

Um Mecanismo de Proteção em Redes WDM em Malha

Marco D. D. Bicudo e Otto Carlos M. B. Duarte *

¹Grupo de Teleinformática e Automação
PEE-COPPE/DEL-POLI
Universidade Federal do Rio de Janeiro
C.P. 68504 - CEP 21945-970
Rio de Janeiro - RJ - Brasil

bicudo@gta.ufrj.br, otto@gta.ufrj.br

Resumo. Este artigo analisa, através de simulação, o desempenho de diferentes mecanismos de proteção em redes IP-sobre-WDM. São analisados alguns mecanismos convencionais e um novo é proposto visando a utilização mais eficiente da rede. Este novo mecanismo aumenta o compartilhamento entre canais ópticos de proteção para que a rede utilize seus recursos mais eficientemente. As simulações mostram que este mecanismo apresenta desempenho superior quando comparado aos mecanismos convencionais. As métricas utilizadas nas análises de desempenho são a probabilidade de bloqueio e a disponibilidade das conexões estabelecidas com sucesso. O simulador utilizado foi desenvolvido em C++, utilizando bibliotecas de softwares livres como o STL (Standard Template Library).

Abstract. This article analyzes, through simulation, the performance of different IP-over-WDM protection mechanisms. We analyze some existing mechanisms and propose a novel one which use network resources more efficiently. This novel mechanism increases the share ability among backup lightpaths to reach a better efficiency. The simulations shows that the mechanism presents superior performance when compared to the conventional ones. The performance metrics used in the analysis are the blocking probability and the connections availability. The simulator developed using C++, uses free-software libraries, like STL (Standard Template Library).

1. Introdução

O modelo atual de redes ópticas para interconexão de redes IP apresenta o ATM (*Asynchronous Transfer Mode*) ou o SONET (*Synchronous Optical Network*) em sua camada óptica. Estas tecnologias, porém, apresentam um comportamento pouco dinâmico, pois seu ambiente operacional, baseado em conexões de banda fixa (OC-n), é geralmente estabelecido manualmente, e, portanto, não é o mais apto para a dinâmica de conexão e desconexão de canais ópticos.

Os principais fatores para o baixo desempenho destas tecnologias de rede são o processamento eletrônico de pacotes, que insere um atraso a cada nó da rede, e o uso ineficiente dos recursos da rede, que acarreta em uma indisponibilidade de recursos. Um modelo apontado por [Vasseur et al., 2004] e [Maesschalk et al., 2002] como sendo mais

*Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ, FINEP, RNP e FUNTTEL.

adaptado às necessidades atuais, é o modelo multicamadas IP/GMPLS (*Multiprotocol Label Switching*)-sobre-WDM (*Wave-length Division Multiplexing*). Neste modelo, o uso do protocolo IP é pré-requisito principalmente devido ao seu sucesso e ampla utilização na Internet. As previsões apontam para um cenário, num futuro não muito distante, onde todas as redes de telecomunicações serão baseadas no protocolo IP para transmissão de dados, voz, imagem e vídeo. Neste modelo utiliza-se a multiplexação por comprimento de onda, o WDM, na camada física para satisfazer a demanda de banda passante. Assim pode-se multiplexar em uma única fibra vários canais ópticos. Embora a tecnologia WDM permita aumentar a capacidade de transmissão dos enlaces, a taxa de transmissão fim-a-fim é limitada pelos comutadores ópticos OXC (*Optical Cross Connects*) opacos. Um OXC é um comutador capaz de encaminhar um feixe de laser de uma porta óptica de entrada para uma porta óptica de saída. Estes comutadores podem utilizar conversores O-E-O para o encaminhamento do feixe ou realizá-lo totalmente no plano óptico, sem conversões para o plano elétrico/eletrônico. Os OXCs totalmente ópticos são chamados de OXCs transparentes, e os OXCs que utilizam conversores O-E-O são chamados OXCs opacos. Os OXCs opacos, por apresentarem conversões óptico-eletrônico-óptico (O-E-O), aumentam o atraso fim-a-fim e o tamanho dos *buffers*, e conseqüentemente diminuem a banda passante agregada da rede. Por este motivo a utilização de um OXC transparente é uma solução para este problema de limitação de banda. Em uma rede opaca a conversão de comprimento de onda, ou simplesmente *lambdas*, é realizada de maneira direta, pois como existem conversões O-E-O. Esta operação não é realizada com a mesma facilidade em uma rede transparente, pois necessita da presença de conversores ópticos. A introdução do MPLS na camada IP agrega funcionalidades à rede, pois seus circuitos virtuais (os LSPs - *Label Switched Path*) fornecem a possibilidade de Engenharia de Tráfego, VPN e QoS. A generalização do MPLS, o GMPLS [Mannie, 2004], proporciona funcionalidades como o estabelecimento dinâmico de canais ópticos, introduzindo o conceito de Redes Ópticas de Comutação Automática (ASON - *Automatic Switched Optical Network*), como é descrito por Colle et al. [Colle et al., 2002].

Neste novo paradigma de rede óptica, a camada óptica utiliza a topologia física da rede para estabelecer estes caminhos. Este procedimento se baseia, principalmente, na disponibilidade de *lambdas* nas fibras. O estabelecimento destes caminhos da camada óptica gera uma topologia virtual da rede para a camada IP/GMPLS. Esta camada, por sua vez, utiliza a topologia virtual para estabelecer suas conexões, os LSPs (*Label Switched Paths*), como apresenta a Figura 1.

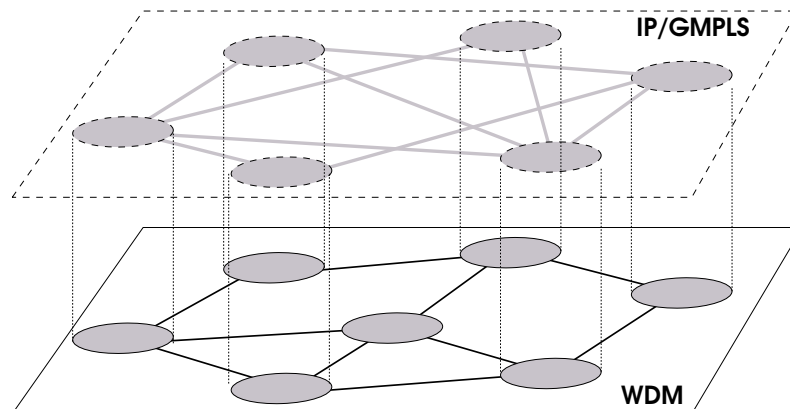


Figura 1: Topologia Física e Virtual

Com a multiplexação de vários canais em uma única fibra-óptica, o evento de uma falha é cada vez mais significativo para a rede, pois o interrompimento de uma fibra pode

interferir no serviço oferecido a diversas conexões. Neste contexto, a sobrevivência a falhas em redes ópticas é quesito essencial no projeto e operação destas redes.

Conforme as redes ópticas migraram da topologia em anel, muito comumente encontrada em redes SONET/SDH, para a topologia em malha, por questões de escalabilidade e de redundância excessiva, as deficiências da nova topologia adotada para implementar mecanismos de sobrevivência a falhas ficaram evidentes. A simplicidade nas decisões a serem tomadas da topologia em anel favorece a implementação destes mecanismos, já que existem somente duas alternativas para o envio de dados. Por outro lado, as redes em malha apresentam múltiplos caminhos e necessitam de estabelecimento de conexões para enviar dados da origem ao destino. Desde então muitas pesquisas relacionadas à restauração/proteção em redes WDM em malha se desenvolveram visando solucionar este problema da confiabilidade da rede, que, conseqüentemente, afeta a disponibilidade das conexões.

Recentemente, foram propostos mecanismos de sobrevivência a falhas, tanto de proteção como de restauração, visando uma rede que possa combinar as vantagens de redundância e resiliência da topologia em anel e as vantagens de eficiência e escalabilidade da topologia em malha. Dentre estas propostas, existem as que oferecem uma abordagem na camada IP/GMPLS como os algoritmos BIRA e HIRA proposto por Zheng et al. [Zheng e Mohan, 2003] e o algoritmo de Kodialam et al. [Kodialam e Lakshman, 2001], visando a versatilidade, maior granularidade e flexibilidade de configuração desta camada. Outras têm um enfoque mais voltado para a recuperação na camada WDM como em [Wang et al., 2002], [Ramamurthy e Mukherjee, 1999] e [Zhang e Mukherjee, 2004], que proporcionam um tempo de recuperação menor, devido à menor granularidade e por não ser necessário sinalização extra. Ou et al. [Ou et al., 2002] e Zang et al. [Zhang, 2003] apresentam esquemas de proteção de sub-caminho como uma alternativa viável para reduzir o tempo de restauração, já que a sinalização não necessita percorrer toda extensão do caminho óptico para ser iniciado o procedimento de recuperação.

Este artigo analisa, através do simulador desenvolvido, o desempenho de esquemas de proteção em redes ópticas WDM. É analisado o impacto destes esquemas de proteção na probabilidade de bloqueio e disponibilidade das conexões. Um novo mecanismo de proteção é proposto visando a utilização mais eficiente da rede. Este novo mecanismo aumenta o compartilhamento de canais de proteção das conexões ópticas, para que a rede atinja uma maior eficiência. O resto do artigo está organizado como segue. Na Seção 2 são introduzidos alguns conceitos sobre redes ópticas IP, Gerenciamento de Falhas em redes ópticas e as métricas mais comumente utilizadas. Nesta seção, também são descritas as vantagens e desvantagens dos mecanismos de proteção e restauração e as vantagens da implementação do mecanismo na camada IP/GMPLS e na camada WDM. Na Seção 3, é descrito o mecanismo de proteção WDM proposto e seu funcionamento. A Seção 4 descreve como foram realizadas as simulações, a aquisição de dados e analisa os resultados das simulações. A Seção 5 discute as conclusões deste artigo.

2. Conceitos Básicos

Conforme o conhecimento na operação e gerenciamento de redes ópticas transparentes amadurece, pesquisas tendem a abordar o problema pela perspectiva de serviço [Fawaz et al., 2004] [Gerstel e Ramaswani, 2000]. Assim, passam a ser o alvo das pesquisas o oferecimento de Qualidade de Serviço (QoS), quais devem ser os parâmetros e seus os valores ideais para garantir o contrato SLA (*Service Level Agreement*) assi-

nado com o cliente. Vamos introduzir brevemente alguns dos principais parâmetros de desempenho das redes ópticas transparentes que serão utilizados neste artigo. O índice de disponibilidade do serviço, ou simplesmente disponibilidade, é definido como a probabilidade de, em um tempo no futuro, o serviço estar operacional. Esta métrica pode ser computada experimentalmente baseada na taxa de falha e taxa de recuperações bem sucedidas. Em termos práticos, significa a porcentagem de tempo que o serviço está operacional durante todo o tempo de serviço. É importante notar que a disponibilidade não depende somente da taxa de falha e de recuperação. Esta depende também da política de operação e dos mecanismos de proteção utilizados. A confiabilidade de uma conexão é a probabilidade desta estar operando, ininterruptamente, por um período de tempo. A confiabilidade e a disponibilidade são parâmetros diferentes. Enquanto a confiabilidade está relacionada com o número de interrupções, a disponibilidade está relacionada à porcentagem de tempo que o serviço esteve operacional. A probabilidade de bloqueio é uma métrica que geralmente não está presente nos contratos de SLA, mas é de grande interesse para as operadoras de redes ópticas. A probabilidade de bloqueio é um parâmetro que pode ser utilizado para medir a eficiência de utilização da rede. Um uso mais eficiente significa poder vender o serviço para um maior número de clientes com a mesma quantidade de recursos.

Nas redes ópticas em malha, os mecanismos de gerenciamento de falhas são divididos, basicamente, em duas classes. Os mecanismos que pré-computam e pré-aloçam os recursos de recuperação, chamados de proteção, e os mecanismos que computam os recursos de recuperação reativamente, chamados de restauração. Os mecanismos de restauração utilizam os recursos da rede mais eficientemente que os mecanismos de proteção, pois não necessitam alocar estes recursos em avanço. Neste mecanismo, o canal óptico de restauração será estabelecido somente quando a falha de um enlace afetar o canal primário da conexão. Os mecanismos de proteção alocam previamente os recursos e, conseqüentemente, prejudicam a aceitação de conexões futuras. Porém, apesar deste uso ineficiente da rede, os mecanismos de proteção oferecem um tempo de restauração consideravelmente menor que os mecanismos de restauração.

Os mecanismos de proteção podem ser classificados com relação a dois aspectos: a camada em que é implementado e o segmento do canal que este se propõe a atuar. Atualmente, existem três segmentações de canal óptico que estão em evidência nas pesquisas em proteção: proteção de canal, de enlace e de sub-canal. Na proteção de canal óptico, apresentada na Figura 2(a), o tráfego é redirecionado, na origem, para um canal de proteção, logo que uma falha é detectada em um dos enlaces pertencentes ao seu canal primário. Isto acarreta em um canal de proteção adicional inteiramente novo da origem ao destino. Este canal de proteção deve utilizar enlaces disjuntos dos enlaces primários para que uma única falha não atinja ambos os canais. A proteção de sub-canal óptico, apresentada na Figura 2(b), é um mecanismo alternativo que reduz o tempo de restauração da conexão. Esta proteção, proposta por Ou et al. [Ou et al., 2002] e Zang et al. [Zhang, 2003], proporciona tempos de restauração menores, pois a sinalização da falha não necessita percorrer todo o canal óptico para iniciar os procedimentos de recuperação. Em contrapartida, este mecanismo prejudica a eficiência dos recursos da rede. A proteção de enlace, apresentada na Figura 2(c), apresenta o menor tempo de recuperação, mas acarreta em uma utilização ineficiente da rede.

A sobrevivência em redes IP-sobre-WDM pode ser implementada tanto na camada WDM quanto na cada IP/GMPLS. Na camada WDM, cada canal óptico primário é protegido por um outro canal óptico. Na camada IP/GMPLS, cada LSP primário é protegido por um outro LSP. A proteção WDM proporciona um tempo de restauração menor que a

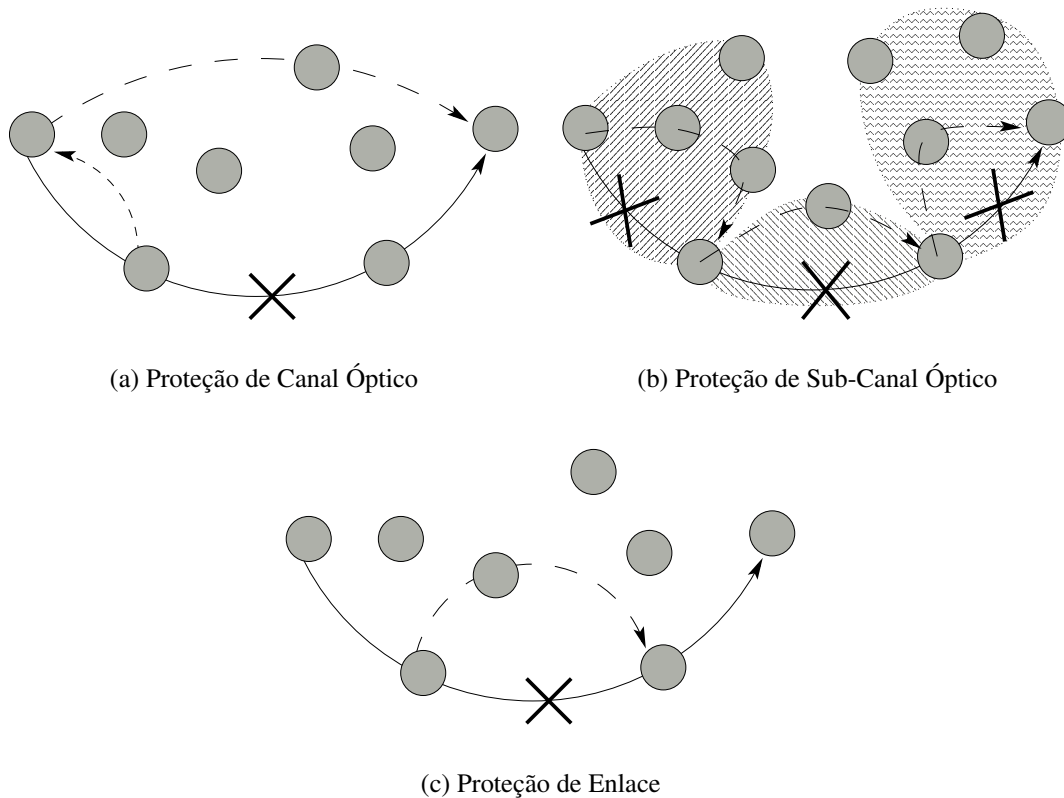


Figura 2: Mecanismos de Proteção

proteção IP, pois não depende de sinalização e temporização para detectar a falha. Como o mecanismo de proteção IP não tem acesso aos sensores/receptores ópticos que detectam a interrupção da portadora, estes necessitam, portanto, enviar periodicamente mensagens de HELLO para detectar a falha. Mesmo na implementação de um mecanismo integrado que permita a sinalização do evento de falha da camada WDM para a camada IP, como proposto por Zheng et al. em [Zheng e Mohan, 2003], o tempo de restauração da proteção IP será superior ao da proteção WDM. Como um único canal óptico pode transportar até milhares de conexões LSPs, o desempenho da camada IP/MPLS continua prejudicado pela sobrecarga computacional associada ao grande número de procedimentos necessários à recuperação da falha. A proteção WDM, em contrapartida, executa o procedimento somente uma vez para cada canal óptico. A desvantagem da proteção WDM é o isolamento entre recursos primários e de proteção. O isolamento significa que, na proteção WDM, uma vez que um canal óptico é reservado para recuperação, este não será cogitado como um recurso disponível. Na proteção IP/MPLS este isolamento não ocorre, pois LSPs primários e de recuperação coexistem em um mesmo canal óptico.

2.1. A Proteção WDM

Alcançar um tempo de restauração equivalente às redes SONET é uma necessidade para a substituição desta tecnologia legada ainda muito utilizada em telecomunicações. Para que uma rede WDM em malha alcance este objetivo é necessário o desenvolvimento de mecanismos de proteção WDM. Apesar da proteção IP ser mais eficiente que a proteção WDM, a proteção WDM é a única capaz de atingir os 50 milissegundos das redes SONET. Por este motivo, somente a proteção WDM será abordada daqui em diante.

A introdução de mecanismos de proteção em redes ópticas acrescenta um ele-

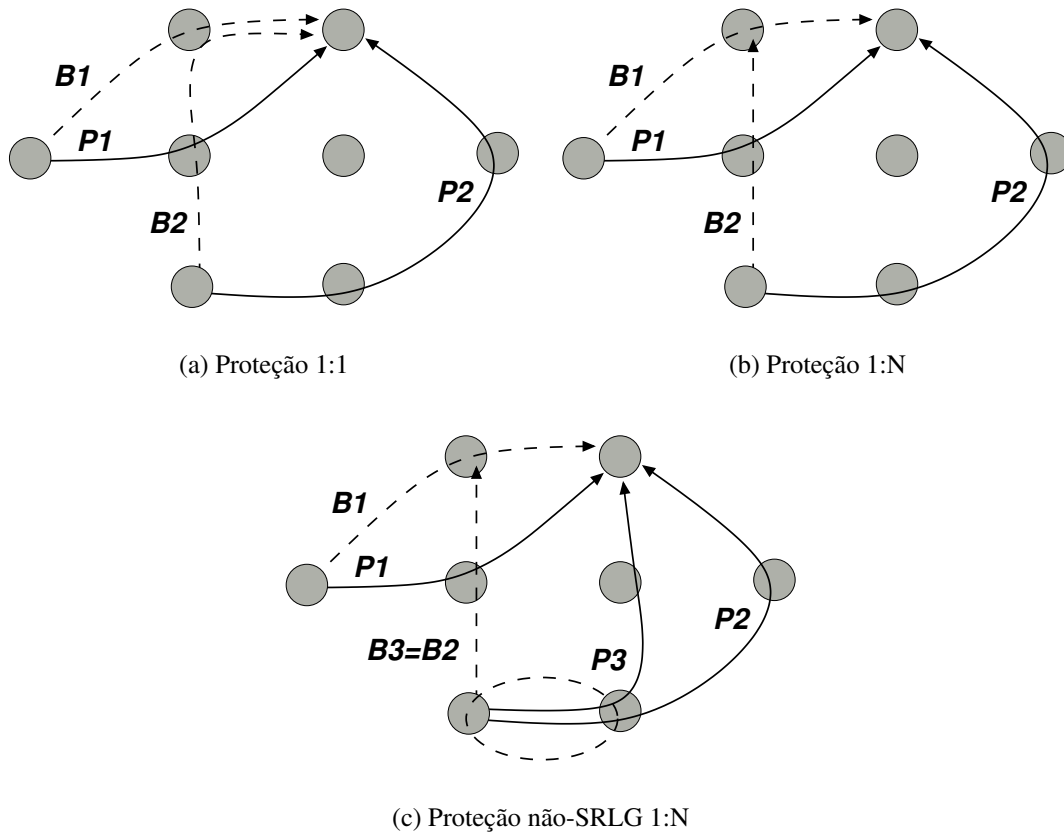


Figura 3: Mecanismos de Proteção WDM

mento no conceito de conexão óptica. Independente do mecanismo de proteção utilizado, uma conexão óptica consiste, agora, em um canal óptico primário e um canal óptico de proteção. A impossibilidade do estabelecimento de um dos dois canais acarreta no bloqueio da conexão. O mecanismo de proteção mais simples e de implementação direta é a proteção 1:1, que implica no estabelecimento de dois canais ópticos para cada conexão óptica. Este mecanismo é ineficiente, e desperdiça preciosos recursos da rede, pois duplica os recursos necessários para uma conexão óptica. A proteção 1:N é uma alternativa mais eficiente à proteção 1:1. Esta proteção permite que dois, ou mais (N), canais de proteção compartilhem lambdas, desde que seus canais primários satisfaçam as restrições SRLG (*Shared Risk Link Group*). A restrição SRLG define que canais de proteção podem compartilhar lambdas em um enlace se, e somente se, seus os canais primários correspondentes não pertencerem ao mesmo grupo de risco de falha de enlace, e, portanto, não falhem simultaneamente. Desta forma, é possível aumentar a eficiência, sem que isto acarrete em um detrimento da disponibilidade das conexões.

O comportamento da proteção WDM 1:1 e 1:N é ilustrado na Figura 3(a) e 3(b), respectivamente. Analisando as figuras, podem-se constatar as diferenças no comportamento de cada mecanismo. A proteção 1:N realoca recursos para o canal de proteção B1 que já foram previamente alocados B2. Já a proteção 1:1 necessita alocar um novo lambda, desnecessariamente, como é verificado na Figura 3(a). Este comportamento acarreta, obviamente, em maior probabilidade de bloqueio, pois o estabelecimento das futuras conexões será comprometido devido a menor disponibilidade de recursos.

3. O Mecanismo Proposto

Apesar da proteção 1 : N apresentar o melhor desempenho dentre os mecanismos convencionais, existem aprimoramentos que podem ser realizados ao estabelecimento de conexões ópticas que podem alcançar uma menor probabilidade de bloqueio de conexões futuras. O operador da rede pode, por algum motivo, querer tornar a rede mais eficiente mesmo que a um custo de alguns parâmetros de QoS, como a disponibilidade das conexões, por exemplo. O mecanismo proposto, chamado Proteção 1 : N não-SRLG, atinge este objetivo e, portanto, reduz perceptivelmente a probabilidade de bloqueio. Esta redução é obtida aumentando o compartilhamento existente entre os canais de proteção. É evidente que estas modificações acarretam em um compromisso entre a probabilidade de bloqueio e a disponibilidade das conexões. As regras de restrição SRLG são modificadas para satisfazer as necessidades do novo mecanismo. A nova condição para o compartilhamento deve permitir que canais de proteção, que apresentem uma porcentagem máxima de enlaces em comum no canal primário, compartilhem recursos entre si. Esta porcentagem máxima de enlaces em comum dos canais primários que é base de decisão para o compartilhamento de recursos de proteção é denominada porcentagem-SRLG. Este índice, que representa uma relação entre duas conexões ópticas, apresenta um comportamento bidirecional. Tomando a Figura 3(c) como referência, a porcentagem-SRLG do canal primário $P2$ em relação a $P3$ é 25%, pois $P2$ utiliza quatro enlaces primários e tem um enlace em comum com o caminho $P3$, enquanto a porcentagem-SRLG de $P3$ para $P2$ é de 33%, pois o canal $P3$ utiliza somente três enlaces da rede. Como o objetivo do índice porcentagem-SRLG visa obter uma justiça no compartilhamento, e este índice apresenta um comportamento bidirecional, é necessário que o índice máximo entre as conexões ópticas seja utilizada. Assim, uma conexão com muitos saltos não será favorecida em detrimento da disponibilidade de conexões de poucos saltos.

A Figura 3 ilustra como o mecanismo não-SRLG se diferencia do mecanismo SRLG. O funcionamento não-SRLG é apresentado na Figura 3(c). É direta a verificação de que as conexões ópticas dos canais primários $P2$ e $P3$ não compartilhariam o canal de proteção $B2$ se a proteção SRLG estiver operacional, pois estas compartilham um enlace, como destacado na Figura 3(c). Visando o compartilhamento na rede, este novo mecanismo permite que a conexão 2 compartilhe o canal de proteção $B2$ com a conexão 3. Desta maneira, a probabilidade de bloqueio de conexões futuras diminui. A contrapartida é o detrimento da disponibilidade das conexões, pois agora existe a possibilidade do canal de proteção $B2 = B3$ estar indisponível na falha dos canais primários $P2$ ou $P3$.

O funcionamento do mecanismo de proteção pode ser dividido em três procedimentos básicos: a ponderação dos pesos dos enlaces; a execução do algoritmo descoberta de rota, como um algoritmo de caminho mínimo (*shortest path*), semelhante ao *Dijkstra*; e a reserva de lambda nos enlaces escolhidos pelo algoritmo de roteamento no procedimento anterior. Estes três procedimentos são executados seqüencialmente, em duas rodadas. A primeira computa a rota e aloca os recursos para o canal primário da conexão, e a segunda computa e reserva os recursos para o canal de proteção. O primeiro procedimento associa a cada enlace da rede um peso que será utilizado pelo algoritmo de descoberta de rota. A computação deste peso pondera o estado da rede e parâmetros específicos do enlace, como a porcentagem de uso dos lambdas do enlace. Se o enlace estiver falho, ou se todos os lambdas não estiverem disponíveis, o peso associado será infinito. Desta maneira o algoritmo de roteamento não utilizará este enlace. Se o enlace não estiver falho, nem com os todos os recursos utilizados, o peso associado ao enlace será ponderado baseado na porcentagem de utilização dos lambdas. Assim, o algoritmo de roteamento efetua, de maneira transparente, a Engenharia de Tráfego, distribuindo o tráfego por possíveis ca-

minhos de mesmo custo. O segundo procedimento executa o algoritmo que computa a melhor rota, como o Dijkstra, utilizando o peso previamente associado aos enlaces. O terceiro procedimento aloca, para cada enlace da rota computada anteriormente, qual lambda deve ser utilizado em cada enlace. Para o estabelecimento do canal de proteção, os procedimentos recebem apenas dois ajustes, um no primeiro procedimento e um no terceiro procedimento. O primeiro procedimento deve ponderar/escalar para infinito os enlaces que são utilizados pelo canal primário. Esta deve ser uma regra prioritária sobre as outras. Desta forma, o algoritmo que computa a melhor rota descarta os enlaces utilizados pelo canal primário. O terceiro procedimento deve verificar a possibilidade de compartilhar lambdas na alocação e reserva dos recursos de proteção, caso a rede utilize a proteção 1 : N. Quando o mecanismo proposto é utilizado, o parâmetro porcentagem-SRLG decide se o compartilhamento dos recursos de proteção será realizado.

Na ocorrência de falha de um enlace, os procedimentos de recuperação verificam a disponibilidade do canal de proteção das conexões que utilizam o enlace falho. Se o canal de proteção está disponível, a conexão comuta para o canal de proteção imediatamente. Esta conexão, portanto, não sofre alterações na sua disponibilidade, pois a utilização da proteção é imediata e transparente. Porém, a indisponibilidade dos recursos de proteção da conexão, que pode ser ocasionada devido ao compartilhamento de recursos de proteção, afeta a indisponibilidade da conexão. Esta indisponibilidade da conexão permanece enquanto não ocorre a recuperação do enlace.

4. Simulações e Resultados

Nas simulações são utilizadas duas topologias de rede. As duas, porém, apresentam o mesmo grau de conectividade. A primeira rede, ilustrada na Figura 4, consiste em 6 nós interconectados por 9 enlaces. A segunda rede é a NSFNet, ilustrada na Figura 5, com 16 nós e 23 enlaces. A NSFNet é a rede de pesquisa dos Estados Unidos e tem Pontos de Presença (POP - *Point of Presence*) nos principais centros de pesquisa em tecnologia do país. Ambas as redes foram simuladas com quatro lambdas por fibra. A chegada de requisição de conexão segue a distribuição de Poisson com 2 horas de média. O tempo de duração de cada conexão segue a distribuição exponencial e a média depende da carga de tráfego na rede. O par origem-destino das conexões é sorteado aleatoriamente entre todos os nós da rede. O evento de falha de um enlace na rede segue a distribuição exponencial com média de 50 dias, e o tempo de restauração da falha também é exponencial com média de 12 horas, como apresentado por Zhang et al. em [Zhang e Mukherjee, 2004]. O critério de parada da simulação não é por tempo simulado. O tempo de simulação é baseado no número de conexões por nó, escolhido um número muito grande para que o efeito transitório inicial da rede seja desprezível e o regime permanente de operação da rede seja alcançado. Cada rodada dura uma média de 100.000 conexões por nó, o que equivalem a mais de 20 anos de operação da rede e a mais de 150 eventos de falhas de enlaces. As rodadas de simulação são repetidas quantas vezes necessárias para alcançar 95% de confiabilidade para os intervalos de confiança que são apresentados nos gráficos.

Após cada rodada de simulação são computadas a probabilidade de bloqueio e a disponibilidade das conexões. O cálculo da probabilidade de bloqueio é realizado com base em dois contadores: o número de requisições de conexões; e o número de conexões bloqueadas, independente do motivo para o bloqueio da conexão. A disponibilidade das conexões se baseia no tempo que o serviço permanece indisponível, e no tempo de duração total da conexão. A disponibilidade é um valor adimensional que varia de 0 a 1. Este valor é calculado através da divisão do tempo total que a conexão não esteve

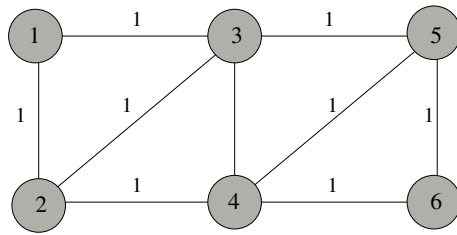


Figura 4: Topologia da Rede 1

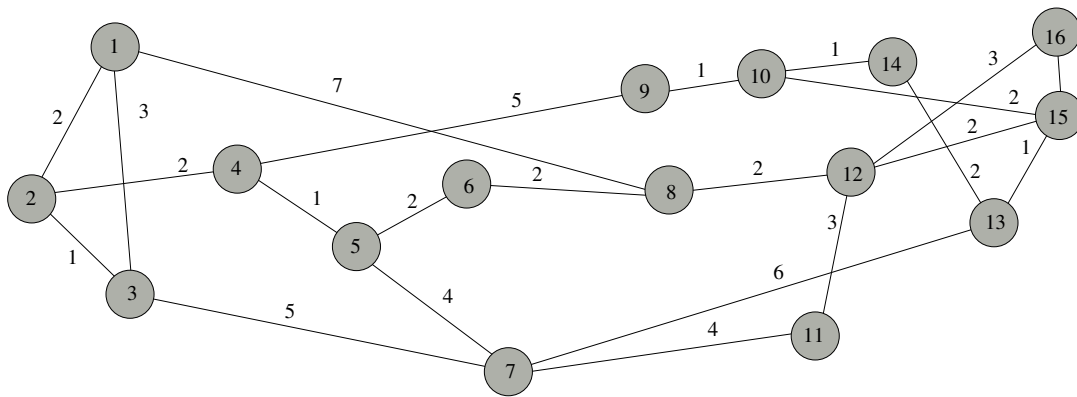


Figura 5: Topologia da Rede 2

operacional pelo tempo de duração total da conexão. Através destes dois parâmetros, o desempenho da rede é comparado para os diferentes mecanismos de proteção.

O simulador, desenvolvido em C++, utiliza a biblioteca de programação genérica STL (*Standard Template Library*) para a manipulação de objetos como a pilha FIFO (*First-In First-Out*) do algoritmo de Dijkstra, criação de listas encadeadas dos eventos, geração de números aleatórios exponenciais e de Poisson, para o escalonamento de eventos de falhas e conexões, etc.

Os gráficos da Figura 6(a) e 6(b) apresentam o comportamento da probabilidade de bloqueio e da disponibilidade da Rede 1, respectivamente. Os gráficos da Figura 7(a) e 7(b) apresentam o mesmo para a Rede 2. As figuras mostram o desempenho das duas redes quando é aplicado nenhum esquema de proteção, proteção 1:1, proteção 1:N, proteção 1:N não-SRLG 50% e proteção 1:N não-SRLG 100%. Como previsto, a resposta de ambas as redes para os mecanismos de proteção foi equivalente. A probabilidade de bloqueio da rede sem mecanismos de proteção foi menor que da rede com qualquer mecanismo de proteção, mas a disponibilidade das conexões, em contrapartida, apresenta os piores resultados. A proteção 1:1 está no outro extremo, pois, apesar de apresentar a melhor disponibilidade entre os mecanismos de proteção, a sua probabilidade de bloqueio é a mais alta, em qualquer cenário, devido à sua ineficiência na utilização dos recursos da rede.

Note que para todos os mecanismos de proteção, a Rede 2 apresenta menor probabilidade de bloqueio que a Rede 1. À primeira vista este comportamento parece óbvio, pois uma rede maior significa mais recursos, e, conseqüentemente, uma melhor acomodação das conexões na rede para uma mesma carga. Porém, este não é o caso. Em ambas, o fator de utilização da rede é o mesmo, ou seja, a razão carga/recursos é igual. O motivo deste desempenho superior da Rede 2 é a multiplexação estatística do estabelecimento de conexões. O maior número de opções possibilita que o algoritmo de descoberta de rotas evite mais facilmente áreas de deficiências de recursos da rede. Estas deficiências

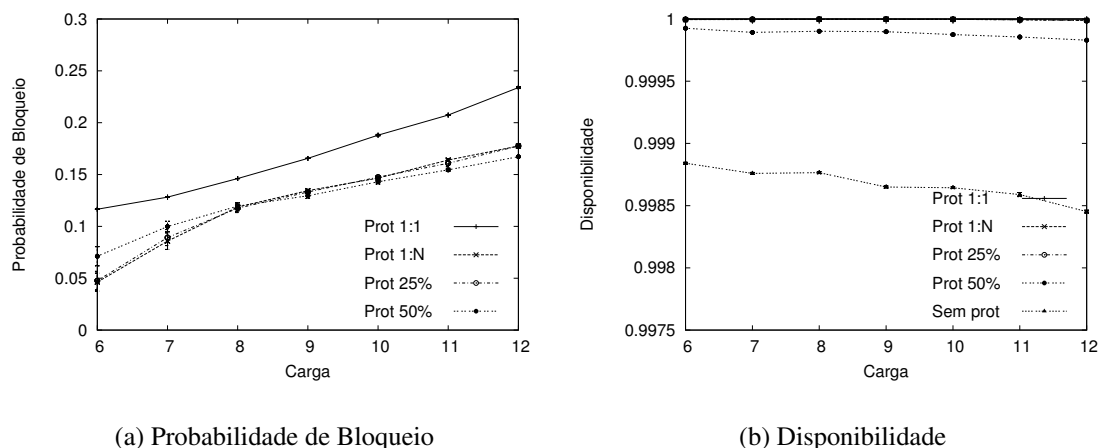


Figura 6: Rede 1

podem ser ocasionadas por motivos variados, como rajadas inesperadas de conexões entre dois nós adjacentes, ou falhas de enlaces.

Analisando a Figura 7(a), vemos que a proteção não-SRLG 50% apresenta um desempenho superior aos outros mecanismos de proteção com relação à probabilidade de bloqueio. A desvantagem, como já previsto, é a disponibilidade das conexões. Devido à disputa de recursos no mecanismo não-SRLG, aumentar a porcentagem-SRLG acarreta na diminuição da probabilidade de bloqueio, mas também diminui a disponibilidade das conexões, o que não é desejado.

Em uma primeira análise, a disponibilidade deveria ser afetada somente pela taxa de falha dos equipamentos da rede, do tempo médio de recuperação das falhas e do mecanismo de proteção utilizado. Percebe-se pelos gráficos um pequeno decremento da disponibilidade das conexões conforme a carga da rede aumenta. Apesar deste comportamento parecer contraditório, ou pelo menos contrário à lógica, pode-se verificar a validade deste comportamento se pensarmos na rede como um conjunto de conexões, e não considerarmos somente uma única conexão. Este comportamento se deve ao número de conexões afetadas pela falha. Quando a rede tem pouca carga, a probabilidade de que nenhuma conexão seja afetada pela falha é grande. No entanto, no da rede estar sobrecarregada, a probabilidade de uma falha afetar muitas conexões é muito alta, e, portanto, a disponibilidade das conexões da rede é prejudicada.

A introdução do parâmetro porcentagem-SRLG possibilita uma flexibilidade na configuração dos mecanismos de proteção. Esta flexibilidade permite que o ajuste do compartilhamento seja realizado em conformidade com as necessidades da rede. Um maior compartilhamento acarreta em menor probabilidade de bloqueio, e, conseqüentemente, o operador pode alocar mais usuários/clientes em uma mesma infra-estrutura de rede.

A probabilidade de bloqueio da rede sem mecanismo de proteção não é representada nos gráficos, pois a escala linear não permite a visualização de valores muito pequenos. Como a ordem de grandeza da probabilidade de bloqueio da rede sem proteção é 10^{-5} , esta só pode ser representada em um gráfico com escala logarítmica. Como o objetivo do trabalho não é comparar o desempenho da rede sem mecanismos de proteção, não foram apresentados gráficos com estas curvas.

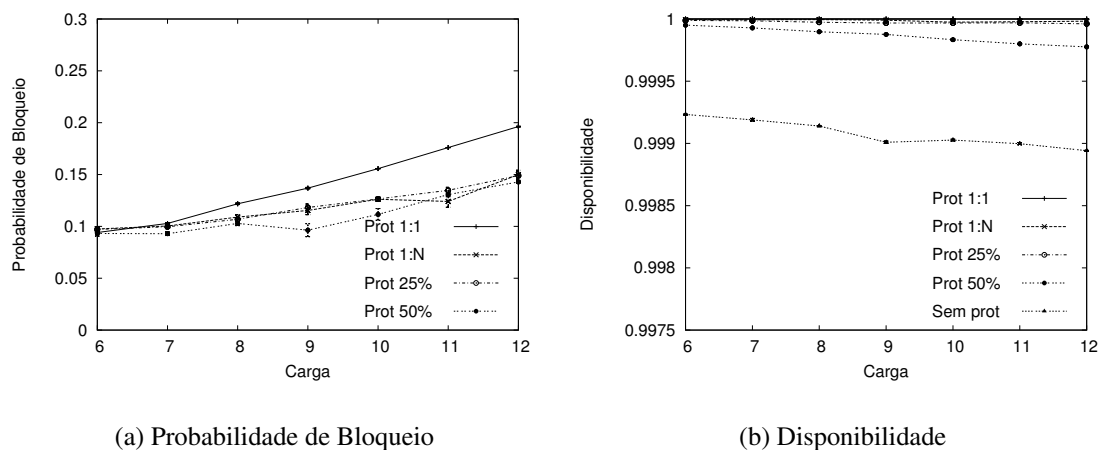


Figura 7: Rede 2

5. Conclusões

O modelo de redes IP-sobre-WDM é considerado o modelo mais apropriado para as necessidades atuais e futuras das redes ópticas que transportam datagramas IP. O conjunto de protocolos GMPLS introduz funcionalidades e extensões de protocolos, como OSPF-TE e CR-LDP, facilitando o gerenciamento e operação destas redes. Este conjunto de protocolos, aliado às necessidades atuais de dinâmica e confiabilidade das redes ópticas, oferece o ambiente propício para as pesquisas na área de proteção e restauração em redes IP-sobre-WDM em malha.

Este artigo apresenta o problema de provimento de sobrevivência à falhas em redes de estabelecimento dinâmico de conexões, e propõe soluções para algumas deficiências dos mecanismos existentes. São estudados diversos mecanismos convencionais de proteção, e novos mecanismos são propostos. O desempenho dos mecanismos é medido através de um simulador próprio desenvolvido em C++. Os gráficos mostram que o mecanismo proposto oferece um compromisso entre vantagens e desvantagens. A introdução do parâmetro porcentagem-SRLG, que possibilita uma maior flexibilidade na configuração dos mecanismos de proteção, permite que o nível de compartilhamento seja ajustado de acordo com a necessidade do operador da rede.

As simulações mostram que o desempenho do mecanismo proposto supera os mecanismos convencionais com relação a probabilidade bloqueio da rede. Isto é possível, pois um maior compartilhamento acarreta em uma menor probabilidade de bloqueio. Com esta flexibilidade de configuração fornece ao operador da rede a possibilidade de alocar mais usuários/clientes para uma mesma quantidade de recursos de rede. Esta alternativa, porém, acarreta em menor disponibilidade da rede, pois nem todas as conexões terão seu canal de proteção disponível no evento de uma falha. Portanto, este mecanismo permite que o operador determine qual parâmetro deve ser priorizado, ponderando suas necessidades e especificações, como contratado pelo cliente através de SLAs. Os gráficos também mostram que a disponibilidade é influenciada pela carga inserida na rede. Este comportamento pode ser explicado pela quantidade de conexões atingidas por uma falha na rede com carga alta e na rede com carga baixa. Quando a rede estiver sobrecarregada de conexões, espera-se que o impacto na disponibilidade seja maior. Outro resultado interessante é a confirmação da multiplexação estatística do estabelecimento das conexões.

Como trabalhos futuros é possível realizar análises matemáticas que descrevam o comportamento teórico dos parâmetros analisados. As teorias de probabilidade e es-

tatística devem ser utilizadas para o estudo. Estes resultados teóricos, comparados com os resultados simulados, resultarão em novas e interessantes conclusões sobre o comportamento da probabilidade de bloqueio e da disponibilidade quando a carga da rede é variada. Também é possível realizar análises de desempenho comparando diferentes topologias de redes, e avaliar o impacto de cada mecanismo de proteção nestas redes e como o grau de conectividade da rede pode afetar estes parâmetros de desempenho.

Referências

- Colle, D., Maesschalck, S., Develder, C., Heuven, P., Groebbens, A., Cheyns, J., Lievens, I., Pickavet, M., Lagasse, P. e Demeester, P. (2002). Data-Centric Optical Networks and Their Survivability. *IEEE JSAC*, 20(1):100–09.
- Fawaz, W., Audouin, B., Berde, B., Vigoureux, M., Du-Pond, M. e Pujolle, G. (2004). Service Level Agreement and Provisioning in Optical Networks. *IEEE Communications Magazine*, 42(1):36–42.
- Gerstel, O. e Ramaswani, R. (2000). Optical Layer Survivability: A Service Perspective. *IEEE Communications Magazine*, 38(3):104–113.
- Kodialam, M. e Lakshman, T. (2001). Integrated Dynamic IP and Wavelength Routing in IP over WDM Networks. Em *Proc. IEEE INFOCOM*.
- Maesschalck, S., Colle, D., Groebbens, A., Develder, C., Lievens, I., Lagasse, P., Pickavet, M., Demeester, P., Saluta, F. e Quagliotti, M. (2002). Intelligent Optical Networking for Multilayer Survivability. *IEEE Communications Magazine*, 40(1):42–49.
- Mannie, E. (2004). Generalized Multi-Protocol Label Switching (GMPLS) Architecture. *Internet RFC 3945*. PROPOSED STANDARD.
- Ou, C., Zhang, H. e Bmukherjee (2002). Sub-Path Protection for Scalability and Fast Recovery in Optical WDM Mesh Network. Em *Proc. OFC*.
- Ramamurthy, S. e Mukherjee, B. (1999). Survivable WDM Mesh Networks: Part I, Protection. Em *ACM Sigcomm*.
- Vasseur, J.-P., Pickavet, M. e Demeester, P. (2004). *Network Recorver: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Morgan Kaufmann Publ., primeira edição.
- Wang, J., Sahasrabudde, L. e Mukherjee, B. (2002). Path vs. Sub-Path vs. Link Restoration for Fault Management in IP-over-WDM Networks. *IEEE Communications Magazine*, 40(11):80–87.
- Zhang, J. (2003). Service Provision to Provide Per-Connection-Based Availability Guarantee in WDM Mesh Network. Em *Proc. OFC*.
- Zhang, J. e Mukherjee, B. (2004). A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges. *IEEE Network*, 18(2):41–48.
- Zheng, Q. e Mohan, G. (2003). Protection Approaches for Dynamic Traffic in IP/MPLS-over-WDM Networks. *IEEE Communications Magazine*, 41(5):S24–29.