

Desempenho de Algoritmos de Proteção por Caminho Compartilhado Sensíveis às Limitações da Camada Física em Redes WDM

Sávio R. A. dos S. Rosa¹, André C. Drummon¹, Nelson L. S. da Fonseca¹

¹Instituto de Computação – Universidade Estadual de Campinas (UNICAMP)

savio@lrc.ic.unicamp.br, {andred,nfonseca}@ic.unicamp.br

Abstract. *In wavelength division multiplexing (WDM) networks, failures can imply in great loss of data due to high transmission rates, leading to the need of employment of protection mechanisms. Moreover, physical impairments in all-optical networks can significantly degrade the signal quality. If the signal quality in a path is below acceptable values, this path cannot be used by incoming requests for lighpath establishment. Therefore, the quality of transmission needs to be checked by the routing and wavelength assignment algorithm. This paper introduces two novel algorithms for shared path protection in WDM networks that take into account the PMD, ASE and crosstalk physical impairments in path selection. The efficacy of these algorithms are compared to those of their impairment unaware counterpart.*

Resumo. *Nas redes com tecnologia wavelength division multiplexing (WDM), as falhas podem implicar em grande perda de dados devido a taxas de transmissão alta, levando à necessidade do emprego de mecanismos de proteção. Além disso, as limitações da camada física em redes transparentes podem degradar, significativamente, a qualidade do sinal. Se esta estiver abaixo de valores aceitáveis, esse caminho não pode ser utilizado, portanto, a qualidade de transmissão tem de ser verificada pelos algoritmos de roteamento e alocação de comprimento de onda. Este artigo introduz dois novos algoritmos que adotam mecanismo de proteção de caminho compartilhado em redes WDM, que levam em consideração os efeitos PMD, ASE e crosstalk na seleção de caminhos. A eficácia destes algoritmos é comparada à eficácia dos algoritmos insensíveis às limitações da camada física.*

1. Introdução

Na tecnologia de multiplexação por comprimento de onda (*wavelength division multiplexing*, WDM), a grande quantidade de banda passante disponível em uma fibra óptica (da ordem de Terabit por segundo) é dividida em uma série de canais não sobrepostos (da ordem de Gigabit por segundo). WDM torna possível a existência de aplicações com demandas por altas taxas de transmissão, tais como aplicações de vídeo e em “e-science”. No entanto, quanto maior a taxa de transmissão, maiores são as taxas de perdas com eventuais interrupções dos serviços. Por conseguinte, mecanismos de proteção adequado são fundamentais para o funcionamento de redes WDM.

Nas redes WDM em malha, a proteção pode ser efetuada em nível de caminho ou de enlace (link). Em nível de caminho, a proteção é realizada através da atribuição

de caminhos de backup fim-a-fim a serem usados para redirecionar o tráfego em caso de falha. O problema de roteamento e alocação de comprimento de onda (RWA) define quais comprimentos de onda devem ser usados por um caminho óptico, conseqüentemente, o esquema de proteção desejado deve orientar a alocação de comprimento de onda. A proteção em nível de caminho pode se dar de duas formas: compartilhada e dedicada [Ramamurthy et al. 2003]. Na proteção compartilhada, o comprimento de onda de um caminho de proteção pode ser usado por diversos caminhos primários associados, dado que estes não possuam qualquer enlace comum. Na proteção por caminho dedicado, cada caminho de backup está associado a apenas um caminho primário. A proteção por caminho compartilhado utiliza recursos de forma mais eficiente, uma vez que não exige caminhos de backup exclusivos.

Em redes WDM, conversão opto-eletro-óptica (O-E-O) pode ser empregada para a regeneração do sinal, no entanto, o custo de tal conversão é alto. Manter o sinal no domínio óptico é preferível. Embora a fibra ótica tenha boas características físicas, ela não é perfeita e pode degradar o sinal, ao longo do caminho da origem para o destino. Em cada *Optical Cross Connect* (OXC), ocorre uma atenuação do sinal, exigindo-se que sejam utilizados amplificadores, para compensar a perda progressiva acumulada ao longo do caminho. Essa comutação transparente do sinal, seguida de compensação pode introduzir deficiências nas transmissões. As limitações da camada física podem deteriorar o sinal até níveis inaceitáveis causando o bloqueio dos pedidos de estabelecimento de caminhos ópticos. Essas deficiências são especialmente relevantes para redes transparente, nas quais não ocorre regeneração do sinal [Huang et al. 2005]. Assim, a avaliação da degradação do sinal deve ser realizada antes do estabelecimento de um caminho óptico. Em outras palavras, o roteamento e a alocação de comprimento de onda tem de considerar a degradação do sinal ao longo de uma trajetória.

Tornar os algoritmos RWA sensíveis às limitações da camada física faz com que eles sejam inevitavelmente mais complexos devido à busca de caminhos com qualidade da transmissão (QoT) aceitável. Neste trabalho, são propostos dois novos algoritmos que têm como objetivo proporcionar proteção por caminho compartilhado no estabelecimento de caminhos ópticos em redes transparentes. Os algoritmos utilizam uma confiabilidade do tipo melhor-esforço (best-effort). Estes algoritmos levam em consideração a Dispersão por Modo de Polarização (PMD), a Emissão Espontânea Amplificada (ASE) e o Crosstalk em sua formulação. ASE e PMD são os principais efeitos físicos lineares em redes WDM e sua importância tem sido sugerida pelo IETF [Strand and Chui 2005]. Os algoritmos seguem o procedimento introduzido em [Huang et al. 2005], que desacopla a busca na camada de rede da busca na camada física, ou seja, a seleção de um caminho é realizada em duas etapas: a identificação de caminhos e a verificação da qualidade de transmissão destes caminhos. Resultados de simulação indicam que o emprego dos algoritmos propostos produz níveis de bloqueio de solicitações de estabelecimento de caminhos ópticos menores do que quando não se consideram as limitações da camada física.

Trabalhos anteriores investigaram sobrevivência em redes ópticas [Ramamurthy et al. 2003, Yuan and Jue 2004, Eshoul and Mouftah 2005], bem como os efeitos limitantes da camada física na transmissão [Ramamurthy et al. 1999, Huang et al. 2005, He et al. 2007, Cardillo et al. 2005, Strand and Chui 2005]. No entanto, os efeitos limitantes da camada física em redes com sobrevivência passaram, recentemente, a ser tópicos de grande in-

teresse. Em [Yang et al. 2005] e [Ouyang et al. 2005], investiga-se a colocação de conversores O-E-O em redes opacas, a fim de se produzir níveis aceitáveis na Qualidade de Transmissão. Em [Ouyang et al. 2005], apresenta-se um algoritmo semelhante, porém com a consideração de que o tráfego é dinâmico. O trabalho em [Zhai et al. 2007] avalia redes transparente com tráfego dinâmico e proteção por caminho dedicado, bem como as limitações da camada física. Os autores de [Wang et al. 2007] utilizam o esquema de proteção SRLG (*Shared Risk Link Group*) com consideração das limitações da camada física. É do nosso conhecimento que nenhum dos trabalhos anteriores propôs algoritmos para proteção por caminho compartilhado em redes transparentes, que levam em consideração a dispersão PMD, e os ruídos ASE e Crosstalk como realizado no presente trabalho.

Este trabalho está organizado da seguinte forma. Na Seção 2, detalha-se o modelo de rede adotado e a computação das limitações do canal físico. Na Seção 3, os novos algoritmos são introduzidos e avaliados na Seção 4. A Seção 5 conclui o artigo.

2. Modelo de Rede

O modelo de rede assume a existência de fibras de longa distância, o que, por sua vez, torna necessário a utilização de amplificadores ao longo do caminho. Neste modelo, utilizam-se amplificadores EDFA (*Erbium-Doped Fiber Amplifier*), devido ao seu bom desempenho em redes de longa distância e de alta velocidade (superior a 10 Gb/s). Os amplificadores são colocados a cada 82 km. Cada trecho de amplificação inclui 70 km de fibra monomodo padrão (SSMF), com atenuação de 0,2 dB/km. A dispersão cromática é compensada por 12 km de Fibras compensadoras de dispersão (DCF), que tem atenuação de 0,5 dB/km. As atenuações de um trecho de amplificação são compensadas exatamente pelos EDFAs.

A arquitetura de um nó OXC considerada neste artigo é constituída por dois interceptadores (usados para monitoramento [Ramamurthy et al. 1999]), dois amplificadores, um multiplexador, um demultiplexador e um comutador. O sinal que chega passa por um interceptador, e segue para um EDFA, onde é amplificado. Em seguida, o sinal é demultiplexado e segue para uma fase de comutação, após a qual é multiplexado e novamente amplificado. Após todo esse processo o sinal passa por outro interceptador rumo a porta de saída do nó.

Para permitir que o sinal siga seu curso através dos nós intermediários e através de longos segmentos de fibra, os comutadores nos nós intermediários empregam comutação passiva, o que acarreta em perdas no sinal. Em redes ópticas transparentes, a eliminação dos benefícios da conversão O-E-O implica em degradação do sinal. A perda progressiva ao longo dos caminhos ópticos requer o uso de amplificadores. Os OXCs e amplificadores introduzem efeitos degradantes, causando deterioração do sinal que pode produzir uma taxa de erro de bit (BER) inaceitável no nó destino. Os efeitos podem ser classificados como linear ou como não-linear. Efeitos lineares são independentes da potência do sinal. Os efeitos lineares mais importantes são: Dispersão por Modo de Polarização (PMD), Emissão Espontânea Amplificada (ASE) e crosstalk. ASE é produzido durante a amplificação do sinal. A geração de crosstalk ocorre quando dois ou mais sinais de mesmo comprimento de onda atravessam um comutador. Exemplos de efeitos não-lineares são: modulação de fase cruzada, auto-modulação de fase e mistura de quatro ondas.

O efeito PMD torna-se o efeito mais limitante com o aumento da taxa de transmissão superior 10 Gb/s. O impacto do PMD sobre a transmissão é dado por [Huang et al. 2005]:

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

onde M é o número de nós intermediários, B é a taxa de transmissão de bits, $D_{PMD}(k)$ é o parâmetro PMD no trecho de fibra k e $L(k)$ e o seu comprimento. A tolerância ao PMD é dada pelo fator de alargamento do pulso (δ), o qual deve ter um valor inferior a 10% do slot de tempo de um bit. Uma vez que fibras diferentes possuem valores diversos para o parâmetro PMD, essa restrição depende das características das fibras constituintes do caminho. Por motivos de simplicidade, assumem-se valores iguais para D_{PMD} .

Os ruídos provocados pelos efeitos ASE e crosstalk propagam-se com o sinal pelo caminho óptico, desde a origem até o destino. O efeito cumulativo destes dois fenômenos deteriora a qualidade do sinal, diminuindo a razão sinal-ruído, possivelmente a valores inaceitáveis.

Tendo verificado que a dispersão PMD apresenta volumes aceitáveis, a razão sinal-ruído óptica (OSNR) pode ser então calculada. A potência do ruído ASE é dada por [Cardillo et al. 2005] através da equação $P_{ASE} = 2 * \eta_{sp} * (G - 1) * h * f$, onde η_{sp} é o fator de emissão espontânea do EDFA, G é seu ganho, h é a constante de Planck e f a frequência de operação.

O efeito crosstalk é dado por [Ramamurthy et al. 1999]:

$$P_{xt} = \sum_{j=1}^J X_{sw} * P_{in}(j) \quad (2)$$

onde X_{sw} é a razão de crosstalk e $P_{in}(j)$ é a potência dos sinais de mesmo comprimento de onda em um comutador.

Tendo calculado as intensidades dos ruídos, pode-se, então, verificar se o valor obtido para OSNR encontra-se dentro de limites aceitáveis. Para um valor de OSNR de 7.4 db, a taxa de erro de bits (BER) equivalente é de 10^{-9} . A Tabela 1 apresenta os parâmetros usados neste artigo, amplamente adotados em estudos na literatura [Ramamurthy et al. 1999, Huang et al. 2005].

3. Proteção por caminho compartilhado sensível às limitações da camada física

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

Tabela 1. Parâmetros usados na simulação

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

Os algoritmos seguem a abordagem introduzida em [Huang et al. 2005], que adota um modelo de RWA hierárquico. De maneira geral, estes algoritmos consistem de duas etapas distintas: na primeira, busca-se um caminho óptico na camada de rede, da mesma forma que se faz em algoritmos tradicionais insensíveis às limitações da camada física; na segunda, faz-se a verificação da qualidade de transmissão deste caminho óptico. No processo de verificação, obtém-se, inicialmente, uma estimativa da qualidade do sinal. Caso o valor obtido para a qualidade estimada seja aceitável, o caminho óptico pode ser estabelecido; caso contrário uma nova rota deve ser calculada. Se, após uma busca exhaustiva, nenhuma rota for encontrada, a conexão é bloqueada.

Os algoritmos assumem uma proteção por caminho compartilhado com uma confiabilidade do tipo melhor esforço [Shao et al. 2008, Fumagalli et al. 2002]. Nesta metodologia, dois caminhos primários podem compartilhar um caminho de backup sem restrição. Esta é uma abordagem diferente da proteção por caminho compartilhado tradicional, na qual dois caminhos primários com um enlace em comum não podem compartilhar um outro enlace no caminho de backup. O relaxamento desta restrição é realista, uma vez que no cenário em que se consideram as limitações da camada física, algumas falhas não podem ser recuperadas.

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

Adota-se notação usada em [Huang et al. 2005]. Considera-se uma topologia baseada em camadas $W_w(N, L)$, onde cada uma das camadas representa um comprimento de onda w , $w = 1, 2, \dots, W$ em uma topologia física $T(N, L)$, onde N é o conjunto de nós, e L o conjunto de enlaces. Todas as camadas da topologia $W_w(N, L)$ assumem, inicialmente,

o mesmo valor da topologia física $T(N, L)$, e o roteamento é baseado nestes grafos auxiliares. A seguir os dois algoritmos são apresentados. Indica-se, também, as linhas do pseudocódigo correspondente ao passo do algoritmo.

3.1. SPPIAFF

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

1. Inicializar o procedimento pelo primeiro comprimento de onda, $w = 1$ (linha 1 do Algoritmo 1);
2. Aplicar o algoritmo do menor caminho, a fim de se achar um caminho primário Pw em $Ww(N, L)$. Se nenhum caminho for encontrado, faça $w = w + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 8 (linha 2 do Algoritmo 1);
3. Obtenha uma estimativa da qualidade do caminho $P\lambda$. Caso o lightpath não seja viável volte ao passo 2 (linha 3 do Algoritmo 1);
4. Faça $T'(N, L) = T(N, L) - Pw$, produzindo um novo conjunto de camadas $W'w'(N, L)$ derivado de $T'(N, L)$ (linha 5 do Algoritmo 1);
5. Inicializar $w' = 1$ (linha 4 do Algoritmo 1);
6. Aplicar o algoritmo do menor caminho a fim de achar um caminho de backup compartilhado Bw' em $W'w'(N, L)$. Se nenhum caminho for encontrado, faça $w' = w' + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2 (linha 6 do Algoritmo 1);
7. Obtenha uma estimativa da qualidade do caminho $B\lambda'$. Caso o lightpath seja viável, aceite a chamada, atualize $W\lambda$ (colocando os enlaces de $P\lambda$ em modo ocupado), atualize $W\lambda'$ (colocando os enlaces de $B\lambda'$ em modo backup), e, por fim, atualize os ruídos gerados por $P\lambda$; caso contrário volte ao passo 6 (linhas 7 e 8 do Algoritmo 1);
8. Pare o procedimento

O pseudocódigo do algoritmo SPPIAFF é apresentado no Algoritmo 1.

Algoritmo 1 SPPIAFF

```

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

```

3.2. SPPIARP

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

A seguir, descreve-se o SPPIARP:

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

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

O Algoritmo 2 apresenta o pseudocódigo do algoritmo SPPIARP.

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

4. Resultados Numéricos

Nesta Seção, a eficácia dos algoritmos propostos é verificada por meio de simulação. Os resultados produzidos por eles são comparados aos de outros algoritmos, a saber:

Algoritmo 2 SPPIARP

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

- Tradicionais para redes ideais: ignoram a existência dos efeitos degradantes do sinal no controle de acesso de chamadas (CAC), ou seja, consideram os equipamentos ao longo de um caminho óptico como sendo ideais. SPPFF/Ideal e SP-PRP/Ideal são os algoritmos que fazem esta hipótese.
- Tradicionais para redes realistas: os componentes de rede infligem ruído sobre o sinal, causando sua degradação, que é levada em consideração pelo CAC na aceitação de chamadas. SPPFF/Realista e SPPRP/Realista são os algoritmos tradicionais simulados em redes realistas. Note que nos algoritmos propostos o problema RWA leva em consideração as limitações da camada física, a fim de encontrar um caminho com qualidade aceitável, ao contrário dos tradicionais para redes realistas, que levam em consideração a degradação do sinal apenas na decisão do controle e admissão de chamadas.

O bloqueio de caminhos com baixa qualidade de sinal ocorre tanto para os algoritmos sensíveis como para os algoritmos tradicionais aos efeitos degradantes do sinal, mas não acontece nas redes ideais. Duas topologias são usadas para ilustrar o desempenho dos algoritmos: a topologia da rede NSFNET (Figure 1(a)), com 16 nós e 25 enlaces; e a topologia da *USA Network* (Figure 1(b)), com 24 nós e 43 enlaces.

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

Nas simulações, considerou-se que o tráfego é dinâmico e que a chegada de chamadas segue um processo de Poisson, enquanto que período de duração de uma chamada (*holding time*) é dado por uma distribuição exponencial com média 1, de modo que a carga da rede seja dada pela taxa de chegada. O modelo de falhas adotado é o de enlace único,

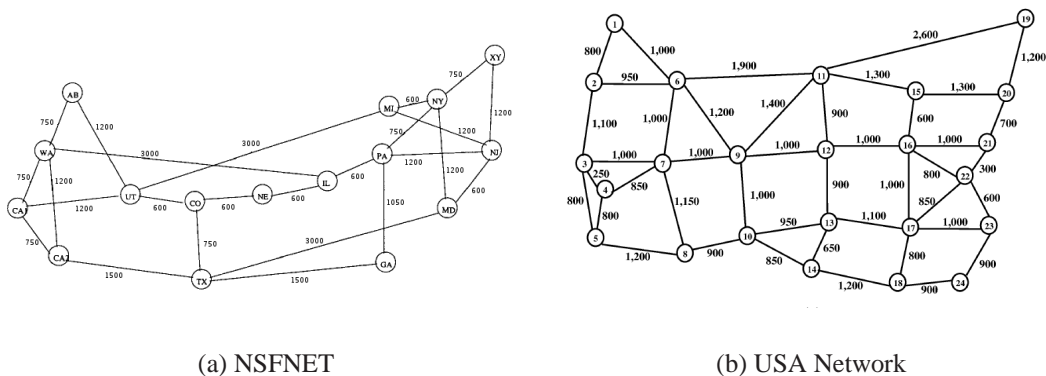


Figura 1. Topologias usadas

ou seja, em qualquer momento da vida da rede existe apenas a falha de um enlace, e a ocorrência de uma nova falha só é possível quando o conserto da anterior já houver ocorrido[Zhai et al. 2007].

Um grande número de experimentos foi realizado. 13 simulações para cada uma das 3 alternativas de algoritmo com 2 políticas de alocação de comprimento de onda, 2 valores para intensidade de crosstalk, 3 valores para número de comprimentos de onda e 2 topologias, num total de 936 experimentos. O intervalo de confiança para nível de significância igual a 95% é inferior a 1% do valor medido. Foram realizadas 10^6 requisições de conexão para cada simulação.

A Figura 2 apresenta os valores de probabilidade de bloqueio produzidos para os algoritmos propostos bem como para suas versões insensíveis aos efeitos degradantes do sinal em redes realistas e ideais. Pode-se perceber uma diferença significativa na probabilidade de bloqueio para redes não-ideais quando comparadas a redes nas quais os efeitos degradantes são desconsiderados. Sob baixas cargas, quando a técnica de alocação de comprimento de onda é First-Fit, tem-se uma diferença de 0.3 para o algoritmo tradicional em uma rede realista com cargas baixas; e quando é Random-Pick, o aumento é de 0.38. Esta diferença indica a magnitude do erro que se comete ao se assumir a inexistência dos efeitos degradantes do meio, ou seja, a diferença indica o percentual de chamadas que são aceitas, quando se considera o efeito degradante, cuja qualidade de transmissão está abaixo do aceitável. Nota-se que os valores de probabilidade de bloqueio produzidos pelos algoritmos propostos são sempre inferiores àqueles produzidos quando os algoritmos RWA não consideram a QoT dos caminhos (denotado no gráfico como redes realistas). A diferença entre estes dois valores indica a vantagem obtida ao se utilizar os algoritmos RWA que consideram a QoT na seleção dos caminhos. Sob uma carga de 50 Erlangs, o algoritmo SPPIAFF reduz a probabilidade de bloqueio de 0.31 a 0.2, enquanto que para SPPIARP redução observada é de 0.38 a 0.17. A diminuição das diferenças da probabilidade de bloqueio deve-se principalmente a escassez de recursos. Sob cargas altas, a probabilidade de bloqueio do SPPIARP se aproxima muito mais daquela produzida por algoritmos tradicionais para redes realistas do que no caso do SPPIAFF. A diferença de resultados entre os algoritmos é explicada pelo modo como se dá a alocação de comprimento de onda: quando a atribuição se dá de forma aleatória, o uso dos recursos é menos

eficiente, o que explica o aumento na probabilidade de bloqueio; por outro lado, o compartilhamento dos caminhos de backup diminui, levando a uma razão de vulnerabilidade menor.

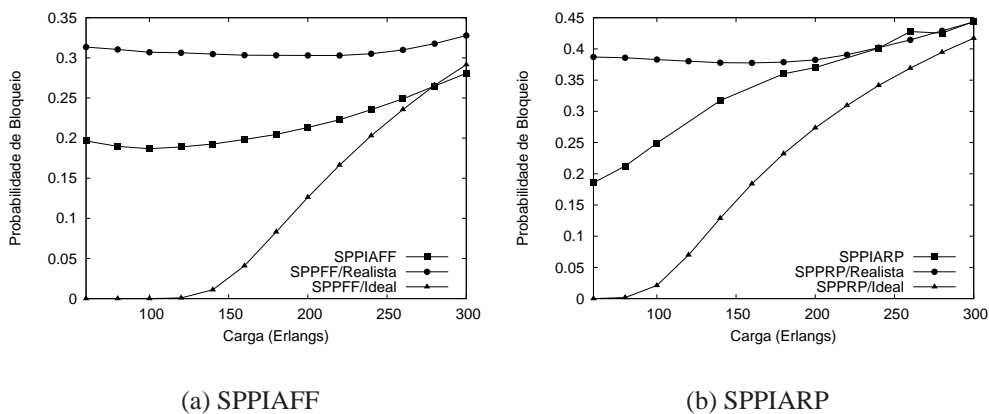


Figura 2. Probabilidade de bloqueio em função da carga

A Figura 3(a) mostra o resultado obtido para a razão de vulnerabilidade em função da carga. O algoritmo SPPIAFF apresenta resultados semelhantes aos obtidos pela abordagem tradicional em redes ideais e realistas, mesmo produzindo uma probabilidade de bloqueio inferior a obtida por estes algoritmos. Já o uso do algoritmo SPPIARP leva a uma razão de vulnerabilidade menor do que quando se usa uma abordagem para redes ideais (Figure 3(b)), ou seja, na ocorrência de falhas, a probabilidade de restauração da conexão é maior quando se usa o algoritmo SPPIARP. Isso se deve ao fato de que a busca exaustiva por um caminho leva a um nível de compartilhamento dos caminhos de backup menor do que nos casos em que a busca é feita de forma tradicional. A medida que a carga aumenta, a diferença da razão de vulnerabilidade entre os algoritmos SPPIARP e a abordagem realista também aumenta. Sob cargas de 300 Erlangs, o SPPIARP reduz a razão de vulnerabilidade de 0.16 para 0.12 quando comparado com a abordagem realista.

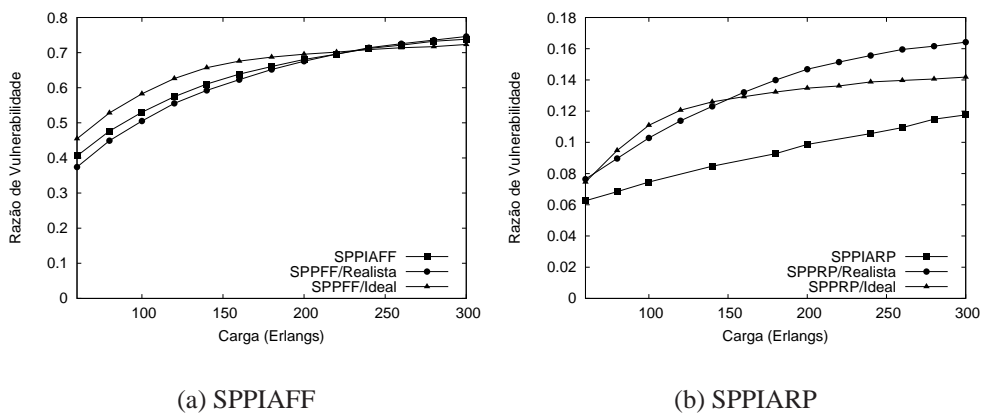
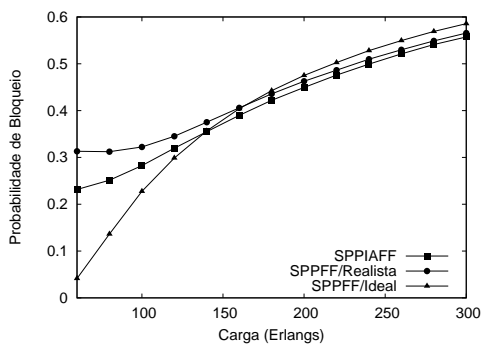
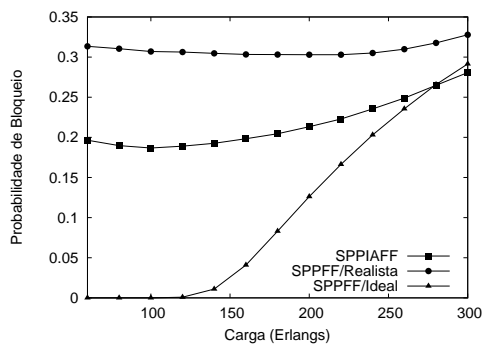


Figura 3. Razão de vulnerabilidade em função da carga

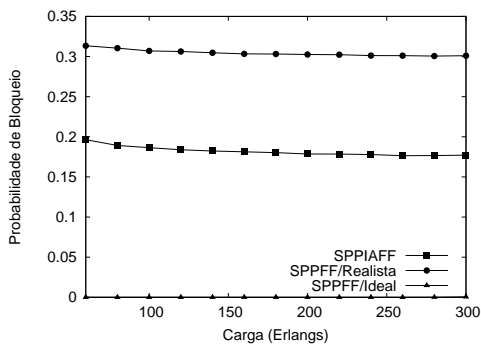
Analisou-se, também, o impacto do número de canais na eficácia dos algoritmos propostos, executando-se a simulação em redes com 8, 16 e 32 comprimentos de onda. A Figura 4 apresenta os resultados para a alocação de comprimento de onda do tipo First-Fit. Em redes com 8 canais por enlace (Figura 4(a)), a redução do número de canais torna sua disponibilidade tão baixa que os efeitos degradantes do sinal são importantes apenas em cargas baixas (menores do que 110 Erlangs). A vantagem da sensibilidade aos efeitos físicos torna-se clara quando o número de canais dobra; a redução da probabilidade de bloqueio é significativa, especialmente para sistemas pouco ou moderadamente carregados. Quando as cargas aumentam, o algoritmo SPPIAFF passa a operar com uma eficiência bem próxima a abordagem ideal. Sob cargas menores que 110 Erlangs a diferença entre as probabilidades de bloqueio produzidas pelo algoritmo SPPIAFF e a abordagem realista é da ordem de 0.1. Quando o número de canais é igual a 32, a diferença obtida entre algoritmos sensíveis e insensíveis para redes realistas é de 0.1 para todas as cargas medidas (até 300 Erlangs), evidenciando as vantagens de se usar algoritmos RWA que considerem os efeitos degradantes do sinal, uma vez que são capazes de diminuir a probabilidade de bloqueio buscando exaustivamente por um caminho óptico que ofereça uma qualidade de transmissão melhor. Em síntese, ao se aumentar o número de canais, o algoritmo SPPIAFF é capaz de reduzir a probabilidade de bloqueio em relação a abordagem realista. Resultados semelhantes foram observados para o algoritmo SPPIARP.



(a) 8 Canais



(b) 16 Canais



(c) 32 Canais

Figura 4. Probabilidade de bloqueio em função da carga para diferentes números de canais

A Figura 5(a) mostra resultados para uma taxa de transmissão de 20Gbps, adotando-se First-Fit como método de alocação de comprimento de onda. A dispersão PMD torna-se a mais importante quando se transmite a taxas desta magnitude, degradando a qualidade do sinal de forma proibitiva, como se percebe na diferença entre as curvas para redes não-ideais e a curva para a rede ideal. Isso faz com que sob estas taxas, a sensibilidade aos efeitos físicos não produza resultados melhores. O mesmo foi observado para taxas de transmissão ainda maiores. Quando essa taxa aumenta para 40 Gbps, a probabilidade de bloqueio sobe de 0.9 a 1.0.

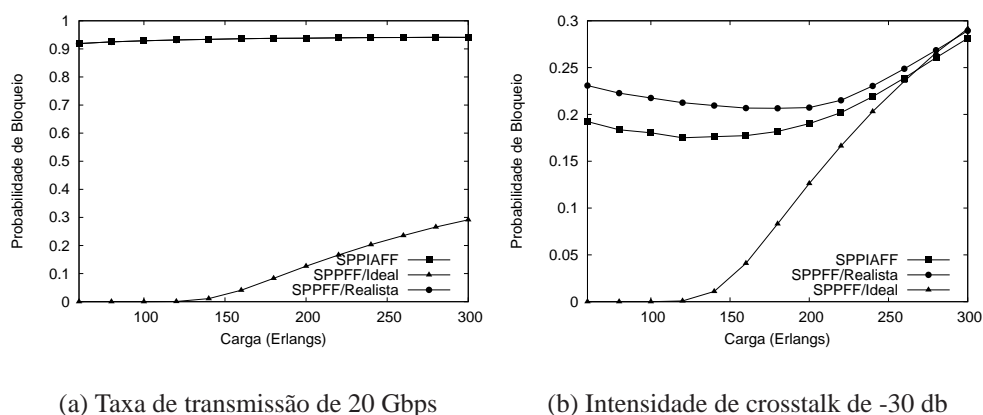


Figura 5. Probabilidade de bloqueio em função da carga com variação da taxa de transmissão e do nível de crosstalk

Foram feitas avaliações dos algoritmos propostos sob diferentes níveis de intensidade de crosstalk. Quando a intensidade de crosstalk atinge valores altos, como -25 db (Figura 2(a)), a sensibilidade aos efeitos degradantes do sinal permite uma redução da probabilidade de bloqueio da ordem de 0.1 para cargas baixas. Mesmo para cargas mais altas, uma diferença relevante pode ser percebida. A partir de 250 Erlangs, o principal fator de bloqueio é a escassez de recursos, o que se pode perceber pela proximidade das duas curvas referentes a redes não-ideais, com a curva relacionada a uma rede ideal. A Figura 5(b) apresenta a probabilidade de bloqueio para uma razão de crosstalk igual a -30db. Quando os níveis de crosstalk são mais baixos a redução do bloqueio é menor. Comparando com níveis de -25db (Figura 2(a)) e sob cargas menores que 150 Erlangs, a redução observada entre as probabilidades de bloqueio do algoritmo SPPIAFF e da abordagem realista foi de 0.05. Dessa forma, conclui-se que os algoritmos propostos são mais eficientes para intensidades mais altas de crosstalk.

Foram, também, realizadas simulações com a topologia da rede USA Network. O grau de conectividade, bem como o diâmetro dessa topologia são maiores do que os mesmos parâmetros na NSFNET. Se, por um lado, as distâncias entre origem e destino são maiores, e conseqüentemente, a intensidade dos efeitos degradantes do sinal, por outro lado, as possibilidades de caminhos alternativos são muito maiores, devido ao maior número de nós e enlaces, tornando mais fácil a busca por caminhos com qualidade de sinal aceitável. A Figura 6 mostra a probabilidade de bloqueio em função da carga usando First-Fit como técnica de alocação de comprimento de onda. Comparando-se os resultados apresentados com os obtidos para a NSFNET, houve um aumento de

0.1 na probabilidade de bloqueio tanto para o algoritmo proposto como para o algoritmo tradicional em redes realistas, tendo como causa a maior degradação do sinal devido ao aumento no diâmetro da rede. Além disso, a topologia da *USA Network* permite um maior número de caminhos alternativos, e, mesmo sob cargas altas, a escassez de recursos não é um fator preponderante para o aumento de bloqueio nas redes não ideais, o que se pode perceber pela distância existente entre os resultados obtidos pelos algoritmos proposto e a abordagem realista, quando comparados ao limitante inferior, representado pelas redes ideais. A razão de vulnerabilidade, entretanto, teve um pequeno aumento. Além disso, o algoritmo SPPIAFF reduziu aproximadamente 0.15 e 0.1 sob baixas e altas cargas, respectivamente, a probabilidade de fracasso ao se tentar restaurar uma conexão. Note que o SPPIAFF reduz cerca de 0.11 a probabilidade de bloqueio quando comparado ao SPPFF/realista, que bloqueia caminhos sem QoS porém que não considera a QoS na escolha do caminho. Note, também, que sob cargas de 160 Erlangs 30% das chamadas seriam aceitas inadequadamente ao se ignorar a QoS, e que esta tendência errônea aceitaria cerca de 10% inadequadamente sob cargas de 300 Erlangs, valor que seria 0.2 caso uma abordagem realista fosse adotada.

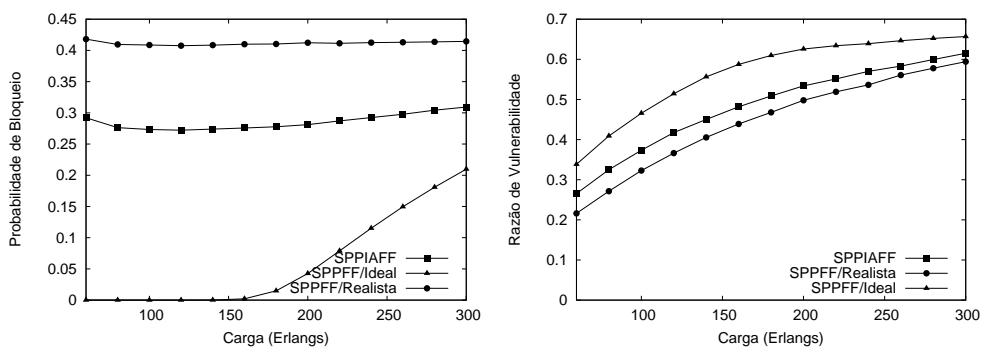


Figura 6. Probabilidade de bloqueio em função da carga para a topologia da USA Network

5. Conclusões

Este artigo apresentou dois novos algoritmos, capazes de apresentar um melhor desempenho no contexto de redes ópticas transparentes com proteção por caminho compartilhado segundo o melhor esforço. Através de simulação, concluiu-se que os algoritmos são capazes de diminuir consideravelmente o bloqueio devido à degradação da qualidade do sinal, principalmente quando a técnica de alocação de comprimento de onda é aquela utilizada em SPPIAFF. Para SPPIARP, observa-se um ganho menor em relação ao bloqueio, e uma diminuição muito grande da razão de vulnerabilidade.

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

A introdução de outros níveis de proteção e de outros efeitos limitantes, bem como a proposição de novos algoritmos de roteamento, constituem possíveis trabalhos que avançariam o conhecimento introduzido no presente artigo.

Acknowledgements

Este trabalho foi parcialmente patrocinado por FAPESP, CNPq e CISCO.

Referências

- Cardillo, R., Curri, V., and Mellia, M. (2005). Considering transmission impairments in wavelength routed networks. *Proc of Conference on Optical Network Design and Modeling*, pages 421–429.
- Eshoul, A. and Mouftah, H. (2005). Shared protection in wavelength-routed optical mesh networks under dynamic traffic and no wavelength conversion. *Proceedings of Systems Communications*, pages 312–319.
- Fumagalli, A., Tacca, M., Unghvary, F., and Farago, A. (2002). Shared path protection with differentiated reliability. *Proc of IEEE International Conference on Communications*, 4:2157–2161 vol.4.
- He, J., Brandt-Pearce, M., Pointurier, Y., and Subramaniam, S. (2007). Qot-aware routing in impairment-constrained optical networks. *Proc of IEEE Global Telecommunications Conference*, pages 2269–2274.
- Huang, Y., Heritage, J., and Mukherjee, B. (2005). Connection provisioning with transmission impairment consideration in optical wdm networks with high-speed channels. *Lightwave Technology, Journal of*, 23(3):982–993.
- Ouyang, Y., Zeng, Q., and Wei, W. (2005). Dynamic lightpath provisioning with signal quality guarantees in survivable translucent optical networks. *Optics Express*, 13:10457–10470.
- Ramamurthy, B., Datta, D., Feng, H., Heritage, J., and Mukherjee, B. (1999). Impact of transmission impairments on the teletraffic performance of wavelength-routed optical networks. *Journal of Lightwave Technology*, 17(10):1713–1723.
- Ramamurthy, S., Sahasrabudhe, L., and Mukherjee, B. (2003). Survivable wdm mesh networks. *Journal of Lightwave Technology*, 21(4):870–883.
- Shao, X., Zhou, L., Cheng, X., Zheng, W., and Wang, Y. (2008). Best effort shared risk link group (srlg) failure protection in wdm networks. *Proc of IEEE International Conference on Communications*, pages 5150–5154.
- Strand, J. and Chui, A. (2005). Impairments and other constraints on optical layer routing. *IETF RFC 4054*.
- Wang, Sheng, Li, and Lemin (2007). Impairment aware optimal diverse routing for survivable optical networks. *Photonic Network Communications*, 13(2):139–154.
- Yang, X., Shen, L., and Ramamurthy, B. (2005). Survivable lightpath provisioning in wdm mesh networks under shared path protection and signal quality constraints. *Lightwave Technology, Journal of*, 23(4):1556–1567.
- Yuan, S. and Jue, J. (2004). Dynamic lightpath protection in wdm mesh networks under wavelength continuity constraint. *Proc of IEEE Global Telecommunications Conference*, 3:2019–2023 Vol.3.

Zhai, Y., Pointurier, Y., Subramaniam, S., and Brandt-Pearce, M. (2007). Performance of dedicated path protection in transmission-impaired dwdm networks. *Proc of IEEE International Conference on Communications*, pages 2342–2347.