao longo deste caminho possuam $S < C$. Se nenhum caminho for encontrado, faça $w' = w' + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2.;
6. Aceite a chamada, atualize $W\lambda$ (colocando os enlaces de $P\lambda$ em modo ocupado), atualize $W\lambda'$ (colocando os enlaces de $B\lambda'$ em modo backup), e, por fim, faça $S = S + 1$ para cada enlace de $B\lambda'$;
7. Pare o procedimento

O pseudocódigo deste mecanismo é apresentado no Algoritmo 3:

7.1.2 Novo SPP Sensível às Limitações da Camada Física - First Fit

Na versão sensível às limitações da camada física, procede-se de forma semelhante ao proposto no Capítulo 6. Assim que um caminho primário é encontrado, faz-se uma estimativa da qualidade do sinal, e caso o resultado esteja dentro de limites aceitáveis, busca-se um caminho de backup, cuja qualidade de sinal, também é aceitável.

Em termos formais, o algoritmo pode ser descrito da seguinte forma:

Entrada: A topologia $T(N, L)$, o estado da rede $Ww(N, L)$, $w = 1, 2, ..., W$, o nível de confiabilidade C e uma requisição de conexão $R(origem, destino)$:

1. Inicializar o procedimento pelo primeiro comprimento de onda, $w = 1$;

Algorithm 3 SPPIAFF

```
1: for w = 1 até W do
2:   Pw ⇐ shortestPath(T, w)
3:   if existe(Pw) then
4:     T' ⇐ topologiaDisjunta(T, Pw)
5:     T' ⇐ limitarCompartilhamento(T', C)
6:     for w' = 1 até W do
7:       P'w' ⇐ shortestPath(T', w')
8:       if existe(P'w') then
9:         setupLightpath(Pw, P'w')
10:        atualizarCompartilhamento(P'w')
11:      end if
12:    end for
13:  end if
14: end for
```

2. Aplicar o algoritmo do menor caminho, a fim de se achar um caminho primário Pw em $Ww(N, L)$. Se nenhum caminho for encontrado, faça $w = w + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 9;

3. Obtenha uma estimativa da qualidade do caminho $P\lambda$. Caso o lightpath não seja viável volte ao passo 2;

4. Faça $T'(N, L) = T(N, L) - Pw$, produzindo um novo conjunto de camadas $W'w'(N, L)$ derivado de $T'(N, L)$;

5. Inicializar $w' = 1$;

6. Aplicar o algoritmo do menor caminho, a fim de achar um caminho de backup compartilhado Bw' em $W'w'(N, L)$, tal que todos os enlaces ao longo deste caminho possuam $S < C$. Se nenhum caminho for encontrado, faça $w' = w' + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2;

7. Obtenha uma estimativa da qualidade do caminho $B\lambda'$. Caso o lightpath não seja viável faça $w' = w' + 1$ e volte ao passo 6;

8. Aceite a chamada, atualize $W\lambda$ (colocando os enlaces de $P\lambda$ em modo ocupado), atualize $W\lambda'$ (colocando os enlaces de $B\lambda'$ em modo backup), faça $S = S + 1$ para cada enlace de $B\lambda'$, e, por fim, atualize os ruídos gerados por $P\lambda$;

9. Pare o procedimento

O pseudocódigo deste mecanismo é apresentado no Algoritmo 4:

Algorithm 4 SPPIAFF

```
1: for w = 1 até W do
2:    Pw ⇐ shortestPath(T, w)
3:    if temQualidadeMinima(Pw) then
4:       T' ⇐ topologiaDisjunta(T, Pw)
5:       T' ⇐ limitarCompartilhamento(T', C)
6:       for w' = 1 até W do
7:          P'w' ⇐ shortestPath(T', w')
8:          if temQualidadeMinima(P'w') then
9:             setupLightpath(Pw, P'w')
10:            atualizarCompartilhamento(P'w')
11:         end if
12:      end for
13:   end if
14: end for
```

7.1.3 Novo SPP - Random Pick

O algoritmo proposto foi também testado em uma versão na qual o método de alocação de comprimento de onda usado é o Random Pick. A principal diferença para a versão na qual First Fit é usado é o modo como se dá a iteração entre as camadas. Ao contrário do outro algoritmo, em Random Pick cada uma das camadas é visitada aleatoriamente. Formalmente, esta versão do algoritmo pode ser descrita da seguinte forma.

Entrada: A topologia $T(N, L)$, o estado da rede $Ww(N, L)$, $w = 1, 2, ..., W$, o nível de confiabilidade C e uma requisição de conexão $R(origem, destino)$:

1. Inicializar w com um inteiro aleatório no intervalo $[1, W]$;

2. Aplicar o algoritmo do menor caminho, a fim de se achar um caminho primário Pw em $Ww(N, L)$. Se nenhum caminho for encontrado, atribua a w o próximo inteiro aleatório não repetido no intervalo $[1, W]$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 7;

3. Faça $T'(N, L) = T(N, L) - Pw$, produzindo um novo conjunto de camadas $W'w'(N, L)$ derivado de $T'(N, L)$;

4. Inicializar w' com um inteiro aleatório no intervalo $[1, W]$;

5. Aplicar o algoritmo do menor caminho a fim de achar um caminho de backup compartilhado Bw' em $W'w'(N, L)$, tal que todos os enlaces ao longo deste caminho possuam $S < C$. Se nenhum caminho for encontrado, atribua a w' um próximo valor aleatório diferente dos anteriores no intervalo $[1, W]$. Repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2;

6. Aceite a chamada, atualize $W\lambda$ (colocando os enlaces de $P\lambda$ em modo ocupado), atualize $W\lambda'$ (colocando os enlaces de $B\lambda'$ em modo backup), e, por fim, faça $S = S + 1$ para cada enlace de $B\lambda'$;

7. Pare o procedimento

O pseudocódigo deste mecanismo é apresentado no Algoritmo 5:

Algorithm 5 SPPIAFF

```
1: for i = 1 até W do
2:    w ⇐ random(1, W)
3:    Pw ⇐ shortestPath(T, w)
4:    if existe(Pw) then
5:       T' ⇐ topologiaDisjunta(T, Pw)
6:       T' ⇐ limitarCompartilhamento(T', C)
7:       for j = 1 até W do
8:          w' ⇐ random(1, W)
9:          P'w' ⇐ shortestPath(T', w')
10:         if existe(P'w') then
11:            setupLightpath(Pw, P'w')
12:            atualizarCompartilhamento(P'w')
13:         end if
14:      end for
15:   end if
16: end for
```

7.1.4 Novo SPP Sensível às Limitações da Camada Física - Random Pick

Por fim, o novo algoritmo é proposto em uma versão sensível às limitações da camada física utilizando-se Random Pick como método de alocação de comprimento de onda. Esta versão é, formalmente, assim descrita:

Entrada: A topologia $T(N, L)$, o estado da rede $Ww(N, L)$, $w = 1, 2, ..., W$, o nível de confiabilidade C e uma requisição de conexão $R(origem, destino)$:

1. Inicializar w com um inteiro aleatório no intervalo $[1, W]$;
2. Aplicar o algoritmo do menor caminho, a fim de se achar um caminho primário Pw em $Ww(N, L)$. Se nenhum caminho for encontrado, atribua a w o próximo inteiro aleatório não repetido no intervalo $[1, W]$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 9;
3. Obtenha uma estimativa da qualidade do caminho $P\lambda$. Caso o lightpath não seja viável volte ao passo 2;
4. Faça $T'(N, L) = T(N, L) - Pw$, produzindo um novo conjunto de camadas $W'w'(N, L)$ derivado de $T'(N, L)$;
5. Inicializar w' com um inteiro aleatório no intervalo $[1, W]$;
6. Aplicar o algoritmo do menor caminho, a fim de achar um caminho de backup compartilhado Bw' em $W'w'(N, L)$, tal que todos os enlaces ao longo deste caminho possuam $S < C$. Se nenhum caminho for encontrado, atribua a w' um próximo valor aleatório diferente dos anteriores no intervalo $[1, W]$. Repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2;
7. Obtenha uma estimativa da qualidade do caminho $B\lambda'$. Caso o lightpath não seja viável faça $w' = w' + 1$ e volte ao passo 6;
8. Aceite a chamada, atualize $W\lambda$ (colocando os enlaces de $P\lambda$ em modo ocupado), atualize $W\lambda'$ (colocando os enlaces de $B\lambda'$ em modo backup), faça $S = S + 1$ para cada enlace de $B\lambda'$, e, por fim, atualize os ruídos gerados por $P\lambda$;
9. Pare o procedimento

O pseudocódigo desta técnica é apresentado no Algoritmo 6:

7.2 Resultados Numéricos

Verifica-se, nesta seção, o desempenho do algoritmo, através de simulação em suas duas versões (sensível e insensível aos efeitos degradantes do sinal) para duas políticas de alocação de comprimento de onda (First Fit e Random Pick).

Algorithm 6 SPPIAFF

```
1: for i = 1 até W do
2:    w ⇐ random(1, W)
3:    Pw ⇐ shortestPath(T, w)
4:    if temQualidadeMinima(Pw) then
5:       T' ⇐ topologiaDisjunta(T, Pw)
6:       T' ⇐ limitarCompartilhamento(T', C)
7:       for j = 1 até W do
8:          w' ⇐ random(1, W)
9:          P'w' ⇐ shortestPath(T', w')
10:         if temQualidadeMinima(P'w') then
11:            setupLightpath(Pw, P'w')
12:            atualizarCompartilhamento(P'w')
13:         end if
14:      end for
15:   end if
16: end for
```

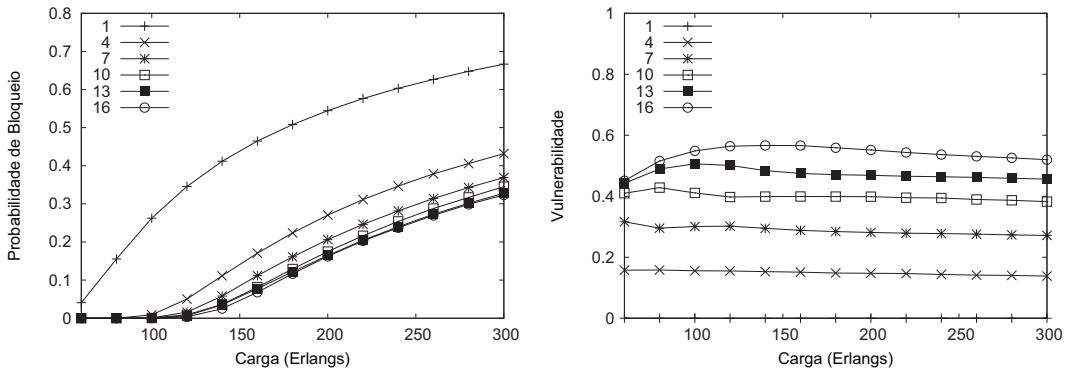
A eficácia do algoritmo foi aferida em duas topologias diferentes: a NSFNET, com 16 nós e 25 enlaces; e a USA Network, com 24 nós e 43 enlaces. As Figuras 5.4 e 5.11 ilustram as topologias usadas. As medidas de interesse aferidas são a probabilidade de bloqueio e a razão de vulnerabilidade.

O cenário utilizado nas simulações considera tráfego dinâmico com chegadas regidas por um processo de Poisson. A duração das chamadas (*holding time*) é dada por uma distribuição exponencial de média 1, e, dessa forma, a carga submetida a rede é igual a taxa de chegadas. Considera-se um esquema de falhas de enlace único, no qual admite-se que apenas um enlace esteja em estado falho num determinado instante do tempo. Para que um novo evento de falha possa ocorrer, é necessário que o anterior seja corrigido. Os resultados obtidos possuem intervalo de confiança com largura igual a 1% para um nível de significância de 95%. Cada uma das simulações foi realizada com 10^6 chamadas.

7.2.1 Resultado do Algoritmo Insensível usando First Fit para a topologia NSFNET

A Figura 7.1 apresenta o desempenho do algoritmo proposto em redes ideais, para a topologia da rede NSFNET. Seis níveis de compartilhamento são mostrados nos dois gráficos: 1, 4, 7, 10, 13 e 16. O nível 1 aceita que apenas um caminho primário refira-se a um enlace de backup, e, portanto, trata-se de proteção dedicada. Em oposição, o nível 16 permite que até 16 caminhos primários compartilhem um caminho de backup, correspon-

dendo a proteção compartilhada, segundo o melhor esforço. Os níveis restantes são valores intermediários, e podem ser usados por clientes que possuem diferentes necessidades. Na Figura 7.1(a), observa-se que a proteção dedicada (nível 1) produz probabilidades de bloqueio muito altas. A explicação para isso é o grande gasto de recursos com redundância, uma vez que cada chamada precisa de, no mínimo, duas vezes mais enlaces para ser estabelecida quando comparada a uma rede sem proteção. O bloqueio é tão alto, que sob 300 Erlangs, é de 67%, tornando o oferecimento deste tipo de proteção praticamente inviável. Quando se aceita o compartilhamento dos caminhos de backup, observa-se uma melhora significativa. Com nível 4, e sob 300 Erlangs, o bloqueio reduz a 42%. Sob 100 Erlangs, a redução observada varia de 27% a zero, o que mostra as vantagens do compartilhamento. Para níveis maiores, observa-se reduções cada vez menores no bloqueio, chegando a 31% para o melhor esforço. Quando se considera a razão de vulnerabilidade (Figura 7.1(b), a proteção dedicada produz o melhor resultado, com todas as chamadas recuperadas. Com nível de compartilhamento 4, 18% das chamadas deixam de ser recuperadas. Considerando-se o ganho com a diminuição de bloqueio, o aumento na razão de vulnerabilidade é compensador. Para níveis maiores de compartilhamento, observa-se aumentos progressivos da vulnerabilidade, chegando a 55% sob 300 Erlangs para o melhor esforço.



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

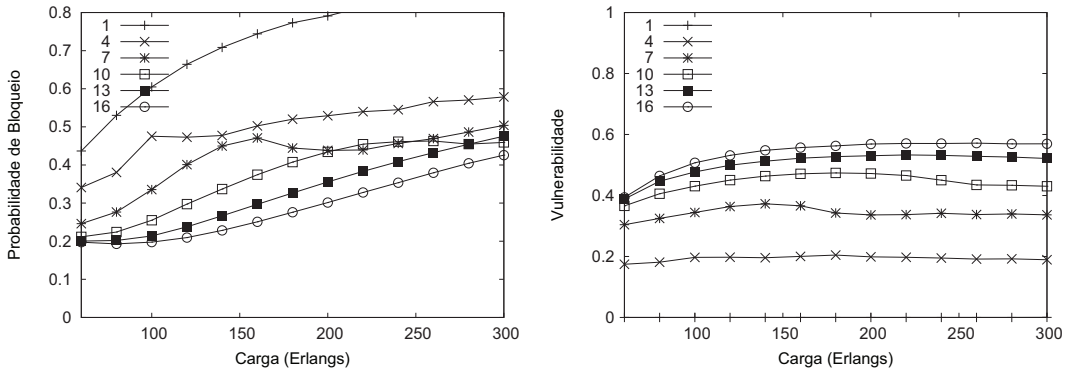
Figura 7.1: Desempenho do novo algoritmo em redes ideais utilizando a topologia NSFNET

7.2.2 Algoritmo Sensível usando First Fit para NSFNET

A Figura 7.2 mostra os resultados obtidos para o cenário em que as limitações da camada física são levadas em consideração tornando algoritmo sensível aos efeitos degradantes do sinal. A topologia da NSFNET também é utilizada. Na Figura 7.2(a), observa-se um aumento generalizado na probabilidade de bloqueio. Sob cargas baixas de 60 Erlangs, 20% das chamadas não são aceitas para o melhor esforço, que produz o menor bloqueio. Quando se adota a proteção dedicada, o número de chamadas bloqueadas é de 45% sob 60 Erlangs, e sob 200 Erlangs este número ultrapassa 80%, o que torna inviável o uso desse esquema de proteção. Isto mostra o quão impactante podem ser os efeitos degradantes do sinal em redes ópticas. Para um nível de compartilhamento igual a 4, o bloqueio diminui para 33% sob 60 Erlangs e para 55% sob 200 Erlangs, mostrando as vantagens do compartilhamento de recursos. Para níveis intermediários, o comportamento é bastante semelhante ao obtido para redes ideais; o bloqueio diminui progressivamente exceto para níveis maiores limitados inferiormente pela curva do menor esforço. Na Figura 7.2(b), observa-se um ligeiro aumento da razão de vulnerabilidade para todos os níveis. O aumento é pequeno por que a viabilidade do sinal de um caminho de backup é testada no momento da aceitação da chamada e, portanto, já apresenta qualidade aceitável. Entretanto, entre o momento da aceitação e a ocorrência da falha, o estado da rede mudou, o que pode tornar o sinal de alguns caminhos de backup inviável, levando ao pequeno aumento observado. Mesmo para a proteção dedicada, não é possível obter 100% de recuperação, embora o aumento de vulnerabilidade observado seja insignificante (cerca de 0,1%). Para o nível 4, a vulnerabilidade aumenta um pouco mais, de 18% para 19%, em média. O valor da grandeza aumenta progressivamente, chegando a 59% para o melhor esforço, 4% maior do que no caso ideal.

7.2.3 Resultados do Algoritmo Insensível usando Random Pick para a topologia NSFNET

Na Figura 7.3, apresentam-se os resultados obtidos para o algoritmo proposto com Random Pick para a topologia da NSFNET. Os níveis de compartilhamento estudados são 1, 2, 3, 7, 11, e 16. Essa escolha foi feita pois tais níveis apresentam níveis de confiabilidade diferenciados. A probabilidade de bloqueio (Figura 7.3(a)) apresenta, em geral, um aumento significativo quando comparada a versão com First Fit. A proteção dedicada é a única exceção, uma vez que o bloqueio apresenta, quase sempre, valores muito semelhantes, independente da política adotada. Quando o nível de compartilhamento é igual a 2, sob 80 Erlangs, a probabilidade de bloqueio é superior a zero, e sob 300 Erlangs o valor observado é 54%, maior do que o produzido com a política First Fit. Os níveis intermediários apresentam crescimentos cada vez menores, e são limitados inferiormento



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

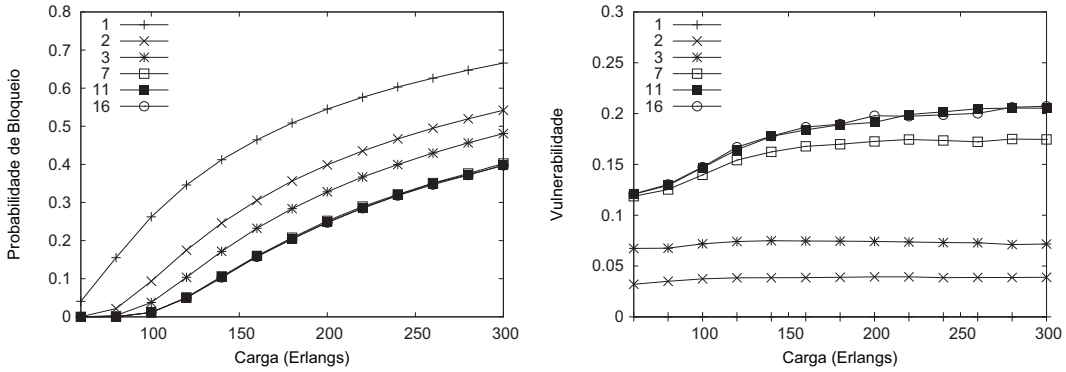
Figura 7.2: Desempenho do novo algoritmo considerando as limitações da camada física utilizando a topologia NSFNET

pela política de melhor esforço, que apresenta um aumento de 31% a 40%. A razão para o aumento observado é o modo como a alocação de comprimento de onda interfere sobre o compartilhamento. Considerando a alocação de caminhos de backup, usando First Fit aloca-se, inicialmente, o primeiro comprimento de onda. Existe uma grande chance deste comprimento de onda já estar alocado. Caso o número de conexões que compartilham o canal seja menor que o nível máximo de compartilhamento, o primeiro comprimento de onda será alocado; caso contrário, o procedimento é executado para o segundo canal. Com isso, os primeiros comprimentos de onda são usados até a exaustão para todos os enlaces, aumentando as chances de se encontrar um canal disponível.

Quando Random Pick é utilizado, a busca por comprimentos de onda ocorre de forma aleatória, e, dessa forma, a ordem em que os canais são alocados é diferente de um enlace para outro. Tornando-se menos possível que todos os enlaces ao longo de um caminho tenham um mesmo canal livre. Suponha-se um exemplo de um caminho com dois enlaces, em que cada um possui dois canais livres. Usando-se First Fit, estes canais são, certamente, o 15 e 16 para ambos, permitindo a alocação do caminho. No entanto, quando Random Pick é empregado, os canais livres são aleatórios, e provavelmente serão diferentes entre os enlaces. Supondo-se que sejam, aleatoriamente, 3 e 10 para o primeiro enlace e, 4 e 11 para o segundo, o caminho não poderá ser alocado. Desta forma, há um aumento do bloqueio, sobretudo quando nível de compartilhamento é menor e os canais se exaurem mais rapidamente. Para a proteção dedicada, que não compartilha caminhos de backup, a diferença é insignificante.

Na Figura 7.3(b), apresenta-se a razão de vulnerabilidade. Observa-se uma diminuição

significativa dessa grandeza para todos os níveis de compartilhamento, com excessão da proteção dedicada, cuja confiabilidade é sempre de 100%. Sob 60 Erlangs, e com proteção de melhor esforço, ocorre uma diminuição de 42% para 12%. Sob 300 Erlangs e com o melhor esforço esta diminuição é de 54% a 20%. O motivo para essa grande diminuição é, mais uma vez, a forma como os comprimentos de onda são alocados. Com First Fit, os primeiros canais são sobrecarregados, e os últimos canais permanecem livres, enquanto que com o Random Pick, os canais são usados de forma muito mais equilibrada, e, com isso, apresentam um nível de compartilhamento menor do que na outra técnica de alocação de comprimento de onda, e assim, mais conexões podem ser recuperadas.



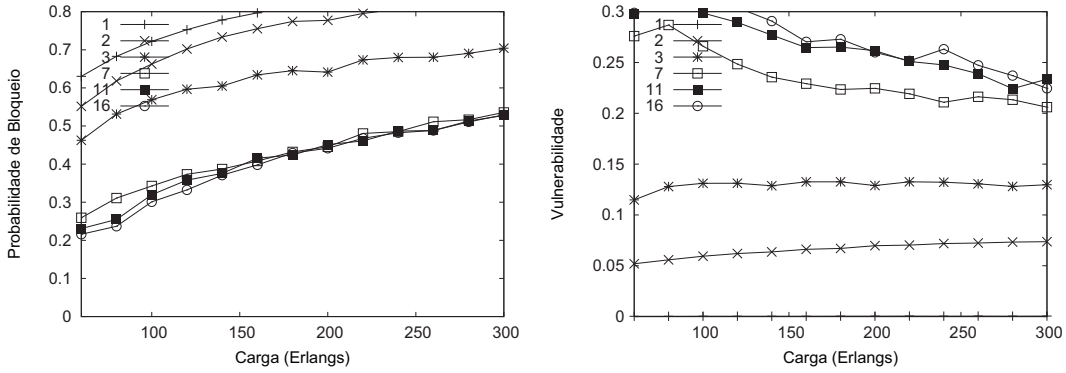
(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

Figura 7.3: Desempenho do novo algoritmo usando Random Pick em redes ideais tendo como base a topologia NSFNET

7.2.4 Resultados do Algoritmo Sensível usando Random Pick para a topologia NSFNET

A Figura 7.4 mostra os resultados para o novo algoritmo considerando as limitações da camada física e usando Random Pick como alocação de comprimento de onda. O bloqueio (Figura 7.4(a)) apresenta valores muito altos quando comparado aos casos anteriormente estudados. Para a proteção dedicada, sob 160 Erlangs o bloqueio é superior a 80%, e enquanto que sob 60 Erlangs atinge 63%. Com o nível 2 de compartilhamento e sob 220 Erlangs, o bloqueio é maior que 80%, enquanto que sob 60 Erlangs é igual a 55%. Com proteção por melhor esforço, verifica-se uma variação de 21% a 52% no bloqueio. O aumento observado é devido a motivos anteriormente citados. O primeira consiste nas limitações da camada física. Devido a baixa qualidade do sinal, muitos caminhos não

oferecem uma taxa de erro de bits aceitável e as chamadas precisam ser bloqueadas. O segundo motivo é a forma como ocorre a alocação de comprimentos de onda. Sendo a alocação aleatória, muitas vezes não é possível encontrar o mesmo canal livre em todos os enlaces de um caminho, e como a rede não apresenta conversão de comprimento de onda, a chamada não pode ser atendida. Na Figura 7.4(b), o gráfico da razão de vulnerabilidade é plotado. Pode-se ver como os efeitos físicos interferem na recuperação de chamadas. Sob 60 Erlangs, o valor da razão de vulnerabilidade é superior a 30%, enquanto que no caso ideal era de 12%. Com nível de confiabilidade igual a 2, o aumento foi de 3% a 5%, e mesmo para a proteção dedicada a confiabilidade não alcança 100% sob 300 Erlangs, como acontece com o caso ideal. Para altas cargas, verifica-se uma diminuição da vulnerabilidade, fato que se deve principalmente ao aumento do bloqueio.



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

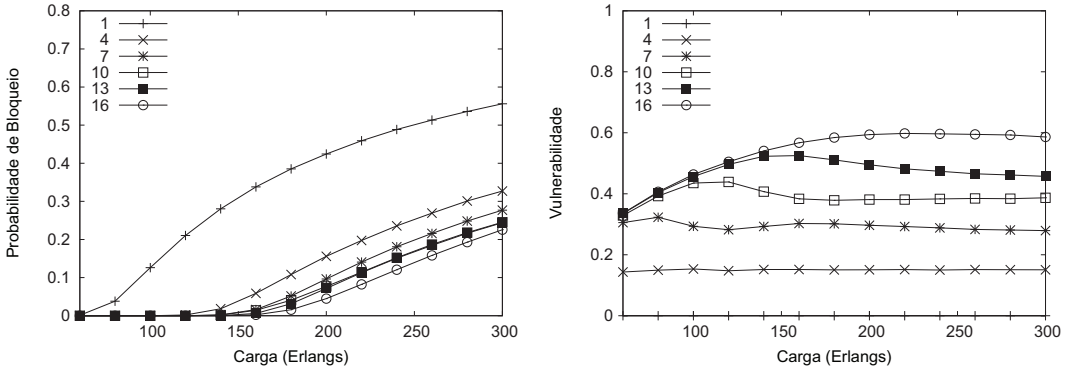
Figura 7.4: Desempenho do novo algoritmo usando Random Pick considerando as limitações da camada física para a NSFNET

7.2.5 Resultados do Algoritmo Insensível usando First Fit para a topologia USA Network

O desempenho do algoritmo proposto também foi aferido tendo como base a topologia da USA Network. A Figura 7.5 apresenta os resultados quando redes ideais são consideradas. Os resultados são bastante semelhantes ao obtido para a topologia NSFNET, o que reforça os resultados encontrados. Observa-se, entretanto, uma diminuição significativa do bloqueio (Figura 7.5(a)), explicada pela maior disponibilidade de recursos nesta topologia. Enquanto a NSFNET possui 25 enlaces, a rede USA possui 43 enlaces, possibilitando um número maior de caminhos interligando dois nós. Na proteção dedicada, o impacto dessa

maior disponibilidade de caminhos leva a uma diminuição do bloqueio de 67% a 55% sob cargas de 300 Erlangs. Para nível de compartilhamento igual a 4, a diminuição observada é de 42% a 32% e a proteção segundo o melhor esforço de 31% a 21%. O padrão de diminuição do bloqueio dos níveis intermediários é igual ao obtido para a NSFNET.

A Figura 7.5(b) apresenta os resultados para a razão de vulnerabilidade. O comportamento do algoritmo também é bastante semelhante ao resultado encontrado para a topologia NSFNET, sobretudo para níveis de compartilhamento baixos. Com proteção dedicada, 100% dos caminhos são recuperados, o que é esperado por este tipo de proteção, e para nível de compartilhamento igual a 4, encontra-se os mesmos 18% de vulnerabilidade. Quando o compartilhamento aumenta, sob cargas baixas, verifica-se uma diminuição da vulnerabilidade, que também é explicada pela maior quantidade de caminhos disponíveis, e consequente diminuição do compartilhamento. Sob cargas altas, observa-se um aumento da vulnerabilidade. Isto ocorre pois o número maior de chamadas aceitas, um maior número de caminhos primários compartilha um caminho de backup, e, no momento de uma falha, o número de chamadas que podem ser recuperadas é menor. Para a proteção segundo o menor esforço, observou-se um aumento de 55% a 60%. Para os níveis intermediários o aumento foi semelhante.



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

Figura 7.5: Desempenho do novo algoritmo em redes ideais utilizando a topologia da USA Network

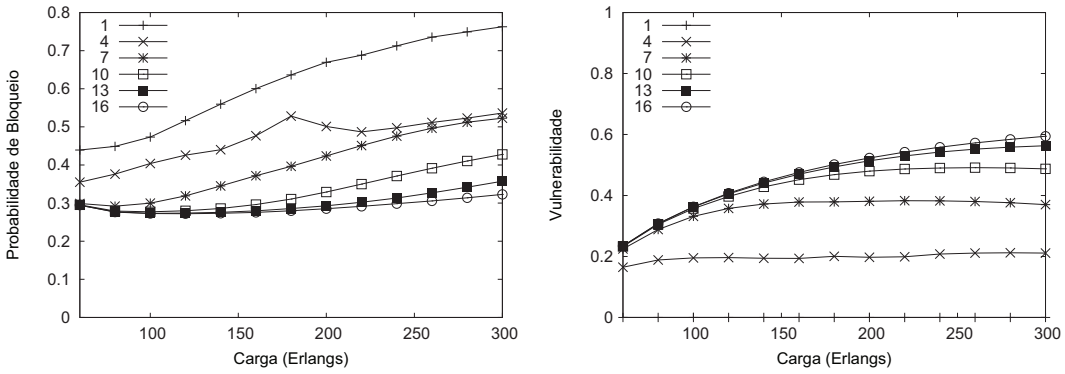
7.2.6 Resultados do Algoritmo Sensível usando First Fit para a topologia USA Network

A Figura 7.6 apresenta o desempenho obtido para o algoritmo proposto para a topologia USA Network quando as limitações da camada física são consideradas. Na Figura 7.6(a), observa-se que o crescimento da curva da probabilidade de bloqueio para a proteção dedicada é menor do que o obtido para a outra topologia. Na NSFNET, o bloqueio a 80% sob 200 Erlangs, enquanto que na USA Network, sob 300 Erlangs, o bloqueio é inferior a 75%. O motivo desta diminuição é o mesmo para o caso ideal. Com o maior número de enlaces na rede, mais caminhos são disponíveis, o que leva a uma diminuição do bloqueio. Com o melhor esforço, observa-se um comportamento bastante diferente. Sob 60 Erlangs (primeiro valor medido), o bloqueio é de 30%, maior do que na NSFNET, na qual esse valor é de 20%. A explicação para isso é o maior bloqueio de conexões devido a qualidade inaceitável do sinal. Embora a topologia USA Network tenha mais nós e enlaces, esta possui um diâmetro maior quando comparada a topologia NSFNET. o que leva a existência de um número maior de caminhos de longa distância. Como a qualidade do sinal está diretamente ligada ao comprimento de um caminho, observa-se um aumento no bloqueio ocasionado pelos efeitos degradantes do sinal. Por outro lado, outra extremidade da mesma curva, este efeito deixa de ser o mais importante, e a maior disponibilidade de caminhos na rede leva a uma diminuição do bloqueio de 41% a 31%. De formas diferentes, estes dois efeitos interferem sobre as curvas intermediárias, tornando o padrão de diminuição de bloqueio semelhante.

Na Figura 7.6(b), verifica-se a evolução da razão de vulnerabilidade para as diferentes curvas. Observa-se uma diminuição generalizada dessa grandeza para cargas baixas e para níveis de compartilhamento altos, quando comparado com condições de carga semelhantes na topologia da NSFNET. Quando o esquema de proteção é o melhor esforço, sob 60 Erlangs, a vulnerabilidade cai de 40% para 21%. Esta diminuição está relacionada a maior probabilidade de bloqueio. Com um número menor de chamadas aceitas, o compartilhamento também cai, e, por consequência, mais chamadas podem ser recuperadas. Na outra extremidade, sob 300 Erlangs, o padrão observado não muda.

7.2.7 Resultados do Algoritmo Insensível usando Random Pick para a topologia USA Network

Na Figura 7.7, são plotados os gráficos do desempenho do algoritmo proposto para redes ideais, usando Random Pick como mecanismo de alocação de comprimento de onda, para a topologia USA Network. A probabilidade de bloqueio (Figura 7.7(a)) gerada é menor do que a obtida para a topologia NSFNET sob as mesmas condições de carga. O motivo



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

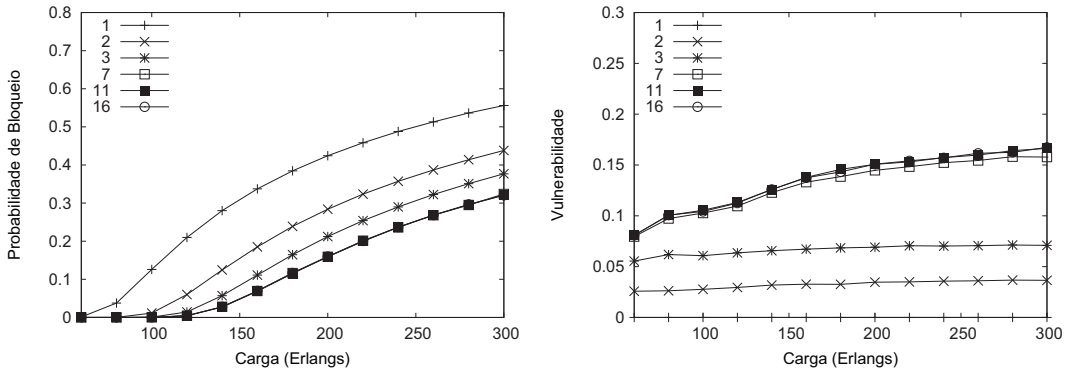
Figura 7.6: Desempenho do novo algoritmo considerando as limitações da camada física utilizando a topologia da USA Network

é o mesmo da diminuição observada para First Fit: como a USA Network possibilita um número maior de caminhos por possuir mais nós e enlaces, mais conexões podem ser estabelecidas, o que diminui o bloqueio. Quando comparado com First Fit, este produz taxas de bloqueio maiores, decorrente da alocação aleatória de comprimentos de onda, o que torna mais difícil escolher um canal livre para todos os enlaces de um caminho.

Na Figura 7.7(b), apresenta-se a razão de vulnerabilidade. Os valores obtidos são semelhantes aos obtidos para a topologia NSFNET com níveis de compartilhamento 1, 2 e 3. Com níveis de compartilhamento maiores, verifica-se uma diminuição da vulnerabilidade, ocasionada também pela maior disponibilidade de caminhos na topologia USA Network. Sob 60 Erlangs, a queda observada foi de 12% a 8% para o melhor esforço, e de 20% a 16% quando a carga imposta sobre a rede é de 300 Erlangs. Para os níveis intermediários, a queda observada é semelhante.

7.2.8 Resultados do Algoritmo Sensível usando Random Pick para a topologia USA Network

A Figura 7.8 mostra os resultados obtidos para o novo algoritmo considerando as limitações da camada física, quando o mecanismo de alocação de comprimento de onda é o Random Pick para a topologia USA Network. A probabilidade de bloqueio (Figura 7.8(a)) aumenta para níveis de compartilhamento mais altos e cargas baixas quando comparada ao resultado obtido para a topologia NSFNET. Isto se deve ao aumento do diâmetro da USA Network. Uma vez que a qualidade do sinal é inversamente proporcional ao tamanho de



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

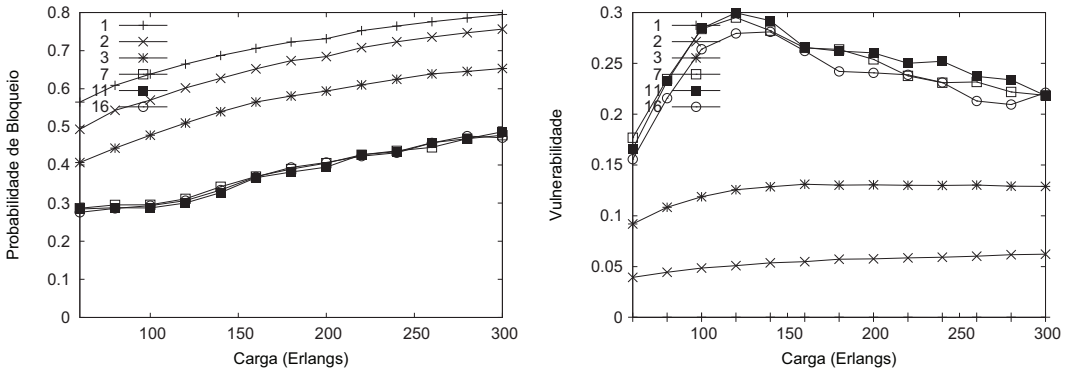
Figura 7.7: Desempenho do novo algoritmo usando Random Pick em redes ideais para a topologia da USA Network

um caminho, o maior número de caminhos longos produz um aumento do bloqueio. Sob para cargas altas o comportamento não se altera. Quando os níveas de compartilhamento são mais baixos (1, 2 e 3), observa-se uma diminuição do bloqueio. A razão é a maior disponibilidade de caminhos na topologia USA Network, permitindo um maior número de chamadas serem aceitas.

Na Figura 7.8(b), o resultado obtido para a razão de vulnerabilidade é apresentado. Para níveis de compartilhamento mais baixos, verifica-se uma sensível diminuição da grandeza, ocasionada pelo maior número de caminhos disponíveis. Para níveis de compartilhamento mais altos, observa-se um comportamento diferente. De 60 a 120 Erlangs a vulnerabilidade aumenta. Com o melhor esforço, por exemplo, o salto é de 18% a 30%. Nesse intervalo, a razão de vulnerabilidade segue aumentando, até atingir o valor máximo permitido sob 120 Erlangs. A partir desse valor, a vulnerabilidade cai, fato justificado pelo aumento do bloqueio. Com menos conexões aceitas, o compartilhamento também diminui, o que leva a consequente queda.

7.3 Conclusões Parciais

Este capítulo apresentou um novo algoritmo de proteção por caminho compartilhado com diferentes níveis de compartilhamento. Apresentou-se, também, uma versão sensível às limitações da camada física para o algoritmo, baseada no algoritmo proposto no Capítulo 6. Conclui-se que o algoritmo é capaz de produzir diferentes níveis de confiabilidade, bem como diferentes níveis de bloqueio, podendo assim atender a clientes com requisitos



(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

Figura 7.8: Desempenho do novo algoritmo usando Random Pick considerando as limitações da camada física para a topologia da USA Network

distintos. Observou-se que em situações nas quais a utilização de proteção dedicada é praticamente impossível, devido ao grande bloqueio gerado pela redundância, permitir que caminhos de backup sejam compartilhados por poucos caminhos primários (4 no exemplo mostrado), pode diminuir significativamente a probabilidade de bloqueio, com um aumento compensador na razão de vulnerabilidade.

Observou-se, também, que as limitações da camada física aumentam muito o bloqueio de conexões, sendo necessário nesses casos o uso de níveis mais altos de compartilhamento. A vulnerabilidade, ao contrário, sofre alterações insignificantes.

Capítulo 8

Conclusões

Nesta dissertação apresentou-se um estudo do efeito que as limitações da camada física impõem sobre a alocação de caminhos ópticos em redes ópticas WDM transparentes com mecanismos de proteção por caminho compartilhado.

Os efeitos degradantes considerados incluem o ruído ASE, a dispersão PMD e o crosstalk intra-canal. Estes foram escolhidos pois são aqueles que impõem maior degradação às transmissões ópticas. Utiliza-se um mecanismo de proteção por melhor esforço, que busca proteger conexões sem desperdiçar recursos devido a redundâncias. Nesta modalidade de proteção, na eventual ocorrência de uma falha não há garantias de que a conexão será recuperada.

Verifica-se, inicialmente, o impacto dos efeitos sobre o bloqueio e sobre a vulnerabilidade das conexões (Capítulo 5). Observou-se que em redes de longa distância o efeito é drástico, causando um grande aumento sobre as variáveis de interesse e, em alguns casos, tornando a rede inutilizável.

Esse aumento de bloqueio torna necessário o desenvolvimento de algoritmos capazes de utilizar os recursos eficientemente aumentando o número de chamadas aceitas. Tal desenvolvimento foi o tópico do Capítulo 6, no qual dois novos algoritmos sensíveis as limitações da camada física foram introduzidos. Nestes, o roteamento e alocação de comprimento de onda consideram os efeitos degradantes do sinal e buscam encontrar caminhos ópticos com qualidade aceitável através de um mecanismo de roteamento adaptativo em camadas. Os algoritmos conseguem diminuir tanto o bloqueio como a vulnerabilidade. Conclui-se, portanto, que os algoritmos são eficientes e que são candidatos ao uso em redes transparentes de longa distância com proteção.

Técnicas de proteção tradicionais garantem que 100% das conexões são recuperadas em caso de falha. O emprego da política de melhor esforço produz grande economia de recursos mas leva a uma vulnerabilidade alta. Consumidores, em geral, possuem necessidades distintas, e podem desejar níveis intermediários de confiabilidade a um menor custo.

O trabalho desenvolvido no Capítulo 7 consegue prover diferentes níveis de confiabilidade, restringindo o compartilhamento de caminhos de backup.

A contribuição principal desta dissertação é a inclusão das limitações de camada física na produção de novos algoritmos de proteção em redes ópticas. Pode-se concluir que efeitos degradantes do sinal são de grande importância, sobretudo em redes de longa distância. Quando o limite para a taxa de erro de bits é de 10^{-9}, a qualidade deixa de ser aceitável a partir de aproximadamente 2000 km, valor que varia de acordo com o crosstalk produzido. Limitando a taxa a valores menores, o efeito torna-se importante mesmo em redes metropolitanas; com BER de 10^{-12}, a partir de 200 km caminhos podem deixar de apresentar qualidade aceitável.

8.1 Proposta de Trabalhos Futuros

O trabalho desenvolvido nesta dissertação pode ser continuado em duas frentes: limitações da camada física e sobrevivência em redes ópticas. São importante tópicos na continuação do estudo dos efeitos degradantes do sinal:

- **Novos efeitos:** ASE, PMD e crosstalk intra-canal foram levados em consideração por esta dissertação. Embora sejam os efeitos mais importantes, para efeitos de completude um número maior de fenômenos deve ser considerados, sobretudo os efeitos não-lineares.

- **Roteamento sensível às limitações da camada física:** O algoritmo RWA apresentado neste trabalho é sensível aos efeitos degradantes do sinal, mas o algoritmo de roteamento, separadamente, não é sensível. Espera-se que a utilização desta técnica seja capaz de produzir melhores resultados.

- **Controle de ruídos sobre conexões ativas:** Assim que uma nova chamada é aceita, passa a impor ruídos sobre as conexões ativas, podendo diminuir a qualidade do sinal a valores inferiores ao limite estimulado. Por esse motivo, deve existe um controle a fim de que a aceitação de novas chamadas não torne a taxa de erro de bits das conexões ativas inaceitável.

Na frente de sobrevivência em redes ópticas, os seguintes tópicos seriam uma importante continuação deste trabalho:

- **Métodos de proteção tradicionais:** Fazer um estudo do impacto dos efeitos degradantes do sinal em técnicas tradicionais de proteção por caminho dedicado, compartilhado, ou compartilhado com restrições SRLG, comparando essas técnicas.

- **Restauração:** Prover proteção só é importante, a partir do momento em que a restauração entra em cena. Levar em consideração as limitações da camada física, a fim de produzir resultados mais eficientes para as técnicas de restauração é também um importante trabalho.

- **Novas políticas de compartilhamento:** O trabalho apresentado no Capítulo 7 apresenta duas políticas diferentes de compartilhamento. Entretanto, no contexto de Serviços diferenciados, um grande número de outras políticas de provisão de QoS são conhecidas e devem ser estudas em conjunto com políticas de proteção a fim de se verificar sua eficácia para o compartilhamento de caminhos de backup.

Referências Bibliográficas

[1] S. Azodolmolky and M. Klinkowski. A survey on physical layer impairments aware routing and wavelength assignment algorithms in optical networks. *Computer Networks, to be published*, 2009.

[2] R. Cardillo, V. Curri, and M. Mellia. Considering transmission impairments in wavelength routed networks. *Proc of Conference on Optical Network Design and Modeling*, pages 421–429, 7-9, 2005.

[3] I. Chlamtac, A. Ganz, and G. Karmi. Lightpath communications: An approach to high-bandwidth optical wans. IEEE Trans. Comm., July 1992.

[4] William Cooper. IPTV guide: Delivering audio and video over broadband, December 2006.

[5] Dantas R. Mariz D. Sadok D. e Kamienski D. Costa, A. Algoritmos para posicionamento de conversores em redes Ópticas. Fortaleza, CE, Brasil, Maio 2005. Simpósio Brasileiro de Redes de Computadores.

[6] Savio Rodrigo Antunes dos Santos dos Santos Rosa, Andre Drummond, and Nelson Fonseca. Path protection wdm networks with impaired-transmission. *Photonic Network Communications*, 19(2):212–222, December 2009.

[7] Savio Rodrigo Antunes dos Santos Rosa, André C Drummond, and Nelson L. S. da Fonseca. Lightpath establishment in WDM networks with best effort shared path protection in Impaired-Transmissions. In *ICC 2009 Optical Networks and Systems Symposium (ICC'09 ONS)*, Dresden, Germany, Germany, 6 2009.

[8] Savio Rodrigo Antunes dos Santos Rosa, André C Drummond, and Nelson L. S. da Fonseca. Performance of shared path protection mechanism under physical impairments in WDM networks. In *13th Conference on Optical Network Design and Modelling (ONDM 2009)*, Braunschweig, Germany, 2 2009.

[9] Savio Rodrigo Antunes dos Santos Rosa, André C Drummond, and Nelson L. S. da Fonseca. Shared path protection with differentiated reliability in transmission impaired WDM networks. In *IEEE ICC 2010 - Communication QoS, Reliability and Modeling Symposium (ICC'10 CQS)*, Cape Town, South Africa, 5 2010.

[10] Sávio Rodrigo Antunes dos Santos Rosa, André Drummond, and Nelson Fonseca. Desempenho de algoritmos de proteção por caminho compartilhado sensíveis às limitações da camada física em redes wdm. In *CSBC 2009 - WPerformance*, jul 2009.

[11] Sávio Rodrigo Antunes dos Santos Rosa, André Drummond, and Nelson Fonseca. Algoritmo para a provisão de confiabilidade diferenciada em redes Ópticas sensíveis às limitacões da camada física. In *SBRC 2010*, may 2010.

[12] André C Drummond, Renato da Silva, Savio Rosa, and Nelson L. S. da Fonseca. IP over WDM module for the NS-2 simulator. In *13th International Workshop on Computer Aided Modeling, Analysis and Design of Communication Links and Networks (CAMAD 2008)*, Beijing, China, P.R. China, 5 2008.

[13] A.E. Eshoul and H.T. Mouftah. Shared protection in wavelength-routed optical mesh networks under dynamic traffic and no wavelength conversion. *Proceedings of Systems Communications*, pages 312–319, Aug. 2005.

[14] Iguatemi Fonseca. *Uma Abordagem para Aprovisionamento e Diferenciação de QoS Óptico na Presença de FWM em Redes Ópticas Transparentes*. PhD thesis, Faculdade de Engenharia Elétrica e de Computação - Universidade Estadual de Campians, 2005.

[15] A. Fumagalli, M. Tacca, F. Unghvary, and A. Farago. Shared path protection with differentiated reliability. *Proc of IEEE International Conference on Communications*, 4:2157–2161 vol.4, 2002.

[16] Jun He, M. Brandt-Pearce, Y. Pointurier, and S. Subramaniam. QoT-aware routing in impairment-constrained optical networks. *Proc of IEEE Global Telecommunications Conference*, pages 2269–2274, Nov. 2007.

[17] Yurong Huang, J.P. Heritage, and B. Mukherjee. Connection provisioning with transmission impairment consideration in optical WDM networks with high-speed channels. *Lightwave Technology, Journal of*, 23(3):982–993, March 2005.

[18] R. R. Iraschko, M. H. MacGregor, and W. D. Grover. Optimal capacity placement for path restoration in mesh survivable networks. In *Proceedings of ICC*, pages 1568–1574, June 1996.

[19] B. Jaumard, C. Meyer, and B. Thiongane. Comparison of ilp formulations for the rwa problem. In *Optical Switching and Networking*, pages 157–172, 2007.

[20] Biswanath Mukherjee. *Optical WDM Networks*. Springer, 2006.

[21] Canhui (Sam) Ou, Jing Zhang, Hui Zang, Laxman H. Sahasrabuddhe, and Biswanath Mukherjee. New and improved approaches for shared-path protection in WDM mesh networks. *Journal of Lightwave Technology*, 22(5):1223–1232, May 2004.

[22] Y. Ouyang, Q. Zeng, and W. Wei. Dynamic lightpath provisioning with signal quality guarantees in survivable translucent optical networks. *Optics Express*, 13:10457–10470, December 2005.

[23] K. Sivarajan R. Krishnaswamy. Algorithms for routing and wavelength assignment based on solutions of lp-relaxation. In *IEEE Communications Letters*, pages 435–437, 2001.

[24] B. Ramamurthy, D. Datta, H. Feng, J.P. Heritage, and B. Mukherjee. Impact of transmission impairments on the teletraffic performance of wavelength-routed optical networks. *Journal of Lightwave Technology*, 17(10):1713–1723, Oct 1999.

[25] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee. Survivable WDM mesh networks. *Journal of Lightwave Technology*, 21(4):870–883, April 2003.

[26] Rajiv Ramaswami and Kumar N. Sivarajan. *Optical Networks - A Practical Perspective*. Academic Press, 2002.

[27] A. Rasala and G. Wilfong. Strictly non-blocking wdm cross-connects for heterogeneous networks. In *Proceedings of Thirty Second Annual ACM Symposium on Theory of Computing*, pages 514–23, 2000.

[28] Xu Shao, Luying Zhou, Xiaofei Cheng, Weiguo Zheng, and Yixin Wang. Best effort shared risk link group (SRLG) failure protection in WDM networks. *Proc of IEEE International Conference on Communications*, pages 5150–5154, May 2008.

[29] V.P. Shuvalov and I.A. Semenchuk. Next generation networks based on optical communication lines. *Proc of International Siberian Workshop on Electron Devices and Materials*, pages 32–34, July 2004.

[30] A. Stavdas, S. Sygletos, M. OMahoney, H. L. Lee, C. Matrakidis, and A. Dupas. Istdavid: Concept presentation and physical layer modeling of the metropolitan area network. *Proc of IEEE International Conference on Communications Workshops*, 21(2):372–383, February 2003.

[31] John Strand and Angela Chui. Impairments and other constraints on optical layer routing. *IETF RFC 4054*, 2005.

[32] M. Tacca, A. Fumagalli, A. Paradisi, F. Unghvary, K. Gadhiraju, S. Lakshmanan, S.M. Rossi, A. de Campos Sachs, and D.S. Shah. Differentiated reliability in optical networks: theoretical and practical results. *Journal of Lightwave Technology*, 21(11):2576–2586, Nov. 2003.

[33] Wang, Sheng, Li, and Lemin. Impairment aware optimal diverse routing for survivable optical networks. *Photonic Network Communications*, 13(2):139–154, April 2007.

[34] Xi Yang, Lu Shen, and B. Ramamurthy. Survivable lightpath provisioning in wdm mesh networks under shared path protection and signal quality constraints. *Lightwave Technology, Journal of*, 23(4):1556–1567, April 2005.

[35] Shengli Yuan and J.P. Jue. Dynamic lightpath protection in WDM mesh networks under wavelength continuity constraint. *Proc of IEEE Global Telecommunications Conference*, 3:2019–2023 Vol.3, Nov.-3 Dec. 2004.

[36] Yuxiang Zhai, Y. Pointurier, S. Subramaniam, and M. Brandt-Pearce. Performance of dedicated path protection in transmission-impaired DWDM networks. *Proc of IEEE International Conference on Communications*, pages 2342–2347, June 2007.

[37] Keyao Zhu, Hongyue Zhu, and Biswanath Mukherjee. Traffic engineering in multigranularity heterogeneous optical wdm mesh networks through dynamic traffic grooming. *IEEE Network*, pages 8–15, March/April 2003.