DYSON PEREIRA JUNIOR

PLANEJAMENTO DE REDES WDM RESILIENTES EM MALHA COM COMPARTILHAMENTO DE RECURSOS DE PROTEÇÃO PARA CONEXÕES COM REQUISITOS DE DISPONIBILIDADE SUJEITAS A MÚLTIPLAS FALHAS

Tese apresentada ao Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Doutor em Informática Aplicada.

CURITIBA

2012

DYSON PEREIRA JUNIOR

PLANEJAMENTO DE REDES WDM RESILIENTES EM MALHA COM COMPARTILHAMENTO DE RECURSOS DE PROTEÇÃO PARA CONEXÕES COM REQUISITOS DE DISPONIBILIDADE SUJEITAS A MÚLTIPLAS FALHAS

Tese apresentada ao Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Doutor em Informática Aplicada.

Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Manoel Camillo Penna

CURITIBA

2012

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central

Pereira Junior, Dyson
P436p 2012 Planejamento de redes WDM resilientes em malha com compartilhamento de recursos de proteção para conexões com requisitos de disponibilidade sujeitas a múltiplas falhas. / Dyson Pereira Junior ; orientador, Manoel Camillo Penna. – 2012
119 f. : il. ; 30 cm

Tese (doutorado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2012.
Bibliografia: f. 111-119

1. Tolerância a falha (Computação). 2. Otimização combinatória. 3. Processos de Markov. 4. Redes ópticas. I. Penna, Manoel Camillo. II. Pontifícia Universidade Católica do Paraná Programa de Pós-Graduação em Informática. III. Título.

CDD 20. ed. – 004

Pontifícia Universidade Católica do Paraná
Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Informática

ATA DE DEFESA DE TESE DE DOUTORADO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

ÁREA DE CONCENTRAÇÃO: CIÊNCIA DA COMPUTAÇÃO

DEFESA DE TESE DE DOUTORADO Nº 013/2012

Aos 24 dias de Agosto de 2012 realizou-se a sessão pública de Defesa da Tese de Doutorado intitulada **"Planejamento de Redes WDM Resilientes em Malha com Compartilhamento de Recursos de Proteção para Conexões com Requisitos de Disponibilidade Sujeitas a Múltiplas Falhas"** apresentada pelo aluno **Dyson Pereira Junior** como requisito parcial para a obtenção do título de Doutor em Informática, perante uma Banca Examinadora composta pelos seguintes membros:

Prof. Dr. Manoel Camillo de O. Penna Neto PUCPR (Orientador)	*(assinatura)*	APROVADO *(aprov/reprov.)*
Prof. Dr. Ricardo Cassiano Nabhen PUCPR		APROVADO
Prof. Dr. Marcelo Eduardo Pellenz PUCPR	APROVADO	
Prof. Dr. Carlos Marcelo Pedroso UFPR		Aprovado
Prof. Dr. Emilio Carlos Gomes Wille UTFPR		APROVADO

Conforme as normas regimentais do PPGIa e da PUCPR, o trabalho apresentado foi considerado APROVADO (*aprovado/reprovado*), segundo avaliação da maioria dos membros desta Banca Examinadora. Este resultado está condicionado ao cumprimento integral das solicitações da Banca Examinadora registradas no Livro de Defesas do programa.

Prof. Dr. Fabrício Enembreck
Diretor do Programa de Pós-Graduação em Informática

Programa de Pós-Graduação em Informática PPGIa PUCPR

Rua Imaculada Conceição, 1155 Prado Velho CEP 80215 901 Curitiba Paraná Brasil
Tel.: (41) 3271 1669 Fax: (41) 3271 2121 www.ppgia.pucpr.br

À minha mãe Enedina, pelo apoio
incondicional durante os estudos.

Agradecimentos

Agradeço aos professores e à Pontifícia Universidade Católica do Paraná que contribuíram de alguma forma para o bom andamento de todo o trabalho.

Agradeço, especialmente, ao meu orientador, Professor Doutor Manoel Camillo Penna que tanto contribuiu e me apoiou durante todo o trabalho com seus questionamentos, motivação e correções.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

F_{max}	Número máximo de falhas de enlace.
$A(t)$	Disponibilidade em função do tempo.
λ	Taxa de ocorrência de falhas (quantidade de falhas por unidade de tempo).
μ	Taxa de ocorrência de falhas (quantidade de falhas por unidade de tempo).
A	Disponibilidade média.
w	Caminho de serviço (*working*).
b	Caminho de proteção (*backup*).
π_0	Probabilidade de estado sem falha da cadeia de *Markov*.
C	O conjunto de todas as conexões necessárias para atender todas as demandas.
c	Uma determinada conexão da rede.
L^c_k	A lista que contém o conjunto dos k caminhos mais curtos para a conexão c.
L^c_p	Subconjuntos de caminhos para proteger a conexão c.
L_p	Lista que contém em cada posição os subconjuntos L^c_p para a conexão c.
$L^c_p(1)$	Subconjunto dos menores caminhos disjuntos em enlace da conexão c.
$L^c_p(x)$	Subconjunto dos caminhos parcialmente disjuntos em enlace da conexão c.
p_{11}	O primeiro caminho do subconjunto $L^c_p(1)$.
n_1	Número de caminhos disjuntos, tamanho de $L^c_p(1)$.
L^c_u	Conjunto de caminhos organizados na sequência de ativação para a conexão c.
L_u	Lista que contém em cada posição o conjunto L^c_u para a conexão c.
DMC	Variável Desvio Médio de Carga nos enlaces.
N	Quantidade de valores de peso entre os enlaces de menor e o de maior carga.
FA^c	Fator de aceitação da conexão c.
FR^c	Fator de rejeição da conexão c.

Lista de Abreviaturas

QoS	*Quality of Service*
IP	*Internet Protocol*
MPLS	*Multiprotocol Label Switching.*
SONET	*Synchronous Optical Network*
WDM	*Wavelength Division Multiplexing*
SLA	*Service Level Agreement*
MSB	*Multiple Shared Backups*
ROADM	*Reconfigurable Optical Add/Drop Multiplexer*
OXC	*Optical Cross-Connect*
OEO	*Optical-Electronic-Optical*
PDL	*Polarization-Dependent Loss*
EDFA	*Erbium-Doped Fiber Amplifier*
ATM	*Asynchronous Transfer Mode*
DWDM	*Dense WDM*
OC-xx	*Sinais Optical Carrier transmitidos sobre uma rede SONET*
OOO	*Optical-Optical-Optical*
WXC	*Wavelength Cross-Connect*
TPA	*Transponder Aggregator*
WR	*Wavelength Routing*
WRON	*Wavelength Routing Optical Network*
WA	*Wavelength Assignment*
S-RWA	*Survivable Routing and Wavelength Assignment*
LP	*Linear Program*
ILP	*Integer Linear Program*
FDBR	*Failure-Dependent Backup Routing*
FIBR	*Failure-Independent Backup Routing*
MTTF	*Mean Time To Failure*
MTTR	*Mean Time To Repair*
MTBF	*Mean Time Between Failure*

TTF	*Time To Failure*
TTR	*Time To Repair*
RBD	*Reliability Block Diagram*
SBPP	*Shared Backup Path Protection*
SRLG	*Shared Risk Link Group*
DCS	*Digital Cross-connect System*
GMPLS	*Generalized Multi-protocol Label Switching*
IETF	*Internet Engineering Task Force*
RFC	*Request for Comments*
ESPI	*Extended Sharing with Partial Information*
SDB	*Single Dedicated Backup*
FIT	*Failure in Time*
CMTC	*Cadeia de Markov em Tempo Contínuo*

Resumo

As falhas de enlace de fibra óptica podem resultar em grande perda de dados em redes de comunicações ópticas de alta velocidade. A resiliência é de importância crítica ao assegurar elevados níveis de disponibilidade e pode torna-se uma questão importante. A abordagem típica em projetos de redes ópticas resilientes é feita através de esquemas de proteção que pré-determina os recursos reservados de proteção considerando cenários de falhas simples e duplas falhas de enlace. O presente trabalho propõe uma heurítica de planejamento para redes WDM que calcula a capacidade de recursos necessária para transportar a demanda de tráfego e proteger as conexões ópticas que satisfaçam aos requisitos de disponibilidade em cenários de falhas múltiplas de enlace. Para proteger uma conexão contra múltiplas falhas, o modelo proposto seleciona, para cada conexão, um caminho óptico de serviço e F_{max} caminhos ópticos de proteção, onde F_{max} é a quantidade de falhas simultâneas a ser considerada. Assim, F_{max} +1 caminhos ópticos serão selecionados e dispostos em uma sequência de ativação, onde o primeiro caminho óptico da lista é o caminho óptico de serviço, e os demais são caminhos ópticos de proteção. Cada conjunto de F_{max} +1 caminhos ópticos com a respectiva sequência de ativação suporta uma conexão. No modelo de rede considerado, o nó de origem da conexão é responsável pela comutação para o caminho óptico de proteção, ou seja, quando uma conexão é interrompida, o nó de origem inicia o processo de restabelecimento da conexão, utilizando o próximo caminho óptico de proteção. O método proposto é denominado MSB (*Multiple Shared Backups*). O método MSB propõe dois algoritmos, um para selecionar os caminhos para cada conexão, e outro para calcular a respectiva indisponibilidade. A partir de um conjunto de *k* menores caminhos, o primeiro algoritmo seleciona os caminhos de cada conexão e a sua ordem de ativação. O segundo algoritmo usa um método para calcular a indisponibilidade de cada conexão (horas por ano), para múltiplas falhas. Os dois algoritmos são utilizados em um procedimento de planejamento visando atender a demanda entre todos os pares de nós, limitando um nível de indisponibilidade pré-definido, utilizando a menor quantidade de recursos.

Palavras-Chave: Tolerância a Falhas, Proteção Compartilhada, Métodos de Otimização, Cadeias de *Markov*.

Abstract

Failures of fiber links can result in major loss of data in high speed optical communication networks. Survivability is of critical importance and assuring high levels of availability becomes an important issue. A typical approach to the design of resilient optical networks is through protection schemes that pre-determines and reserves protection resources considering single and double link-failure scenarios. This thesis proposes a heuristic planning for WDM networks that computes the resource capacity required to transport the traffic demand and to protect the optical connections meeting the availability requirements in scenarios of multiple link failures. To protect a connection against multiple failures, the model selects, for each connection, a service lightpath and F_{max} protection lightpaths, where F_{max} is the quantity of simultaneous failures to be considered. Thus, F_{max} +1 lightpaths are selected and arranged in a sequence of activation, where the first lightpath of the list is the service lightpath, and the others are protection lightpaths. Each set of F_{max} +1 lightpaths in a row of activation supports a connection. For the network model considered, the source node of the connection is responsible for switching the protection lightpath, then, when a connection is interrupted, the source node initiates the re-establishment of the connection, using the next protection lightpath. The proposed method is called MSB (*Multiple Shared Backup*). The MSB method proposes two algorithms, one for selecting the lightpaths for each connection, and another to calculate its unavailability. From a set of k shortest paths, the first algorithm selects the lightpaths of each connection and their order of activation. The second algorithm uses a method to calculate the availability of each connection (hours per year) for multiple failures. Both algorithms are used by a planning procedure to meet the demand between all pairs of nodes, ensuring a pre-defined level of availability, using the least possible amount of resources.

Keywords: Fault Tolerance, Shared Protection, Optimization Methods, Markov Chains.

Capítulo 1

Introdução

1.1) Engenharia de Tráfego em Redes Tolerantes a Falhas.

Uma rede pode ser projetada considerando apenas seus fatores iniciais (topologia, capacidade dos enlaces, etc.), mas as condições da rede, tais como características de carga e de tráfego, mudam com o tempo. Os recursos de rede também variam devido aos pedidos por novos recursos ou mudanças de topologia (por exemplo, falhas de nó ou de enlace), como mostrado em [LEE02], [GIA04], [DOV01].

A Engenharia de Tráfego é um conjunto de métodos e ferramentas que permitem planejar, monitorar, avaliar e corrigir o desempenho das redes de telecomunicações, diante de situações em constantes mudanças, considerando os diversos parâmetros das redes de telecomunicações. A carga em uma rede é a soma de todos os fluxos de dados que todos os nós da rede estão preparados para enviar em um determinado momento. Em uso normal, os fluxos podem não utilizar a largura de banda total alocada, em um dado momento a rede apresenta um fator de utilização, que é expresso em percentual da utilização ótima. A utilização ótima é a máxima utilização antes que a rede seja considerada saturada.

A demanda de tráfego em uma rede é caracterizada por um conjunto de solicitações, onde cada conexão define uma necessidade de tráfego entre dois pontos, o nó de origem e o nó de destino. Um caminho é uma sequência de nós e enlaces que torna possível uma conexão entre um nó de origem e um nó de destino. Uma das principais responsabilidades da Engenharia de Tráfego é dimensionar a rede para que a demanda de tráfego seja atendida. Para cada conexão é verificado na rede se existe largura de banda disponível entre o par de nós, isto é, se há capacidade de largura de banda para o transporte de dados em um caminho de serviço na rede em bits por segundo.

As redes devem ser projetadas para atingir determinados objetivos de QoS (*Qualidade de Serviço*), no entanto, existem diversas métricas para QoS, sendo a confiabilidade um dos principais objetivos de QoS em projetos de redes. A confiabilidade é um termo amplo, ligado à precisão, taxas de erros, estabilidade nos períodos de tempo entre falhas e recuperação após as falhas. A confiabilidade pode ser provida por meio de diferentes mecanismos de gerenciamento de falha aplicados em diferentes níveis de rede e de escala de tempo. A maneira usual de se melhorar a confiabilidade é através da redundância. A redundância é obtida pela adição de caminhos que protegem a demanda por tráfego na ocorrência de falhas para evitar a inatividade da rede, isto é, permitir a recuperação da rede quando submetida a falhas de componentes em seus caminhos de serviço. A capacidade de recuperação se refere ao intervalo de tempo no qual uma rede se recupera de problemas [KUW09].

Muita pesquisa tem sido direcionada para as técnicas de proteção e recuperação da demanda por tráfego em redes [AHN02], [AWD99], [FEL00], [FOR02], que podem ser classificadas por seus modelos fundamentais. O modelo de proteção 1+1 (dedicado) provê um caminho de proteção dedicado que é estabelecido com seus recursos totalmente reservados. Os caminhos de serviço e de proteção são usados simultaneamente ao serem duplicados todos os pacotes no nó de origem e enviados por ambos os caminhos. O nó de destino monitora os dois fluxos de pacotes e seleciona o melhor. Tal esquema provê a melhor proteção da demanda por tráfego, pois a recuperação é rápida enquanto preserva a QoS. O modelo de proteção 1:1 (compartilhado) provê um caminho de proteção para cada caminho de serviço, mas os recursos de tal caminho de proteção podem ser compartilhados com o tráfego de baixa prioridade. Quando a falha ocorre, o tráfego de baixa prioridade sofre preempção pelo caminho de proteção para conduzir o tráfego protegido. A vantagem do esquema 1:1 é que no caso de uma única falha, pode ser obtida uma economia significativa de largura de banda. Em tal caso, como nem todos os caminhos de proteção serão ativados simultaneamente, os recursos que devem ser reservados para os diferentes caminhos de proteção podem ser compartilhados. Devido à significativa reserva de recursos no modelo 1+1, a maioria dos modelos de proteção-recuperação recentes são baseados no modelo 1:1 considerando a ocorrência de uma única falha por vez e os recursos de recuperação compartilhados [AHN02].

Uma segunda classificação organiza os modelos de proteção da demanda por tráfego em duas categorias: rerroteamento (*online*) e comutação (*offline*). De acordo com o modelo de rerroteamento, um caminho de proteção é somente estabelecido quando acontece uma falha.

O caminho de proteção é criado com base na informação de falha e na topologia da rede. Por outro lado, o modelo de comutação envolve uma predeterminação e o estabelecimento de um caminho de proteção antes da falha ocorrer. Quando uma falha acontece, o tráfego é comutado de seu caminho de serviço para o caminho de proteção. No modelo de comutação, o tráfego é rerroteado rapidamente a fim de reduzir o tempo de interrupção do fluxo de tráfego. Em tal caso, o tempo de recuperação é o assunto central, devido à necessidade da recuperação ser rápida, os modelos de proteção-recuperação mais recentes são baseados nos modelos de comutação.

Os modelos de comutação, como mostrado em [FOR02], podem ainda ser classificados como proteção de enlace (proteção local) ou proteção de caminho (proteção fim-a-fim). Na proteção de caminho, a demanda em um caminho de serviço é protegida por um ou mais caminhos de proteção a partir do nó de origem até o nó de destino. Como o caminho de proteção deve proteger a demanda contra falha em qualquer enlace ao longo do caminho de serviço, eles devem ser disjuntos. Na ocorrência de falha em um enlace, o tráfego é comutado para o caminho de proteção pelo nó de origem. Na proteção de enlace, a demanda em cada enlace do caminho de serviço é protegida por um caminho de desvio local com garantia de largura de banda equivalente. Na ocorrência de falha de um enlace, o nó anterior à referida falha cria um caminho de proteção em torno do enlace defeituoso em direção ao segundo nó, rerroteando o tráfego. Depois de o tráfego ser roteado em torno do enlace com defeito, o tráfego continua sem que os nós de origem e de destino tenham conhecimento da falha. A proteção de enlace pode recuperar o atendimento da demanda mais rapidamente que a proteção de caminho, porque não há necessidade de propagação da informação de falha até o nó de origem.

Finalmente, o modelo de proteção pode ou não considerar a demanda por largura de banda. A implementação independente do tráfego considera o preparticionamento da capacidade dos enlaces em capacidade de serviço e proteção independentemente da definição da necessidade de tráfego [ALI04]. Para cada enlace, a solução determina o total da capacidade a ser reservada para a proteção da demanda. Por outro lado, a implementação dependente de tráfego considera a necessidade de tráfego, usualmente organizada em demandas, onde cada demanda define a necessidade de transmissão entre um nó de origem e um nó de destino. A vantagem dos modelos independentes de tráfego é que o tráfego não precisa ser conhecido durante o planejamento da proteção da demanda. As demandas deverão

ser em algum momento definidas e alocadas na rede, mas os algoritmos independentes de tráfego não são projetados para executar alocação de demandas.

O ciclo de ações usado nos métodos de proteção da demanda começa quando a falha é detectada e finaliza quando o caminho de serviço é recuperado. A seleção dos caminhos de serviço e de proteção e a reserva da largura de banda em tais caminhos são os dois componentes principais do ciclo. A entidade de rede responsável pela reação à falha e pelas ações corretivas apropriadas, precisa de dois mecanismos: de detecção de falha ao longo de um caminho e de notificação de falha. Deve haver também um mecanismo de comutação para mover o tráfego do caminho de serviço para o caminho de proteção.

1.2) Escopo do trabalho

A demanda crescente por tráfego e qualidade de serviço nas redes de telecomunicações torna essencial a oferta de níveis elevados de desempenho e eficiência [BHA08]. Uma função importante em tal contexto diz respeito à habilidade de fornecer conexões com largura de banda garantida e com capacidade de recuperação. Proteção e recuperação ocorrem em vários níveis nas redes, mas grande parte do esforço de pesquisa relacionado às redes IP (*Internet Protocol*) adotam soluções IP-MPLS (*Multiprotocol Label Switching*). Além disso, muitas propostas focam na extensão dos mecanismos de proteção e recuperação para as redes ópticas. Portanto, o tema recuperação e proteção tem sido um tema central nas redes ópticas, desde a implantação dos mecanismos tradicionais baseados em anel das redes SONET (*Synchronous Optical Network*).

Existem assim, muitos trabalhos relacionados ao tema proteção e recuperação (ver seção 5.1), nos quais a hipótese mais usual é considerar uma quantidade máxima de falhas simultâneas F_{max}, supondo-se que todos os enlaces e nós tenham a mesma probabilidade de falha. Tais trabalhos assumem que a probabilidade de muitos enlaces falharem simultaneamente é desprezível, sendo então desconsiderada.

Conforme discutido anteriormente, o modelo de proteção da demanda 1:1 comutado é o mais usual, havendo inúmeras propostas para proteção de caminho ou local. Entretanto, independentemente do modelo de proteção, a hipótese de uma quantidade máxima de falhas $F_{\max}$ (na maioria, $F_{\max} = 1$) é amplamente adotada. Conforme já mencionado, a idéia por traz de tal hipótese é considerar desprezível a probabilidade de muitos enlaces falharem simultaneamente. Na realidade, mesmo os trabalhos que consideram uma quantidade de falhas

simultâneas F_{max} maior que 1, não abordam o problema com os requisitos de disponibilidade por conexão.

A limitação da quantidade de falhas simultâneas é uma maneira simplificada de abordar o problema, mas nem sempre representa a realidade. Sabe-se que embora menos provável, mais de uma falha pode acontecer simultaneamente [MEL05].

Conforme já dito anteriormente, uma demanda define uma necessidade de tráfego entre dois nós da rede. A demanda de tráfego estabelecida flui por um ou mais caminhos que estabelecem a conexão entre o seu nó de origem e o seu nó de destino. A Engenharia de Tráfego deve determinar os caminhos por onde a demanda de tráfego definida pelas conexões fluirá. No caso de funcionamento normal da rede, o tráfego demandado por uma conexão flui pelo caminho de serviço. Na ocorrência de falha em pelo menos um dos componentes de um caminho de serviço, haverá a interrupção ou degradação da demanda de tráfego solicitada pela conexão. Nota-se que, quanto maior o caminho (maior número de componentes), menor será a disponibilidade da conexão.

Uma conexão tem uma disponibilidade igual ao produto entre as disponibilidades de seus componentes (nó e enlace). Um aumento na disponibilidade da conexão acontece com a adição de caminhos paralelos (caminhos de proteção) ao caminho de serviço, que receberão o fluxo comutado quando houver falha no caminho de serviço. Mas, a inclusão de caminhos de proteção provoca a queda na eficiência da rede, pois ela inclui recursos de rede que serão utilizados apenas para aumentar a confiabilidade.

A falha de um componente (enlace ou de um nó) em uma rede WDM (*Wavelength Division Multiplexing*) representa a interrupção de todos os caminhos ópticos que percorrem os componentes em estado de falha. Tal estado pode provocar a perda de uma grande quantidade de informações e a possível paralisação de serviços de missão crítica. Diante de tal fato, as redes ópticas transparentes (ver seção 2.2.1) precisam de mecanismos para garantir que falhas de equipamentos e de fibras sejam recuperadas de maneira rápida e eficiente. A capacidade de continuar operando na eventualidade de ocorrência de falhas é conhecida como resiliência [ZHO00]. A classificação e as principais técnicas de resiliência em redes ópticas transparentes podem ser encontradas em [AST03], [ZHA04], [AST04], [MOH01], [TAP03], [RAM03].

De modo geral, a resiliência pode ser classificada de acordo com as estratégias e topologias de sobrevivência utilizadas. Um primeiro critério tem relação com os componentes

que farão parte da estratégia de resiliência. Os componentes que poderiam ser considerados pelas estratégias de resiliência são os nós e os enlaces da rede. Entretanto, para os primeiros, as estratégias de resiliência normalmente envolvem apenas estruturas locais (ex., replicação dos nós em um mesmo ambiente físico), o que as tornam mais simples quando comparadas com resiliência de enlaces. Por tal razão a grande maioria dos estudos considera estratégias de resiliência envolvendo apenas os enlaces das redes. Outro critério considera o alcance dos mecanismos de sobrevivência, podendo envolver a proteção e recuperação de caminhos ou de enlaces (ou segmentos). A primeira, também conhecida como proteção fim-a-fim, tende a utilizar menos recursos, enquanto que a segunda, também conhecida como proteção local, tende a introduzir menores tempos de recuperação. Outro critério que influencia na estratégia de resiliência é a possibilidade ou não do compartilhamento dos recursos de proteção. Na proteção dedicada, os recursos não são compartilháveis enquanto que na proteção compartilhada eles são. No presente estudo não foi considerada a proteção de nós, e sim uma estratégia de resiliência fim-a-fim compartilhada.

O momento de realização das ações relacionadas à resiliência também produz estratégias distintas. Três momentos fundamentais podem ser considerados: o momento de cálculo do caminho de serviço, o momento de cálculo do caminho de proteção, e o momento de ativação do caminho de proteção. O primeiro conduz a duas estratégias possíveis, ou seja, calcular o caminho de serviço sob demanda, ou calcular todos os caminhos *a-priori*. A segunda estratégia, que necessita do conhecimento prévio das demandas, é melhor para os algoritmos de planejamento e será utilizada no presente trabalho. O segundo momento também conduz a duas estratégias distintas, a saber, calcular o caminho de proteção junto com o caminho de serviço, ou apenas no instante de ocorrência da falha. A literatura denomina os mecanismos da primeira estratégia de mecanismos de proteção e os da segunda de mecanismos de restauração [GER00]. Finalmente o momento de ativação do caminho de proteção também conduz a duas estratégias distintas: ativação no momento de cálculo da rota do caminho de proteção, ou ativação no momento da falha.

A topologia de compartilhamento também conduz a estratégias de resiliência distintas. Duas estratégias são encontradas na literatura. Na primeira, caminhos de serviço com mesma origem e destino são protegidos por um conjunto de caminhos de proteção. Na segunda, caminhos de serviço com origem e destinos distintos podem ter caminhos de proteção que compartilham um ou mais enlaces. A segunda estratégia é conhecida por compartilhamento

mesh, que tende a consumir menor quantidade de recursos de proteção, à custa da maior complexidade do tratamento.

Outro critério que influencia bastante na estratégia de resiliência é levar em consideração ou não a disponibilidade das conexões (uma conexão atende uma demanda existente entre uma origem e um destino). Pelo fato do limite de indisponibilidade ser um dos indicadores mais importantes dos acordos de nível de serviço (SLA – *Service Level Agreement*), as estratégias de resiliência que visam atingir níveis de disponibilidade pré-definidos possuem relevância diferenciada. Tais estudos, por sua vez, diferenciam-se entre si, pela quantidade de falhas simultâneas que são capazes de tratar. Devido à complexidade do tratamento, a maioria dos estudos limita-se a esquemas de sobrevivência que levam em conta apenas uma ou duas falhas simultâneas.

No presente trabalho, é investigada uma estratégia de resiliência para determinar os requisitos de capacidade em termos de alocação de comprimentos de onda, e o roteamento e respectivas atribuições de comprimentos de onda para caminhos ópticos de serviço e de proteção, para um esquema de proteção de caminho do tipo *mesh* compartilhado, que leva em conta a disponibilidade das conexões. Propõe uma heurística de planejamento, onde as demandas são conhecidas a-priori, e que leva em conta os requisitos de disponibilidade das conexões considerando múltiplas falhas simultâneas.

1.3) Objetivos da Tese de Doutorado

No presente trabalho é apresentado um novo método heurístico para executar o planejamento de uma rede WDM: dada a topologia física, e uma estimativa da demanda entre quaisquer dois nós da rede, é apresentado um algoritmo que realiza simultaneamente a alocação de recursos (*wavelengths*), e a configuração de rotas dos caminhos de serviço e de proteção contra múltiplas falhas para cada demanda com a respectiva alocação de recursos, minimizando os recursos alocados.

No modelo considerado, a rede WDM é definida pela topologia física, composta pelos enlaces e pelos nós de comutação, organizados em um grafo, e pela topologia lógica, composta pelo conjunto de todas as conexões ópticas que a rede deve estabelecer. Um enlace é um cabo com múltiplas fibras, e em cada enlace (bidirecional) algumas fibras são utilizadas em uma direção de propagação e outras (não necessariamente na mesma quantidade) na direção oposta. A localização geográfica dos nós e os comprimentos físicos dos enlaces são

conhecidos. Cada fibra de um enlace transporta uma quantidade determinada de comprimentos de onda, e é assumido, por simplicidade, que todos os comprimentos de onda na rede são caracterizados pela mesma taxa de bits, que na prática pode variar de 2,5 até 160 Gbit/s. A capacidade física de um enlace é equivalente à quantidade de comprimentos de onda que ele suporta. Enquanto a topologia física é conhecida, a capacidade de cada enlace é uma variável de dimensionamento do problema. Sem perda de generalidade, optou-se por pré-atribuir a mesma quantidade de comprimentos de onda para todas as fibras da rede, deixando como variável a quantidade de fibras por enlace. Os nós da topologia física são os OXCs (*Optical Cross-Connect*), cada um sendo considerado como um nó de origem e como um nó de destino potencial do tráfego WDM.

Uma conexão é definida como uma unidade de demanda entre um nó de origem e um nó de destino. Uma unidade de demanda corresponde, por definição, à capacidade de um comprimento de onda. A conexão é um serviço protegido, implementado por um conjunto de caminhos ópticos, um de serviço e os demais de proteção. Cada par de nós pode precisar de mais de uma conexão quando a largura de banda total necessária para atender a demanda entre eles exceder a capacidade de um caminho óptico.

O objetivo do planejamento é ativar todas as conexões necessárias para atender a demanda com o nível de disponibilidade determinado. A solução é encontrada apenas quando todas as conexões forem configuradas, isto é, quando todos os caminhos ópticos de serviço e proteção estiverem roteados. A capacidade dos enlaces físicos é dimensionada com o objetivo de acomodar todos os caminhos ópticos de todas as conexões. Para atingir os requisitos de disponibilidade é proposto um esquema de proteção de caminho do tipo *mesh* compartilhado, que leva em conta tais requisitos, considerando um cenário com múltiplas falhas simultâneas.

1.4) Estrutura do Documento

O documento está organizado em 7 capítulos. O capítulo 2 mostra conceitos básicos de redes ópticas necessários para o desenvolvimento da presente tese, as tecnologias de transmissão em fibra óptica, as redes ópticas totalmente transparentes e as redes ópticas WDM. O capítulo 3 mostra as estratégias de proteção e restauração baseadas em caminho, a classificação e as principais técnicas de resiliência em redes ópticas transparentes. O capítulo 4 mostra os requisitos de alta disponibilidade das conexões de comunicação como um fenômeno que pode ser modelado por dois estados nos quais um sistema ou componente pode

se encontrar: em funcionamento ou em reparo. O capítulo 5 mostra os trabalhos relacionados com o planejamento de redes de telecomunicações de baixo custo e tolerantes a falhas. O capítulo 6 mostra o método de planejamento MSB (*Multiple Shared Backups*), que propõe dois algoritmos, um para selecionar os caminhos para cada conexão, e outro para calcular a respectiva indisponibilidade. O capítulo 7 mostra a avaliação de resultados, onde é apresentada a metodologia de simulação para um cenário com rede de referência, bem como, a comparação com os resultados obtidos pelo planejamento usando o método MSB. Mostra também os resultados ótimos (busca exaustiva) obtidos em uma rede exemplo, bem como, a comparação com os resultados obtidos pelo planejamento usando o método MSB. A conclusão é apresentada a partir dos resultados numéricos mostrando os objetivos atingidos pelo método de planejamento MSB, referentes ao grau de resiliência alcançado pela rede, compartilhamento de recursos, redução significativa da vulnerabilidade das conexões, bem como, algumas das possíveis ações que podem melhorar o desempenho do método MSB, tanto operacionalmente como em resultados.

Capítulo 2

Redes Ópticas

A enorme largura de banda disponível hoje em redes de comunicação se deve à rápida e contínua evolução da capacidade das tecnologias de redes ópticas e suas funcionalidades. Os principais agentes no desenvolvimento das redes ópticas são os centros de pesquisa, a indústria de equipamentos de telecomunicações e as organizações de padronização, tais como o IEEE (*Institute of Electrical and Electronics Engineers*) e o ITU-T (*International Telecommunications Union Telecommunication Standardization Sector*). No presente capítulo, são abordados alguns conceitos básicos de redes ópticas, as tecnologias de transmissão em fibra óptica, as redes ópticas totalmente transparentes e seus principais componentes. A tecnologia de multiplexação por comprimento de onda WDM é também apresentada.

2.1) Os Serviços das Redes Ópticas

Uma classificação fundamental [ELB02], [REN97], [THE05], divide as infra-estruturas de rede em relação à comutação na rede: as redes de comutação de circuito e as redes de comutação de pacotes. Nas redes de comutação de circuito os circuitos dedicados são ofertados aos seus clientes. Tais conexões, após estabelecidas, possuem largura de banda garantida e dedicada até que haja a desconexão. Em tais redes, a soma de todos os fluxos das conexões em um enlace deve ser menor ou igual à capacidade de transmissão do enlace. As redes de telefonia pública são a aplicação mais comum para tal tipo de rede óptica, que oferecem uma conexão de banda fixa, tipicamente de 4 kHz, aos seus usuários finais. Tal conexão é, então, convertida para um canal digital de 64 kbps. Porém, tais redes oferecem diversas outras taxas de transmissão. As taxas de transmissão para os serviços de linha

privada vão de algumas dezenas de kbps a até dezenas de gigabits por segundo. A ineficiência de utilização dos recursos da rede é o principal problema das redes de comutação de circuito, pois ficam ociosos quando um usuário não transmite dados e é comum em tráfegos em rajadas. Em redes de dados, como a Internet, são frequentes os tráfegos em rajadas. Para lidar de forma eficiente com tráfegos em rajadas foram propostas as redes de comutação de pacotes. Em tais redes, a capacidade do enlace é compartilhada entre os fluxos de pacotes dos usuários através de multiplexação. Assim, se um usuário deixar de transmitir pacotes, outro poderá transmitir além do usual, utilizando de modo eficiente a capacidade do enlace. Porém, é comum a imprevisibilidade do controle na utilização dos recursos, e principalmente, no estabelecimento de circuitos ou conexões que garantam reserva de recursos e assim torna-se impossível garantir banda nem latência. As redes ópticas, como foram implementadas até recentemente, eram baseadas em comutação de circuitos. Tal situação se devia a algumas deficiências tecnológicas, tal como, à incapacidade de processar opticamente um pacote, o que obrigava a conversão óptica da informação para um plano eletrônico e o seu processamento. Ainda mais, nas redes ópticas em malha, um nó pode estar conectado a vários outros nós ópticos através de dezenas de fibras ópticas. Assim, a ineficiência na utilização da banda nas fibras é observada ao processar, encaminhar e comutar eletronicamente todos os pacotes ópticos gerando latência. A crescente procura por redes ópticas com grande capacidade e elevada flexibilidade levou ao desenvolvimento do nó ROADM (*reconfigurable optical add*/*drop multiplexer*), (ver seção 2.2.5). A cada concessão de linha privada existe um crescimento da largura de banda passante alocada. Taxas de transmissão que eram pouco comuns para transmissão em longas distâncias, tais como 155 Mbps, 2,5 Gbps e até 10 Gbps estão sendo cada vez mais utilizadas. O período de contrato de clientes de tais redes ópticas tem sido cada vez menor, devido à expectativa de obtenção de taxas de transmissão mais elevadas a custos cada vez menores. Contratos com períodos de duração de dias ou até horas já é possível encontrar, seja para um *backup* de dados, proteção de uma falha eventual ou até devido a algum evento especial. Um modelo que permita suprir tais necessidades pode dar solução à dinâmica do estabelecimento de conexões ópticas. A disponibilidade de conexões, como percentagem do tempo que a conexão permanece operacional é outro aspecto importante. É cada vez mais comum encontrar operadoras de rede ópticas que oferecem disponibilidade com cinco 9's (99,999), [RAM02], [FAW04], equivalente a um período não operacional de 5 minutos por ano. Já se fala em sete 9's e até nove 9's para se definir

disponibilidade. Somente com a implementação de mecanismos de resiliência a falhas uma rede pode alcançar tais níveis de disponibilidade.

2.2) Terminologia e Conceitos

Na presente seção são introduzidos os conceitos e terminologias utilizados na arquitetura de rede óptica. Algumas das definições apresentadas na seção são baseadas em [RAJ04] e podem apresentar definições diferentes em outra abordagem de redes ópticas.

2.2.1) Transparência e Opacidade

O conjunto de nós interconectados por fibras ópticas constitui uma rede óptica. Cada nó é um comutador OXC (*Optical Cross-Connect*) constituído por uma matriz de comutação óptica e seu controlador. Tais matrizes de comutação óptica podem ser opacas ou transparentes. As que realizam conversões óptico-eletrônico-óptico (*Optical-Electronic-Optical* - OEO) para efetuar a comutação são chamadas opacas. As matrizes de comutação opacas podem manipular eletronicamente os sinais ópticos que atravessam um nó, e assim, efetuar operações de reformatação, regeneração, retemporização e amplificação do sinal. Em uma rede óptica transparente os sinais ópticos são transportados do emissor ao receptor ao longo da rede totalmente no domínio óptico, sem conversões OEO. Os sinais que trafegam pelo núcleo de uma rede transparente são amplificados opticamente pelo EDFA (*Erbium-Doped Fiber Amplifier*) sem a possibilidade de acesso aos dados por eles transportado.

2.2.2) Multiplexação por Comprimento de Onda

A transmissão de múltiplos sinais ópticos, de diferentes comprimentos de onda, utilizando uma única fibra é realizada através de multiplexação por comprimento de onda (*Wavelength Division Multiplexing* - WDM). Diferentes conteúdos digitais a taxas de transmissões variadas podem ser transportados por um comprimento de onda, tais como, OC-3 (155 Mbps), OC-12 (622 Mbps), etc., e em diferentes formatos ou encapsulamentos, como SONET, Ethernet e ATM. A alta capacidade e flexibilidade da tecnologia WDM é obtida com a transmissão paralela de diversos comprimentos de onda, onde um comprimento de onda de sinal SONET OC-48 de 2,5 Gbps e outro de sinal Ethernet OC-192 de 10 Gbps podem trafegar pela mesma fibra óptica. Com as pesquisas em WDM denso (*Dense WDM* - DWDM), a quantidade de comprimentos de onda multiplexados em uma única fibra cresce a cada dia e já

ultrapassa a casa do milhar, bem como a máxima taxa de transmissão já ultrapassou o Tbps [RAM02]. Em breve, equipamentos comerciais serão capazes de transmitir até 160 comprimentos de onda com capacidade superior a OC-192, em uma única fibra em até 1,6 Tbps [RAM02], [GRE01]. A transmissão em fibra óptica realizada pela técnica WDM não especifica requisitos necessários aos nós da rede e nem procedimentos de comutação dos sinais ópticos. Tipicamente, nas redes ópticas mais avançadas, tal comutação é realizada através de dispositivos ópticos, como as matrizes de comutação ópticas, as OXCs, apresentadas na Seção 2.2.5. A arquitetura das redes ópticas WDM em malha é apresentada na Seção 2.3.

2.2.3) O canal Óptico

Uma conexão da camada óptica fim-a-fim entre dois nós da rede é chamada de Canal óptico (*lightpath*). O conceito de canal óptico não se aplica somente a redes ópticas com comutadores OXCs transparentes. Apesar das conversões OEO, uma rede que apresenta somente comutadores opacos também resulta em canais ópticos. No presente trabalho o termo canal óptico tem o mesmo significado de caminho óptico.

2.2.4) Conversor de Wavelength

Quando um caminho óptico é transportado pelo mesmo comprimento de onda, por toda a sua extensão, em todos os enlaces, afirma-se que são satisfeitas as restrições da propriedade de continuidade de comprimento de onda, ou simplesmente continuidade de comprimento de onda. Tal restrição não é problema para as redes opacas, onde a comutação do feixe de luz é realizada através de conversões OEO, então o comprimento de onda disponível na fibra é escolhido durante a conversão eletrônico-óptica da porta de saída. As conversões OEO não ocorrem nas redes transparentes, onde a restrição de continuidade de comprimento de onda pode acarretar em altas probabilidades de bloqueio. O uso eficiente dos comprimentos de onda da rede é obtido com a presença de conversor óptico de comprimento de onda em seus nós [RAM98], [CHU03], e surge como alternativa por não apresentar as limitações de banda dos dispositivos eletrônicos e por reduzir a probabilidade de bloqueio. A ausência de conversores ópticos de comprimento de onda nos comutadores OXCs de uma rede transparente eleva a probabilidade de bloqueio, pois é mais frequente a disputa por recursos. A liberdade na escolha pelo comprimento de onda disponível evita a tal disputa por recursos, e ocorre somente nas redes opacas ou redes transparentes com conversores. Uma rede de conversão total de

comprimento de onda é uma rede que inclui em cada nó, ou OXC, conversores ópticos para cada comprimento de onda de cada interface óptica, ou fibra óptica. Assim, não existe a possibilidade de faltar conversores de comprimento de onda e, conseqüentemente, bloquear o estabelecimento de uma conexão. Até recentemente, devido ao custo relativamente elevado dos conversores ópticos de comprimento de onda, recomendava-se minimizar o seu uso no projeto e implementação de tais redes ópticas. Redes ópticas relativamente baratas com a mínima quantidade de conversores necessária podem ser eficientes e com baixa probabilidade de bloqueio. Assim, o posicionamento esparso de conversores [ALF04], a utilização parcial de conversores nos nós da rede [CHU04] e a combinação das duas técnicas [LIU04] obtiveram resultados significativos na redução do custo de implementação de redes ópticas e na melhora da probabilidade de bloqueio. Segundo Chu *et al.* [LIU04], não é necessário que todos os nós da rede sejam habilitados com a conversão total de comprimento de onda para que a rede obtenha uma baixa probabilidade de bloqueio equivalente a uma rede transparente de conversão total.

2.2.5) O Comutador Óptico OXC

A comutação de um feixe de luz de uma porta de entrada para uma porta de saída é realizada pelo comutador óptico OXC [SHI98], [CAO04], [CAO03]. Ele é constituído, basicamente, de duas entidades: uma entidade da camada WDM, a matriz de comutação óptica e uma entidade da camada IP que controla a matriz de comutação óptica. Tal comutação pode utilizar uma conversão óptico-eletrônica na porta de entrada e uma conversão eletrônico-óptica na porta de saída, ou realizar a comutação totalmente óptica. No primeiro caso, a conversão OEO apresenta limitações, como a limitação em banda passante, que não é desejada em redes de alta velocidade. No segundo caso, a comutação é dita OOO (*Optical-Optical-Optical*). O OXC é um dispositivo que funciona no plano óptico comutando sinais ópticos, sem decodificar os sinais ópticos em dados, para obtenção de endereços para a comutação, como acontece em comutadores *Ethernet*, por exemplo. Tal função é realizada pela matriz de comutação óptica, que, por ser totalmente passiva, necessita de uma unidade de controle. Tal unidade controladora deve implementar protocolos de sinalização e de roteamento que são necessários para calcular e estabelecer as conexões do plano óptico. É através de tal controlador que os nós da rede trocam informações de estado de enlace e de ocorrência de falhas de recursos, além de sinalizar o estabelecimento de caminhos ópticos.

2.2.6) ROADM (*Reconfigurable Optical Add/Drop Multiplexer*)

A procura crescente por redes ópticas com grande capacidade e elevada flexibilidade levou ao desenvolvimento do nó ROADM (*reconfigurable optical add/drop multiplexer*), mostrado em [SAH09]. Os nós ROADM com múltiplos graus foram implantados em redes de longa distância e metropolitanas. Tais nós com um núcleo WXC (*wavelength cross-connect*) entre múltiplas fibras de entrada e saída, habilita qualquer sinal WDM vindo de qualquer direção a ser roteado para qualquer outra direção. No entanto, os *transponders* (dispositivo que atua automaticamente a um sinal de entrada, sua denominação é uma contração das palavras: *transmitter* e *responder*) são conectados às portas *add/drop* e os seus comprimentos de onda e fibras de entrada/saída são atribuídos em função das portas às quais estão conectados.

A Porta de Comutação Óptica

Uma matriz de comutação óptica é constituída da porta de comutação óptica, ou porta comutadora. O redirecionamento, ou alteração do curso, de um feixe de luz ou laser dentro da matriz de comutação óptica é executado por tal elemento. Existem diversos tipos de portas ópticas e tais tipos de portas podem ser organizados em arquiteturas distintas, como apresentado mais adiante. As redes ópticas utilizam as portas de comutação óptica para diversos tipos de aplicações. Alguns parâmetros de desempenho do tipo de porta indicam o seu tipo de aplicação, como o tempo de comutação e quantidade de portas comutadoras. Uma das aplicações de tais portas é a provisão de canais ópticos. Com tal finalidade, as portas ópticas atuam como componentes das matrizes de comutação que constitui as matrizes de comutação óptica, presente nos comutadores OXCs, e reorganizam a arquitetura de controle interno, permitindo o estabelecimento de novos canais ópticos. Em tal aplicação, tais portas funcionam como substituições aos cabos (*patch cables*) manuais, mas exigem softwares de gerenciamento de conexões fim-a-fim. Portanto, para tal tipo de aplicação é aceitável um tempo total de comutação de alguns milissegundos. A comutação de proteção de fibra ou de comprimento de onda é outra importante aplicação para uma porta óptica. Tais dispositivos realizam a comutação do tráfego de um recurso, que pode ser uma fibra ou um comprimento de onda, de serviço para um recurso de proteção no caso de falha. O tempo de detecção da falha, a comunicação da falha para os elementos apropriados da rede, o tempo de comutação e configuração de tais elementos, constitui tal operação que deve ser efetuada em um tempo

total de algumas dezenas de milissegundos. As portas de comutação óptica têm outras aplicações, tais como encaminhar pacotes ópticos ou até modular dados definindo os estados *on* e *off* na saída do laser. Para um funcionamento eficiente [RAM02], a comutação de pacotes ópticos necessita de portas que comutem na ordem de poucos nanossegundos. Já a modulação do laser necessita de tempo de comutação da ordem de picossegundos [RAM02]. Outros parâmetros são utilizados para caracterizar a adequação da porta ao tipo de aplicação em redes ópticas, além do tempo de comutação e ao número de portas necessárias.

2.3) As Redes Ópticas WDM

Uma rede WDM encaminha as mensagens da origem até o destino baseada no comprimento de onda associado ao canal óptico. Tal paradigma de encaminhamento de mensagens em redes ópticas é também conhecido como Roteamento de Comprimento de Onda (*Wavelength Routing* - WR), utilizado nas redes WRON (*Wavelength Routing Optical Network*). Para o transporte dos dados é necessário que antes seja estabelecida uma conexão na camada óptica, o canal óptico. Tal conexão define os enlaces da rede e os respectivos comprimentos de onda. Com o estabelecimento dos comprimentos de onda, a banda passante do canal óptico fica totalmente disponível para a conexão, até que seja efetuada sua finalização, ou desconexão. A escolha dos enlaces permite o estabelecimento do canal óptico. Qualquer protocolo de roteamento pode realizar tal procedimento. A seguir é necessário escolher os comprimentos de onda que serão utilizados em cada enlace do canal. Alguns algoritmos fazem a escolha de comprimento de onda [HAR98], tal aspecto das redes WDM não foi abordado visando manter o foco principal do presente trabalho. A combinação dos dois procedimentos é denominada Roteamento e Atribuição de Comprimento de Onda (*Routing and Wavelength Assignment* - RWA) [OZD03], [SAA04]. O roteamento e a atribuição de comprimentos de onda podem ocorrer simultaneamente e não serem sequencialmente. Assim, o roteamento pode fazer uso da disponibilidade dos comprimentos de onda das fibras ópticas [YOO03]. Uma rede WDM transparente, que apresenta conversão total de comprimento de onda em todos os seus nós, ou seja, sem a restrição de continuidade de comprimento de onda, pode encaminhar pacotes e estabelecer conexões de maneira semelhante às redes convencionais de comutação de circuito de telefonia.

2.4) Técnicas de Proteção em Redes Ópticas de Tipo Mesh

As redes ópticas transparentes possibilitam o transporte de grandes quantidades de informações e o fornecimento de serviços para aplicações que exigem requisitos de qualidade de serviço como, por exemplo, máximo tempo de atraso. Além da alta sensibilidade ao atraso, tais aplicações geralmente exigem uma alta disponibilidade de serviços da rede funcionando 24 horas por dia. A falha de um enlace ou de um nó representa a interrupção de todos os caminhos ópticos que percorrem os componentes em estado de falha. Tal estado pode provocar a perda de uma grande quantidade de informações e a paralização de serviços de missão crítica. Diante de tal fato, as redes ópticas transparentes precisam de mecanismos para garantir que falhas de equipamentos e de fibras sejam recuperadas de maneira rápida e eficiente. A capacidade de continuar operando na eventualidade de ocorrência de falhas é conhecida como resiliência em redes ópticas transparentes [ZHO00].

A resiliência em redes ópticas é tipicamente classificada em estratégias de proteção ou restauração [GER00]. A proteção é uma estratégia pró-ativa que consiste na reserva antecipada (isto é, antes da ocorrência de falhas) de recursos redundantes que somente serão utilizados para recuperar uma eventual falha. Na estratégia de restauração não é feita a reserva antecipada de recursos redundantes. De forma reativa, depois da detecção da falha, as estratégias de restauração tentam alocar recursos disjuntos ao componente em estado de falha com o objetivo de garantir a resiliência da rede. As estratégias de proteção e restauração podem ser baseadas no enlace, no caminho ou no segmento (trecho de caminho). A classificação e as principais técnicas de resiliência em redes ópticas transparentes podem ser encontradas em [AST03], [ZHA04], [AST04], [MOH01], [TAP03].

Tais estudos apresentam diferentes esquemas de resiliência às falhas de enlace. Os esquemas são baseados em dois paradigmas de resiliência: 1) proteção e restauração de enlace e 2) proteção e restauração de caminho.

2.4.1) Proteção e Restauração de Enlace

Em proteção de enlace, os recursos de proteção são reservados em torno de cada enlace durante a configuração de conexão, enquanto na restauração de enlace, os nós do enlace em estado de falha descobrem dinamicamente uma rota em torno do enlace. Na restauração de enlace, todas as conexões que percorrem o enlace em estado de falha são

rerroteadas em torno do referido enlace e os nós de origem e de destino das conexões são indiferentes à falha do enlace.

- Proteção dedicada de enlace: Em proteção dedicada de enlace, no momento da configuração da conexão, para cada enlace do caminho de serviço, um caminho de proteção e um comprimento de onda são reservados em torno do referido enlace e são dedicados à tal conexão. Em geral, não é possível alocar um caminho de proteção dedicado em torno de cada enlace com o mesmo comprimento de onda do caminho de serviço da conexão.

A prática indica que a proteção dedicada de enlace utiliza os comprimentos de onda de maneira ineficiente, e o presente trabalho não utiliza a proteção dedicada de enlace [RAM03].

- Proteção compartilhada de enlace: Em proteção compartilhada de enlace, os recursos reservados de proteção ao longo do caminho de proteção podem ser compartilhados com outros caminhos de proteção. Como resultado, os canais de proteção são multiplexados entre diferentes cenários de falha (que não se espera que ocorram simultaneamente), e, por conseguinte, a proteção compartilhada de enlace é mais eficiente em capacidade quando comparada com a proteção dedicada de enlace.
- Restauração de enlace: Na restauração de enlace, os nós de cada enlace em estado de falha participam em um algoritmo distribuído para descobrir dinamicamente uma rota em torno do enlace. Se nenhuma rota estiver disponível para uma conexão interrompida, então a conexão é descartada.

2.4.2) Proteção e Restauração de Caminho

Na proteção de caminho, os recursos de proteção são reservados durante a configuração da conexão, enquanto na restauração de caminho, as rotas de proteção são descobertas dinamicamente após a falha do enlace. Quando um enlace falhar, o nó de origem e o nó de destino de cada conexão que percorre o enlace em falha são informados sobre a falha através de mensagens oriundas dos nós adjacentes ao enlace em estado de falha [RAM03].

- Proteção dedicada de caminho: Em proteção dedicada de caminho (também chamado de proteção 1:1), os recursos são dedicados ao longo do caminho de proteção para apenas uma conexão e não são compartilhados com os caminhos de proteção de outras conexões.

- Proteção compartilhada de caminho: Em proteção compartilhada de caminho, os recursos ao longo do caminho de proteção podem ser compartilhados com outros caminhos de proteção. Como resultado, os canais de proteção são multiplexados entre os diferentes cenários de falha (que não se espera que ocorram simultaneamente) e, portanto, proteção compartilhada de caminho é mais eficiente em capacidade quando comparada com a proteção dedicada de caminho.
- Restauração de caminho: Na restauração de caminho, os nós de origem e de destino de cada conexão que percorre o enlace em estado de falha participam de um algoritmo distribuído para dinamicamente descobrir uma rota de proteção fim-a-fim. Se nenhuma das rotas estiver disponível para uma conexão interrompida, então a conexão é descartada.

A seguir, são apresentados os principais problemas no gerenciamento de falhas e algumas técnicas adequadas para resolvê-los.

2.4.3) Atribuição de Comprimentos de Onda

A atribuição de comprimento de onda (WA - *wavelength assignment*) pode ser feita após o roteamento dos caminhos de serviço e de proteção. Diferentes heurísticas [ZHA03] executam WA junto com o cálculo dos caminhos de serviço e de proteção. Em caso de atendimento da restrição de continuidade do comprimento de onda, o procedimento se torna um problema NP-completo [ZHA03], [RAM95]. Quando uma rede tem completa capacidade de conversão de comprimento de onda, o procedimento é reduzido a um problema de roteamento de um conjunto de caminhos disjuntos e parcialmente disjuntos em enlace, que pode ser resolvido usando algoritmos existentes como por exemplo o algoritmo de Suurballe [SUU84].

2.4.4) Otimização de Compartilhamento

Uma das principais vantagens das redes WDM em malha contra o legado das redes interconectadas por anéis com base na rede SONET é que as redes WDM em malha são capazes de dar suporte a diferentes esquemas de proteção e podem ser mais eficientes do que as redes em anel SONET. Particularmente, através de proteção compartilhada baseada em caminho, as redes WDM em malha podem exigir de 40 a 60 por cento de capacidade extra para proteger contra qualquer falha única na rede, em comparação com um requisito de capacidade reservada de 100 por cento em esquemas de proteção com base em anel SONET

[RAM03]. Em um esquema de proteção compartilhada, os recursos de rede ao longo do caminho de proteção podem ser compartilhados entre caminhos de proteção de conexões diferentes, pois apenas uma conexão irá comutar seu tráfego do caminho de serviço para o caminho de proteção quando ocorrer uma falha na rede. Existe muita pesquisa sobre como maximizar o compartilhamento de recursos para o esquema de proteção compartilhada nas redes WDM em malha para otimizar a eficiência de recursos de rede [MOH01], [CHE08]. Geralmente é assumido que:

- A falha de enlace é o cenário dominante na rede.
- Existe no máximo uma única falha de enlace em qualquer momento, e é reparado antes que ocorra a próxima falha, assim o cenário de múltiplas falhas é um evento relativamente raro na rede.

Os seguintes esquemas e considerações permitem maximizar o compartilhamento de recursos com ou sem a restrição de continuidade do comprimento de onda.

Otimização do Caminho de Proteção

Uma forma de alcançar alto índice de compartilhamento de recurso é distribuir o caminho de serviço das diferentes conexões, e simultaneamente planejar seus caminhos de proteção de modo que eles compartilhem os mesmos recursos extensivamente [MUK04]. Tal otimização conjunta é um problema de difícil solução. Portanto, não se encontram disponíveis esquemas eficazes. Um esquema alternativo é fixar o caminho de serviço de acordo com o estado atual da rede (por exemplo, caminho de custo mínimo), e otimizar o caminho de proteção para uma conexão solicitada. Tal esquema pode ser realizado, ao ajustar o custo de cada enlace com base nas informações atuais dos recursos da rede, o caminho de proteção pode ser calculado usando um algoritmo de busca do caminho mais curto (por exemplo, o algoritmo *Dijkstra*).

Restrição Física na Otimização do Caminho de Proteção

Embora a técnica de otimização do caminho de proteção possa melhorar muito a eficiência dos recursos, pode surgir um problema. Quando tal esquema é amplamente usado, uma conexão pode ter um caminho de proteção percorrendo longas distâncias (vários enlaces), mesmo que o caminho de serviço seja curto [RAM03]. Um caminho de proteção longo pode levar a um problema de degradação da qualidade de sinal, especialmente em uma

rede WDM totalmente óptica. Recentemente, diferentes grupos de pesquisa começaram a investigar tal problema. Os autores em [QIA02] propuseram um modelo baseado em ILP (*Integer Linear Program*) para calcular em conjunto o par de caminhos de serviço e de proteção com compartilhamento para o tráfego dinâmico. O modelo considera o uso dos recursos de rede e o tamanho dos caminhos de proteção. A idéia de tal modelo é incorporar um custo ao enlace, de tal forma que reflita em recursos extras utilizados pelo caminho de proteção e o tamanho que ele pode alcançar.

Roteamento de Proteção Independente e Dependente da Falha

Outro esquema possível para melhorar o compartilhamento dos recursos de proteção é o roteamento de proteção dependente de falha (FDBR - *failure-dependent backup routing*). Em tal esquema, um caminho de proteção pode ser calculado de acordo com uma certa falha de rede sobre o caminho de serviço. Ou seja, se o caminho de serviço percorre *m* enlaces, pode existir *m* caminhos de proteção, um para cada uma das *m* falhas de enlace. Em um esquema de roteamento de proteção independente de falha (FIBR - *failure-independent backup routing*), um único caminho de proteção será utilizado independente da falha do enlace; FIBR é o método dominante usado pela maioria dos esquemas na literatura de pesquisa hoje. É fácil ver que o FIBR é um caso especial de FDBR no sentido de que os *m* caminhos de proteção são representados por um único. Os *m* caminhos de proteção no FDBR podem compartilhar recursos com outros caminhos de proteção ou mesmo entre si. Os recursos ao longo do caminho de serviço também podem ser reutilizados pelos *m* caminhos de proteção. Desta forma, FDBR poderá melhorar o compartilhamento de recursos entre os caminhos de proteção e eventualmente aumentar a eficiência global dos recursos de rede [QIA02].

Controle Distribuído e Centralizado

Em um sistema de controle distribuído, o nó de origem de cada conexão interrompida pode recuperar o serviço utilizando um caminho pré-calculado ou um caminho dinamicamente calculado. Uma vez que as conexões sejam restauradas de forma distribuída, é possível que um bloqueio eventual de recurso possa ocorrer em algum enlace da rede. Embora tais disputas possam ser resolvidas por meio de sucessivas tentativas de restauração, elas podem afetar o desempenho da rede. Em um sistema de controle centralizado, as conexões

serão restauradas uma a uma, então o bloqueio eventual de recurso é evitado, mas tal regime pode afetar o desempenho na recuperação de algumas conexões. Comparado ao controle distribuído, um esquema de restauração por controle centralizado pode obter melhor desempenho pois ele pode executar a otimização global no uso de recursos da rede.

Caminhos de Restauração Pré-Planejados e Dinamicamente Calculados (online)

Em um sistema de controle distribuído, as rotas de restauração podem ser pré-planejadas ou calculadas dinamicamente [MUK04]. Em um esquema pré-planejado, a partir de um conjunto de caminhos candidatos, um caminho de restauração pode ser pré-calculado para cada conexão. Quando uma conexão falhar, um caminho a partir de tal conjunto pode ser selecionado como um caminho de restauração sem cálculo *online*. Outros caminhos candidatos podem também se submeter a tentativa se falhar a restauração do caminho selecionado. Tal esquema pode reduzir o tempo de restauração. O conjunto de caminhos pode ser periodicamente atualizado de acordo com os diferentes estados da rede com a finalidade de aumentar a probabilidade de sucesso da restauração.

A Reversibilidade dos Mecanismos de Proteção

A reversibilidade é uma característica predominante na operação dos mecanismos de proteção e influi no desempenho da rede. Em mecanismos de proteção dedicados (tipo 1:1) a reversibilidade não é um fator preponderante, pois o caminho óptico de proteção não é compartilhado [ZHA07]. No entanto, nos mecanismos de proteção compartilhada (tipo 1:N) há enlaces dos caminhos de proteção que são compartilhados e isto pode influir no desempenho. Um mecanismo de proteção é classificado como reversível se, após a recuperação de um enlace em estado de falha, as conexões afetadas pela falha voltam ao seu caminho óptico de serviço. Um mecanismo de proteção não-reversível, por sua vez, não reverte ao caminho óptico de serviço as conexões afetadas por uma falha após a recuperação do enlace em estado de falha. A vantagem da não-reversibilidade é a redução da quantidade de comutações entre o caminho de serviço e o caminho de proteção que são efetuadas para oferecer resiliência às possíveis falhas das fibras ópticas e outros componentes da rede. O efeito das comutações na disponibilidade depende do tempo necessário para serem realizadas. A disponibilidade é pouco afetada se as comutações forem realizadas em um curto período de tempo. Alguns parâmetros de desempenho são prejudicados com não-reversibilidade dos

mecanismos de proteção. A probabilidade de bloqueio não é afetada. Porém, a disponibilidade das conexões pode ser prejudicada, se o mecanismo de proteção compartilhar recursos, ou pode ser beneficiada, se o tempo de permanência da conexão for pequeno o suficiente. Em uma rede que utiliza proteção 1:N não-reversível, o caminho óptico de proteção de uma conexão que foi afetada por falhas não é liberado até que a desconexão seja efetuada. Enquanto tal conexão não for liberada, as conexões que compartilham recursos com ela não poderão requisitar o caminho óptico de proteção.

Disponibilidade de Serviço

Sabe-se que um esquema de proteção contribuirá para o aumento da disponibilidade de uma conexão desde que o tráfego no segmento de serviço que sofreu uma falha (enlace, caminho ou subcaminho) seja rapidamente comutado para o segmento de proteção [MUK04]. Por exemplo, uma conexão protegida por um caminho terá 100% de disponibilidade na presença de qualquer simples falha. No entanto, em um cenário mais realista de múltiplas falhas, quase simultâneas, a disponibilidade da conexão depende intimamente dos detalhes precisos das falhas (localização, tempos de reparo, etc.), quantidade de recursos de proteção que estão reservados (isto é, um único ou múltiplos caminhos de proteção), e como os tais recursos de proteção são alocados (isto é, dedicado ou compartilhado). Então, quanto mais recursos de proteção houver (caminhos), maior será a disponibilidade da conexão, e quanto mais compartilhamento da proteção menor será a disponibilidade da conexão. O que é necessário agora é uma metodologia sistemática para quantitativamente estimar a disponibilidade da conexão, especialmente quando vários esquemas de proteção (dedicado ou compartilhado) são aplicados à conexão. Tal metodologia pode ajudar a entender quanto de proteção deve ter uma conexão e se a qualidade de serviço pode ser garantida em vez de simplesmente informar que a conexão está protegida.

Capítulo 3

Modelo de Disponibilidade em Redes Ópticas com Proteção Fim-a-Fim

Para atender aos requisitos de alta disponibilidade das conexões de comunicação, os prestadores de serviços de telecomunicações oferecem garantias sobre a qualidade de serviço (QoS) que é aferida por indicadores definidos em SLAs, especialmente a disponibilidade. Por ser um acordo contratual entre o prestador de serviços e seus clientes, o SLA (*Service Level Agreement*) estipula requisitos mínimos para os indicadores de QoS, incluindo muitas vezes penalidades severas para o prestador de serviço se os requisitos não são atendidos.

A disponibilidade é um fenômeno que pode ser modelado por dois estados nos quais um sistema ou componente pode se encontrar: em funcionamento ou em reparo. A disponibilidade instantânea, $A(t)$, é a probabilidade de que o sistema esteja pronto para uso em um instante de tempo qualquer, enquanto a disponibilidade média é a fração de tempo em que o sistema estará pronto para uso durante algum período de tempo. Existem dois tipos de disponibilidade média: a retrospectiva, cujo valor de disponibilidade é obtido conhecendo-se o período de tempo decorrido através de dados históricos, sendo avaliada como a proporção do período de tempo que o sistema (ou componente) permaneceu em funcionamento dividido pelo período de tempo total [CLO02]; e a prospectiva, que utiliza dados históricos para deduzir um modelo de como a disponibilidade pode se comportar no futuro.

Pela modelagem da disponibilidade, os dados obtidos conduzem às expectativas de disponibilidade futura. Se λ é a taxa de ocorrência de falhas (quantidade de falhas por unidade de tempo) e μ é a taxa de recuperação (quantidade de reparos por unidade de tempo), a disponibilidade pode ser dada em função do tempo como [MYK06]:

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda - \mu).t} \quad (1)$$

Com $t \longrightarrow \infty$, o segundo termo da equação tende a zero, conduzindo à disponibilidade média dada por:

$$A = \frac{\mu}{\lambda + \mu} \quad (2)$$

$$A = \frac{MTTF}{MTTF + MTTR} \quad (3)$$

onde MTTF=1/λ é o tempo médio para falhar (*Mean Time To Failure*) e MTTR=1/μ é o tempo médio para recuperar (*Mean Time To Repair*), que refletem a confiabilidade e a manutenibilidade, do sistema ou componente. Observe que MTTF e MTTR são as médias das variáveis aleatórias TTF e TTR, como mostrado na Figura 3.1, onde cada uma delas tem a sua própria distribuição de probabilidade. Outra variável aleatória usada na determinação da disponibilidade é o tempo entre falhas (TBF), que é a soma das variáveis TTR e TTF (ver Figura 3.1) e o respectivo tempo médio entre falhas (MTBF - *Mean Time Between Failure*), que é a soma de MTTF e MTTR. É interessante notar que existem infinitos conjuntos de combinações de MTTF e MTTR que podem produzir a mesma disponibilidade.

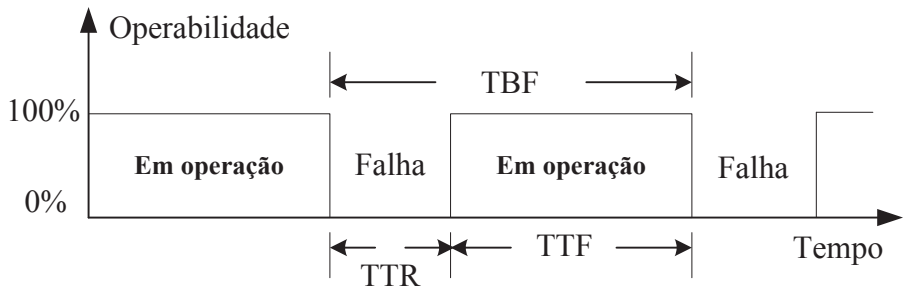


Figura 3.1: Parâmetros de recuperação de rede após uma falha.

Os parâmetros de falha de um componente normalmente podem ser obtidos a partir dos operadores de rede. Os componentes considerados no presente estudo são os enlaces de fibra, cujo MTTF está relacionado com a distância, e pode ser deduzido de acordo com estatísticas registradas a partir dos cortes (TTF) que ocorrem na fibra. Também assume-se que os processos de reparo dos enlaces são independentes um do outro, tal que dois enlaces serão reparados em paralelo se seus estados de falha se sobrepuserem.

A análise de disponibilidade de uma conexão pode ser vista como uma enumeração dos estados em funcionamento e em falha da mesma. Conforme apontam [ZHO07], [MEL05], as seguintes hipóteses podem ser tomadas para uma análise aproximada da disponibilidade: (i) falha apenas dos enlaces; (ii) descrição dos estados dos enlaces através de um modelo de dois estados (em funcionamento e em reparo). (iii) os enlaces falham de forma independente; (iv) os tempos de permanência nos estados em funcionamento e em reparo são exponencialmente distribuídos com MTTR e MTTF constantes. (v) O MTTR é muito menor do que o MTTF. Os pressupostos (i) a (iv) são típicos para redes de comunicação, e a suposição (v) é a base para uma aproximação comum para o cálculo da disponibilidade do caminho *i* (A_i) através de diagramas em bloco de confiabilidade (*Reliability Block Diagram* - RBD) em série formado por *n* componentes (enlaces) de um caminho [CLO02]:

$$\mathrm{A_i} = \prod_{j=1}^{n} a_j \approx 1 - \sum_{j=1}^{n} U_j \tag{4}$$

onde a_j é a disponibilidade do enlace *j* e U_j é a indisponibilidade do enlace *j*. Se uma conexão *c* é realizada por um único caminho, sua disponibilidade (denominada por A_c) será igual à disponibilidade do caminho. Se *c* tem proteção dedicada ou compartilhada, A_c deve ser determinada considerando os caminhos de serviço e de proteção.

Se *c* for protegida por um caminho dedicado, *c* estará interrompida somente quando ambos os caminhos de serviço (*w*) e de proteção (*b*) não estiverem disponíveis, assim A_c pode ser calculada da seguinte forma:

$$\mathrm{A_c} = 1 - (1 - \mathrm{A_w}).(1 - \mathrm{A_b}) \tag{5}$$

onde A_w e A_b denominam as disponibilidades de *w* e *b*, respectivamente.

Uma conexão *c*, ao ser protegida por um caminho compartilhado, estará disponível se *w* estiver disponível ou se *w* não estiver disponível, *b* estiver disponível e *P* puder obter os recursos de proteção, mesmo quando os outros caminhos compartilhados no grupo S_c também falharem. Portanto, A_c pode ser calculada da seguinte forma:

$$\mathrm{A_c} = \mathrm{A_w} + (1 - \mathrm{A_w}) \times \mathrm{A_b} \times \sum_{\mathrm{i}=0}^{\mathrm{N}} \delta_{\mathrm{c}}^{\mathrm{i}} \times \mathrm{P_i} \tag{6}$$

onde A_w e A_b denominam a disponibilidade de w e b, respectivamente; N é o tamanho de S_c; δ_c^i é a probabilidade com que c pode obter os recursos de proteção quando o caminho w e outros i caminhos de serviço em S_c falharem; e P_i é a probabilidade de que exatamente i caminhos de serviço em S_c estejam indisponíveis. O valor de P_i pode ser obtido ao enumerar todas as possíveis i combinações de falha de conexão. Considerando que w e todos os caminhos em S_c falham independentemente, então $\delta_c^i = 1/(i+1)$.

3.1) Modelo para duas falhas baseado em CMTC

Na concepção original do SBPP (*shared backup path protection*) [MEL05], um caminho de serviço e um caminho de proteção são atribuídos a cada conexão, e recursos podem ser compartilhados entre os caminhos de proteção, se seus correspondentes caminhos de serviço não utilizarem enlaces de fibra em comum. No entanto, a economia de capacidade permitida através do compartilhamento de capacidade de proteção é conseguida à custa da degradação da resiliência de conexão.

O presente trabalho realiza uma extensão do método mostrado em [MEL05] e [PEL05], porém, aplicado a uma quantidade maior de grupos de valores (múltiplas falhas simultâneas), e implementa um algoritmo que executa um esquema analítico derivado de um modelo da cadeia de *Markov* em tempo contínuo, tanto para selecionar caminhos candidatos para cada conexão ao manter simultaneamente o balanceamento de carga da rede, como para calcular a indisponibilidade de cada conexão, considerando F_{max} como a quantidade máxima de falhas simultâneas de enlaces. O método de cálculo de indisponibilidade tem base nas hipóteses de análise de disponibilidade estabelecidas no modelo a seguir.

A estratégia proposta em [MEL05] e [PEL05] tenta prover conexões com disponibilidade garantida, enquanto minimiza a capacidade reservada alocada. A estimativa de disponibilidade de conexão usa um esquema derivado a partir de um modelo de *Markov* em tempo contínuo que assume que não mais do que duas falhas simultâneas de enlaces de fibra ocorrem na rede. Suas derivações baseiam-se nas seguintes premissas:

1) Um modelo de dois estados, "em operação" e "em falha", descreve o estado de todos os enlaces de fibra.
2) Os nós de rede têm disponibilidade igual a um.
3) Todos os enlaces de fibra falham independentemente.

4) O tempo de reparo e o tempo de falha de um enlace de fibra assumem valores sem memória para processos aleatórios exponencialmente distribuídos, com média constante (tempo médio de reparo MTTR, e tempo médio para falha MTTF).
5) Em SBPP, o primeiro caminho que falhar detém os recursos de proteção até que ele seja completamente reparado.
6) No máximo dois enlaces de fibra podem falhar simultaneamente no estado de falha dentro da rede.

As premissas 1-4 são típicas para as redes de transporte. A premissa 5 é uma implementação própria de SBPP. Observe que pela premissa 2, os nós da rede são tratados como entidades atômicas que não falham. Na verdade, os nós são muito confiáveis em comparação com os enlaces e sua disponibilidade pode ser sempre controlada por redundância interna. A premissa 6 torna o esquema aplicável à maioria das redes (mesmo as grandes).

No modelo proposto [MEL05], os estados da rede são descritos por sequências de falhas de enlaces. Por exemplo, o estado da rede com nenhuma falha é representado por (0) e o estado da rede com os enlaces 3,2,4 falhados, na ordem apresentada, é representado por (3,2,4). Se a rede estiver no estado (0), todos os enlaces estão em operação; se a rede estiver no estado (i), todos os enlaces exceto o enlace (i), estão em operação; se a rede estiver no estado (i, j), todos os enlaces exceto os enlaces i e j, estão em operação. O modelo considera até duas falhas de enlace e a probabilidade *steady state* de se encontrar em um estado (i, j) qualquer é representado por $\pi_{(i,j)}$.

Para calcular a indisponibilidade das conexões, o algoritmo de cálculo percorre os estados da cadeia de *Markov* conforme ilustrado na Figura 3.2.

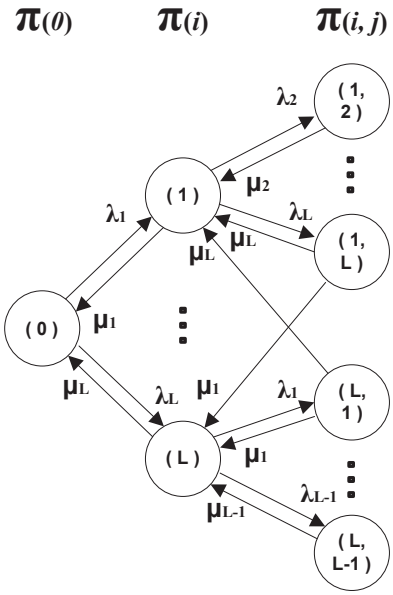


Figura 3.2: A cadeia de *Markov* em tempo contínuo.

Então, a probabilidade do estado sem falhas ($\pi_{(0)}$) pode ser obtida pela equação (7), onde *L* é a quantidade de enlaces da rede:

$$\pi_{(0)}\left[1+\sum_{i=1}^{L}\frac{\lambda_i}{\mu_i}+\sum_{i=1}^{L}\sum_{\substack{j=1,\\ j\neq i}}^{L}\frac{\lambda_i}{\mu_i}\frac{\lambda_j}{\mu_i+\mu_j}\right]=1 \tag{7}$$

As probabilidades de estado estão interrelacionadas pelas equações:

$$\pi_{(i)}=\frac{\lambda_i}{\mu_i}\pi_{(0)} \tag{8}$$

$$\pi_{(i,j)}=\frac{\lambda_j}{\mu_i+\mu_j}\pi_{(i)} \tag{9}$$

Na concepção original de SBPP, um caminho de serviço *w* e um caminho de proteção *b* são atribuídos a cada conexão *c*, e a capacidade pode ser compartilhada entre os caminhos de proteção se os seus correspondentes caminhos de serviço não utilizarem enlaces de fibras em comum (*shared risk link group constraint*, ou restrição SRLG). Tal grupo de caminhos de

serviço cujos caminhos de proteção compartilham alguma capacidade com *b* é chamado de SG (*shared group*).

3.2) Modelo para 3 falhas baseado em CMTC

A extensão da cadeia de Markov descrita em 3.1 é realizada considerando-se os estados correspondentes à sequência de três falhas (*i*, *j*, *k*), conforme ilustrado na Figura 3.3.

Se a rede estiver no estado (0), todos os enlaces estão em operação; se a rede estiver no estado (*i*), todos os enlaces exceto o enlace (*i*), estão em operação; se a rede estiver no estado (*i*, *j*), todos os enlaces exceto os enlaces *i* e *j*, estão em operação; se a rede estiver no estado (*i*, *j*, *k*), todos os enlaces estão em operação, exceto os enlaces *i*, *j* e *k*, e assim por diante (ver Figura 3.3).

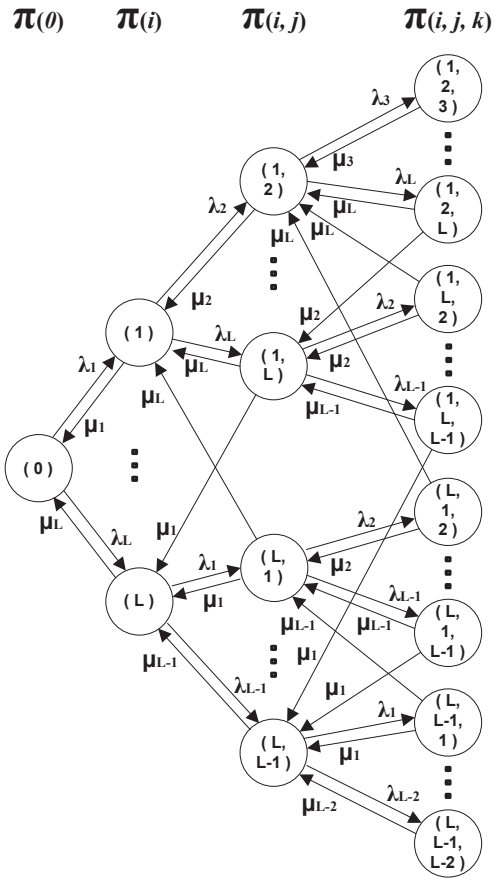


Figura 3.3: Exemplo de cadeia de Markov para F_{max} = 3.

Para uma determinada quantidade máxima de falhas simultâneas de enlace, é conhecida a probabilidade de ocorrência de cada uma das possíveis combinações de falha. A Equação 10 mostra as condições de equilíbrio para uma rede com L enlaces e um limite de três falhas simultâneas.

$$\pi_0 \left[1 + \sum_{i=1}^{L} \frac{\lambda_i}{\mu_i} + \sum_{i=1}^{L} \sum_{j=i+1}^{L} \frac{\lambda_i . \lambda_j}{\mu_i . \mu_j} + \sum_{i=1}^{L} \sum_{j=i+1}^{L} \sum_{k=j+1}^{L} \frac{\lambda_i . \lambda_j . \lambda_k}{\mu_i . \mu_j . \mu_k} \right] = 1 \qquad (10)$$

A equação mostra todas as possíveis combinações de falhas da rede, sem considerar a sequência de falhas, onde π_0 é a probabilidade na qual a rede permanece no estado sem falhas. Ao admitir a ocorrência de um único evento por vez, considera-se que o estado da rede definido por uma combinação de falhas simultâneas pode ser alcançado após diferentes sequências de estado da rede.

A proporção de tempo na qual ocorre uma combinação de duas falhas simultâneas pode ser obtida através de duas possíveis sequências de falhas, assim:

$$\frac{\lambda_i . \lambda_j}{\mu_i . \mu_j} = \frac{\lambda_i . \lambda_j}{\mu_i + \mu_j} \left[\frac{\mu_i + \mu_j}{\mu_i . \mu_j} \right] = \frac{\lambda_i . \lambda_j}{\mu_i + \mu_j} \left[\frac{1}{\mu_j} + \frac{1}{\mu_i} \right] \qquad (11)$$

A proporção de tempo na qual ocorre uma combinação de três falhas simultâneas pode ser obtida através de seis possíveis sequências de falhas, assim:

$$\frac{\lambda_i . \lambda_j . \lambda_k}{\mu_i . \mu_j . \mu_k} = \frac{\lambda_i . \lambda_j . \lambda_k}{\mu_i + \mu_j + \mu_k} \left[\frac{1}{\mu_j + \mu_k} \left(\frac{1}{\mu_k} + \frac{1}{\mu_j} \right) + \frac{1}{\mu_i + \mu_k} \left(\frac{1}{\mu_k} + \frac{1}{\mu_i} \right) + \frac{1}{\mu_i + \mu_j} \left(\frac{1}{\mu_j} + \frac{1}{\mu_i} \right) \right] \qquad (12)$$

Então, se cada termo individual da Equação 10 for substituído pelos termos correspondentes a cada sequência mostrada nas equações 11 e 12, o resultado pode ser observado na Equação 13 que calcula a probabilidade do estado sem falhas ($\pi_{(0)}$):

$$\pi_{(0)}\left[1+\sum_{i=1}^{L}\frac{\lambda_i}{\mu_i}+\sum_{i=1}^{L}\sum_{\substack{j=1,\\ j\neq i}}^{L}\frac{\lambda_i}{\mu_i}\frac{\lambda_j}{\mu_i+\mu_j}+\sum_{i=1}^{L}\sum_{\substack{j=1,\\ j\neq i,}}^{L}\sum_{\substack{k=1,\\ k\neq i,\\ k\neq j}}^{L}\frac{\lambda_i}{\mu_i}\frac{\lambda_j}{\mu_i+\mu_j}\frac{\lambda_k}{\mu_i+\mu_j+\mu_k}\right]=1 \quad (13)$$

A probabilidade estacionária de uma sequência de falhas (o estado da cadeia) pode ser obtida a partir da probabilidade do estado anterior (antes da ocorrência da última falha da sequência), de acordo com as equações (14-16):

$$\pi_{(i)}=\frac{\lambda_i}{\mu_i}\pi_{(0)} \quad (14)$$

$$\pi_{(i,j)}=\frac{\lambda_j}{\mu_i+\mu_j}\pi_{(i)} \quad (15)$$

$$\pi_{(i,j,k)}=\frac{\lambda_k}{\mu_i+\mu_j+\mu_k}\pi_{(i,j)} \quad (16)$$

Para uma quantidade maior de falhas simultâneas de enlace, a Equação 10 deve conter o número de termos correspondente ao tamanho máximo da combinação de falhas admissível. É preciso conhecer a sequência de falhas correspondente a cada combinação de falhas realizável e montar a equação final correspondente à Equação 13.

Capítulo 4

Trabalhos Relacionados

A demanda por tráfego com Qualidade de Serviço (QoS) é crescente nas redes de telecomunicações e assim exigindo cada vez mais um alto nível de desempenho e eficiência. Uma alternativa importante é a capacidade para prover as conexões com banda garantida, associada à capacidade de recuperação após falhas na rede. Entretanto, tal tema tem sido sempre uma questão central nas redes ópticas, desde os mecanismos de proteção e recuperação das tradicionais redes em anel SONET, até um interesse mais recente nas redes ópticas em malha (*mesh*).

No capítulo 3 foi apresentada uma classificação para as técnicas de proteção e recuperação investigadas nos últimos anos. Pode-se dizer que as duas primeiras classificações organizam modelos superados, pois conforme já explicado, devido à significativa reserva de recursos no modelo 1+1, a maioria dos modelos de proteção-recuperação recentes são baseados no modelo 1:1; e devido à necessidade de rapidez nas recuperações, os modelos de proteção-recuperação mais recentes são baseados nos modelos de comutação em vez do modelo de rerroteamento.

O projeto de redes de telecomunicações de baixo custo e tolerantes a falhas é um processo extremamente complexo. Grande parte dos produtos disponíveis no mercado com tal objetivo utiliza um processo baseado em simulação e/ou heurística. As linguagens para modelagem combinadas com poderosos procedimentos de otimização reduzem sensivelmente a dificuldade de implementação da teoria matemática de programação nos projetos de rede comerciais práticos [KEN07].

O grau de um dado nó corresponde ao número de enlaces incidentes sobre ele. Um grafo conectado no qual cada nó tem grau 2 é chamado anel. Um grafo é dito *two-edge-*

connected se existirem ao menos dois caminhos disjuntos entre cada par de nós. O problema de selecionar um conjunto de arestas entre dois nós, com custo mínimo que assegure uma rede *two-edge-connected* é um problema fundamental no projeto de redes e é amplamente estudado.

Todo grafo *two-edge-connected* que tenha pelo menos um nó com grau maior que 2 é chamado *mesh*. Assim, toda rede *two-edge-connected* pode ser classificada como uma arquitetura em anel ou *mesh*. Um anel é a topologia de rede mais simples e é *two-edge-connected*, e também executa um serviço de recuperação relativamente fácil de implementar. Os anéis são amplamente usados no projeto de redes tolerantes a falhas. Em uma arquitetura baseada em anel como em [GRO98], uma grande rede é composta de uma coleção de pequenas redes em anel e sua arquitetura é mais adaptada nas situações onde a rede pode ser construída de tal maneira que a maioria do tráfego que ela conduz esteja entre os pares de nós de um mesmo anel (*chord-link*).

Em [RAM02] foi observado que os *backbones* típicos das redes norte americanas têm aproximadamente 50 nós com grau médio entre 3 e 4, e alguns dos nós podem alcançar graus entre 5 e 10. Para redes de tal tipo, arquiteturas de proteção *mesh* usualmente requerem menor capacidade reservada do que as arquiteturas em anel.

Podem ser encontradas na literatura várias estratégias de resiliência em redes de comunicação, todas são baseadas em um conjunto de características que têm um impacto sobre o funcionamento da rede e/ou projeto [GRO04]. Em primeiro lugar, uma rede tolerante a falhas pode usar um esquema de *proteção* ou de *recuperação*. Em um esquema de proteção, os recursos redundantes são pré-calculados e reservados com antecedência. Ao contrário, os esquemas de recuperação tomam ações em tempo real (*online*), incluindo a alocação de recursos e de caminhos, com base na falha e no estado da rede no momento da falha. Enquanto os esquemas de recuperação são geralmente mais eficientes em termos de largura de banda, porque não alocam capacidade de recuperação com antecedência, os esquemas de proteção têm menores tempos de restabelecimento e sempre podem garantir a recuperação da falha. Em segundo lugar, pode-se optar por proteção de *enlace* ou de *caminho*. *Proteção/recuperação de enlace* consiste em proteger cada enlace como uma entidade, independentemente das demandas de conexão que passam por ele, enquanto a *proteção/recuperação de caminho* protege individualmente cada demanda, fornecendo um caminho de proteção sobrevivente entre os nós fins. Embora os esquemas de proteção

(recuperação) de caminho conduzam a uma utilização eficiente dos recursos de *backup*, eles também conduzem a um tempo maior de detecção e recuperação de falha que a proteção (recuperação) de enlace.

4.1) Recuperação de Caminho

No *esquema de recuperação de caminho*, a falha de um enlace pode afetar um ou mais caminhos usados para conduzir o tráfego de serviço. Portanto, a recuperação requer a alocação de capacidade reservada em um conjunto de caminhos que não utilizem o enlace que falhou. A diferença entre a recuperação de caminho e a recuperação de enlace é que a recuperação de caminho usa rotas alternativas a partir da origem até o destino das conexões afetadas pela falha do enlace em vez de simplesmente fazer um *desvio* em torno do defeito. Tal característica faz a distinção entre rerroteamento *global* e *local*.

Em [DOV94] é mostrado que uma questão crucial na gerência de redes de telecomunicações é a recuperação após uma falha na rede. O artigo compara a eficiência de capacidade (o total de tráfego recuperado após a capacidade fixada) de vários tipos de métodos de recuperação para *Digital Cross-connect System* (DCS) sob falhas de nó e de enlace em redes metropolitanas. Tais métodos de recuperação podem ser amplamente categorizados com base no tipo de controle do processo de recuperação e no tipo de procedimento para o rerroteamento do tráfego em torno da falha. É evidente que métodos com proteção de caminho recuperam um percentual maior do tráfego do que os métodos de proteção de enlace. Portanto, a quantificação da diferença em eficiência entre os métodos é importante para avaliar completamente outros fatores como custo e velocidade da recuperação. Para avaliar a diferença de eficiência, foram geradas distribuições de tráfego de rede aleatoriamente por simulação e então geradas falhas de nós e enlaces para cada exemplo de simulação. Estatísticas foram geradas sobre o total esperado de tráfego recuperado em cada método de recuperação. Foi concluído que a vantagem da eficiência dos métodos de proteção de caminho sobre os métodos de proteção de enlace é maior para falhas de enlace do que para falhas de nós. Também, a diferença não foi estatisticamente significativa em menores níveis de congestionamento de rede (isto é, redes com excesso de capacidade) e se tornou mais significativa com o crescimento do congestionamento de rede.

Na recuperação de caminho, é possível liberar as partes sobreviventes de um caminho de serviço e usá-las para a recuperação. Tal opção é conhecida como *stub release*. Os artigos [IRA96] e [IRA98] mostram um estudo que concluiu que as redes *mesh* recuperáveis utilizando recuperação de caminho com *stub release* são mais eficientes em capacidade. A alocação de capacidade reservada em tais redes exigiu até 19% menos da capacidade total do que as redes estudadas com recuperação de enlace. A eficácia global da recuperação de caminho também é evidente quando se considera que a redundância média em todos os projetos de recuperação de caminho que otimiza a alocação de capacidade reservada é de 66%, em comparação aos 87% para os projetos de recuperação de enlace. Os resultados também mostraram que a capacidade necessária em uma rede com 100% de recuperação de caminho com *stub release* pode ainda ser minimizada em média 7%, quando uma otimização conjunta for utilizada para alocar capacidade de serviço e reservada. Os benefícios da otimização conjunta de roteamento dos caminhos de serviço e de alocação de capacidade reservada são, no entanto, muito mais pronunciadas em projetos com recuperação de enlace.

O trabalho em [XIO99] também compara proteção de enlace e de caminho com e sem *stub release*, e também mostra que o *stub release* e a proteção de caminho podem ser muito eficazes para grandes redes esparsas (isto é, redes que apresentam nós com grau médio muito pequeno).

4.1.1) Proteção Offline

Reservar largura de banda suficiente para proteção assegura que todos os caminhos de serviço estejam protegidos sem se importar com o modo como eles foram encontrados, pois a capacidade de proteção não é utilizada nos caminhos de serviço, como realizado no presente trabalho. A reserva de capacidade ajuda a simplificar as operações de rede tal como conexões de roteamento a serem realizadas com proteção garantida. Além do mais, a reserva pode ser feita por um algoritmo *off-line* tendo como dados todas as informações de rede. Tal característica torna possível maximizar a largura de banda compartilhada entre os caminhos de proteção, assim minimizando a quantidade total de capacidade necessária a ser reservada para a proteção.

Arci et al. [AEC03] aplicaram a análise de disponibilidade em redes ópticas e desenvolveram uma formulação para analisar e comparar o desempenho da disponibilidade de esquemas de proteção de caminho. Várias configurações dedicadas e compartilhadas foram analisadas por meio de técnicas RBD (*reliability block diagram*), e as equações algébricas correspondentes foram derivadas. Algumas das equações derivadas são aproximações, e nesses casos foram validadas por simulação. Clouqueur e Grove [CLO02] definiram o conceito de restaurabilidade de uma rede como a porção da capacidade de serviço em falha que pode ser restaurada por um mecanismo resiliência. Eles usaram o conceito de indisponibilidade equivalente, definida como a probabilidade de que um enlace *i* falhe e não possa ser restaurado, para estudar a restaurabilidade da rede quando falhas duplas de enlace ocorrem em redes ópticas *mesh* projetadas para falhas de um único enlace. O método proposto utiliza um procedimeto computacional para avaliar os efeitos das falhas duplas de enlace em esquemas de resiliência fim-a-fim compartilhados.

Considerando que a análise de disponibilidade com base em RBD não é adequada quando existe compartilhamento de recursos de proteção, Zhou et al. [ZHO07] desenvolveram o conceito de indisponibilidade equivalente de caminhos. Em seu modelo, eles assumem que o caso de falha dupla domina a indisponibilidade caminho, e levam em conta a quantidade de tráfego de serviço não-restaurado devido às falhas duplas. O esquema de resiliência proposto adota uma regra para determinar uma sequência de alocação, através de prioridades, ao definir a ordem com a qual as conexões podem acessar a capacidade reservada remanescente. Para determinar o tráfego de serviço não restaurado em um determinado enlace devido à ocorrência de duplas falhas, um procedimento em dois passos é considerado. O passo 1 define as rotas de proteção de cada conexão assumindo uma determinada regra de atribuição, tanto para redes 1+1 dedicadas como para redes compartilhadas. Após assumir uma sequência de alocação para as conexões, no passo 2 realiza-se a busca por enlaces que afetam a restauração de uma conexão devido à insuficiência de capacidade reservada. Tal fato acontece quando duas falhas de enlace interrompem caminhos de serviço de duas conexões diferentes que compartilham parte de seus caminhos de proteção. Se a falha dupla causa perda de tráfego na conexão considerada, o enlace em falha, pertencente ao caminho de serviço da outra conexão, deve ser levado em conta no RBD equivalente da conexão. A contribuição da dupla falha para a indisponibilidade da conexão assume um valor de 0,5.

De modo alternativo, Mello et al. [MEL05] introduziram um modelo baseado em uma cadeia de *Markov* de tempo contínuo para calcular a disponibilidade de conexões em esquemas de resiliência fim-a-fim compartilhados. Os autores conduziram um estudo onde a cadeia de *Markov* é limitada a sequências de no máximo duas falhas e o trabalho apresentado na presente tese faz uma extensão do seu uso para uma quantidade maior de falhas (ver seção 6). Devido à importância de tal estudo para o modelo de disponibilidade, o mesmo foi discutido em detalhes no capítulo 4. Com base em tal método, a mesma equipe de pesquisa propôs um algoritmo de provisionamento para caminhos fim-a-fim compartilhados em redes ópticas [PEL05].

Kantarci et al. [KAN09] usaram o modelo de *Markov* proposto em [MEL05] para desenvolver dois esquemas dinâmicos de provisionamento de conexões em redes ópticas que levam em conta a disponibilidade. Nos esquemas clássicos, os custos dos enlaces são atualizados conforme as conexões são estabelecidas. Um custo infinito é atribuído para um enlace se ele não tem mais recursos disponíveis para proteção ou se ele pertence a um caminho de serviço. Se existe um comprimento de onda reservado para proteção, o custo é degradado para um valor desprezível. O custo é mantido se nenhuma das condições anteriores for satisfeita. Os esquemas de provisionamento propostos organizam as conexões em classes de disponibilidade, de acordo com a previsão do grau de compartilhamento possível para uma determinada classe. Uma função baseada no grau de compartilhamento de recursos e na disponibilidade média das conexões da classe calcula a previsão do grau de compartilhamento possível para uma classe. O custo do enlace que tiver um comprimento de onda reservado não é mais degradado por um valor desprezível, mas sim pelo inverso do grau de compartilhamento da classe. No segundo esquema proposto o grau de compartilhamento é calculado enlace a enlace.

Zhang et al. [ZHA07] desenvolveram um outro modelo baseado em cadeia de *Markov* para avaliar a disponibilidade de conexões em esquemas de resiliência fim-a-fim compartilhados, cujo desenvolvimento levou em consideração os seguintes pontos: (i) se o compartilhamento se dá através de caminhos de proteção únicos ou através de um *pool* de caminhos de proteção; (ii) se a estratégia para a restauração do tráfego for reversível, isto é, o tráfego é re-comutado para o caminho principal quando a falha for restaurada; ou não

reversível, ou seja, o tráfego de serviço permanece fluindo através do caminho de proteção; e (iii) para a estratégia reversível, a recuperação pode ser ativa (os recursos de proteção liberados são usados para restaurar o caminho de serviço de outras conexões) ou passiva. O modelo de disponibilidade desenvolvido calcula a probabilidade condicional de que uma conexão tenha sucesso em obter os recursos de proteção em uma situação de contenção (isto é, mais de um caminho competindo pelo recurso). Um modelo de Markov em tempo contínuo para a estratégia reversível ativa foi usado para derivar as equações de disponibilidade das conexões.

4.1.2) Proteção Online

No modelo *online* de proteção de caminho, os caminhos de proteção são configurados junto com os caminhos de serviço. Considera-se que as demandas por caminhos de serviço chegam uma de cada vez ao nó de origem, com a decisão do roteamento sendo tomada sem o conhecimento dos pedidos futuros. Se a rede não tiver largura de banda suficiente para acomodar os caminhos de serviço e proteção, o pedido é rejeitado. As principais propostas para os modelos de proteção de caminho tinham por objetivo melhorar a eficiência da rede protegida realizando o compartilhamento dos recursos reservados para a proteção. A idéia básica é considerar um cenário onde uma ou pouquíssimas falhas simultâneas podem ocorrer. Na verdade a hipótese subjacente é que a probabilidade de ocorrência de *múltiplas falhas simultâneas* é muito baixa e tais eventos *podem ser desconsiderados*. Uma redução significativa da capacidade de proteção pode então ser obtida com o compartilhamento dos recursos reservados para proteção, desde que protejam diferentes locais da rede.

Chujo et. al. [CHU91] apresenta uma heurística baseada em proteção de caminho para atribuir a capacidade reservada junto com um algoritmo distribuído para recuperação em tempo real (*online*). O algoritmo foi implementado com uma atribuição inicial usando caminhos de serviço mais curtos. Os caminhos alternativos são examinados em uma tentativa de reduzir a capacidade reservada total. O procedimento é repetido até alcançar um objetivo pré-especificado.

As redes de telecomunicações necessitam de esquemas de recuperação que ofereçam técnicas que reduzam o tempo de interrupção de serviço. As soluções com base no modelo de

recuperação compartilhada de caminho fornecem soluções atrativas em tal contexto. Entretanto, o uso eficiente da capacidade para a recuperação compartilhada depende fortemente do procedimento de seleção de caminhos de recuperação. O artigo [GUA02] propõe um algoritmo de seleção de caminho para a recuperação de conexões com larguras de banda compartilhadas em uma arquitetura inteiramente distribuída GMPLS (*Generalized Multi-protocol Label Switching*). Também descreve como estender os protocolos de sinalização GMPLS para coletar eficientemente a informação necessária. Para avaliar o desempenho do algoritmo, o resultado é comparado através de simulação com outros dois algoritmos conhecidos em um *backbone* de rede interurbana típica. O estudo propõe uma métrica para medir a eficiência da capacidade de recuperação denominada *restoration overbuild*, isto é, a capacidade extra exigida para atender o objetivo de recuperação da rede como um percentual da capacidade da rede sem a recuperação. Os resultados da simulação mostram que o algoritmo usa significativamente menos *restoration overbuild* (63-68%) comparado com os dois algoritmos mencionados (83-90%).

O artigo [GUA08] apresenta novos algoritmos para roteamento dinâmico (*online*) de caminhos recuperáveis com largura de banda garantida. O artigo oferece uma solução para a gerência eficiente da distribuição de largura de banda. Tal trabalho é uma extensão do artigo [GUA02], e assume que os pedidos de conexão chegam um por vez e devem ser roteados sem o conhecimento antecipado das chegadas futuras. A solução permite o compartilhamento de banda entre os caminhos de proteção dos diferentes e dos mesmos caminhos de serviço, ou seja, tanto intra-compartilhamento como inter-compartilhamento, com uma garantia de proteção de largura de banda para qualquer falha única de nó ou de enlace. Também é proposto um algoritmo para a seleção de caminho de proteção com as extensões de sinalização associadas à distribuição e coleta de informações adicionais. Para avaliar os esquemas, foram comparados através de simulação com a proposta de rerroteamento rápido MPLS básico mostrado na IETF RFC 4090, em duas redes. Os resultados da simulação mostram que usando tal esquema de gerência de largura de banda é possível reduzir significativamente o *overbuild* de recuperação de aproximadamente 250% para cerca de 100%, a seleção otimizada de caminhos de proteção pode reduzir ainda mais o *overbuild* de recuperação para aproximadamente 60%.

4.1.2.1) Múltiplas Falhas

A maioria dos esquemas mencionados anteriormente assume que a proteção é provida para falha em um único enlace. O trabalho [LUM01] avalia a robustez dos esquemas de recuperação de enlace na presença de falhas em múltiplos enlaces. Uma classificação hierárquica das razões pelas quais os algoritmos de recuperação falham ao garantir a recuperação de falhas em múltiplos enlaces é fornecida e ilustrada para algumas redes padrão. Em [RAM03], os autores concluíram que proteção de caminho é mais sujeita às falhas de múltiplos enlaces do que a recuperação de enlace e para falhas de múltiplos enlaces a proteção dedicada tem mais resiliência do que a proteção compartilhada.

Os estudos apresentados a seguir tratam do problema para redes WDM sujeitas a múltiplas falhas através de esquemas de resiliência do tipo fim-a-fim compartilhado, para cenários de alocação dinâmica [XIA07], [CHE08], [AMI11] e [GUO09]. Em [XIA07], para proteger a rede contra até F falhas de enlace, um caminho de serviço e F caminhos de proteção (disjuntos em enlace) são escolhidos na chegada de uma nova conexão ao nó de origem. Os caminhos são selecionados a partir de uma lista de rotas pré-calculadas de modo a minimizar a largura de banda adicional necessária em cada enlace. Em cada enlace do caminho de serviço será necessário reservar uma largura de banda adicional igual à necessidade de banda da conexão. Para calcular os caminhos de proteção o custo de cada enlace é atualizado levando-se em conta a quantidade de banda anteriormente reservada e a quantidade requisitada. Se a quantidade necessária for menor do que a quantidade já reservada, o custo de utilização do enlace é nulo. Se for maior, mas ainda há recursos reservados suficientes para acomodar a conexão, então o custo é o incremento de banda necessário no enlace. Se for maior e não houver recursos suficientes, o custo será um valor muito grande. Após a atribuição do custo dos enlaces, o algoritmo percorre a lista de caminhos pré-calculados escolhendo aquele que ocupar menor capacidade adicional com base no cálculo realizado pelo procedimento anterior. Devido à complexidade computacional do procedimento, os autores propõem uma heurística gulosa para tratar o problema.

O artigo [XIA07] considera uma rede G com L enlaces bidirecionais e N nós. F é o número de falhas simultâneas de enlace. Com a finalidade de prover largura de banda com 100% de garantia para um tráfego dinâmico (*online*), quando um novo pedido de conexão

chega até um nó de ingresso, tal nó de ingresso escolhe um caminho de serviço (*Working Path*) e *F* caminhos de proteção disjuntos em enlace (*Backup Path*) que percorre o grafo até o nó de egresso desejado a partir de uma tabela de roteamento calculada antecipadamente. Com a finalidade de prover 100% de garantia para as conexões da rede, a largura de banda reservada no enlace contra *F* falhas de enlace aleatórias e simultâneas, deve ser suficiente para atender o pior caso. O objetivo é encontrar um caminho de serviço e *F* caminhos de proteção a partir de uma tabela de roteamento calculada antecipadamente com o mínimo de largura de banda total adicional para atender a conexão. O tempo de cálculo aumenta exponencialmente com o número *F* de falhas simultâneas de enlace. Para resolver tal problema é utilizado um algoritmo guloso (*greedy*) para calcular a largura de banda de proteção no enlace. Foram simulados diferentes esquemas de roteamento e alocação de largura de banda em três topologias com grau médio 5, 4 e 3 respectivamente. Os esquemas maximizam o compartilhamento de larguras de banda e mostram o resultado em um tempo de cálculo satisfatório. As simulações mostraram que o algoritmo poupou mais largura de banda total do que o algoritmo ESPI (*Extended Sharing with Partial Information*) e poupou 32% da largura de banda total consumida pela utilização do algoritmo *NS* (caminho de serviço sem proteção compartilhada).

O artigo [CHE08] propõe duas heurísticas para calcular rotas e alocar largura de banda para o esquema de proteção, nas quais os caminhos de serviço e de proteção são determinados a partir dos *k* caminhos mais curtos. Na primeira heurística, os caminhos de serviço e de proteção são calculados de modo a se obter o consumo mínimo da largura de banda total, enquanto que na segunda o objetivo é satisfazer as restrições dos comprimentos dos caminhos. O algoritmo é acionado na chegada de um novo pedido de conexão com requisito de largura de banda conhecido. Inicia procurando os caminhos mais curtos (disjuntos ou parcialmente disjuntos) entre a origem e o destino da conexão, a partir de uma tabela de rotas alternativas pré-calculadas, sendo o mais curto o caminho de serviço. A necessidade adicional de largura de banda para os enlaces do caminho de serviço da nova conexão é igual à necessidade da conexão. Para os enlaces dos caminhos de serviço o consumo de largura de banda adicional é calculado emulando-se as falhas possíveis e incrementando-se a capacidade reservada para proteção nos enlaces correspondentes.

O estudo em [AMI11] descreve dois algoritmos, um para roteamento e outro para alocação de comprimentos de onda. De acordo com o algoritmo de roteamento, para um determinado par de nós (origem e destino) são calculados todos os caminhos possíveis, que são arranjados em uma ordem de preferência de acordo com o seu comprimento, do mais curto para o mais longo. As falhas de enlace são identificadas e verificadas em todos os caminhos, do mais curto para o mais longo: se a falha não afetar o caminho, então ele é selecionado. Se a falha afetar o caminho, então ele é descartado e o próximo caminho na ordem de preferência é verificado. Tal processo é repetido até que o caminho se demonstre resiliente com relação à quantidade máxima de falhas. Com a confirmação do caminho, seus enlaces utilizarão os comprimentos de onda disponíveis na rede. O algoritmo de atribuição de comprimentos de onda é acionado após a ocorrência de uma falha. O algoritmo verifica quais comprimentos de onda estão disponíveis e então organiza um arranjo com todos os comprimentos de onda atribuindo uma prioridade a cada um deles. Quando o algoritmo for chamado, ele verifica se é possível estabelecer um caminho livre de falha para a conexão. Caso não seja possível a conexão fica em estado de espera até que seja possível, quando então o algoritmo atribui o comprimento de onda de menor prioridade no arranjo.

O artigo [GUO09] propõe um mecanismo de recuperação em escala para estabelecer o roteamento e a proteção. O caminho de serviço é calculado com base no menor caminho e no balanceamento de carga da rede. Evita-se o aparecimento do estado de desbalanceamento fazendo com que o caminho de serviço utilize os enlaces que possuam a maior quantidade de recursos livres. Então, o custo dos enlaces é atualizado de acordo com o seguinte critério: se não houver comprimentos de onda livres no enlace o custo recebe um valor muito alto. Caso contrário o custo corrente é atenuado pela proporção entre a quantidade de comprimentos de onda usados na fibra e a quantidade máxima de comprimentos de onda por fibra. Durante o processo de cálculo do caminho de proteção o não balanceamento é evitado ajustando-se o custo do enlace de acordo com o seguinte procedimento. Procura-se entre os demais enlaces aquele com a maior quantidade de recursos de proteção reservados necessários no enlace analisado. Se a maior quantidade encontrada for maior do que a soma entre a quantidade de comprimentos de onda livres no enlace e a quantidade de comprimentos de onda de proteção reservados no enlace, atribui-se um valor muito alto para o custo do enlace. Se a maior quantidade encontrada for menor ou igual do que a soma entre a quantidade de comprimentos

de onda livres no enlace e a quantidade de comprimentos de onda de proteção reservados no enlace, e também for maior do que a quantidade de comprimentos de onda de proteção reservados no enlace, o custo não é alterado. Caso contrário, o custo do enlace é atenuado por um fator α (uma constante positiva). Para o cálculo dos caminhos de serviço e proteção, é utilizado o seguinte procedimento: (i) Gera-se aleatoriamente um grupo *N* de solicitações de conexão. (ii) Sorteia-se uma das solicitações de conexão a ser alocada na rede. (ii) Procura-se o caminho de serviço, se não for encontrado, a solicitação da conexão deve ser bloqueada. (iv) Decrementa-se uma conexão do grupo *N* e sorteia-se uma nova solicitação. O procedimento é repetido até a última solicitação do grupo. (v) Com as conexões alocadas, gera-se aleatoriamente uma combinação de falhas de enlace com a quantidade de falhas igual àquela que se pretende proteger e para cada conexão ainda não verificada, se um dos enlaces em estado de falha for utilizado pelo caminho de serviço, deve ser feita a comutação para o caminho de proteção e a liberação dos enlaces não utilizados no caminho de serviço. Pode haver falhas que afetem o caminho de serviço e de proteção, então os comprimentos de onda do caminho de serviço são liberados e uma nova rota é calculada para o tráfego e um novo teste de falhas é executado.

Como observado, os estudos levam em conta a disponibilidade das conexões e assumem a hipótese simplificadora de haver no máximo duas falhas simultâneas em seus modelos e algoritmos de resiliência. Por outro lado, os estudos para múltiplas falhas não realizam a alocação de recursos e roteamento levando em conta um objetivo pré-definido de disponibilidade. Tanto quanto foi possível investigar, o estudo apresentado na presente tese é o único que leva em consideração as duas questões simultaneamente.

Capítulo 5

Método Proposto Para o Planejamento de Rede WDM Resiliente

5.1) Introdução

Uma rede WDM transparente consiste de nós de comutação óptica interligados por fibras ópticas, onde caminhos de comunicação óptica (*lightpaths*) são configurados para oferecer suporte a conexões entre nós terminais. Cada caminho óptico está associado a um comprimento de onda, e pode atingir atualmente taxas de transmissão da ordem de 160 Gbps [WUT08], [AKI09], e podem ser modulados de forma independente com o objetivo de acomodar dados em diferentes formatos e taxas de transmissão. Para estabelecer um caminho óptico é necessário alocar e rotear um comprimento de onda para cada enlace da rota definida. Tal problema é conhecido como o problema de roteamento e alocação de comprimento de onda RWA (*Routing and Wavelength Assignment*). Após o estabelecimento da conexão, os comprimentos de onda alocados na rota selecionada ficam reservados exclusivamente ao caminho óptico até a finalização da conexão.

A falha de um enlace de fibra resulta na interrupção de todos os caminhos ópticos que utilizam o enlace. Considerando que cada caminho óptico no estado operacional transfira seus dados a uma taxa de dezenas de gigabits por segundo, uma falha pode resultar em uma grande perda de dados. Embora os protocolos de camadas mais elevadas incluam procedimentos de recuperação de falhas de enlace, o tempo de recuperação é ainda significativamente grande (na ordem segundos), e espera-se que os tempos de recuperação na camada óptica sejam da ordem de 50 milissegundos [HUA04], [ZHA07]. É desejável considerar os mecanismos de recuperação na camada óptica pelas seguintes razões [GER00]: a camada óptica pode multiplexar de forma eficiente os recursos de proteção (tais como, comprimento de onda e

fibras reservadas) entre as várias aplicações das camadas mais altas da rede; e a resiliência na camada óptica provê proteção para os protocolos das camadas mais altas que podem não ter proteção interna.

A rede apresentada no presente trabalho é modelada por um conjunto de nós, cada um correspondendo a um OXC, interconectados por um conjunto de cabos (enlaces) contendo uma ou mais fibras. Considera-se que todos os nós podem ser origem e destino de tráfego, sendo conhecida a demanda entre quaisquer dois nós. Cada demanda poderá ser atendida por um conjunto de conexões, todas com mesma origem e destino. Cada conexão tem um caminho óptico de serviço e um conjunto de caminhos ópticos de proteção. Para proteger uma conexão contra múltiplas falhas, o modelo proposto seleciona, para cada conexão, um caminho óptico de serviço e F_{max} caminhos ópticos de proteção, onde F_{max} é a quantidade de falhas simultâneas a ser considerada. Assim, F_{max} +1 caminhos ópticos serão selecionados e dispostos em uma sequência de ativação, onde o primeiro caminho óptico da lista é o caminho óptico de serviço, e os demais são caminhos ópticos de proteção. Cada conjunto de F_{max} +1 caminhos ópticos com a respectiva sequência de ativação suporta uma conexão. No modelo de rede considerado, o nó de origem da conexão é responsável pela comutação para o caminho óptico de proteção, ou seja, quando uma conexão é interrompida, o nó de origem inicia o processo de restabelecimento da conexão, utilizando o próximo caminho óptico de proteção. O método proposto é denominado MSB (*Multiple Shared Backups*).

O método MSB propõe dois algoritmos, um para selecionar os caminhos para cada conexão, e outro para calcular a respectiva indisponibilidade. A partir de um conjunto de k menores caminhos, o primeiro algoritmo seleciona os caminhos de cada conexão e a sua ordem de ativação. O segundo algoritmo usa o método proposto em [MEL05], estendido para múltiplas falhas, para calcular a indisponibilidade de cada conexão (horas por ano). Os resultados dos dois algoritmos são utilizados durante o procedimento de planejamento visando atender a demanda entre todos os pares de nós, garantindo um nível de disponibilidade pré-definido, utilizando a menor quantidade de recursos possível.

As decisões do algoritmo de seleção são tomadas levando-se em conta os estados de falha da rede. De modo a minimizar a quantidade de recursos necessária, a seleção dos caminhos é realizada procurando-se manter a rede com o melhor balanceamento de carga possível. O algoritmo de balanceamento assume que quando ocorre uma falha de enlace, o tráfego existente em cada caminho interrompido deve necessariamente ser comutado para o

próximo caminho de proteção na sequência de ativação. Não sendo isso possível, o tráfego da conexão é interrompido até que haja a recuperação de um enlace que torne a conexão disponível. O sucesso da comutação de um caminho depende da existência de capacidade reservada suficiente nos enlaces percorridos pelo próximo caminho de proteção na sequência de ativação. Em cada estado da rede é conhecida a probabilidade com a qual a tentativa de recuperação de uma determinada conexão interrompida será malsucedida. O somatório das probabilidades de insucesso em cada estado da rede corresponde à indisponibilidade da conexão.

O algoritmo alcança seu objetivo de minimizar o uso de recursos procurando o balanceamento de carga da rede em qualquer estado de falha. Para obter um balanceamento de carga ótimo, cada conexão teria que possuir uma tabela indicando o caminho óptico de proteção a ser comutado, com uma entrada para cada falha de enlace, o que ocasionaria uma necessidade muito grande de espaço para as informações durante o cálculo e durante a comutação. O método MSB possibilita a comutação para os caminhos ópticos de proteção sem o conhecimento do enlace que falhou, promovendo um balanceamento aproximado. O balanceamento é alcançado considerando-se apenas a combinação de falhas, desconsiderando a ordem das mesmas. As combinações de falhas conduzem a um estado que caracteriza a utilização de mais recursos reservados (*wavelengths*) em alguns enlaces. A decisão de escolher quais enlaces que receberão recursos reservados é um procedimento que considera as disponibilidades dos mesmos. Um aspecto que interfere na escolha da ordem de ativação de caminhos ópticos de proteção para cada conexão, é que para uma mesma conexão, cada enlace em estado de falha do caminho atualmente ativo conduz a um balanceamento diferente. O próximo caminho óptico de proteção na lista é selecionado levando-se em conta o estado de falha com maior probabilidade de ocorrência.

O procedimento de balanceamento é executado considerando-se os conjuntos de estados de falha, de zero até a quantidade máxima de falhas F_{max}. O primeiro conjunto contém apenas o estado com nenhuma falha, o segundo contém os estados com apenas uma falha, o terceiro contém os estados com sequências de duas falhas, e assim por diante. A aplicação do procedimento de balanceamento de carga no estado com nenhuma falha resulta na definição do caminho de serviço, a aplicação no conjunto de estados referentes a uma falha, resulta na seleção do primeiro caminho de proteção da sequência, e assim sucessivamente. O balanceamento de carga entre um conjunto de alternativas de caminhos é

obtido avaliando-se todas as combinações possíveis envolvendo os tais caminhos, e escolhendo-se aquela que reduz a diferença entre a carga do enlace mais carregado em relação à carga dos enlaces menos carregados. Tal combinação de caminhos deve ser avaliada para cada estado do conjunto de estados que está sendo analisado. A análise de todas as combinações provoca uma explosão combinatória e o método MSB propõe uma heurística para tratar a questão.

A aplicação do procedimento de balanceamento de carga no estado com nenhuma falha é realizado entre os caminhos disjuntos do conjunto dos *k* menores caminhos. Ao se avaliar a rede em cada estado com uma falha de enlace, cada conexão que tiver o seu caminho ativo interrompido terá um conjunto de caminhos de proteção candidatos. Assim, o balanceamento é obtido avaliando-se, para cada estado, todas as combinações possíveis entre os caminhos de proteção. Em uma determinada conexão, quando um caminho ativo é interrompido em mais de um estado, usa-se aquele caminho de proteção produzido pelo estado com maior probabilidade de ocorrência.

No algoritmo de cálculo da indisponibilidade das conexões considera-se que a taxa de ocorrência e de recuperação de falhas de cada enlace são conhecidas. Ao ser estabelecida a quantidade máxima de falhas simultâneas de enlaces na rede, a probabilidade de cada sequência de falhas pode ser calculada através da extensão do método proposto em [MEL05] para múltiplas falhas descrito na seção 3.2. Cada sequência de falhas estabelece um estado na rede. Um conjunto de estados da rede pode ser caracterizado por ter em comum uma mesma sequência de falhas anterior (estado anterior). Para um conjunto de estados da rede, o algoritmo efetua o cálculo ao percorrer todos os estados da cadeia de *Markov* que apresentam um mesmo estado anterior, ou seja, um conjunto completo por vez. Um novo estado da rede é obtido quando ocorre uma falha, e o número do novo enlace é concatenado à última combinação ou a uma das combinações anteriores (uma nova sequência será iniciada). Tal procedimento permite que as seguintes informações calculadas em estados anteriores possam ser armazenadas: o caminho ativo atual em cada conexão e a capacidade reservada em todos os enlaces remanescentes. Tais informações permitem atribuir capacidade reservada ao próximo caminho de proteção para cada conexão interrompida no atual estado da rede. Assim, é possível analisar a existência dos recursos reservados após a ocorrência de uma falha qualquer, e por outro lado, efetuar o reparo dos recursos que permitem que a rede retorne a um dos estados anteriores.

Conhecida a forma pela qual os estados da cadeia de *Markov* serão percorridos durante o cálculo e a probabilidade de ocorrência de cada estado, resta conhecer os efeitos causados pelo compartilhamento de recursos da rede. Significa dizer que, embora haja caminho de proteção disponível em um determinado estado da rede, se houver recursos reservados insuficientes, nem todas as demandas interrompidas pela falha encontrarão recursos reservados disponíveis. As demandas participarão, com igualdade de condições, de uma disputa por recursos reservados estabelecida por ordem de chegada. Algumas das tentativas de comutação serão malsucedidas e tornarão indisponível uma determinada conexão. Tal comportamento conduzirá à formação de um fator de rejeição (*FR*) da respectiva conexão para todo estado da rede em que ela é interrompida. A probabilidade de uma conexão se tornar indisponível em um determinado estado da rede é encontrada executando-se o produto entre a probabilidade de ocorrência do estado e o fator de rejeição da tal conexão durante a ocorrência do referido estado. Ao ser efetuada a soma da probabilidade de uma determinada conexão se tornar indisponível durante a ocorrência de cada estado da rede, é obtido o valor da indisponibilidade da referida conexão na rede.

O objetivo do método MSB é planejar a rede selecionando a quantidade necessária de caminhos para cada conexão de modo que sua indisponibilidade não ultrapasse um valor máximo estabelecido. O resultado determina a quantidade mínima de caminhos para cada conexão da rede de modo a atender aos requisitos estabelecidos. Na primeira fase do planejamento, o algoritmo de seleção de caminhos é utilizado considerando que os enlaces da rede apresentam capacidade ilimitada, ou seja, para todo estado da rede existe capacidade disponível para a comutação de um caminho de proteção, não havendo compartilhamento de recursos. A primeira fase é interativa, sendo que a cada interação são identificadas as conexões com indisponibilidade abaixo do que se espera, significando que a quantidade de caminhos de proteção excede o necessário para prover a disponibilidade desejada. A cada ciclo é realizado um ajuste em tais conexões, decrementando-se em uma unidade a quantidade correspondente de caminhos de proteção. Ao término da fase, algumas conexões terão indisponibilidade superior ao estabelecido. Um novo ajuste é realizado, incrementando-se em uma unidade a quantidade de caminhos de proteção para tais conexões. O algoritmo de seleção de caminhos é executado uma última vez com a configuração final, o mesmo acontece para o algoritmo de cálculo de indisponibilidade, que é executado na última vez considerando

capacidade dos enlaces resultante do último ciclo da primeira fase, e levando em conta o compartilhamento de recursos.

5.2) Algoritmo de Seleção de Caminhos

O algoritmo de seleção de caminhos escolhe, a partir do conjunto dos *k* caminhos mais curtos, uma lista de caminhos com tamanho igual à máxima quantidade de falhas (F_{max}) tratadas mais 1, ordenada segundo a sequência em que devem ser ativados em caso de falha utiliza como parâmetros de entrada uma lista de caminhos candidatos para cada conexão, organizada em subconjuntos de caminhos ópticos, o primeiro contendo os caminhos ópticos candidatos disjuntos, e os demais contendo os caminhos ópticos candidatos parcialmente disjuntos.

Seja *C* o conjunto de todas as conexões necessárias para atender todas as demandas. Seja L_k^c uma lista que contém o conjunto dos *k* caminhos mais curtos para a conexão *c*. A partir de cada lista L_k^c, o objetivo é criar uma lista L_p^c, que contém o conjunto de caminhos ópticos candidatos para proteger a conexão *c*, organizados em subconjuntos de caminhos, ou seja, $L_p^c = \{L_p^c(1), L_p^c(2), \dots, L_p^c(|L_p^c|)\}$. O subconjunto $L_p^c(1)$ contém os menores caminhos disjuntos em enlace e os demais subconjuntos contêm caminhos parcialmente disjuntos em relação aos caminhos incluídos em $L_p^c(1)$. Para construir $L_p^c(1)$, L_k^c é ordenada do menor para o maior caminho, procurando-se então em L_k^c o menor caminho que possua pelo menos um caminho disjunto (p_{11}). $L_p^c(1)$ é então formado incluindo-se p_{11} e todos os caminhos de L_k^c que sejam disjuntos em relação a p_{11}, e mutuamente disjuntos entre si. Ao final de tal procedimento, $L_p^c(1)$ conterá $n_1 = |L_p^c(1)|$ caminhos disjuntos entre si, ou seja, $L_p^c(1) = \{p_{11}, p_{12}, \dots, p_{1n_1}\}$. Todos os caminhos contidos em $L_p^c(1)$ farão parte da solução encontrada pelo algoritmo de proteção de caminhos, sendo que um deles será o caminho de serviço.

Se $n_1 \leq F_{max}$, será necessário construir $L_p^c(2)$ que deve conter os menores caminhos que protegem a conexão contra as falhas ocorridas nos caminhos de $L_p^c(1)$. Para construir $L_p^c(2)$, forma-se os conjuntos de enlaces de cada caminho pertencente a $L_p^c(1)$. Sejam $E_1, E_2, \dots, E_{n_1}$ os conjuntos de enlaces de $p_{11}, p_{12}, \dots, p_{1n_1}$, respectivamente. O conjunto de tuplas que correspondem às falhas simultâneas que interrompem os n_1 caminhos de $L_p^c(1)$ é dado pelo produto carteziano $E_1 \times E_2 \times \dots \times E_{n_1}$. Para cada tupla deve ser encontrado um caminho parcialmente disjunto que não utilize os enlaces da tupla (sempre será possível desde

que o nó não seja desconectado). Os caminhos encontrados formarão $L_p^c(2)$. O algoritmo de seleção de caminhos escolherá apenas um dos caminhos pertencentes a $L_p^c(2)$, que vai proteger a conexão c contra a n_1-ésima falha. Assim, se $n_1 = F_{max}+1$ o procedimento de construção de L_p^c terminou, caso contrário será necessário construir $L_p^c(3)$, segundo o mesmo procedimento usado para construir $L_p^c(2)$, e assim sucessivamente até que a quantidade de subconjuntos incluídos na lista L_p^c seja $|L_p^c| = \left(F_{max} - min[\mathrm{F_{max}}, \left|\mathrm{L_p^c}(1)\right| - 1]\right) + 1$.

O algoritmo trata sequencialmente cada uma das quantidades de falha (de 0 até F_{max}), tratando cada uma das posições de L_p^c. O resultado do algoritmo de seleção de caminhos é a lista L_u^c contendo, para cada conexão, o conjunto de caminhos organizados na sequência de ativação. O conjunto de todas as conexões com os respectivos caminhos na ordem de ativação é $L_u = \{L_u^c | c \in C\}$.

Para a definição do caminho de serviço (nenhuma falha) o procedimento a seguir é executado. Se houver um caminho de comprimento unitário em $L_p^c(1)$ ele é escolhido como caminho de serviço para a conexão c. O caminho de serviço para as conexões que não possuem caminhos unitários, é escolhido considerando-se, para todas as conexões, todos os caminhos em $L_p^c(1)$, mais os caminhos de serviço já determinados (os de tamanho 1), executando-se o procedimento de balanceamento de carga (ver seção 5.2.1). Para a definição do primeiro caminho de proteção, o algoritmo utiliza os caminhos disjuntos em $L_p^c(1)$ ainda não utilizados em cada conexão. Para a definição do segundo caminho de proteção, o algoritmo utiliza os caminhos disjuntos ainda não utilizados (quando existentes) ou os caminhos de $L_p^c(2)$, e assim sucessivamente. A cada passo o procedimento de balanceamento determina o caminho a ser usado.

A Tabela 1 mostra um exemplo para a escolha dos caminhos de serviço e de proteção de uma conexão (c) entre os nós 2 e 4 da rede exemplo mostrada na Figura 5.1, para $F_{max} = 4$.

Para o subconjunto $L_p^{(2,4)}(1)$ são escolhidos todos os menores caminhos disjuntos entre os nós da conexão, ou seja, $L_p^{(2,4)}(1) = \{\{2,3\},\{8,4\},\{1,6,9\}\}$.

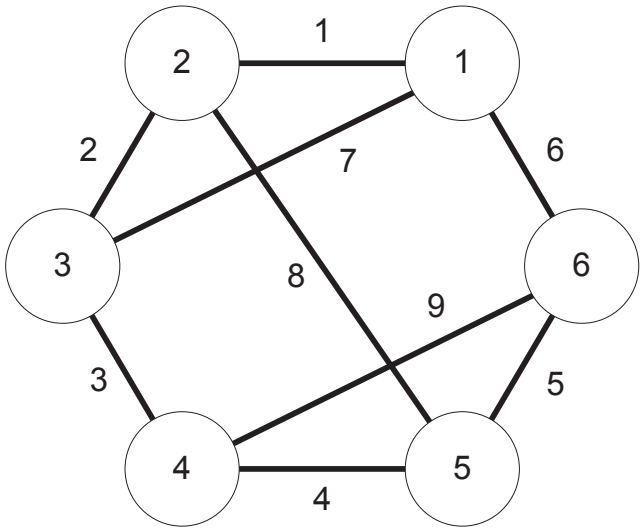


Figura 5.1: Um exemplo de rede para a organização da lista de caminhos de ativação para a conexão *c* (entre os nós 2 e 4).

O conjunto $L_p^{(2,4)}(2)$ é formado considerando-se os caminhos parcialmente disjuntos em relação aos caminhos em $L_p^{(2,4)}(1)$ considerando-se apenas os menores, com a mesma quantidade de enlaces. No exemplo, os caminhos selecionados são {1,7,3} e {8,5,9}, ambos com 3 enlaces. Portanto, $L_p^{(2,4)}(2) = \{\{1,7,3\},\{8,5,9\}\}$.

Do mesmo modo, cada caminho parcialmente disjunto no subconjunto $L_p^{(2,4)}(3) = \{\{1,6,5,4\},\{2,7,6,9\}\}$ tem a mesma quantidade mínima de enlaces.

Em $L_p^{(2,4)} = \{\{\{2,3\},\{8,4\},\{1,6,9\}\},\{\{1,7,3\},\{8,5,9\}\},\{\{1,6,5,4\},\{2,7,6,9\}\}\}$ está o conjunto de caminhos obtido no final do procedimento. Para simplificar a apresentação da tabela, os subconjuntos de caminhos candidatos obtidos serão denominados como segue: $L_p^{(2,4)} = \{\{p_{11}, p_{12}, p_{13}\},\{p_{21}, p_{22}\},\{p_{31}, p_{32}\}\}$.

O algoritmo é executado uma única vez para selecionar o caminho de serviço de cada conexão, através da análise do balanceamento de carga, sem haver falha na rede. A primeira coluna da tabela mostra que o primeiro caminho selecionado para a conexão foi p_{12}, aquele que proporciona o melhor balanceamento de carga possível. Observa-se que o balanceamento de carga leva em conta todos os caminhos disjuntos em $L_p^c(1)$ de cada conexão, ou seja, todos os caminhos em $\bigcup_{c \in C} L_p^c(1)$. O caminho de serviço selecionado para cada conexão é excluído do subconjunto $L_p^c(1)$ correspondente.

Tabela 1: Passos para a organização da lista de caminhos de ativação para a conexão (2,4).

$L_p^{(2,4)} = \{\{\{2,3\},\{8,4\},\{1,6,9\}\},\{\{1,7,3\},\{8,5,9\}\},\{\{1,6,5,4\},\{2,7,6,9\}\}\}$					
Falhas	0	1	2	3	4
Subconjunto de caminhos candidatos	$\{p_{11}, p_{12}, p_{13}\}$	$\{p_{11}, p_{13}\}$	$\{p_{13}\}$	$\{p_{21}, p_{22}\}$	$\{p_{31}, p_{32}\}$
Caminhos já selecionados	Ø	$\{p_{12}\}$	$\{p_{12},p_{11}\}$	$\{p_{12},p_{11},p_{13}\}$	$\{p_{12},p_{11},p_{13},p_{22}\}$
Enlaces dos caminhos já selecionados	Ø	{8,4}	{{8,4}, {2,3}}.	{{8,4}, {2,3}, {1,6,9}}.	{{8,4},{2,3}, {1,6,9},{8,5,9}}.
Combinação de falhas de enlaces - Caminho sugerido pelo balanceamento de carga	Ø	{8} – p_{11}; {4} – p_{13}.	{8,2}– p_{13}; {8,3}– p_{13}; {4,2}– p_{13}; {4,3}– p_{13}.	{8,2,1} - #; {8,2,6} - p_{21}; {8,2,9} - p_{21}; {8,3,1} - #; {8,3,6} - #; {8,3,9} - #; {4,2,1} - p_{22}; {4,2,6} - p_{22}; {4,2,9} - p_{21}; {4,3,1} - p_{22}; {4,3,6} - p_{22}; {4,3,9} - #.	{8,2,1,5} - #; {8,2,1,9} - #; {8,2,6,5} - #; {8,2,6,9} - #; {8,2,9,5} - #; {8,3,1,5} - p_{32}; {8,3,1,9} - #; {8,3,6,5} - #; {8,3,6,9} - #; {8,3,9,5} - #; {4,2,1,8} - #; {4,2,1,5} - #; {4,2,1,9} - #; {4,2,6,8} - #; {4,2,6,5} - #; {4,2,6,9} - #; {4,2,9,8} - #; {4,2,9,5} - #; {4,3,1,8} - p_{32}; {4,3,1,5} - p_{32}; {4,3,1,9} - #; {4,3,6,8} - #; {4,3,6,5} - #; {4,3,6,9} - #; {4,3,9,8} - #; {4,3,9,5} - #.
Caminho selecionado	p_{12}	p_{11}	p_{13}	p_{22}	p_{32}

A segunda coluna da tabela ilustra a seleção do primeiro caminho de proteção para a conexão (2,4), obtido avaliando-se a rede com uma falha de enlace, usando-se como opção os caminhos em $L_p^c(1)\backslash\{p_{12}\} = \{p_{11}, p_{13}\}$. Para cada estado de falha $\{i\}$ (que corresponde à falha do enlace *i*), haverá um conjunto diferente de conexões afetadas. Cada estado é avaliado segundo o procedimento de balanceamento de carga, considerando todas as conexões interrompidas, o qual sugerirá um caminho de proteção para cada uma. Para a conexão avaliada no exemplo, o único caminho que até então suporta a conexão, (p_{12}) seria interrompido apenas se um de seus enlaces (8 ou 4) fosse interrompido. Para a falha do enlace 8 o algoritmo de balanceamento de carga definiu o caminho p_{11} como a melhor opção de proteção, enquanto que para falha do enlace 4, o caminho p_{13} foi a melhor opção. O caminho p_{11} foi então escolhido como o caminho de proteção para a primeira falha da conexão observada, porque a probabilidade de falha do enlace 8 é maior do que a probabilidade de

falha do enlace 4. Como no momento não é o valor da probabilidade que importa, mas a proporção entre as probabilidades, a métrica usada é a razão entre a taxa de falha e a taxa de recuperação ($P_{\{i\}}$ = - log(λ_i/μ_i)). O logaritmo é usado para acelerar o cálculo no caso de mais de um enlace simultâneo porque permite que o resultado possa ser obtido através de uma soma, ao invés do produto das razões, da mesma maneira que [HUA04].

A terceira coluna da tabela ilustra a seleção do segundo caminho de proteção para a conexão *c*, obtido avaliando-se a rede com duas falhas de enlace, usando-se como opção um único caminho em $L_p^c(1)\backslash\{p_{12}, p_{11}\} = \{p_{13}\}$. Para cada estado de falha $\{i, j\}$ que corresponde à falha simultânea dos enlaces *i* e *j* (em qualquer ordem), haverá um conjunto diferente de conexões afetadas. Novamente, cada estado é avaliado segundo o procedimento de balanceamento de carga, considerando todas as conexões interrompidas, sugerindo um caminho de proteção para cada uma. Para a conexão avaliada no exemplo, os caminhos p_{12} e p_{11} suportam a conexão, e ambos seriam interrompidos quando alguma das combinações de falha de enlace mostradas na tabela ({8, 2}, {8, 3}, {4, 2} ou {4, 3}) ocorrer. No exemplo, para todas as combinações de falha, o algoritmo de balanceamento de carga definiu o caminho p_{13} como melhor opção (é o único), e ele foi então escolhido como o caminho de proteção para a segunda falha de enlace da conexão observada. Conforme explicado anteriormente, $P_{\{8,2\}}$ = - log(λ_8/μ_8) - log(λ_2/μ_2).

A quarta coluna da tabela ilustra a seleção do terceiro caminho de proteção para a conexão (2,4), obtido avaliando-se a rede com três falhas de enlace, através de um procedimento análogo. Observa-se que as opções são os caminhos em $L_p^c(2) = \{p_{21}, p_{22}\}$, já que o conjunto $L_p^c(1)$ está vazio. Observa-se ainda que o estado de falha considerado é $\{i, j, k\}$ e que nem todas as combinações de falhas possibilitam a existência de um caminho de proteção com a mínima utilização de recursos, o que é representado por "#".

A quinta coluna ilustra a seleção do quarto caminho de proteção para a conexão (2,4), obtido avaliando-se a rede com quatro falhas de enlace. Observa-se que as opções são os caminhos em $L_p^c(3) = \{p_{31}, p_{32}\}$, porque os caminhos no subconjunto $L_p^c(2)$ não foram previstos para proteger a quarta falha. Após a última execução do algoritmo, cada conexão terá uma lista de caminhos de proteção organizada por ordem de ativação (L_u^c). No exemplo, para a conexão analisada a lista é $L_u^{(2,4)} = \{\{8,4\}, \{2,3\}, \{1,6,9\}, \{8,5,9\}, \{2,7,6,9\}\}$, onde o primeiro é o caminho de serviço $\{p_{12}\}$ e os demais são caminhos de proteção.

É importante observar que a quantidade de caminhos de proteção calculados pelo algoritmo para uma determinada conexão não é necessariamente igual a F_{max} . A quantidade de caminhos de proteção é um parâmetro, que será usado pelo algoritmo de planejamento de rede, conforme explicado na seção 6.4.

5.2.1) Algoritmo de Balanceamento de Carga

O algoritmo de balanceamento de carga sugere como proteção para cada conexão interrompida pela combinação de falhas, um caminho que ofereça o consumo de recursos mais distribuído entre os enlaces. O algoritmo é chamado pelo algoritmo de seleção de caminhos. A entrada para o algoritmo é, o conjunto de conexões interrompidas no estado de falha, e para cada uma delas, um subconjunto de caminhos candidatos é selecionado de acordo com a combinação de falhas que provocou a interrupção.

Após a ocorrência de uma falha, o consumo de recursos em cada enlace da rede é determinado pelo caminho ativo das conexões que permaneceram disponíveis. Durante a busca por caminhos de proteção para as conexões interrompidas, a nova quantidade de comprimentos de onda nos enlaces é calculada tendo como informação o consumo de recursos em cada enlace, as conexões interrompidas pelo estado de falha, e o subconjunto de caminhos candidatos específico para cada uma delas.

Portanto, existe uma demanda que necessita de distribuição balanceada, que é formada pelas conexões interrompidas por uma combinação de falhas. O problema consiste em selecionar, para cada conexão interrompida, um de seus caminhos de proteção, considerando a demanda já alocada e procurando o melhor balanceamento de carga.

Após a escolha dos enlaces que serão ativados para a proteção, a carga em um enlace é recalculada como o total de comprimentos de onda utilizados no referido enlace.

Método de Otimização do Balanceamento de Carga

O algoritmo é uma formulação de programação inteira que tem o objetivo de manter o enlace com a menor carga possível. A entrada para o algoritmo consiste em: 1) a topologia da rede; 2) uma matriz de demanda, ou seja, a quantidade de *lightpaths* necessários entre os pares de nós; e 3) um subconjunto específico de caminhos candidatos $L_p^c(x)$ para cada conexão c. Também são utilizadas as seguintes variáveis:

m : Enlaces na rede (enumerados de 1 até L).

c : Cada uma das conexões (enumeradas de 1 até $|L_p|$).

x : Posição do subconjunto de caminhos candidatos em L_p^c correspondente ao estado da rede que provocou a interrupção da conexão.

$L_p^c(x)$: Subconjunto de caminhos candidatos para a proteção de uma conexão c.

w_m : Quantidade de comprimentos de onda no enlace m usados pelos caminhos já alocados.

s_m : Quantidade de comprimentos de onda no enlace m usados pelos caminhos a serem alocados.

$\alpha_{c,m}^r$: Assume o valor 1 se o r-ésimo caminho candidato que está ativo para a conexão c utiliza um comprimento de onda no enlace m; 0 caso contrário.

$\gamma_{c,m}^b$: Assume o valor 1 se um caminho de proteção dedicado b que utiliza um comprimento de onda no enlace m for alocado para proteger a conexão c; 0 caso contrário.

A função custo minimiza o quadrado da quantidade de comprimentos de onda utilizados:

$$C_{Total} = Minimize \sum_{m=1}^{L} (w_m + s_m)^2 \tag{17}$$

As variáveis consideradas no domínio e na tomada de decisão para o problema são:

$$\sum_{b=1}^{|L_p^c(x)|} \gamma_c^b = 1 \qquad \forall c \in C \qquad \forall b \in L_p^c(x) \tag{18}$$

$$\gamma_c^b \in \{0,1\} \qquad \forall c \in C, \qquad \forall b \in L_p^c(x) \tag{19}$$

A restrição (20) formaliza o cálculo da quantidade de comprimentos de onda do enlace m que são utilizados pelos caminhos ativos das conexões não interrompidas:

$$w_m = \sum_{c \in C} \sum_{r \in L_p^c(x)} \alpha_{c,m}^r \qquad \forall m \in L \tag{20}$$

A restrição (21) formaliza o cálculo da quantidade de comprimentos de onda do enlace *m* utilizados pelos caminhos a serem alocados para proteger as conexões interrompidas:

$$s_m = \sum_{c \in C} \sum_{b \in L_p^c(x)} \gamma_{c,m}^b \qquad \forall m \in L \tag{21}$$

A idéia de custo total é que um enlace com baixa utilização contém comprimento de onda de baixo custo. Como a alta utilização torna o enlace caro, tal fato provoca um desbalanceamento de carga na rede. Com a função custo definida em (17), se a utilização crescer demasiadamente, o enlace será penalizado pesadamente, pois o custo cresce de forma não linear (quadrática).

Cada conexão a ser protegida pela falha terá um caminho de proteção escolhido a partir do correspondente subconjunto de caminhos candidatos. A solução ótima para o problema, obtida por otimização, é importante como referência para análise da qualidade da solução obtida pela heurística de balanceamento de carga. Uma vantagem em utilizar a soma da carga nos enlaces em vez de um valor máximo por enlace é que mesmo que não exista um gargalo em um enlace pesadamente carregado, a função custo total ainda tenta minimizar as cargas nos enlaces restantes da rede. Se todos os caminhos ópticos tiverem o menor custo, o custo total dos enlaces alcança o valor mínimo.

O método de otimização descrito não se aplica a redes grandes, pois sua complexidade computacional inviabiliza seu uso.

Método Heurístico de Balanceamento de Carga

O método heurístico utiliza os mesmos parâmetros de entrada do algoritmo de otimização com resultados semelhantes, porém com escalabilidade.

O algoritmo parte de uma solução inicial, que protege cada conexão *c* interrompida, ao utilizar como caminho selecionado o primeiro caminho candidato do subconjunto $L_p^c(x)$ em uso no estado atual da rede. A demanda formada pelos caminhos de proteção da solução inicial e pelos caminhos ativos de cada conexão não afetada constitui a carga inicial nos enlaces da rede.

O método se baseia em interações sucessivas de redução do desvio médio da carga nos enlaces DMC, ou seja, os ciclos de execuções permanecem enquanto o resultado da etapa atual for melhor que o da anterior, mostrado na Figura 5.2.

O primeiro passo calcula a carga em cada enlace (quantidade de comprimentos de onda), ou seja, identifica os recursos de rede atualmente consumidos pelas conexões.

Para atribuir uma nota a uma determinada escolha de enlaces de proteção, define-se uma métrica denominada Desvio Médio de Carga, calculado pela seguinte equação:

$$DMC = \frac{1}{L}\sum_{m=1}^{L} |W_m - \bar{W}| \tag{22}$$

A carga em cada enlace e a carga média entre os enlaces são calculadas como mostram as equações:

$$W_i = l_m - l_{min} \tag{23}$$

$$\bar{W} = \frac{1}{L}\sum_{m=1}^{L} (l_m - l_{min}) \tag{24}$$

As variáveis l_m e l_{min} representam a quantidade de comprimentos de onda no enlace m e no enlace com menor carga, respectivamente. Então, DMC_{Ant} é calculado como descrito.

O próximo passo é medir o equilíbrio de carga na rede. Para isso, foi definido um esquema de pontuação para os enlaces, onde o enlace com menor carga recebe a pontuação mínima (peso 1), e para os demais enlaces, o incremento de peso é correspondente ao incremento de carga. O enlace com maior carga recebe a pontuação máxima (peso N).

O passo a seguir é a busca da conexão *c**. A conexão *c** é aquela que possui um caminho candidato que oferece maior êxito na redução do desbalanceamento de carga na rede. Conhecendo-se o peso de cada enlace da rede, então o peso de cada caminho candidato dentro do subconjunto $L_p^c(x)$ da conexão *c* é calculado pela soma dos pesos dos enlaces utilizados. A conexão *c** é identificada como aquela que tem a maior diferença de peso entre o caminho selecionado e o seu caminho de menor peso, ambos contidos no seu subconjunto de caminhos candidatos $L_p^{c^*}(x)$.

A tarefa a seguir é realizar a ativação do caminho candidato de menor peso na conexão *c**. A utilização de um novo caminho para a conexão *c** provoca uma alteração de carga nos enlaces, então um novo desvio médio de carga nos enlaces DMC_{Atual} deve ser calculado.

O resultado obtido com a nova distribuição de carga é medido e comparado com o resultado anterior. Para verificar se a nova tentativa de redução do desbalanceamento teve sucesso, a condição $DMC_{Atual} < DMC_{Ant}$ deve ser satisfeita. Se houver redução, a atualização do subconjunto da conexão *c** é seguida de uma nova interação, caso contrário, a configuração anterior será considerada.

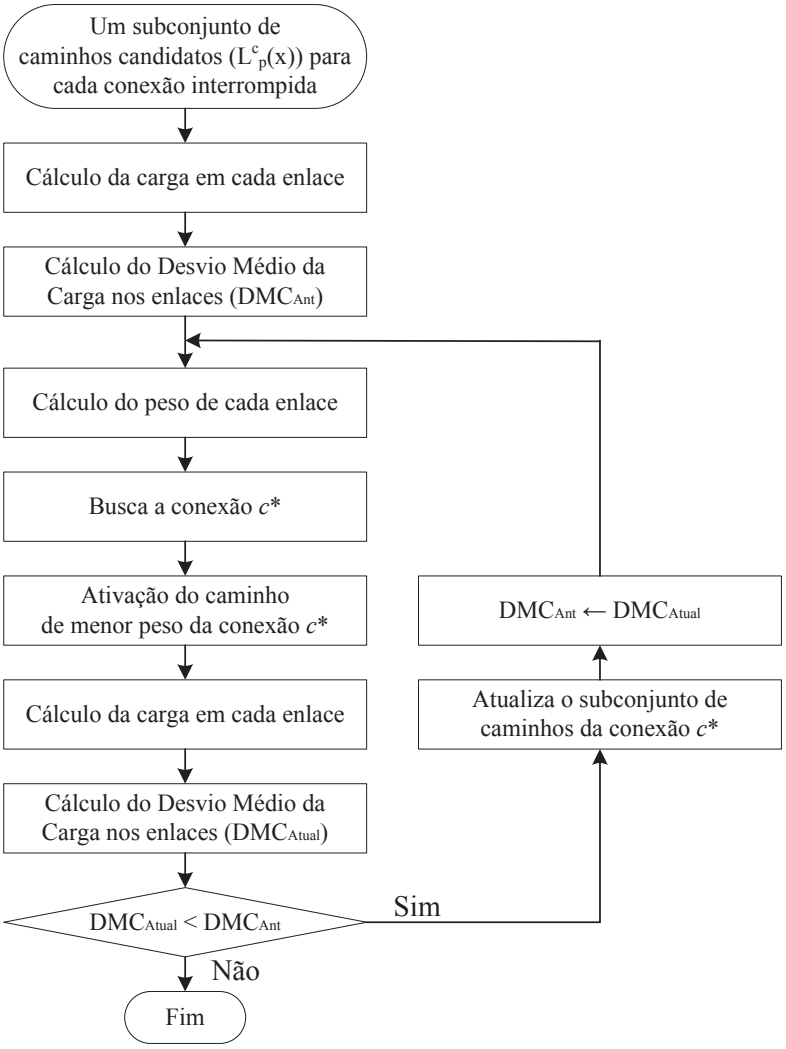


Figura 5.2: Diagrama de fluxo do algoritmo de obtenção do caminho de proteção para cada uma das conexões interrompidas por uma falha adicional mantendo o balanceamento de carga na rede.

A Figura 5.3 mostra o diagrama de fluxo do algoritmo de busca da conexão *c**, aquela que terá um novo caminho selecionado. Para a execução do algoritmo, a combinação de falhas especifica um subconjunto de caminhos candidatos para cada conexão interrompida e a distribuição de carga atual da rede estabelece um peso de 1 a N para cada enlace. A conexão *c** deve satisfizer três condições: 1) seu caminho selecionado tem pelo menos um enlace com peso maior que N/2; 2) seu caminho de menor peso não apresenta enlace com peso N e 3) tem a maior diferença de peso entre o caminho selecionado e o de menor peso. A conexão que atender tais condições terá maior êxito na redução do desbalanceamento da rede no referido estado. Ao final de sua execução, serão conhecidos a conexão *c** e o caminho de menor peso dentro do seu subconjunto de caminhos candidatos.

Os parâmetros de entrada do algoritmo são um subconjunto de caminhos candidatos para cada conexão interrompida e cada um dos *L* enlaces da rede associado a um peso.

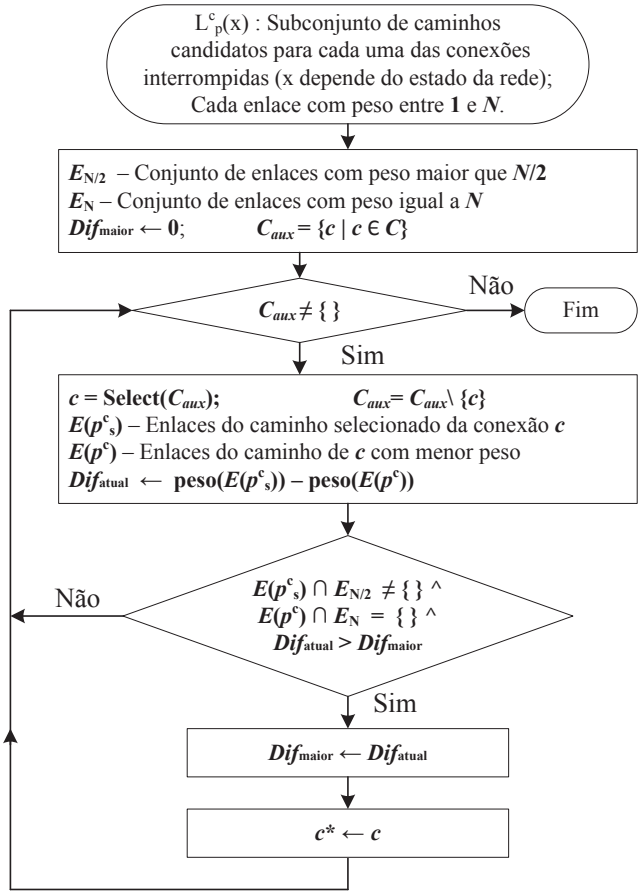


Figura 5.3: Diagrama de fluxo do algoritmo de busca da conexão *c** mostrando a sequência de operações para a identificação do caminho de menor peso.

Antes de analisar os caminhos de cada uma das conexões, é necessário classificar os enlaces da rede. O conjunto $E_{N/2}$ contém os enlaces sobreutilizados, ou seja, com peso superior a N/2. O conjunto E_N contém os enlaces com peso máximo igual a *N*. Como já foi mencionado, o caminho selecionado p_s^c da conexão *c* é o primeiro caminho candidato do subconjunto $L_p^c(x)$ em uso. Em uma conexão *c*, o conjunto de enlaces utilizados por um caminho selecionado é $E(p_s^c)$ e por um caminho de menor peso é $E(p^c)$. O peso de um caminho selecionado $peso\big(E(p_s^c)\big)$, e de um caminho de menor peso $peso\big(E(p^c)\big)$, é igual à soma do peso de cada enlace percorrido por ele. Toda conexão *c* cujo caminho selecionado p_s^c utilize pelo menos um enlace do conjunto $E_{N/2}$ poderá se tornar uma conexão *c**. Tal condição permite que a substituição do caminho selecionado reduza a carga de um enlace sobreutilizado. Toda conexão *c* cujo caminho de menor peso p^c não utilize enlace do conjunto E_N poderá se tornar uma conexão *c**. Tal condição permite que a sua utilização contribua para a redução da quantidade de pesos *N*. A conexão *c* que apresentar a maior diferença de peso Dif_{atual} entre o caminho selecionado $peso\big(E(p_s^c)\big)$, e o caminho de menor peso $peso\big(E(p^c)\big)$, será a conexão *c**. Tal critério se deve ao objetivo de executar a troca entre caminhos da conexão que ofereça maior êxito na redução do Desvio Médio de Carga DMC_{Atual}.

Considerando que cada combinação de falhas representa um estado da cadeia de *Markov*, a complexidade computacional do algoritmo de seleção de caminhos pode ser representada como $O(m^{F_{max}})$, onde m é a quantidade de enlaces na rede.

5.3) Algoritmo de Cálculo de Indisponibilidade de Conexão

O algoritmo de seleção de caminhos produz para cada conexão *c* uma sequência de F_{max} +1 caminhos (L_u^c), que são usados na referida ordem para proteger a conexão *c*. O conjunto L_u^c é usado como parâmetro de entrada para o algoritmo de cálculo de indisponibilidade da conexão, juntamente com a lista de enlaces da rede, incluindo as suas capacidades e taxas de falha e de reparo.

O algoritmo executa um esquema analítico derivado de um modelo da cadeia de *Markov* em tempo contínuo considerando F_{max} como a quantidade máxima de falhas simultâneas de enlaces, descrito na seção 3.2.

Para calcular a indisponibilidade das conexões, a cadeia de *Markov* ilustrada na Figura 3.3 é percorrida em profundidade. O percurso pelos estados da cadeia de *Markov* é organizado através de uma lista enumerada, conforme mostra a Figura 5.4, onde L é a quantidade de enlaces da rede. Foi utilizada uma notação onde o próximo estado a ser visitado (s^{-1}, s) é o resultado da concatenação de uma das sequências de falhas anteriores s^{-1} com a falha adicional s. Significa dizer que as informações calculadas durante a visita ao estado s^{-1} são preservadas, sendo possível determinar na visita ao estado atual (s^{-1}, s) os caminhos ativos de cada conexão e os recursos reservados ainda disponíveis durante o estado anterior, que são calculados e mantidos pelo algoritmo.

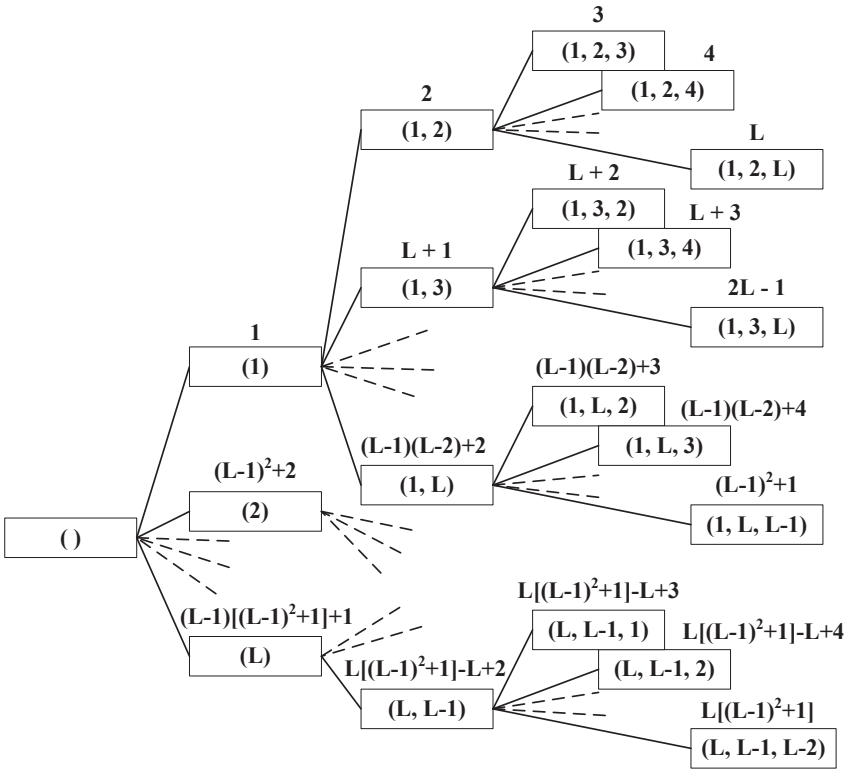


Figura 5.4: Árvore mostrando a ordem de pesquisa em profundidade ao organizar a lista de estados para o cálculo da indisponibilidade das conexões da rede.

Cada fase do cálculo é iniciada ao se visitar um novo estado na cadeia, considerando uma falha adicional de enlace (s). O novo enlace em estado de falha é utilizado por um conjunto de conexões, que buscarão recursos na rede para ativar o próximo caminho na sua lista de caminhos de proteção que ainda não tenha sido afetado por uma falha. A capacidade de recursos remanescentes para os caminhos de proteção em um dado estado (quantidade de

comprimentos de onda disponíveis em um enlace) é igual à diferença entre a quantidade total do enlace e quantidade de comprimentos de onda utilizada no estado antes da falha. Devido ao compartilhamento de recursos, durante a tentativa de ativação de caminhos de proteção das conexões interrompidas pode não haver comprimentos de onda suficientes para atender todas as conexões.

No modelo MSB, considera-se que a probabilidade de um caminho de proteção obter um recurso em um enlace compartilhado é igual para todas as conexões, sendo calculada pela relação entre a quantidade de unidades do recurso disponível no enlace compartilhado e a quantidade de conexões que concorrem ao uso do tal recurso. A conexão afetada pela falha que estiver disputando recursos presentes em mais de um enlace compartilhado terá sua comutação efetuada somente se obtiver os recursos em todos os enlaces utilizados pelo seu caminho de proteção.

A probabilidade de uma conexão obter todos os recursos necessários para ativar o caminho de proteção é denominada fator de aceitação (FA^c), que deve ser calculado a cada estado de falha. FA^c é o produto das probabilidades de um caminho de proteção obter um recurso em cada um dos enlaces compartilhados que ele utiliza. Tal produto é uma aproximação da probabilidade real, já que deixa de considerar algumas combinações possíveis, subestimando o seu valor. Portanto, haverá um erro no cálculo para conexões com mais de um enlace compartilhado, cuja influência é pouco significativa sobre o resultado final, já que, tal cenário está mais presente durante a ocorrência de grande quantidade de falhas simultâneas, onde a probabilidade é menor. O fator de rejeição (FR^c) de uma conexão em um dado estado de falha é o complemento de FA^c ($FR^c = 1 - FA^c$). A indisponibilidade de uma conexão em um dado estado de falha pode ser estimada pelo produto entre o fator de rejeição e a probabilidade de ocorrência do estado, calculada através da cadeia de Markov representada na Figura 3.3.

Ao visitar o estado de falhas (s^{-1}, s) o algoritmo identifica todas as conexões (c) que foram afetadas pela falha do enlace s, considerando em L_u os caminhos que estavam ativos. O algoritmo calcula o fator de rejeição $FR^c_{(s^{-1},s)}$ de cada conexão afetada no estado (s^{-1}, s) considerando o próximo caminho de sua sequência de proteção, e estima a sua indisponibilidade percorrendo todos os estados da árvore representada na Figura 5.4, como mostrado na Equação 25.

$$U^c = \sum_{i=1}^{L} FR^c_{(i)} . \pi_{(i)} + \sum_{i=1}^{L} \sum_{\substack{j=1, \\ j \neq i}}^{L} FR^c_{(i,j)} . \pi_{(i,j)} + \sum_{i=1}^{L} \sum_{\substack{j=1, \\ j \neq i,}}^{L} \sum_{\substack{k=1, \\ k \neq i, \\ k \neq j}}^{L} FR^c_{(i,j,k)} . \pi_{(i,j,k)} \qquad (25)$$

Para as conexões já interrompidas no estado anterior s^{-1}, ou seja, na ausência de caminho de proteção, o fator de rejeição é igual a 1.

Para as conexões não interrompidas no estado s^{-1}, mas que se tornarão interrompidas no estado s, FR^c é calculado de acordo com os recursos existentes para o caminho de proteção. Os seguintes casos estabelecem as condições para a proteção da conexão.

Caso 1 – Pelo menos um dos enlaces utilizados pelo caminho de proteção da conexão *c* tem capacidade nula. $FR^c = 1$.

Caso 2 – Existe recurso suficiente para todas as conexões que compartilham qualquer enlace com a conexão *c*. $FR^c = 0$.

Caso 3 – Existe pelo menos um enlace do caminho de proteção que tenha capacidade não nula, mas insuficiente para atender todas as conexões que compartilham o enlace com a conexão *c*, FR^c = (quantidade de wavelengths)/(quantidade de conexões).

Tal cenário conduz as conexões a uma disputa por capacidade disponível. Significa dizer que algumas conexões ficarão indisponíveis por falta de recursos enquanto outras voltam a se tornar disponíveis. Em tal caso, o fator de rejeição de cada conexão interrompida estará entre 0 e 1.

A Figura 5.5 mostra como são considerados os parâmetros no cálculo da indisponibilidade de cada conexão afetada por uma transição entre os estados da rede. A figura mostra como são considerados os parâmetros em uma transição entre dois estados da rede. Durante o estado s^{-1} da rede, antes de uma falha, são conhecidas as seguintes informações: as conexões que já foram interrompidas em um estado anterior pela ausência de caminho de proteção, os recursos ainda disponíveis, o caminho ativo de cada conexão e os caminhos de proteção ainda disponíveis. Com a ocorrência da falha do enlace *s*, tornam-se conhecidas as conexões afetadas, cujo caminho ativo foi interrompido.

Para as conexões interrompidas, segundo a ordem definida pelo algoritmo de seleção de caminhos, deve ser ativado o primeiro caminho de proteção ainda disponível. Caso os

caminhos de proteção já tenham se esgotado, a conexão passa para o estado interrompido. Caso contrário, o caminho de proteção selecionado disputará recursos com os caminhos de proteção das demais conexões interrompidas (uma conexão interrompida permanece indisponível até que seja reparado algum enlace que ative um dos caminhos da sua lista de caminhos de proteção).

As conexões interrompidas e as que disputam recursos reservados terão um fator de rejeição calculado para o novo estado da rede. A parcela de indisponibilidade de cada conexão afetada durante o estado (s^{-1}, s) é obtida pelo produto entre o fator de rejeição ($FR^{c}_{(s^{-1},s)}$) e a probabilidade de ocorrência do referido estado ($\pi_{(s^{-1},s)}$). A indisponibilidade final de cada conexão é a somatória de cada parcela de indisponibilidade correspondente a um estado da cadeia de *Markov*.

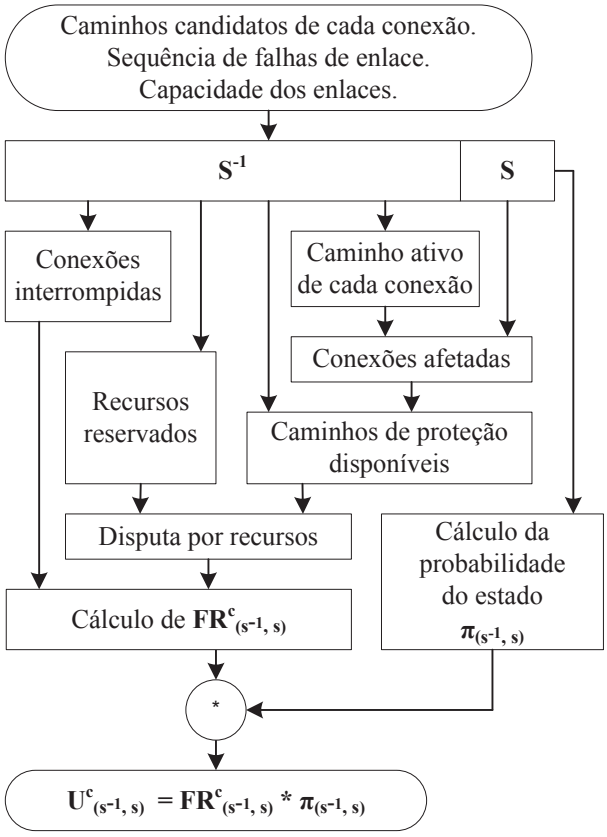


Figura 5.5: Diagrama de fluxo mostrando as atividades realizadas pelo algoritmo em uma transição entre dois estados da rede.

O resultado obtido com o algoritmo de cálculo de indisponibilidade é o conjunto $L_u^+ = \{(L_u^c, U^c) | \forall c \in C, L_u^c \in L_u\}$.

Considerando que cada sequência (em ordem cronológica) de falhas representa um estado da cadeia de *Markov* e para cada estado o procedimento contabiliza todas as conexões da rede, a complexidade computacional do algoritmo de cálculo de indisponibilidade pode ser representada como $O(m^{F_{max}\,!})$, onde m é a quantidade de enlaces.

5.4) Método de Planejamento de Rede

O método MSB é um procedimento dividido em duas etapas (ver Figura 5.6), que utiliza os algoritmos de seleção de caminhos e de cálculo de indisponibilidade de conexão. A partir da lista L_u, a primeira etapa dimensiona a rede com capacidade dedicada, de modo que todas as conexões tenham indisponibilidade maior ou igual à desejada. Para que a rede seja dimensionada com capacidade dedicada, considera-se que ao executar o algoritmo de cálculo de indisponibilidade de conexões sempre existe recurso suficiente para todas as conexões que compartilham qualquer enlace com a conexão c, ou seja, $FR^c = 0$. A primeira etapa é um procedimento interativo, que ao término de cada interação verifica se existem conexões que estão protegidas além do necessário (indisponibilidade abaixo da requerida), e em tal caso reduz em uma unidade a quantidade de caminhos de proteção da conexão com excesso de proteção. Ao final da fase, todas apresentam indisponibilidade acima da desejada e não há mais necessidade de redução na quantidade de caminhos de proteção.

Na segunda etapa, todas as conexões que tiveram redução na sua lista de caminhos de proteção terão a quantidade de caminhos de proteção incrementada em uma unidade, chamando-se o algoritmo de seleção de caminhos com a mais recente configuração, e considerando-se as capacidades dos enlaces inalteradas em relação à configuração resultante da última interação. A rede é dimensionada com capacidade compartilhada sem impor a condição $FR^c = 0$ (FR^c é calculado como explicado anteriormente). Finalmente o algoritmo de cálculo de indisponibilidade da conexão é executado para a configuração final.

O método MSB separa as conexões em dois conjuntos: o conjunto L_u^1, que contém as conexões com proteção excessiva e que terão a quantidade de caminhos de proteção decrescida durante o procedimento, o conjunto L_u^2, que contém as conexões com indisponibilidade acima do valor desejado, tendo os seus caminhos de proteção sido mantidos durante todo o procedimento. Em geral as conexões de L_u^1 têm caminhos de serviço e de proteção menores do que as conexões de L_u^2. Conforme dito, a primeira etapa dimensiona a rede com proteção dedicada, resultando em conexões de L_u^1 com indisponibilidade superior ao

valor desejado, que não necessitam de todos os caminhos de proteção. As conexões de L_u^2 sempre utilizarão todos os caminhos de proteção disponíveis.

Quando a demanda entre um par de nós necessita de múltiplas conexões para ser atendida, a indisponibilidade requerida para cada conexão é inversamente proporcional à quantidade de conexões necessárias, já que se deseja manter o volume de perda de dados independente do tamanho da demanda. Ou seja, espera-se que a perda de dados entre o par de nós mencionado, após uma falha, não seja superior à perda que ocorre em uma conexão (demanda unitária) durante o período de tempo de indisponibilidade estabelecido no planejamento. Também tendem a fazer parte de L_u^2 as conexões que suportam demandas que necessitam de múltiplas conexões, já que a indisponibilidade requerida pode assumir valores muito pequenos tornando necessário todos os caminhos de proteção inicialmente previstos.

Cada conexão de L_u^1 terá a exclusão de pelo menos um de seus caminhos de proteção, um por vez em cada interação da primeira etapa, até que a sua indisponibilidade seja superior ao valor máximo estabelecido. Ao final da primeira etapa, toda conexão de L_u^1 apresenta a quantidade de caminhos de proteção insuficiente para alcançar a indisponibilidade prevista inicialmente, enquanto que toda conexão de L_u^2 continua com seus caminhos de proteção originais e a sua indisponibilidade inalterada. A capacidade total a ser instalada na rede é calculada com a referida configuração. Observe que tal capacidade instalada mantém a indisponibilidade das conexões de L_u^1 acima do valor desejado, necessitando de um caminho de proteção adicional, para que seu valor de indisponibilidade possa alcançar o valor requerido. O caminho adicional em cada conexão de L_u^1 compartilhará recursos com as conexões de L_u^2. O caminho a ser adicionado é decidido através do balanceamento de carga quando for realizada a última execução do algoritmo de seleção de caminhos com limitação de recursos.

Além de reduzir a indisponibilidade das conexões em L_u^1, a inclusão de um caminho de proteção adicional nas conexões em L_u^1 sem alterar a capacidade dos enlaces, elevará a indisponibilidade das conexões de L_u^2. Apesar disso, tal heurística pode ser justificada por três motivos: 1) embora haja muitas conexões em L_u^1, o comprimento de seus caminhos de proteção é pequeno. 2) o balanceamento de carga na rede evita a sobre-utilização de enlace. 3) haverá capacidade disponível nos enlaces para alguns dos diversos caminhos de proteção das conexões de L_u^2.

O diagrama de fluxo apresentado na Figura 5.6 mostra os passos e os resultados intermediários durante a execução do método MSB, no qual as seguintes informações estão disponíveis de acordo com a numeração indicada apresentada na sequência e as seguintes variáveis utilizadas na descrição do algoritmo:

$Limite^c$: Valor de indisponibilidade esperado para a conexão c.

L_u^1 : Conjunto de conexões com proteção excessiva.

L_u^2 : Conjunto de conexões com indisponibilidade acima do valor desejado.

U^c: Indisponibilidade da conexão c.

NCP^c: Número de caminhos de proteção da conexão c.

L_u^- : Conjunto contendo, para cada conexão, os caminhos de serviço e proteção (L_u^c) e a indisponibilidade da conexão U^c. Somente fazem parte do conjunto os pares onde $U^c < Limite^c$.

L_u^+ : Conjunto produzido pelo algoritmo de cálculo de indisponibilidade.

1) Dados para o planejamento da rede: topologia da rede, F_{max} , MTTF e MTTR de todos os enlaces e o valor limite da indisponibilidade máxima desejada para cada conexão ($Limite^c$).
2) Resultado da execução do algoritmo de seleção de caminhos. Cada execução resulta em uma nova versão de L_u.
3) Resultado da execução do algoritmo de cálculo da indisponibilidade das conexões. Tal execução resulta em uma nova versão de L_u^+. Na primeira etapa do planejamento, por não haver limitação de recursos, a quantidade necessária de wavelengths por enlace para toda conexão protegida em cada estado pode ser calculada. Assim, a última interação de tal etapa revela a capacidade máxima utilizada em cada enlace da rede.
4) Ao final de cada interação da primeira etapa, haverá redução no tamanho de L_u^- devido à retirada dos caminhos onde $U^c \geq Limite^c$. As interações sucessivas ocorrerão enquanto houver conexão com excesso de proteção.
5) A inexistência de conexões com excesso de proteção torna o conjunto L_u^- vazio. Em tal momento, é finalizada a primeira etapa do planejamento e torna-se conhecida a capacidade máxima utilizada em cada enlace com proteção mínima dedicada para cada conexão.
6) Resultado da execução do algoritmo de seleção de caminhos com a versão final de L_u.

7) Resultado da execução do algoritmo de cálculo da indisponibilidade das conexões com versão final de L_u^+.

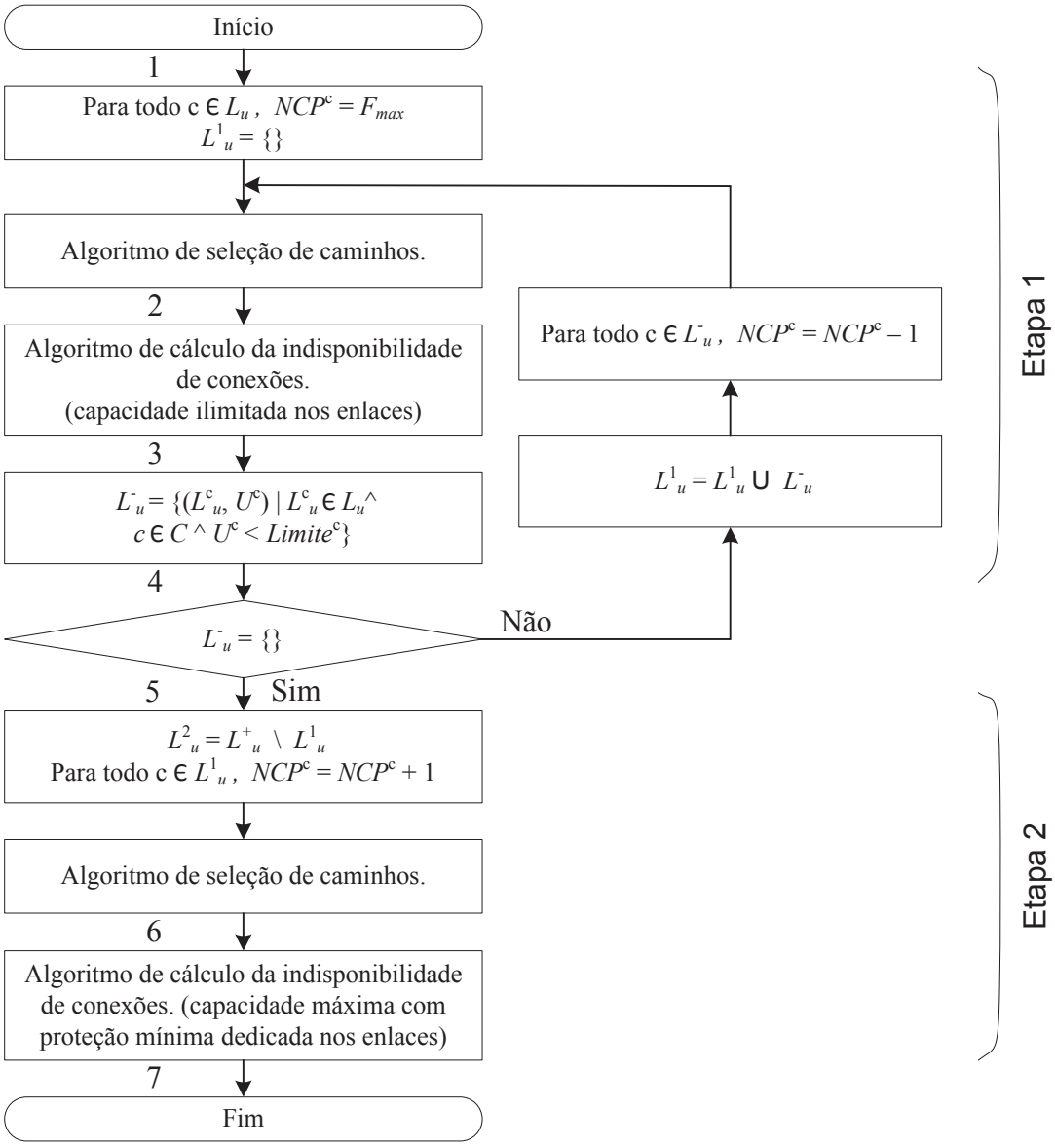


Figura 5.6: Diagrama de fluxo do método MSB.

Na segunda etapa do planejamento, a limitação de recursos, provoca a necessidade de compartilhamento entre as conexões de L_u^1 e L_u^2. Tal compartilhamento de recursos permite que a indisponibilidade das conexões de L_u^1 se aproxime do valor limite definido no início do planejamento. Ao final da execução do planejamento pelo método MSB, a rede com a sua topologia estabelecida e um conjunto de conexões com indisponibilidade máxima definida, poderá operar com mínima capacidade instalada. Tal objetivo é alcançado ao compartilhar a

quantidade de recursos que a topologia permitir e ao selecionar caminhos de proteção que mantenham o balanceamento de carga em cada estado da rede.

Capítulo 6

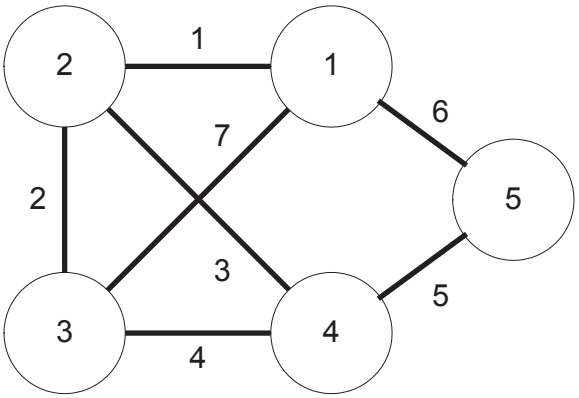
Avaliação de Resultados

6.1) Introdução

Duas topologias de rede foram utilizadas durante a implementação do método MSB. O primeiro experimento utilizou uma rede com tamanho suficiente para demonstrar o efeito do balanceamento de carga e do compartilhamento de recursos diante de condições ótimas. Para o cálculo da indisponibilidade de cada conexão foi utilizado um procedimento simulado de busca exaustiva com objetivo de demonstrar a existência da imprecisão. O segundo experimento utilizou uma rede com dimensões reais, demonstrando os efeitos e os resultados calculados e simulados sob prováveis condições catastróficas.

6.2) Comparação com Resultados Ótimos

Um primeiro experimento foi desenvolvido com o objetivo de demonstrar a aplicação de cada uma das duas fases do método MSB e demonstrar o efeito que a imprecisão dos valores calculados pode causar na interpretação do resultado final. Tal objetivo foi alcançado ao comparar o valor da indisponibilidade calculada para cada conexão com o valor obtido através de busca exaustiva, onde são realizadas as permutações da fila de conexões na tentativa de se manterem disponíveis. A rede considerada é apresentada na Figura 6.1, com demanda de uma única conexão entre cada par de nós da rede (*full-mesh*) formando um grupo de 20 conexões. Foi previsto a proteção contra até 3 falhas simultâneas de enlace, ou seja, cada conexão possui quatro caminhos alternativos (F_{max} +1 = 4). A indisponibilidade desejada para todas as conexões foi definida como uma hora por ano. As taxas de falhas (λ) e de recuperação (μ) estão apresentadas na tabela ao lado da rede.



Enlaces	λ	μ
1	0,0002480	0,05
2	0,0003660	0,05
3	0,0005704	0,05
4	0,0002880	0,05
5	0,0002976	0,05
6	0,0002040	0,05
7	0,0002824	0,05

Figura 6.1: Um exemplo de rede com 5 nós e 7 enlaces.

O gráfico na Figura 6.2 mostra para todas as conexões o valor da indisponibilidade em horas por ano. As conexões foram ordenadas pelo valor de indisponibilidade. Observa-se que quando todas as conexões apresentam a quantidade máxima de caminhos de proteção (F_{max} +1=4), algumas conexões ficarão excessivamente protegidas, utilizando recursos desnecessários.

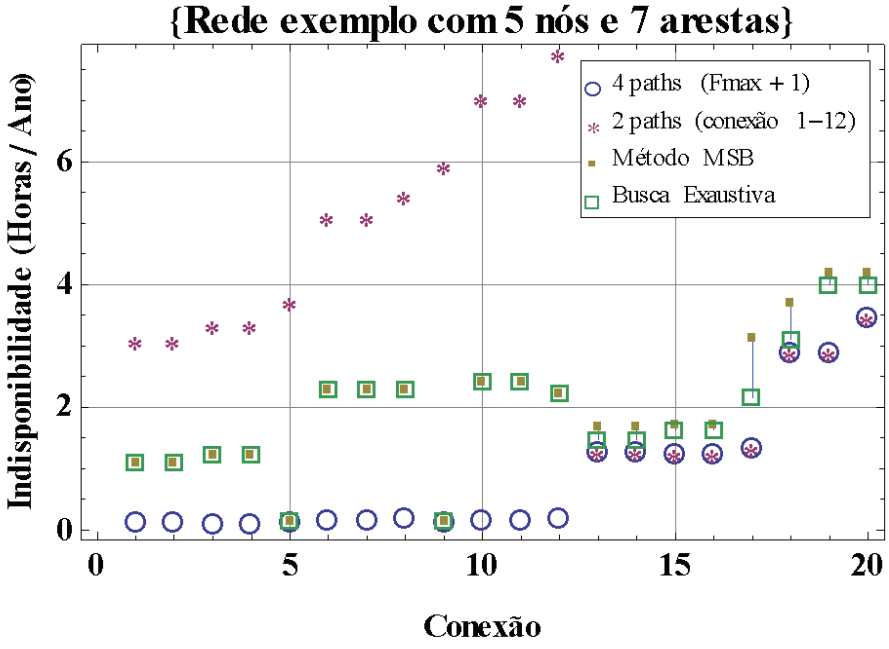


Figura 6.2: Indisponibilidades das conexões protegidas: (1) dedicada com 4 caminhos candidatos para todas as conexões; (2) dedicada com 2 caminhos candidatos apenas para as conexões de 1 até 12; (3) resultado do método MSB (compartilhamento, com um caminho adicional nas conexões de 1 até 12); (4) resultado do procedimento de busca exaustiva (compartilhamento, com caminho adicional nas conexões de 1 até 12).

O gráfico apresenta o valor da indisponibilidade após a primeira fase do algoritmo de planejamento da rede (a título de ilustração), onde se observa a subtração de dois caminhos nas doze primeiras conexões. Em tal etapa do método MSB, todas as conexões estão com indisponibilidade acima da indisponibilidade desejada. Relembrando que na atual fase, o método MSB determina a capacidade dos enlaces sem compartilhamento de recursos, o que resultaria na indisponibilidade mostrada no gráfico. Na segunda fase, o método MSB adiciona um caminho para cada conexão que tenha sofrido subtração de caminhos, sem adicionar capacidade para os respectivos enlaces, forçando o compartilhamento, e trazendo a indisponibilidade para valores próximos do desejado. O gráfico também mostra o resultado final da indisponibilidade obtida por um procedimento de busca exaustiva. O método de busca exaustiva pretende contabilizar cada uma das possíveis permutações que pode apresentar uma fila de conexões interrompidas que precisam dos insuficientes recursos para manter a disponibilidade. Então, durante a execução do método, para cada novo estado da rede, haverá uma nova busca exaustiva (todas as permutações das conexões interrompidas) para encontrar o fator de rejeição (FR^c) de cada conexão interrompida. Por se tratar de busca exaustiva, em tal simulação, o intervalo de confiança é nulo, pois para encontrar o fator de rejeição de cada conexão, todas as combinações da fila de conexões interrompidas são executadas.

Observa-se na Figura 6.3 a diferença entre os valores de indisponibilidade calculados pelo método MSB e por busca exaustiva. Existe um erro no cálculo da indisponibilidade que é diretamente proporcional à quantidade de enlaces compartilhados. É compreensível que tal erro se apresente mais fortemente nas conexões situadas na parte final do gráfico, pois são as conexões que têm caminhos com maior quantidade de enlaces. Tal erro ocorre por não serem considerados todos os eventos de conectividade possíveis realizáveis através dos enlaces compartilhados (combinação de conexões realizadas). Assim, em tais casos, nota-se que o valor de indisponibilidade obtido pelo algoritmo para uma dada conexão é sempre maior que o valor real, ou seja, o algoritmo é conservador. Os valores somente serão iguais para o caso no qual a conexão dependa de um único enlace compartilhado, nas 12 primeiras conexões do gráfico. Observa-se que o maior valor de diferença no exemplo foi de 0,95 horas por ano na conexão 17, correspondendo a um erro de 31% em relação à indisponibilidade obtida com a busca exaustiva.

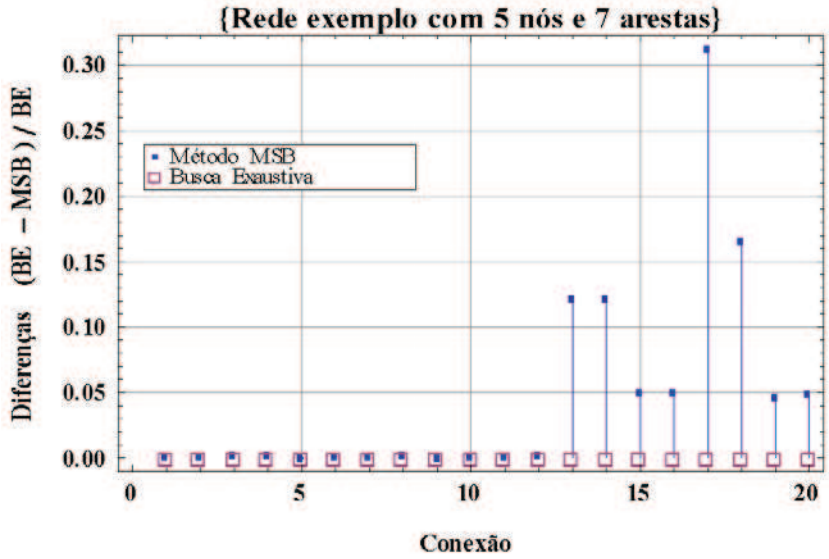


Figura 6.3: Diferença entre o valor de indisponibilidade obtido pelo método MSB e por busca exaustiva.

A Figura 6.4 compara os valores de indisponibilidade entre o método MSB com o método de proteção dedicada com um caminho de proteção para cada conexão (*single dedicated backup* – SDB). Os valores de indisponibilidade observados para o método SDB são todos maiores que os valores obtidos pelo método MSB.

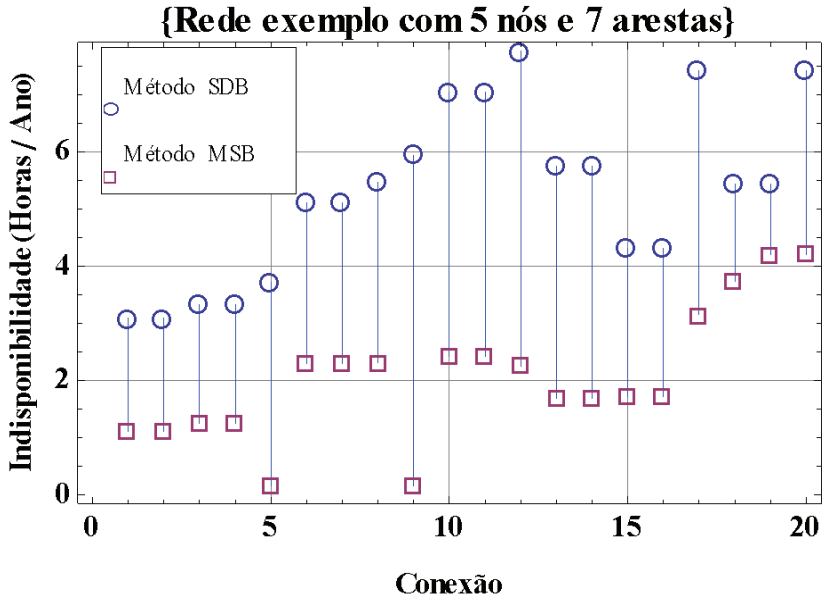


Figura 6.4: Indisponibilidades das conexões pelo método SDB com proteção dedicada de apenas um caminho de proteção por conexão, comparadas com proteção compartilhada pelo método MSB.

Tal comportamento mostra o resultado obtido pela utilização eficiente dos recursos disponíveis quando o balanceamento de carga e o compartilhamento de recursos são considerados em uma rede sujeita a múltiplas falhas de enlace. Admitindo-se até 3 falhas simultâneas de enlace, a média dos valores de indisponibilidade das conexões para a proteção dedicada é 5,29 hora por ano com desvio padrão de 1,52, e a média dos valores de indisponibilidade para o método MSB ficou em 2,06 horas por ano, com desvio padrão de 1,14. O método SDB utiliza uma quantidade de capacidade reservada equivalente a 108% da capacidade de serviço, enquanto que o método MSB utiliza uma quantidade de capacidade reservada equivalente a 158% da capacidade de serviço.

Considerando que cada combinação de falhas representa um estado da cadeia de *Markov* e $|c_s|$, a quantidade média das conexões interrompidas em cada estado da rede, a complexidade computacional do algoritmo de busca exaustiva seria $O(m^{F_{max}} \times |c_s|!)$, onde m é a quantidade de enlaces.

6.3) Avaliação em Cenário com Rede de Referência

O segundo experimento visa demonstrar a escalabilidade do método MSB. O método foi aplicado à rede *pan-European BT*, que apresenta um tamanho adequado para demonstrar a sua utilização prática. A Figura 6.5 mostra a rede, que consiste de 28 nós situados nas maiores cidades européias e conectados através de 41 enlaces em uma topologia *mesh*, onde a distância média de cada enlace de fibra é de 625 km com os valores mínimo de 218 km e máximo de 1500 km [MAE03]. Conforme afirmado por [MEL05], os valores atribuídos aos parâmetros de rede, tais como: λ = 1 / MTTF = 200 FIT/km, onde FIT = 1 falha em 10^9 horas (FIT – *Failure in Time*) e MTTR = 20 horas, para redes intercontinentais, 95% das possíveis falhas na rede não acontece em mais de dois enlaces simultaneamente. A aplicação do método MSB em tal configuração causaria grande redução de indisponibilidade nas conexões (com valores de até segundos por ano) e os efeitos que se procura demonstrar com a aplicação do método não teriam a evidência desejada. Para que a indisponibilidade das conexões se mantivesse na ordem de horas por ano, e que fosse possível a constatação mínima dos efeitos do compartilhamento de recursos, foram utilizados: λ = 1 / MTTF = 800 FIT / km e MTTR = 20 horas. Para avaliar o efeito da alocação de conexões compartilhadas, o valor máximo da indisponibilidade desejada para as conexões foi 4 horas por ano.

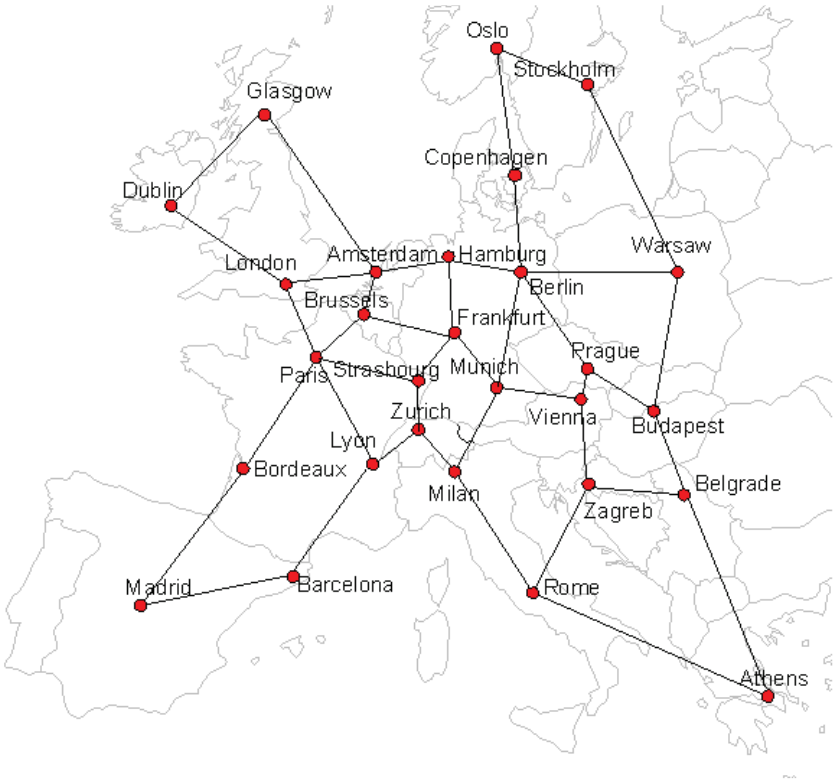


Figura 6.5. A rede de fibra óptica de referência *pan-European BT* [MAE03].

A matriz de tráfego na rede *pan-European BT* (ver Figura 6.5) foi criada com valores obtidos da estimativa de crescimento do tráfego mostrada em [MAE03] para transmissão de voz e de dados. Todos os comprimentos de onda foram considerados com a mesma capacidade igual a 20 Gbps. A quantidade de conexões entre quaisquer dois nós foi estabelecida da seguinte maneira: considerou-se 8 conexões para a maior demanda (160 Gbps) e 1 conexão para a menor, e para as demais demandas, valores inteiros proporcionais.

Tabela 2: Distribuição das 1632 conexões entre os 756 pares de nós.

Wavelengths	Quantidade de pares de nós
1	337
2	196
3	107
4	54
5	26
6	20
7	12
8	4
Total	756

Observar que uma conexão corresponde a 1 comprimento de onda. O total de conexões para a rede passa a ser de 1632. As demandas dos 756 pares de nós (28 x 27) estão demonstradas na Tabela 2.

A quantidade de comprimentos de onda necessários para suportar os caminhos ópticos de serviço é 5103, enquanto que a quantidade para os caminhos ópticos de proteção é 9206 e 11688, para as estratégias SDB e MSB, respectivamente. No segundo experimento, o valor da indisponibilidade desejada foi considerado 4 horas por ano. A Figura 6.6 mostra a distribuição de comprimentos de onda por enlace. Os comprimentos de onda de proteção adicionados pelo método MSB foram distribuídos através dos critérios de balanceamento de carga em cada estado da rede, onde os enlaces são organizados em ordem crescente de carga relativa aos caminhos ópticos de serviço.

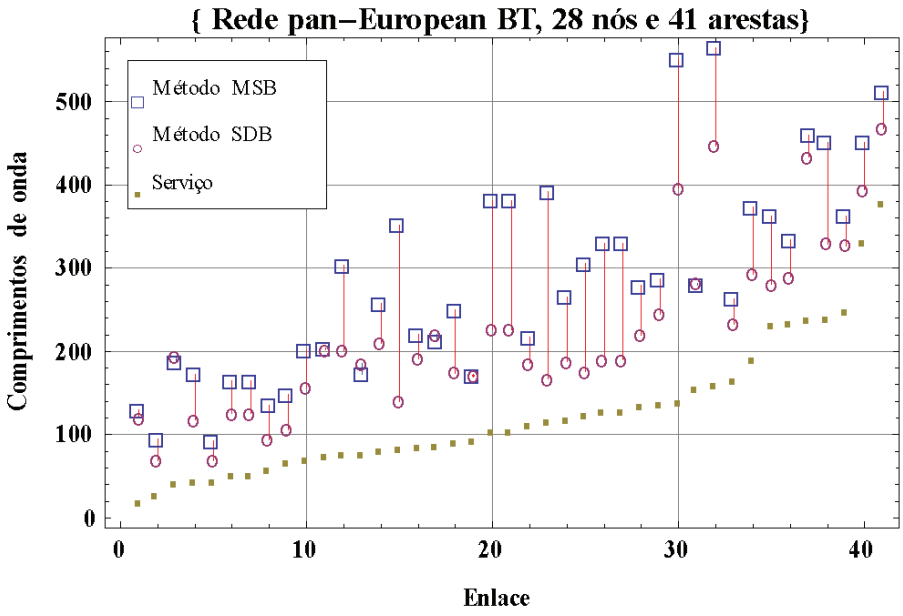


Figura 6.6: Capacidade dos enlaces da rede: (1) apenas caminhos ópticos de serviço, (2) caminhos ópticos de serviço e proteção para a estratégia SDB e (3) caminhos ópticos de serviço e proteção para a estratégia MSB (indisponibilidade desejada de 4 horas por ano).

O método SDB utiliza uma quantidade adicional de capacidade reservada equivalente a 80% da capacidade de serviço da rede (utilizada nos caminhos de serviço), enquanto que o método MSB utiliza uma quantidade de capacidade reservada equivalente a 129% da capacidade de serviço da rede.

A Figura 6.7 mostra os valores calculados de indisponibilidade de todas as conexões da rede, e faz a comparação entre os métodos SDB e MSB. Para o método SDB, a indisponibilidade média é de 5,97 e desvio padrão de 5,16, com valor máximo de 26,10 horas por ano; para o método MSB a indisponibilidade média é de 3,38 e desvio padrão de 3,70, com valor máximo de 22,26 horas por ano. A redução da indisponibilidade média é uma consequência direta do incremento de proteção, enquanto que a redução do desvio padrão indica uma distribuição mais homogênea dos recursos de rede, indicando o funcionamento adequado do método, cujos objetivos eram o aumento da resiliência da rede com utilização racional dos recursos.

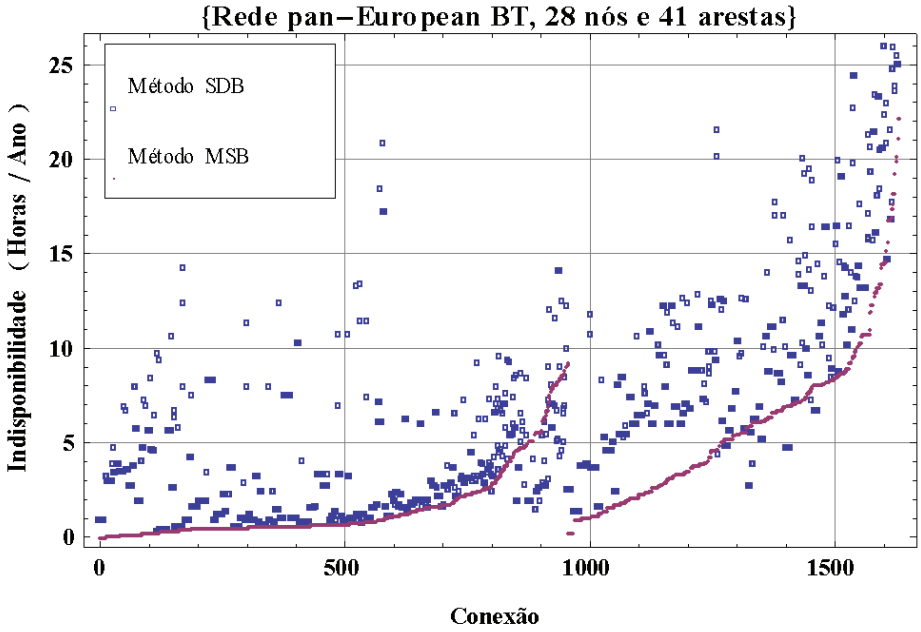


Figura 6.7: Valores calculados de indisponibilidade das conexões obtidos pelo método: SDB com capacidade reservada dedicada com um caminho de proteção para cada conexão, e MSB com valor desejado de indisponibilidade de 4 horas por ano.

Para facilitar a visualização dos efeitos do compartilhamento, as conexões estão organizadas de ordem crescente de indisponibilidade, separadas de acordo com os dois conjuntos que se formam durante a execução do procedimento (ver seção 6.4). Conforme explicado, as conexões de L_u^1 são aquelas que quando configuradas com F_{max} +1 caminhos apresentam indisponibilidade menor do que o valor máximo desejado, enquanto que para as

conexões de L_u^2 a indisponibilidade permanece maior. O conjunto L_u^1 é formado pelas conexões numeradas de 1 a 956, enquanto que o conjunto L_u^2 pelas conexões de 957 a 1632. Na primeira etapa do método MSB, cada conexão terá sua máxima indisponibilidade limitada pelo valor máximo desejado dividido pela quantidade de conexões necessárias para atender a demanda entre o par de nós correspondente. Entretanto, é possível observar na Figura 6.7, conexões de L_u^2 com valor de indisponibilidade abaixo do valor desejado. Tal comportamento apresentam as conexões que atendem conjuntamente demandas que necessitam de mais de uma conexão, porque o valor desejado para tais conexões será estabelecido como uma fração da indisponibilidade desejada para a demanda, $1/n$, onde n é a quantidade de conexões que atendem conjuntamente a demanda entre o par de nós. As conexões que são observadas no gráfico nas posições mais a esquerda do conjunto L_u^2 são as conexões correspondentes ao referido caso. A indisponibilidade das conexões calculadas pelo método MSB na região mais a direita do conjunto L_u^1 apresentam valores superiores aos do método de capacidade dedicada. Para um melhor desempenho, tais conexões devem ser configuradas com apenas um caminho de proteção dedicado (estratégia SDB) porque estão em uma localização topológica na rede que não viabiliza o compartilhamento de recursos. As conexões de L_u^2 com valor de indisponibilidade mais afastado do valor desejado apresentam os caminhos alternativos relativamente longos na rede. Tais conexões sofreram elevações de suas indisponibilidades devido ao compartilhamento com as conexões de L_u^1, que também sofreram elevações de indisponibilidade.

A Figura 6.8 mostra os dois conjuntos de conexões, organizados em ordem crescente de indisponibilidade, obtida quando todas as conexões possuem os quatro caminhos candidatos (F_{max} + 1), descrevendo uma linha formada por pontos sucessivos. Em tal cenário, cada conexão apresenta o melhor desempenho permitido pela topologia e pela proteção dedicada, ou seja, não há compartilhamento de recurso. Os demais pontos são os valores de indisponibilidade das conexões calculados pelo método MSB utilizando um valor máximo de indisponibilidade de 4 horas por ano.

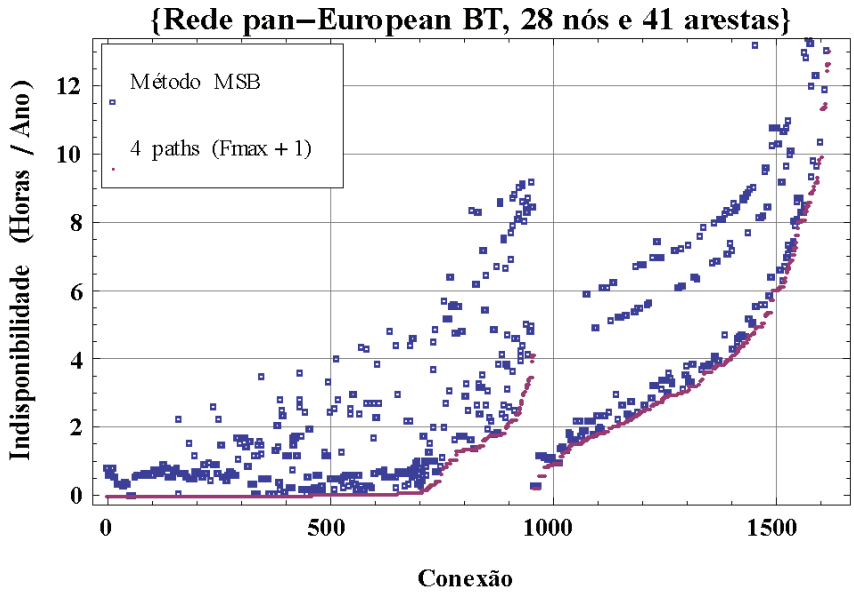


Figura 6.8: Valores de indisponibilidade de conexões calculadas: todas as conexões com quatro caminhos candidatos (capacidade na rede de 15149 comprimentos de onda) e planejada pelo método MSB com valor desejado de 4 horas por ano (capacidade na rede de 11688 comprimentos de onda, com redução de 22,8%).

Cada conexão de L_u^2 com valor de indisponibilidade maior que 4 horas por ano apresenta caminhos de proteção relativamente longos na rede. Tais conexões sofreram elevações de suas indisponibilidades devido ao compartilhamento com as conexões de L_u^1, que também sofreram elevações de indisponibilidade. As conexões de L_u^2 com indisponibilidade inferior a 4 horas por ano apresentam caminhos com comprimentos menores, portanto, por isso sofreram menor elevação de indisponibilidade. As conexões em locais topologicamente inadequados ao compartilhamento de recursos, após a aplicação do método MSB, tiveram indisponibilidade ainda maior do que a obtida com proteção dedicada. Tal fato ocorre com as conexões à direita de L_u^1, que apresentam maiores valores de indisponibilidade mesmo com proteção dedicada pela máxima quantidade (F_{max} +1) de caminhos.

6.4) Metodologia de Simulação

O cenário da rede *pan-European BT* foi simulado para o segundo experimento com o objetivo de validar os resultados calculados pelo método MSB. A metodologia geral da simulação é a seguinte:

1) Gerar aleatoriamente para cada enlace uma sequência falhas durante o período de simulação. Os intervalos de falhas são simulados por um gerador de números aleatórios com distribuição exponencial com parâmetro igual à taxa de falha de cada enlace.
2) Para cada falha, gerar o tempo de reparo correspondente através de um gerador de números aleatórios com distribuição exponencial com um parâmetro igual à taxa de reparo do enlace.
3) Para todas as interrupções de enlace, identificar as conexões interrompidas. Todas as possíveis combinações de falhas de enlace, mesmo combinações com quantidade de enlaces em falha superiores a F_{max} são contabilizadas.
4) Para o conjunto de conexões interrompidas, gerar uma ordem aleatória para tratamento das interrupções, e tentar ativar (na ordem sorteada) o primeiro caminho de proteção da sequência de ativação não interrompido de cada conexão.
5) Identificar as conexões para as quais a ativação do caminho de proteção (se houver) não foi possível, devido inexistência de recurso. Em tal situação a conexão falhou.
6) Registrar os tempos de falha das conexões.

A indisponibilidade da conexão *c* pode ser calculada pela a seguinte equação:

$$U^c = \frac{\sum_k T_k^c}{T} \tag{26}$$

Onde *T* é o tempo de simulação, *k* é a *k*-ésima falha da conexão *c* durante o período *T*, e T_k^c é a duração da *k*-ésima falha da conexão *c*.

Na simulação, foi utilizado o método de recuperação ativa com reversão [ZHA07]. Pelo referido método, o tráfego em uma conexão é comutado para o seu caminho de proteção quando ocorrer uma falha no caminho de serviço, e após a falha ser reparada, o tráfego da conexão é comutado de volta para o caminho de serviço e os recursos de proteção compartilhados serão liberados. Se houver várias conexões em estado de falha aguardando por

recursos de proteção, que estão sendo utilizados por outras conexões também em estado de falha, as conexões são recuperadas na ordem com a qual as falhas de enlace vão sendo reparadas. Também assume-se que os recursos de proteção em uso podem ser liberados não só quando o caminho de serviço é recuperado, mas também quando for um caminho de proteção prioritário em relação ao atualmente utilizado.

6.5) Comparação com Resultados Simulados

A Figura 6.9 compara o resultado obtido na simulação com a indisponibilidade de cada conexão obtida pelo método MSB. As conexões estão organizadas em ordem crescente de valores calculados. Para uma determinada conexão, o ponto acima da curva, indica que a indisponibilidade obtida na simulação é superior à calculada. E quando o ponto estiver abaixo da curva, o valor simulado foi inferior ao calculado. A indisponibilidade média é de 3,59 e o desvio padrão de 4,09, com valor máximo de 24,07 horas por ano, para a simulação, enquanto que os valores encontrados para o método MSB foram: indisponibilidade média de 3,38 com desvio padrão de 3,70 e valor máximo de 22,26 horas por ano.

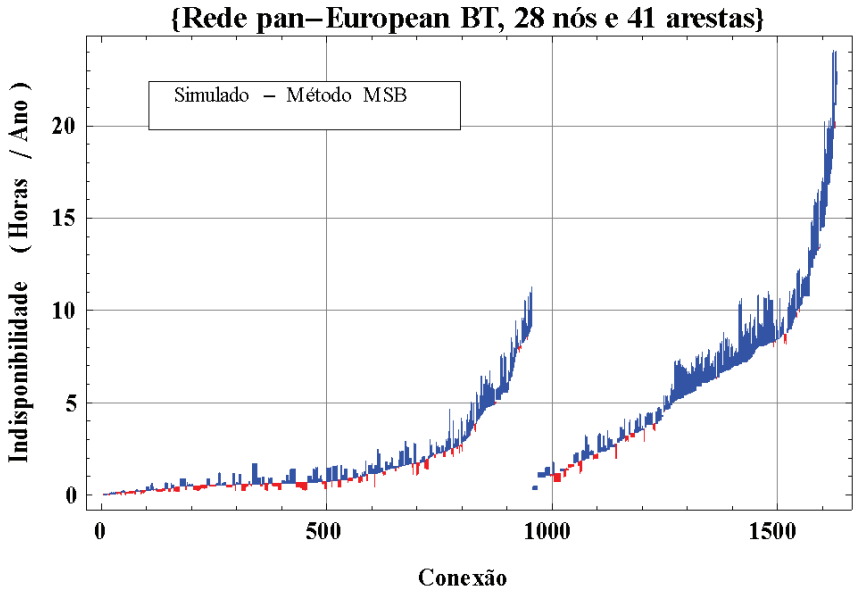


Figura 6.9: Valores de indisponibilidade das conexões obtidos pelo método MSB com indisponibilidade desejada de 4 horas por ano e os valores simulados para cada conexão.

Cada conexão da Figura 6.9 está representada na Figura 6.10 como uma diferença entre os valores absolutos de indisponibilidade (horas por ano) obtidos pela simulação e pelo

método MSB. O valor de indisponibilidade obtido pelo método MSB para cada conexão é usado como referência (zero no gráfico). Cada valor representa o comportamento de uma conexão quando a rede é submetida a um cenário de falhas sucessivas aleatórias em comparação com o resultado obtido pelo método MSB. Um valor de indisponibilidade simulado superior é representado por um ponto acima de zero e de um inferior por um ponto abaixo de zero. Como se trata de valores aleatórios, conexões com indisponibilidades semelhantes (setores do gráfico) apresentam alternância regular de pontos acima e abaixo de zero. Tal fato é verificado nas conexões com indisponibilidade baixa, pois a falha delas ocorre com pouca frequência durante a simulação. Tais conexões apresentam o maior intervalo de confiança de indisponibilidade da rede, pois a quantidade de ocorrência durante a simulação foi insuficiente para a estabilização de seus valores finais. O seu valor (1,547) foi obtido ao realizar a diferença entre o maior valor (1,691) e a média (0,144) das indisponibilidades das primeiras conexões (800). A média entre os desvios observados durante a simulação e o cálculo foi de 0,513 e o desvio médio foi de 0,583. Até para as primeiras conexões de L_u^1, a predominância de pontos acima de zero acontece porque durante a simulação ocorreram combinações de falhas simultâneas de enlace de ordem superior ao valor de F_{max} , ou seja, são combinações não previstas no cálculo usando o método MSB.

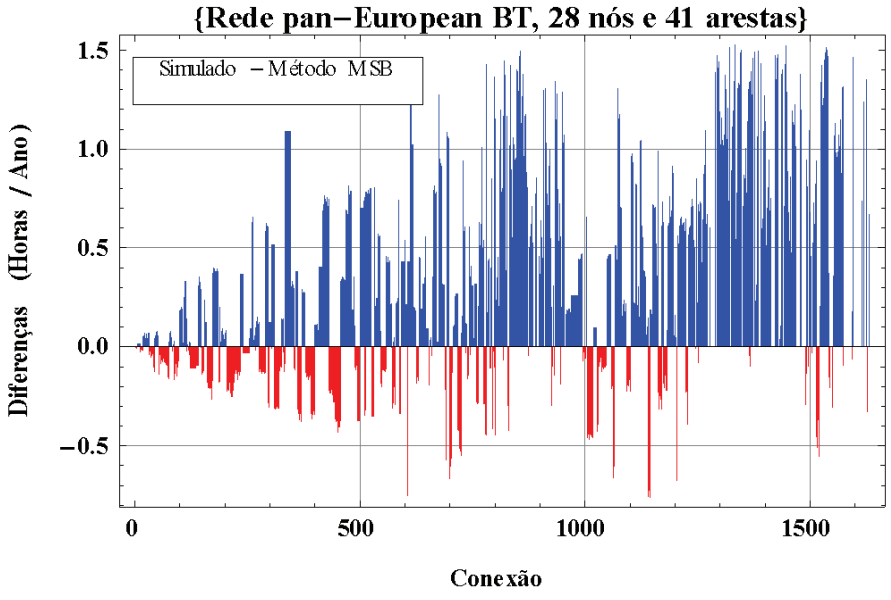


Figura 6.10: Diferença entre indisponibilidade simulada e calculada pelo método MSB para cada conexão observada na Figura 6.9.

Pela baixa probabilidade de ocorrência, o efeito de tais combinações de falhas é menos evidente para as conexões com menor indisponibilidade (as primeiras 800 conexões de L_u^1 e as primeiras 300 conexões de L_u^2). Importante destacar, é que tais conexões apresentam indisponibilidade inferior ao valor máximo desejado, estabelecido inicialmente. As conexões à direita de L_u^1 se situam em locais topologicamente inadequados ao compartilhamento de recursos e as conexões à direita de L_u^2 apresentam disponibilidade diretamente proporcional ao valor de F_{max} .

O maior desvio absoluto, de 5,672 horas por ano, ocorreu na conexão de número 1605 com valor simulado de 20,23 horas por ano, correspondendo a uma variação percentual de 28%, como mostra a Figura 6.11. A maior variação percentual ocorreu nas conexões de números 335-346 e foi de 64,4%, correspondendo a um valor calculado de 0,602 horas por ano e um valor simulado de 1,691 horas por ano.

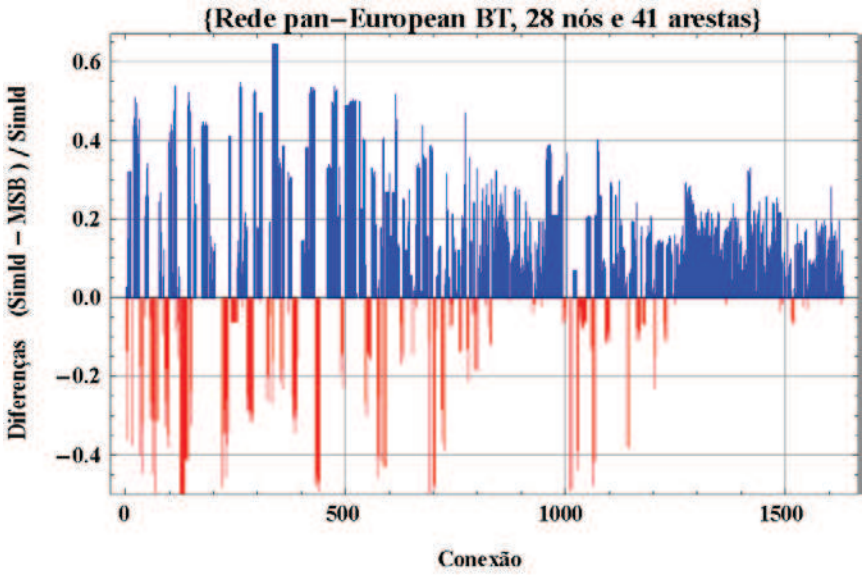


Figura 6.11: Cada conexão é representada pela diferença entre a disponibilidade simulada e calculada pelo método MSB comparada com o valor obtido por simulação (%).

O resultado da simulação representa um comportamento natural da rede. A execução do cálculo utilizando uma quantidade máxima de falhas simultâneas insuficiente associado à imprecisão do resultado para as conexões de caminhos mais longos (à direita de L_u^2), conduziu o resultado a um comportamento semelhante ao da simulação. Tal fato se deve à ocorrência

de combinações de falhas de ordem superior ao valor de F_{max} . O efeito pode ser constatado com a predominância de erros positivos (pontos acima da curva) nas conexões de L_u^1, onde a precisão do cálculo é maior. Nota-se que apesar de tal imprecisão, a indisponibilidade desejada (4 horas por ano) nas conexões selecionadas não foi ultrapassada. Assim, pode-se concluir que o método MSB permite estabelecer um critério de escolha de um valor máximo desejado de indisponibilidade admissível para conexões situadas em regiões topologicamente adequadas ao compartilhamento de recursos reservados.

Conclusão

No presente trabalho, foi apresentado um novo método heurístico de planejamento para o tráfego estático de rede (com mínima capacidade reservada) que realiza proteção de cada conexão através de uma lista ordenada de caminhos candidatos, contra múltiplas falhas de enlaces, mantendo o melhor balanceamento de carga na rede possível.

Priorizando o balanceamento de carga em cada estado da rede, o método MSB permite que a cada comutação do tráfego os recursos reservados sejam consumidos com a melhor distribuição permitida pela topologia. Tal comportamento conduz a um elevado grau de compartilhamento de recursos reservados (wavelengths) e a consequente economia de seu uso. O método MSB faz o planejamento para rede de alto desempenho, pois eleva a resiliência da rede ao proteger as conexões e obtém um resultado eficiente em relação à quantidade total de recursos reservados, ao elevar o grau com que eles são compartilhados.

O método permite que as conexões sejam protegidas contra um número qualquer de falhas, caracterizado pela variável F_{max} . Tal variável estabelece a quantidade de caminhos de proteção para cada conexão, todos eles com recursos inicialmente dedicados que serão compartilhados com os caminhos das conexões mais confiáveis da rede.

O método MSB faz uso eficaz da distribuição topológica de rede, estabelece uma quantidade limitada de perda de dados para demandas de múltiplas conexões e identifica as conexões com baixa capacidade de compartilhamento de recursos reservados, deixando ao planejador de rede a opção por proteção máxima (quantidade total de caminhos, F_{max} +1) ou proteção SDB.

Além de atingir os objetivos, o método proposto colocou em evidência que o compartilhamento de recursos é obtido pela organização das conexões em dois conjuntos: as conexões menos vulneráveis que necessitam de recursos reservados e as conexões mais vulneráveis com recursos abundantes. O método MSB, além de identificar e possibilitar tratamento especial às conexões em posições topológicas desfavoráveis, também permite igualdade no acesso aos recursos reservados nos enlaces da rede.

Os resultados numéricos mostram que, usando o método MSB, o elevado grau de resiliência da rede permite explorar as condições topológicas para uma redução significativa da vulnerabilidade de qualquer conexão da rede.

Outras contribuições secundárias foram obtidas no desenvolvimento do presente trabalho.

- Extensão do método de cálculo de indisponibilidade de conexões para sequências de 2 falhas através de Cadeia de Markov em tempo contínuo para sequências de *n* falhas.
- Proposição de um modelo de otimização para o balanceamento de carga de conexões.
- Proposição de heurística escalável para o balanceamento de carga de conexões.

Algumas das possíveis ações que podem melhorar o desempenho do método MSB, tanto operacionalmente como em resultados, estão relacionadas como uma proposta para trabalhos futuros. Entre eles, melhorar a precisão no cálculo do fator de rejeição de conexões interrompidas e utilizar valores maiores para F_{max} daria maior confiabilidade ao resultado final do planejamento. Fazer o cálculo da indisponibilidade utilizando combinações de falhas de ordem superior ao valor atribuído a F_{max} também pode melhorar a precisão nos resultados, pois terá um comportamento mais semelhante ao da simulação. Acelerar o procedimento de planejamento ao pular passos intermediários para alcançar a fase final evitaria processamentos desnecessários. Identificar e excluir do planejamento as conexões topologicamente desfavorecidas para um tratamento especial daria maior eficiência ao método MSB.

Referências Bibliográficas[1]

[AEC03] ARCI, D.; MAIER, G.; PATTAVINA, A.; PETECCHI, D.; TORNATORE, M.; Availability models for protection techniques in WDM networks. Design of Reliable Communication Networks, 2003. (DRCN 2003). Proceedings. Fourth International Workshop on, vol., no., pp. 158 - 166, 19-22 October, 2003.

[AHN02] AHN, G.; JANG, J.; CHUN, W.; *An Efficient Rerouting Scheme for MPLS-Based Recovery and Its Performance Evaluation*. Telecommunication Systems 19:3, 4; pp. 481–495, 2002.

[AKI09] AKIMOTO, R.; GOZU, S.; MOZUME, T.; AKITA, K.; CONG, G. W.; HASAMA, T.; E ISHIKAWA, H.; *All-optical wavelength conversion at 160Gb/s by intersubband transition switches utilizing efficient XPM in InGaAs/AlAsSb coupled double quantum well*. Proceedings, 35th European Conference on Optical Communication (ECOC '09), pp. 1-2, September, 2009.

[ALF04] AL-FUQAHA, A.; CHAUDHRY, G.; GUIZANI, M.; E LABRADOR, M.; *Routing framework for all-optical DWDM metro and long-haul transport networks with sparse wavelength conversion capabilities*. *IEEE JSAC 22*, 8, pp. 1443–1459, October, 2004.

[ALI04] ALICHERRY, M.; BHATIA, R.; *Pre-Provisioning Networks to Support Fast Restoration with Minimum Over-Build*. INFOCOM 2004.

[AMI11] WASON, A.; KALER, R.S.; *Survivable routing and wavelength assignment algorithm for multiple link failures in wavelength-routed all-optical WDM networks*; Optik 122 (2011), pp. 1095–1099.

[1] O modelo segue o estilo “alpha” do sistema LaTeX, que permite memorizar melhor as referências durante a leitura do texto e é bem mais compacto que o proposto pela ABNT. Em caso de dúvidas, consultar [ISK00].

[AST03] ASTHANA, R.; E SINGH, Y. N.; *Survivibility in all optical networks, in Proc. Of Int. Conf. on Optical Communication Networks*. Paper no. 2038, Bangalore, India, pp. 20-22, October, 2003.

[AST04] ASTHANA, R.; E SINGH, Y. N.; *Protection and restoration in optical networks*. IETE Journal of Research, vol. 50, no. 5, pp. 319-329, Sept-Oct. 2004.

[AWD99] AWDUCHE, D.; *MPLS and Traffic Engineering in IP Networks*. IEEE Communications Magazine, December 1999, pp. 42-47.

[BHA08] BHATIA, R. S.; KODIALAM, M.; SENGUPTA, S.; *Bandwidth Guaranteed Routing With Fast Restoration Against Link and Node Failures*. IEEE/ACM Transactions on Networking, Vol. 16, no. 6, December 2008.

[CAO03] CAO, X.; ANAND, V.; E QIAO, C.; *Waveband switching in optical networks*. IEEE Communications Magazine 41, 4; April, 2003, pp. 105–112.

[CAO04] CAO, X.; ANAND, V.; E QIAO, C.; *Multilayer versus single-layer optical crossconnect architectures for waveband switching*. In Proc. IEEE INFOCOM; March 2004, pp. 2295–2302.

[CHE08] CHENG, X.; SHAO, X.; WANG, Y.; YEO, Y.; *Differentiated Resilient Protection against Multiple-Link Failures in Survivable Optical Networks*. IEEE, Optical Society of America, 2008.

[CHU91] CHUJO, T.; KOMINE, H.; MIYAZAKI, K.; OGURA, T.; SOEJIMA, T.; *Distributed self-healing network and its optimum spare-capacity assignment algorithm*. Electronics and Communications in Japan 1991; 74(1): pp. 479–86.

[CHU03] CHU, X.; LI, B.; E CHLAMTAC, I.; *Wavelength converter placement under different RWA algorithms in wavelength-routed all-optical networks*. IEEE Transactions on Communications 51, 4; April 2003, pp. 607–617.

[CHU04] CHU, X.; LI, B.; E CHLAMTAC, I.; *Wavelength converter placement under different RWA algorithms in wavelength-routed all-optical networks*. IEEE/ACM Transactions on Networking 51, 4; April 2004, pp. 607–617.

[CLO02] CLOUQUEUR, M.; AND GROVER, W. D.; *Availability Analysis of Span-Restorable Mesh Networks*, IEEE JSAC, vol. 20, May 2002, pp. 810–21.

[DOV94] DOVERSPIKE, R.; WILSON, B.; *Comparison of capacity efficiency of DCS network restoration routing techniques*. Journal of Network and Systems Management 1994; 2(2): pp. 95–123.

[DOV01] DOVERSPIKE, R.; YATES, J.; *Challenges for MPLS in Optical Network Restoration*, IEEE Communications Magazine, 2001, pp. 89-96.

[ELB02] EL-BAWAB, T.; JONG-DUG, S.; *Optical packet switching in core networks: between vision and reality*. IEEE Communications Magazine 40, 9; September 2002, 60–65.

[FAW04] FAWAZ, W.; AUDOUIN, B.; BERDE, B.; VIGOUREUX, M.; DU-POND, M.; E PUJOLLE, G.; *Service Level Agreement and Provisioning in Optical Networks*. IEEE Communications Magazine 42, 1; January 2004, pp. 36–42.

[FEL00] FELDMANN, A.; GREENBERG, A.; LUND, C.; REINGOLD, N.; E REXFORD, J.; *NetScope: Traffic engineering for IP networks*. IEEE Network Magazine, March 2000, pp. 11 - 19.

[FOR02] FORTZ, B.; REXFORD, J.; E THORUP, M.; *Traffic Engineering with Traditional IP Routing Protocols*. IEEE Communication magazine, Vol. 40, 10; 2002, pp. 118-124.

[GER00] GERSTEL, O.; E RAMASWAMI, R.; *Optical layer survivability, An implementation perspective*. IEEE J. Select. Areas Communications, vol. 18, 10; October 2000, pp. 1885–1899.

[GIA04] GIANSANTE, E.; IOVANNA, P.; ORIOLO, G.; PASCALI, F.; ROMAGNOLI, A.; SABELLA, R.; *Offline Protection Algorithm in a MPLS-based scenario*. Workshop on Traffic Engineering, Protection and Restoration for NGI, 2004.

[GRO98] GROVER, W. D.; E STAMATELAKIS, D.; *Cycle-oriented distributed preconfiguration: Ring-like speed with mesh-like capacity for self-planning network restoration*. IEEE International Conference on Communications (ICC 1998), pp. 537-543.

[GRO04] GROVER, W.; *Mesh-based survivable networks: options and strategies for optical, MPLS, SONET and ATM networks*. Upper Saddle River, NJ: Prentice-Hall PTR; 2004.

[GUA02] GUANGZI, LI; WANG, D.; KALMANEK, C.; E DOVERSPIKE, R.; *Efficient distributed path selection for Shared Restoration Connections*. INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE Volume 1, 2002, pp. 140 – 149.

[GUA08] WANG, D.; GUANGZHI, LI*, Efficient Distributed Bandwidth Management for MPLS Fast Reroute*. IEEE/ACM Transactions on Networking, Vol. 16, No. 2; April 2008; pp. 486-495.

[GUO09] GUO, L.; WANG, X.; CAO, J.; ZHENG, X.; *Recovery escalation with load balancing and backup resources sharing in survivable WDM optical networks*. Photon Network Communication, Vol. 18; 2009; pp. 393–399.

[GRE01] GREEN, P.; *Progress in optical networking*. IEEE Communications Magazine Vol. 39, 1; January 2001, pp. 54–61.

[HAR98] HARAI, H.; MURATA, M.; E MIYAHARA, H.; *Performance analysis of wavelength assignment policies in all-optical networks with limited-range wavelength conversion*. IEEE JSAC Vol. 16, 7; September 1998, pp. 1051–1060.

[HUA04] HUANG, Y.; WEN, W.; HERITAGE, J. P.; MUKHERJEE, B.; *A generalized Protection Framework Using a New Link-State Availability Model for Reliable Optical Networks*. Journal of Wavelength Technology, vol. 22, n. 11, November 2004, pp. 2536-2547.

[IRA96] IRASCHKO, R.; MACGREGOR, M.; GROVER, W.; *Optimal capacity placement for path restoration mesh survivable networks*. In IEEE International Communications and Conference (ICC'96), Vol. 3, 1996, pp. 1568–74.

[IRA98] IRASCHKO, R.; MACGREGOR, M.; GROVER, W.; *Optimal capacity placement for path restoration in STM or ATM mesh survivable networks*. IEEE/ACM Transactions on Networking 1998; Vol. 6, 3; pp. 325–336.

[KAN09] KANTARCI, B.; MOUFTAH, H. T.; OKTUG, S. F.; *Adaptive Schemes for Differentiated Availability-Aware Connection Provisioning in Optical Transport Networks*. Journal of Lightwave Technology, Vol. 27, no. 20, Oct. 2009, pp. 4595-4602.

[KEN07] KENNINGTON, J.; OLINICK, E.; SPIRIDE, G.; *Basic mathematical programming models for capacity allocation in mesh-based survivable networks*. Study Omega 35, 2007, pp. 629 – 644.

[KUW09] AL-KUWAITI, M.; KYRIAKOPOULOS, N.; E HUSSEIN, S.; *A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability*. IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Second Quarter 2009.

[LEE02] LEE, Y.; SEOK, Y.; e CHOI, Y.; *Traffic Engineering with Constrained Multipath Routing in MPLS Networks*. IEICE Transaction. Communications., Vol. E85–A, No.1 January 2002.

[LIU04] CHU, X.; LIU, J.; E ZHANG, Z.; *Analysis of sparse-partial wavelength conversion in wavelength-routed WDM networks*. In Proc. IEEE INFOCOM, March 2004, pp. 1363–1371.

[LUM01] LUMETTA, S. S.; E MEDARD, M.; *Towards a deeper understanding of link restoration algorithms for mesh networks*. In Proc. IEEE INFOCOM 2001, pp. 367–375.

[MAE03] MAESSCHALCK, S.; COLLE D.; LIEVENS I.; PICKAVET M.; DEMEESTER, P.; *Pan-European Optical Transport Networks: An Availability-based Comparison*. Photonic Networks Communications, Vol. 5, No. 3; 2003, pp. 203 - 225.

[MEL05] MELLO, D. A. A.; SCHUPKE, D. A.; WALDMAN, H.; *A Matrix-Based Analytical Approach to Connection Unavailability Estimation in Shared Backup Path Protection*. IEEE Communications Letters, Vol. 9, No. 9, September 2005.

[MOH01] MOHAN, G.; MURTHY, C. S. R.; E SOMANI, A.; *Efficient algorithms for routing dependable connections in WDM optical networks*. IEEE/ACM Transactions on Networking, Vol. 9; 2001, pp. 553 - 566.

[MUK04] ZHANG, J.; E MUKHERJEE, B.; *A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges*. IEEE Network, March/April 2004, pp. 41 - 48.

[MYK06] MUKHERJEE, B.; *Optical Networks*. New York: Springer-Verlag, 2006.

[OZD03] OZDAGLAR, A.; E BERTSEKAS, D.; *Routing and wavelength assignment in optical networks*. IEEE/ACM Transactions on Networking Vol. 11, 2; April 2003, pp. 259 – 272.

[PEL05] MELLO, D.A.A.; PELEGRINI, J.U.; RIBEIRO, R.P.; SCHUPKE, D.A.; WALDMAN, H.; *Dynamic provisioning of shared-backup path protected connections with guaranteed availability requirements*. Broadband Networks, 2005. BroadNets 2005, 2nd International Conference on, Vol. 2, October 2005, pp. 1320 - 1327.

[QIA02] QIAO, C.; XIONG, Y. E XU, D.; *Novel Models For Efficient Shared-Path Protection*, Proc. OFC, March 2002, pp. 546–547.

[RAJ04] RAJAGOPALAN, B.; LUCIANI, J.; E AWDUCHE, D.; *IP over Optical Networks: A Framework*. Internet RFC 3717, March 2004: Informational.

[RAM95] RAMASWAMI, R.; E SIVARAJAN, K. N.; *Routing and wavelength assignment in all-optical networks*. IEEE/ACM Trans. Networking, vol. 3, October 1995, pp. 489–500.

[RAM02] RAMASWAMI, R.; SIVARAJAN, K.; *Optical networks: a practical perspective*. New York, NY: Morgan Kaufman Publishers, Inc.; 2002.

[RAM03] RAMAMURTHY, S.; SAHASRABUDDHE, L.; E MUKHERJEE, B.; *Survivable WDM mesh networks*. Journal of Lightwave Technology, Vol. 21, no. 4, 2003, pp. 870 – 883.

[RAM98] RAMAMURTHY, S.; E MUKHERJEE, B.; *Fixed-alternate routing and wavelength conversion in wavelength-routed optical networks*. In IEEE GLOBECOM 98, November 1998, pp. 2295–2302.

[REN97] RENAUD, M.; MASETTI, F.; GUILLEMOT, C.; E BOSTICA, B.; *Network and system concepts for optical packet switching*. IEEE Communications Magazine Vol. 35, no. 4, September 1997, pp. 96–102.

[SAA04] SAAD, M.; E LUO, Z.; *On the routing and wavelength assignment in multifiber WDM networks*. IEEE JSAC Vol. 22, no. 9, September 2004, pp. 1708–1717.

[SAH09] SAHARA, A.; TSUKISHIMA, Y.; TAKAHASHI, T.; OKUBO, Y.; YAMADA, K.; MATSUDA, K. E TAKADA, A.; *Demonstration of colorless and directed/directionless ROADMs in Router network*. OSA/OFC/NFOEC 2009, pp. 1 - 3.

[SHI98] SHIRAGAKI, T.; HENMI, N.; KATO, T.; FUJIWARA, M.; SHIOZAWA, M.; E SUZUKI, S.; *Optical cross-connect system incorporated with newly developed operation and management system*. IEEE JSAC, Vol. 16, no. 7, September 1998, pp. 1179–1189.

[SUU84] SUURBALLE, J. W. E TARJAN, R. E.; *A Quick Method For Finding Shortest Pairs of Disjoint Paths*. Networks, vol. 14, 1984, pp. 325 – 336.

[TAP03] HO, P-H.; TAPOLCAI, J.; E MOUFTAH, H. T.; *Diverse Routing for Shared Protection in survivable optical networks*. In Proc. IEEE Global Telecommunications Conference (GLOBECOM 2003), Vol. 5, December 2003, pp. 2519-2523.

[THE05] THEOPHILOPOULOS, G.; KALYVAS, M.; YIANNOPOULOS, K.; VLACHOS, K.; VARVARIGOS, E.; AVRAMOPOULOS, H.; *An alternative implementation perspective for the scheduling switch architecture*. IEEE Journal of Lightwave Technology, Vol. 23, no. 2, February 2005, pp. 732–739.

[WUT08] WUTH, T.; CHBAT, M.W.; E KAMALOV, V.F.; *Multi-rate (100G/40G/10G) Transport over Deployed Optical Networks*. Proceedings, Optical Fiber communication /National Fiber Optic Engineers Conference 2008, February, 2008, pp. 1 - 9.

[XIA07] XIAOFEI CHENG; XU SHAO; YIXIN WANG; *Multiple link failure recovery in survivable optical networks*. Photon Network Communications, Vol. 14, 2007; pp. 159-164.

[XIO99] XIONG, Y., MASON, L.; *Restoration strategies and spare capacity requirements in self-healing ATM networks*. IEEE/ACM Transactions on Networking 1999; 7(1), pp. 98–110.

[YOO03] YOO, Y.; AHN, S.; E KIM, C.; *Adaptive routing considering the number of available wavelengths in WDM networks*. IEEE JSAC Vol. 21, no. 8, October 2003, pp. 1263 – 1273.

[ZHA03] ZHANG, J. *et al.*, *On The Study Of Routing And Wavelength-Assignment Approaches for Survivable Wavelength-routed WDM Mesh Networks*. SPIE Optical Networks Magazine, November/December, 2003.

[ZHA04] ZHANG, J.; E MUKHERJEE, B.; *A review of fault management in WDM mesh networks: basic concepts and research challenges*. IEEE Network, vol. 18, no. 2, March-April 2004, pp. 41 - 48.

[ZHA07] ZHANG, J.; ZHU, K.; ZANG, H.; MATLOFF, N.S.; MUKHERJEE, B.; *Availability-Aware Provisioning Strategies for Differentiated Protection Services in Wavelength-Convertible WDM Mesh Networks*. IEEE/ACM Transactions on Networking, vol.15, no.5, October 2007, pp.1177-1190.

[ZHO00] ZHOU, D.; E SUBRAMANIAM, S.; *Survivability in optical networks*. IEEE Network, vol. 14, November–December 2000, pp. 16 – 23.

[ZHO07] ZHOU, L.; HELD, M.; SENNHAUSER, U.; *Connection Availability Analysis of Shared Backup Path-Protected Mesh Networks*. Journal of Lightwave Technology, Vol. 25, No. 5, May 2007.