Algoritmo para a Provisão de Confiabilidade Diferenciada em Redes Ópticas Sensíveis às Limitações da Camada Física.

Sávio R. A. dos S. Rosa[1], **André C. Drummond**[1], **Nelson L. S. da Fonseca**[1]

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

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

Abstract. *Traditional protection schemes guarantees 100% reliability in case of single link failure while differentiated reliability provides a granular protection scheme. Moreover, if the signal quality in a path is below acceptable values, a path cannot be used by incoming requests for lighpath establishment. Therefore, the signal quality needs to be checked by the routing and wavelength assignment algorithm (RWA). This paper investigates the provisioning of shared path protection with differentiated reliability scheme under Polarized Mode Dispersion (PMD), Amplified Spontaneous Emission (ASE) and crosstalk impairments. The efficacy of the algorithm proposed is compared to that of its impairment unaware counterpart.*

Resumo. *O amadurecimento da tecnologia WDM possibilitou um grande aumento nas taxas de transmissão sobre fibra. Mecanismos de proteção tornaram-se, consequentemente, mais importantes, pois uma falha leva a perdas de um volume muito grande de dados. As técnica de proteção tradicionais garantem que 100% das conexões estabelecidas possam ser recuperadas em caso de falha de enlace único, ao custo de alto nível de redundância. Entretanto, os usuários do serviço nem sempre estão dispostos a pagar muito mais por esse requisitos, dado que possuem diferentes necessidades de confiabilidade. Este artigo introduz um novo algoritmo de proteção por caminho compartilhado com diferentes níveis de confiabilidade, a fim de atender uma diversidade de requisitos dos usuários. As limitações da camada física são abordadas na formulação do problema; considera-se os efeitos físicos ASE, PMD e diafonia (*crosstalk*). O algoritmo proposto é avaliado através de simulação.*

1. Introdução

A tecnologia de multiplexação por comprimento de onda (*Wavelength Division Multiplexing* - WDM) permitiu um desenvolvimento sem precedentes nas transmissões ópticas. A grande quantidade de banda passante disponível passou a ser dividida em uma série de canais independentes e não sobrepostos transmitidos de forma simultânea em uma mesma fibra. Isto permitiu que a banda passante pudesse ser utilizada de forma muito mais eficiente, e uma fibra capaz de transmitir poucos gigabits por segundo, passou a ter capacidade da ordem de terabits por segundo. Esse avanço, permitiu o surgimento de um elevado número de novos serviços com demandas por altas taxas de transmissão, tornando o uso de redes ópticas ainda mais vantajoso, sobretudo para as redes de núcleo. Por outro lado, as transmissões precisaram ser mais confiáveis, uma vez que a ocorrência de uma falha leva a grandes perdas de pacotes. Em consequência, mecanismos de proteção vem

sendo desenvolvidos para permitir a continuidade das transmissões em eventuais falhas dos enlaces.

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 proteção 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, consequentemente, o esquema de proteção desejado deve ser orientado 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 primário está associado a um caminho de proteção. A proteção por caminho compartilhado utiliza recursos de forma mais eficiente, uma vez que não exige caminhos de proteção exclusivos.

Os métodos de proteção tradicionais têm como requisito 100% de confiabilidade no caso de falhas únicas de enlace, ou seja, todas as conexões prejudicadas por uma falha devem ser recuperadas. Esta técnica apresenta um custo muito alto, pois, em geral, o dobro de recursos ou mais são necessários para garantir este requisito. No entanto, o custo-benefício deste esquema de proteção não é interessante para todos os usuários, dado que nem todos estão dispostos a ter o custo elevado para se recuperar de eventuais falhas. Para outros usuários, tais como instituições financeiras, 100% de confiabilidade é imprescindível.

Trabalhos anteriores estudaram a diferenciação da proteção. Em [Rosa et al. a, Rosa et al. b], propõe-se uma proteção por caminho compartilhado do tipo melhor esforço. Permite-se que um comprimento de onda seja compartilhado por dois caminhos primários diferentes, e, na ocorrência de uma falha, recuperam-se tantos caminhos primários quanto forem possível. Em [Shao et al. 2008], a idéia é semelhante, entretanto, a proteção possui restrições do tipo SRLG (*Shared-Risk Link Group*). Algoritmos de proteção com confiabilidade diferenciada (*Differentiated in Reliability* - DiR) [Fumagalli et al. 2002, Tacca et al. 2003], permitem que conexões não sejam 100% protegidas, considerando-se que caminhos com menor probabilidade de falha devem fazer menor uso de recursos.

Além da confiabilidade obtida com proteção, deve-se levar em consideração a degradação do sinal, a fim de se prover serviços de qualidade. Em redes WDM, a regeneração do sinal resultante da conversão opto-eletro-óptica (O-E-O) tem um custo muito alto, e, por este motivo, manter o sinal no domínio óptico é preferível. 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. Nas redes transparentes, em cada *Optical Cross Connect* (OXC), o sinal é transferido da porta de entrada à porta de saída sem passar pelo domínio eletrônico, o que leva a um aumento progressivo das deficiências nas transmissões [Huang et al. 2005]. As limitações da camada física podem deteriorar o sinal até níveis inaceitáveis causando o bloqueio dos pedidos de estabelecimento de caminhos ópticos. 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 um caminho.

Neste artigo, propõe-se um novo algoritmo de proteção por caminho compartilhado com diferentes níveis de confiabilidade, a fim de que seja possível atender a uma diversidade de requisitos de proteção. O algoritmo considera as limitações da camada física, a fim de que os serviços prestados possuam uma boa qualidade de sinal, tratando das degradações geradas pelos efeitos de Emissão Espontânea Amplificada (*Amplified Spontaneous Emission* - ASE), Dispersão por Modo de Polarização (*Polarization Mode Dispersion* - PMD) e Crosstalk intracanal. Estes efeitos foram considerados os mais importantes de acordo com sugestão feita pelo IETF [Strand and Chui 2005].

Este trabalho está organizado da seguinte forma: na Seção 2, apresenta-se o modelo de rede adotado. Na Seção 3, detalha-se os efeitos degradantes considerados. Na Seção 4, introduz-se o novo algoritmo, e na Seção 5 seu desempenho é avaliado. Por fim, a Seção 6 conclui o artigo.

2. Modelo de Rede

O modelo de rede, ilustrado pela Figura 1, 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.

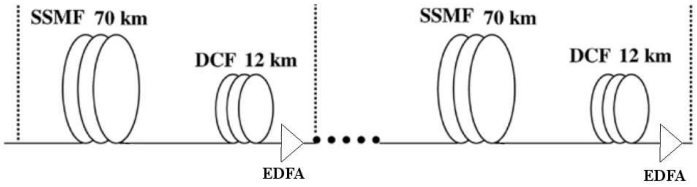


Figura 1. Modelo de rede

A Figura 2 ilustra a arquitetura de um nó WRN (*wavelength routing node*) constituído por comutadores, receptores e transmissores [Ramamurthy et al. 1999]. Após passar pelo demultiplexador, o sinal segue para um comutador WRS (*wavelength-routing switches*), para em seguida sofrer multiplexação. Os sinais que sofreram demultiplexação e que possuem o mesmo comprimento de onda seguem para um mesmo comutador, que roteia o sinal e o encaminha para um multiplexador. Estes, por sua vez, combinam sinais de todos os comprimentos de onda e enviam o sinal combinado para a porta de saída. Existem tantas opções de comutadores quantos comprimentos de ondas um WRN pode suportar. Os componentes incluem um par de amplificadores EDFA, além de interceptadores em ambos os lados do WRN. O par de EDFAs compensa exatamente a atenuação sofrida pelo sinal devido aos componentes do WRN.

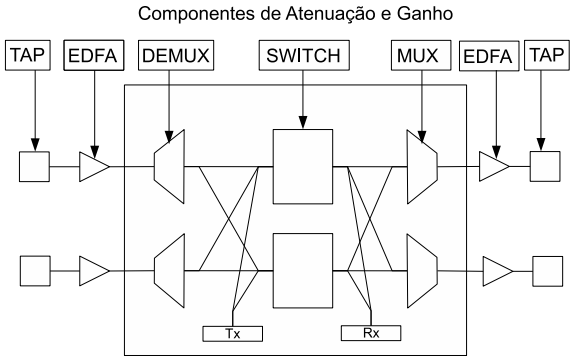


Figura 2. Arquitetura de um nó WRN

3. Efeitos Degradantes do Sinal Óptico

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 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 diafonia. ASE é produzido durante a amplificação do sinal. A geração de diafonia 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. Os efeitos não-lineares não são considerados pois o modelo adotado admite OSNR de 10^{-9}. Para modelos mais restritivos, com OSNR de 10^{-12}, tais efeitos devem ser considerados.

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 [Huang et al. 2005] é dado por:

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

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 diafonia 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 níveis aceitáveis, a razão sinal-ruído óptica (OSNR) pode ser então calculada. A potência do ruído ASE é dada por [Cardillo et al. 2005]:

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

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

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

$$P_{xt} = \sum_{j=1}^{J} X_{sw} * P_{in}(j) \quad (3)$$

onde X_{sw} é a razão de diafonia e $P_{in}(j)$ é a potência dos sinais de mesmo comprimento de onda em um comutador e J é o número total de fontes de diafonia.

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].

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 $ps/(km)^{1/2}$
OSNR mínimo	7.4 db

4. Algoritmo de Proteção por Caminho Compartilhado com Diferentes Níveis de Confiabilidade

Nesta seção, introduz-se um novo algoritmo para estabelecimento de caminhos ópticos em redes com proteção com diferentes níveis de confiabilidade. Serão apresentadas duas versões: uma para redes ideais, nas quais as limitações da camada física

são desconsideradas; e uma versão sensível aos efeitos degradantes, que são levados em consideração no momento da escolha de um novo caminho óptico.

O algoritmo é baseados na abordagem de melhor esforço [Rosa et al. a]. Nesta técnica, dois caminhos primários não-disjuntos podem compartilhar comprimentos de onda de proteção. No momento em que uma falha ocorre, são recuperados tantas chamadas quanto possíveis. Assim, ao final do processo de restauração, parte das chamadas que sofreram com a falha é recuperada, e outra parte permanece com seus serviços interrompidos. A razão entre caminhos não recuperados e o total de chamadas pertencentes a um enlace falho é denominada razão de vulnerabilidade.

O novo algoritmo de proteção proposto busca limitar o compartilhamento de comprimentos de onda introduzido pela abordagem do melhor esforço. Na técnica apresentada em [Rosa et al. a], um comprimento de onda pode ser compartilhado por tantos caminhos primários quanto se queira, o que leva a uma razão de vulnerabilidade alta. Já em um algoritmo de proteção por caminho compartilhado tradicional, a razão de vulnerabilidade é zero, uma vez que em caso de falha todas as chamadas são recuperadas. O novo algoritmo busca uma alternativa a estas duas propostas. Limitando-se o compartilhamento dos comprimentos de onda, consegue-se razões de vulnerabilidade não tão altas quando a abordagem em [Rosa et al. a] é adotada, e nem tão baixa quando a obtida por algoritmos tradicionais, permitindo, assim, atender a clientes com necessidades diversas.

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

Nas próximas subseções, descreve-se o novo algoritmo. Na Subseção 4.1, o algoritmo é descrito para redes ideais, insensíveis às limitações da camada física, e na Subseção 4.2, os efeitos degradantes do sinal são considerados. O formalismo adotado na descrição considera a seguinte notação: dada uma topologia baseada em camadas $W_w(N, L)$, onde cada uma das camadas representa um comprimento de onda w, $w = 1, 2, ..., W$ em uma topologia física $T(N, L)$. N é o conjunto de nós, e L o conjunto de enlaces. Todas as camadas da topologia $W_w(N, L)$ assumem, inicialmente, o mesmo valor da topologia física $T(N, L)$, e o roteamento é baseado nestes grafos auxiliares. O algoritmo opera sobre um nível de confiabilidade constante C. Comprimentos de onda utilizados como caminho de proteção estão associados com um nível de compartilhamento S, correspondente ao número de caminhos primários que utilizam o canal para proteção.

4.1. Algoritmo SPP com Níveis de Compartilhamento

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

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

O pseudocódigo deste algoritmo é apresentado no Algoritmo 1:

Algoritmo 1 Algoritmo para redes ideais

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

4.2. Algoritmo SPP com Níveis de Compartilhamento Sensível às Limitações da Camada Física

Na versão sensível às limitações da camada física, procede-se de forma semelhante ao proposto em [Rosa et al. a]. Assim que um caminho primário é encontrado,

faz-se uma estimativa da qualidade do sinal, e apenas se os níveis de degradação estiverem dentro de limites aceitáveis é que se busca um caminho de proteção, que também deve ter a qualidade de sinal testada para a aceitação da conexão.

O algoritmo pode ser descrito da seguinte forma:

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

1. Inicializar o procedimento pelo primeiro comprimento de onda, $w = 1$;
2. Aplicar o algoritmo do menor caminho, a fim de se achar um caminho primário P_w 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 um caminho, faça $\lambda = w$; caso contrário, bloqueie a chamada e siga ao passo 9;
3. Obtenha uma estimativa da qualidade do caminho P_λ. Caso o lightpath não seja viável volte ao passo 2;
4. Faça $T'(N, L) = T(N, L) - P_w$, produzindo um novo conjunto de camadas $W'_{w'}(N, L)$ derivado de $T'(N, L)$;
5. Inicializar $w' = 1$;
6. Aplicar o algoritmo do menor caminho a fim de achar um caminho de proteção compartilhado $B_{w'}$ em $W'_{w'}(N, L)$, tal que todos os enlaces ao longo deste caminho possuam $S < C$. Se nenhum caminho for encontrado, faça $w' = w' + 1$, e repita este procedimento para a próxima camada até que se possa encontrar um caminho. Caso seja encontrado, faça $\lambda' = w'$; caso contrário, siga ao passo 2;
7. Obtenha uma estimativa da qualidade do caminho $B_{\lambda'}$. Caso o lightpath não seja viável faça $w' = w' + 1$ e volte ao passo 6;
8. Aceite a chamada, atualize W_λ (colocando os enlaces de P_λ em modo ocupado), atualize $W_{\lambda'}$ (colocando os enlaces de $B_{\lambda'}$ em modo proteção), faça $S = S + 1$ para cada enlace de $B_{\lambda'}$, e, por fim, atualize os ruídos gerados por P_λ;
9. Pare o procedimento

O pseudocódigo deste mecanismo é apresentado no Algoritmo 2:

5. Avaliação de Desempenho

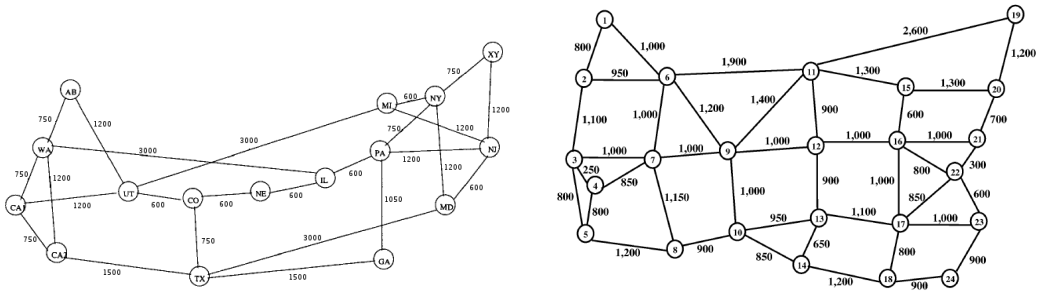
Avalia-se, nesta seção, o desempenho do algoritmo proposto em suas duas versões (sensível e insensível aos efeitos degradantes do sinal), por meio de simulação.

A eficácia do algoritmo foi aferida em duas topologias diferentes: a NSFNET, com 16 nós e 25 enlaces; e a USA Network, com 24 nós e 43 enlaces; as Figuras 3(a) e 3(b) ilustram, respectivamente estas topologias.

As medidas de interesse aferidas são a probabilidade de bloqueio e a razão de vulnerabilidade. A primeira determina a proporção de chamadas que não podem ser aceitas em virtude da falta de recursos na rede, ou da qualidade inaceitável estimada para o sinal dos caminhos ópticos que interligam origem e destino. A segunda medida é uma razão entre chamadas que não podem ser recuperadas e o total de chamadas que tiveram seu serviço interrompido por uma falha de enlace. Essa medida expressa o nível de confiabilidade de um caminho de proteção.

Algoritmo 2 Algoritmo sensível às limitações da camada física

for $w = 1$ até W **do**
  $P_w \Leftarrow shortestPath(T, w)$
  if $temQualidadeMinima(P_w)$ **then**
    $T' \Leftarrow topologiaDisjunta(T, P_w)$
    $T' \Leftarrow limitarCompartilhamento(T', C)$
    for $w' = 1$ até W **do**
      $B_{w'} \Leftarrow shortestPath(T', w')$
      if $temQualidadeMinima(B_{w'})$ **then**
        $setupLightpath(P_w, B_{w'})$
        $atualizarCompartilhamento(B_{w'})$
      end if
    end for
  end if
end for



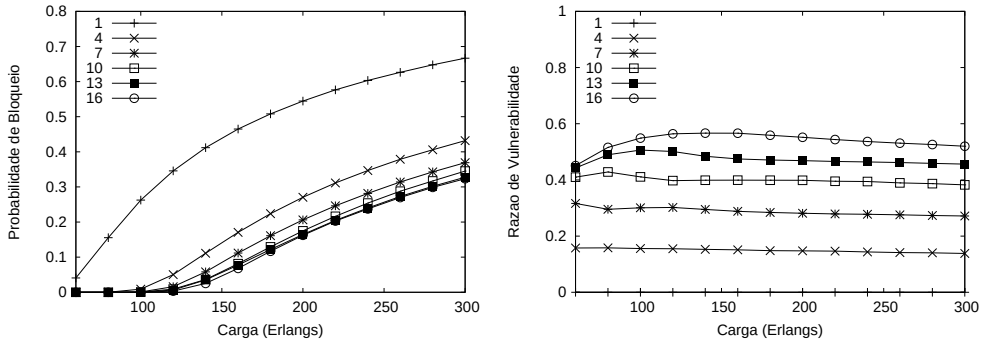
(a) NSFNET (b) SPPIARP

Figura 3. Topologias usadas

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

A Figura 4 apresenta o desempenho do algoritmo proposto em redes ideais, tendo como base a topologia da rede NSFNET para simulações. Seis níveis de compartilhamento são mostrados nos dois gráficos: 1, 4, 7, 10, 13 e 16. O nível 1 aceita que apenas um caminho primário refira-se a um enlace de proteção, e, portanto, trata-se de proteção dedicada, enquanto que o nível 16 permite que até 16 caminhos primários compartilhem um caminho de proteção, correspondendo a proteção compartilhada com política de melhor esforço. Os níveis restantes são valores intermediários, e podem ser usados por clientes que possuem necessidades diversas. Na Figura 4(a), observa-se que a proteção dedicada

(nível 1) produz probabilidades de bloqueio muito elevadas. A explicação para isso é a grande alocação de recursos para se obter redundância, uma vez que cada chamada precisa de, no mínimo, duas vezes mais enlaces para ser estabelecida quando comparada a uma rede sem proteção. O bloqueio é tão alto, que sob 300 Erlangs, este chega a 67%, tornando este esquema de proteção inviável. Quando se aceita o compartilhamento dos caminhos de proteção, observa-se uma melhora significativa. Com nível 4, e sob 300 Erlangs, o bloqueio reduz a 42%. Sob 100 Erlangs, a redução observada é de no mínimo 27%, o que mostra as vantagens do compartilhamento. Para níveis maiores, observa-se reduções cada vez menores no bloqueio, chegando a 31% para o melhor esforço. Quanto se trata da razão de vulnerabilidade (Figura 4(b), para proteção dedicada tem-se o melhor resultado, com todas as chamadas recuperadas. Com o compartilhamento com nível 4, 18% das chamadas deixam de ser recuperadas. Considerando-se o ganho com a diminuição de bloqueio, o aumento na razão de vulnerabilidade é compensador. Para níveis maiores de compartilhamento, observa-se aumentos progressivos da vulnerabilidade, chegando a 55% sob 300 Erlangs para o melhor esforço.

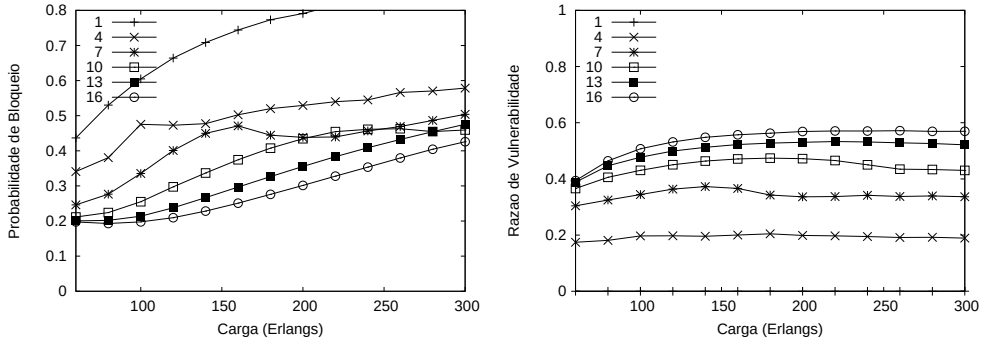


(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

Figura 4. Desempenho do novo algoritmo em redes ideais utilizando a topologia NSFNET

A Figura 5 mostra os resultados obtidos para o cenário em que as limitações da camada física são levadas em consideração, ou seja, para o algoritmo sensível aos efeitos degradantes do sinal. Na Figura 5(a), observa-se um aumento generalizado na probabilidade de bloqueio. Mesmo para cargas de baixa intensidade, sob 60 Erlangs, 20% das chamadas não são aceitas quando se considera melhor esforço. Para a proteção dedicada, o número de chamadas bloqueadas é de 45% sob 60 Erlangs, e ultrapassa 80% sob 200 Erlangs, o que torna inviável o uso desse esquema de proteção. Isto mostra o quão devastador podem ser os efeitos degradantes do sinal em redes ópticas. Com um nível de compartilhamento igual a 4, o bloqueio diminui para 33% sob 60 Erlangs e 55% sob 200 Erlangs, o que ilustra que o compartilhamento leva a melhores resultados. Para níveis intermediários, o comportamento é bastante semelhante ao obtido para redes ideais, com o bloqueio diminuindo progressivamente exceto para níveis limitados inferiormente pela curva do menor esforço. Na Figura 5(b), observa-se um ligeiro aumento da razão de vulnerabilidade para todos os níveis. O aumento é pequeno por que a viabilidade do sinal de um caminho de proteção é testada no momento da aceitação da chamada e, portanto, já possuem qualidade aceitável. Entretanto, entre o momento da aceitação e a ocorrência da falha, o estado da rede pode mudar, o que pode tornar o sinal do caminho de

proteção inviável, levando ao pequeno aumento observado. Mesmo para a proteção dedicada, não é possível obter 100% de recuperação, embora o aumento de vulnerabilidade observado seja insignificante (cerca de 0,1%). Para o nível 4, a vulnerabilidade aumenta ligeiramente, pulando de 18% para 19% em média. Progressivamente o valor da grandeza aumenta, chegando a 59% para o melhor esforço, 4% maior do que no caso ideal.

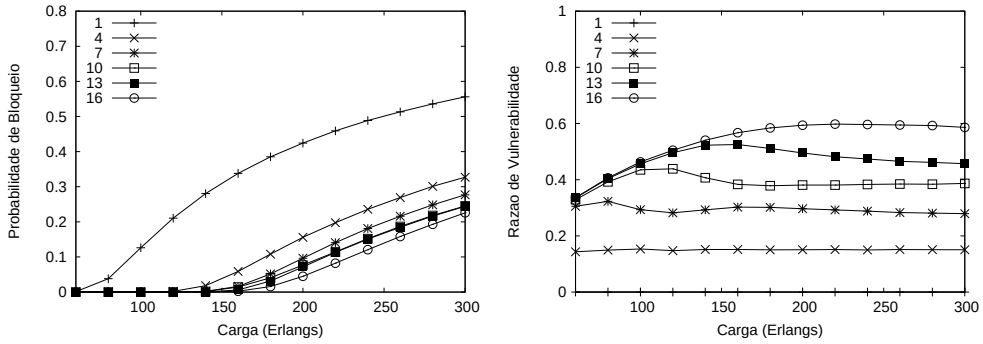


(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

Figura 5. Desempenho do novo algoritmo considerando as limitações da camada física utilizando a topologia NSFNET

5.1. USA Network

O desempenho do algoritmo proposto foi também avaliado utilizando-se a topologia da USA Network. A Figura 6 apresenta os resultados para redes ideais. O comportamento geral é bastante semelhante ao obtido para a topologia NSFNET, o que reforça os resultado encontrados. Observa-se, entretanto, uma diminuição significativa do bloqueio (Figura 6(a)), explicada pela maior disponibilidade de recursos nesta topologia. Enquanto a NSFNET possui 25 enlaces, a rede USA apresenta 43, possibilitando um número maior de caminhos interligando dois nós. Na proteção dedicada, o impacto dessa maior disponibilidade de caminhos leva a uma diminuição do bloqueio de 67% a 55% sob carga de 300 Erlangs. Para nível de compartilhamento igual a 4, a diminuição observada é de 42% a 32% e a proteção segundo o melhor esforço de 31% a 21%. O padrão de diminuição do bloqueio dos níveis intermediários é igual ao obtido para a NSFNET. A Figura 6(b) apresenta os resultados para a razão de vulnerabilidade. O comportamento do algoritmo é também bastante semelhante ao resultado encontrado para a topologia da NSFNET, sobretudo para níveis de compartilhamento baixos. Para proteção dedicada, 100% dos caminhos são recuperados, o que é esperado por este tipo de proteção, e para nível de compartilhamento igual a 4, obteve-se os mesmos 18% de razão vulnerabilidade. Quando o compartilhamento aumenta, em cargas baixas, verifica-se uma diminuição da vulnerabilidade, que também é explicada pela maior quantidade de caminhos disponíveis, e consequente diminuição do compartilhamento real experimentado na rede. Já para cargas altas, observa-se um aumento da vulnerabilidade. A explicação para isso, é que com o número maior de chamadas aceitas, um maior número de caminhos primários compartilha um caminho de proteção, e, no momento de uma falha, o número de chamadas que podem ser recuperadas é menor. Para a proteção segundo o menor esforço, observou-se um aumento de 55% a 60%. Para os níveis intermediários o aumento foi semelhante.



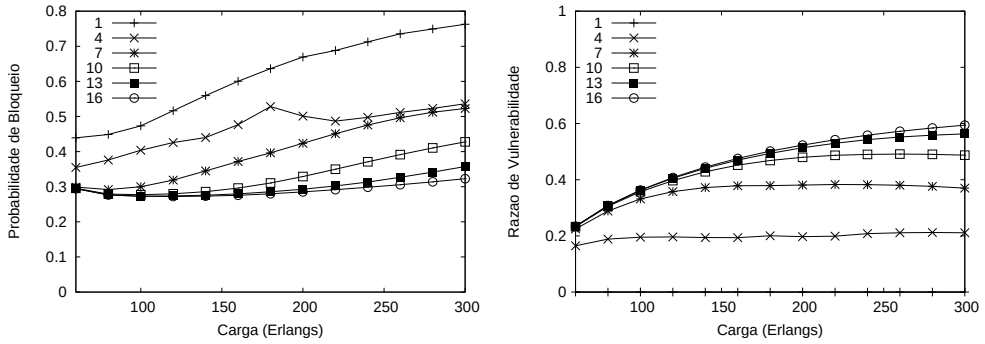
(a) Probabilidade de Bloqueio (b) Razão de Vulnerabilidade

Figura 6. Desempenho do novo algoritmo em redes ideais utilizando a topologia da USA Network

A Figura 7 apresenta o desempenho obtido para o algoritmo proposto quando se considera as limitações da camada física. Na Figura 7(a), observa-se que o crescimento da curva da probabilidade de bloqueio para a proteção dedicada é menor do que o obtido para a topologia da NSFNET. Nesta, o valor obtido para essa grandeza sob 200 Erlangs é superior a 80%, enquanto que na USA Network, sob 300 Erlangs, o bloqueio é inferior a 75%. O motivo desta diminuição é o mesmo relatado no caso ideal. Com o maior número de enlaces na rede, há um maior número de caminhos disponíveis, o que leva a uma diminuição do bloqueio. Para o melhor esforço, observa-se um comportamento diferente. Sob 60 Erlangs (primeiro valor medido), o bloqueio é de 30%, maior do que na NSFNET, para a qual esse valor é de 20%. A explicação para isso é o maior bloqueio de conexões devido a qualidade inaceitável do sinal. Embora a USA Network tenha mais nós e enlaces, também apresenta um diâmetro maior do que a NSFNET. Isto faz com que um número maior de caminhos de longa distância seja possível, e como a qualidade do sinal está diretamente ligada ao tamanho de um caminho, observa-se um aumento no bloqueio ocasionado pelos efeitos degradantes do sinal. Já na outra extremidade da mesma curva, este efeito deixa de ser o mais importante, e a maior disponibilidade de caminhos na rede leva a uma diminuição do bloqueio de 41% a 31%. De formas diferentes, estes dois efeitos interferem sobre as curvas intermediárias, mas o padrão de diminuição de bloqueio é bastante semelhante. Na Figura 7(b), verifica-se a evolução da razão de vulnerabilidade para as diferentes curvas. Observa-se uma diminuição generalizada dessa grandeza para cargas baixas e para níveis de compartilhamento mais altos, quando comparado ao mesmo cenário com a topologia da NSFNET. Quando o esquema de proteção é o melhor esforço, sob 60 Erlangs, a vulnerabilidade cai de 40% para 21%. Esta diminuição está relacionada a maior probabilidade de bloqueio. Com um número menor de chamadas aceitas, o compartilhamento também cai, e, por consequência, mais chamadas podem ser recuperadas. Na outra extremidade, sob 300 Erlangs, o padrão observado não muda.

6. Conclusão

Este artigo apresentou um novo algoritmo de proteção por caminho compartilhado com diferentes níveis de compartilhamento. Apresentou também uma versão sensível às limitações da camada física para o algoritmo, baseada em [Rosa et al. a]. Através de simulação, concluiu-se que o algoritmo é capaz de produzir diferentes níveis de confiabi-



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

Figura 7. Desempenho do novo algoritmo considerando as limitações da camada física utilizando a topologia da USA Network

lidade, bem como diferentes níveis de bloqueio, podendo assim atender a usuários com necessidades distintas. Observou-se que em situações nas quais a utilização de proteção dedicada é praticamente impossível, devido ao grande bloqueio gerado pela redundância, permitir que caminhos de proteção sejam compartilhados por poucos caminhos primários (4 no exemplo mostrado) pode diminuir significativamente a probabilidade de bloqueio, a custo de um aumento compensador na razão de vulnerabilidade.

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

A integração de provisão de QoS e proteção diferenciada constitui um possível trabalho futuro capaz de avançar o conhecimento apresentado neste artigo.

Agradecimentos

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.

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.

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.

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

Rosa, S. R. A. S., Drummond, A. C., and Fonseca, N. S. (2009). Lightpath establishment in WDM networks with best effort shared path protection in impaired-transmissions. *Accepted for publication Proc of IEEE ICC 2009*.

Rosa, S. R. A. S., Drummond, A. C., and Fonseca, N. S. (2009) Performance of best effort shared path protection mechanism under physical impairments in WDM networks. *Accepted for publication Proc of ONDM 2009*.

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*.

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