Proteção Compartilhada por Enlace para Redes Totalmente Ópticas

Valdenir Souza Silva, Yasmine Gabriele da Silva Souza e Rodrigo Choji de Freitas

***Resumo*— Neste artigo são apresentados os resultados de avaliação de robustez para o algoritmo de proteção compartilhada por enlace. A referida análise considera as métricas de taxa de proteção e taxa de vulnerabilidade obtidas pela simulação de três algoritmos (*shortest path, minimum number of hops e least resistance weight*).**

Palavras-Chave*— *Falhas, Proteção, Redes Totalmente Ópticas, Sobrevivência.

***Abstract*—In this paper we present the robustness evaluation results for the link-shared protection algorithm. This analysis considers the protection rate and vulnerability rate metrics obtained by the simulation of three algorithms (*shortest path, minimum number of hops e least resistance weight*).**

Keywords*—*Failure, Protection, All-Optical Networks, Survivability.

I. INTRODUÇÃO

Todo o tráfego convergente (áudio, vídeo, imagem) é transportado por meio da Internet que, por sua vez, utiliza a tecnologia de comunicações ópticas de alta capacidade para a interligação entre os principais provedores. A interrupção dos serviços ou perda de dados pode gerar impactos tanto produtivos quanto econômicos. Mantê-las funcionando e garantir a integridade dos dados transportados por meio delas é fundamental. Um requisito comum é que o sistema esteja disponível 99,999% do tempo, o que corresponde a uma inatividade de menos de 5 minutos por ano [1].

Tais falhas podem ser causadas por erro humano, falhas dos equipamentos utilizados ou catástrofes naturais [1]. Para garantir a disponibilidade do sistema é necessário provê-lo de mecanismos de sobrevivência que garantam a continuidade dos serviços mesmo que ocorram falhas. Existem duas principais técnicas, são elas:

- Proteção: é um mecanismo de proativo e, portanto pré-aloca recursos que serão usados em caso de falha. Esta pré-alocação resulta na diminuição da eficiência da rede e acarreta um aumento do bloqueio de circuitos, uma vez que os recursos reservados de forma redundante para a proteção não podem ser mais disponibilizados [1,2];
- Restauração: esta técnica utiliza os recursos da rede de forma mais eficiente, pois apenas quando ocorre falha na rede são alocados recursos para recuperar uma conexão. Por outro lado, este método exige um tempo maior para o restabelecimento da chamada [1].

Tais técnicas garantem a recuperação dos dados que trafegam pela rede, em caso de falhas, diminuindo a probabilidade de perda de dados. Neste artigo é abordada a técnica de proteção compartilhada por enlace, considerando redes totalmente ópticas. As métricas taxa de proteção (razão entre a quantidade de enlaces protegidos e o total de enlaces) e taxa de vulnerabilidade (razão entre a quantidade de enlaces vulneráveis e o total de enlaces da rota são utilizadas para avaliação de desempenho [3].

O restante deste artigo está organizado da seguinte maneira: na Seção II são apresentados os conceitos fundamentais e de proteção compartilhada por enlace, bem como o seu pseudocódigo. Na Seção III sãoapresentados os resultados parciais desta pesquisa. Na Seção IV são apresentadas as considerações finais sobre a pesquisa.

II. PROTEÇÃO COMPARTILHADA POR ENLACE: CONCEITO E PSEUDOCÓDIGO

O método de proteção compartilhada por enlace define *a priori* rotas secundárias para cada enlace de rota principal das chamadas que estão sendo estabelecidas. Na Figura 1 a rota principal da chamada, representada pela seta verde, tem como origem o nó "O" e destino o nó "D". Os enlaces que compõem a rota principal estão protegidos cada um respectivamente por sua rota secundária, representada pelas setas em vermelho. A rota secundária deve possuir o mesmo canal de transmissão que o enlace de rota principal a ser protegido. Os enlaces da rota secundária podem ser compartilhados para compor a rota secundária de outros enlaces que utilizam o mesmo canal de transmissão [1,3].

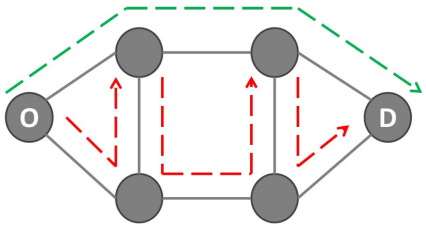

Fig. 1. Rotas secundárias dos enlaces da rota principal.

A. *Pseudocódigo*

Algoritmo 1: Proteção Compartilhada por Enlace	
1.	**para** *cada chamada requisitada* **faça**
2.	Determinar origem e destino da chamada;
3.	Buscar menor rota entre origem e destino;
4.	**se** *rota inexistente* **então**
5.	Bloquear chamada;
6.	**senão**
7.	Alocar comprimento de onda

Valdenir Souza Silva, Yasmine Gabriele da Silva Souza e Rodrigo Choji de Freitas, Universidade do Estado do Amazonas, Manaus-AM, Brasil, E-mails: vassi.mati@uea.edu.br, ygss.eng@uea.edu.br, rcfreitas@uea.edu.br.

```
8.          para cada enlace da rota principal faça
9.              Buscar rota alternativa com menor custo;
10.             se rota inexistente então
11.                 Bloquear rota alternativa;
12.             senão
13.                 Alocar comprimento de onda;
14.                 Incrementar contador de uso do lambda;
15.             fim se
16.         fim para
17.     fim se
18. fim para
```

III. RESULTADOS

Na Figura 2 é apresentado o desempenho da taxa de proteção em função do limite de compartilhamento para os algoritmos SP (*shortest path*), MH (*mininum number of hops*) e LRW (*least resistance weight*). Neste cenário são considerados 20 comprimentos de onda por enlace. A partir do limite de compartilhamento igual a 1 os três algoritmos atingem seus respectivos pontos de saturação. A taxa de proteção para o algoritmo SP fica em torno de 34,5%, para o algoritmo MH fica em torno de 36% e para o algoritmo LRW a taxa de proteção fica próxima de 37%. É importante destacar a vantagem de se utilizar a estratégia compartilhada em proteção por enlace, visto que entre o limite de compartilhamento igual a 0 (proteção dedicada por enlace) e o limite de compartilhamento igual a 1, a taxa de proteção obtém um crescimento em torno de 15%.

No gráfico da Figura 3 são apresentados os desempenhos dos algoritmos SP, MH e LRW em relação à taxa de vulnerabilidade *versus* a limitação de compartilhamento, considerando 20 comprimentos de onda por enlace para a topologia Finlândia. Embora o algoritmo LRW apresente a maior taxa de proteção dentre os algoritmos avaliados, ele é o que permite a geração de mais chamadas vulneráveis a uma falha. Por este gráfico é possível também concluir que quando a proteção é dedicada a taxa de vulnerabilidade é zero. A taxa de vulnerabilidade não atinge um ponto de saturação, isto é, quanto mais um recurso é compartilhado, maior é a taxa de vulnerabilidade.

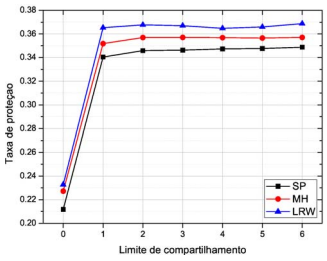

Fig. 2. Taxa de proteção em função do limite de compartilhamento para a topologia Finlândia, 60 erlangs, 20 comprimentos de onda.

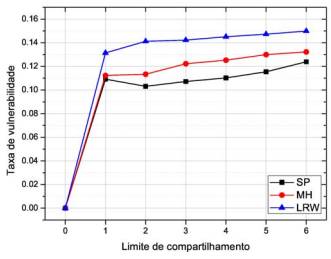

Fig. 3. Taxa de vulnerabilidade em função do limite de compartilhamento para a topologia Finlândia, 60 erlangs, 20 comprimentos de onda.

Na Figura 4 é apresentado o gráfico da taxa de proteção em função do limite de compartilhamento para cada um dos três algoritmos avaliados, considerando o cenário de 40 comprimentos de onda por enlace da topologia Finlândia. As curvas possuem comportamento similar ao do cenário com 20 comprimentos de onda por enlace. No entanto, é possível notar uma maior capacidade de proteção de cada um dos algoritmos. Isso pode ser explicado pela maior quantidade de comprimentos de onda disponíveis. Ainda em função dessa maior quantidade de recursos, o ponto de saturação é deslocado para o limite de compartilhamento igual a 2.

Na Figura 5 é apresentado o gráfico da taxa de vulnerabilidade em função do limite de compartilhamento para 40 comprimentos de onda por enlace da topologia Finlândia. Em função da maior quantidade de comprimentos de onda, as chamadas ficam menos vulneráveis. Comparando com o cenário de 20 comprimentos de onda é possível se notar uma diminuição de cerca de 6 pontos percentuais na taxa de vulnerabilidade. Novamente, não é possível determinar o ponto de saturação para a taxa de vulnerabilidade, que cresce conforme o limite de compartilhamento aumenta.

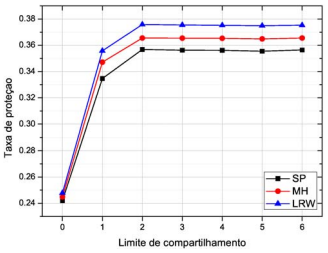

Fig. 4. Taxa de proteção em função do limite de compartilhamento para a topologia Finlândia, 60 erlangs, 40 comprimentos de onda.

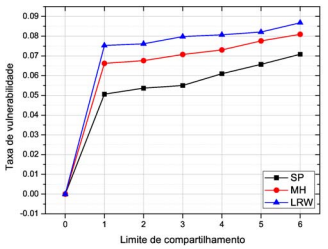

Fig. 5. Taxa de vulnerabilidade em função do limite de compartilhamento para a topologia Finlândia, 60 erlangs, 40 comprimentos de onda.

IV. CONCLUSÕES

O método de proteção compartilhada por enlace apresenta uma taxa de proteção baixa, se comparado com o método de proteção compartilhada por caminho. Isto pode ser justificado pela obrigatoriedade de continuidade de comprimento de onda e pela necessidade de utilizar um número maior de recursos da topologia.

Foram considerados três importantes algoritmos de roteamento da literatura, LRW, SP e MH, dentre os quais o algoritmo LRW apresenta maior taxa de proteção, enquanto que o algoritmo SP apresenta a menor taxa de vulnerabilidade. A variação de 20 para 40 comprimentos de onda utilizados não gerou uma grande diferença entre os valores da taxa de proteção do algoritmo LRW, ficando ainda em torno de 37%.

Com base nos resultados é possível dizer que a proteção por enlace compartilhado apresenta o seu melhor desempenho quando utilizada em uma topologia cujo nó menos conectado possui, pelo menos, duas conexões, com 40 comprimentos de onda, utilizando o algoritmo de roteamento LRW.

AGRADECIMENTOS

À Universidade do Estado do Amazonas.

REFERÊNCIAS

[1] R. RAMASWAMI, K. N. SIVARAJAN, G. H. SASAKI, Optical Networks: A Practical Perspective, 3ª ed. Morgan Kaufmann, 2010.

[2] A. SOARES, G. DURÃES, J. MARANHÃO, W. GIOZZA. Sobrevivência em Redes Óptica WDM sob Influência de Algoritmos de Alocação de Rota e de Comprimento de Onda. XXII Simpósio Brasileiro de Telecomuincações - SBrT05, 04-08 de setembro de 2005, Campinas, SP.

[3] R. C. FREITAS, J. F. MARTINS-FILHO, C. J. A. BASTOS-FILHO. Redes Ópticas - Estratégias deSobrevivência a Falhas. 1ª ed. Manaus: UEA Edições, 2015.