Planejamento e Segurança em Redes Ópticas: Uma Estratégia para Minimizar os Efeitos do Ataque *Jamming*

K.D.R. Assis e Clécio. C. Santos

Universidade Federal da Bahia (UFBA)
Escola Politécnica da Universidade Federal da Bahia - DEE
Rua Aristides Novis, 02, Federação, CEP: 40210-630 – Salvador – BA – Brasil.
E-mail: karcius.assis@ufba.br

Abstract. *This paper proposes a strategy to prevent unwanted attacks that occur in transparent optical networks. The strategy proposed heuristic is capable of providing good solutions in network planning. In traditional planning strategies for optical networks, there is no a priori consideration of the attacks that may affect the network, and once the solution is implemented, the attack can not be avoided or can be avoided with a very high cost (if planned network is fully protected). Taking into account the effects of unwanted attacks, planned a route that allows limiting the possible interference of these attacks.*

Resumo. *Neste artigo propomos uma estratégia para prevenir ataques indesejáveis que possam surgir em redes ópticas transparentes. A estratégia heurística proposta é capaz de fornecer boas soluções no planejamento da rede. Nas estratégias tradicionais de planejamento de redes ópticas, não há consideração a priori sobre os ataques que podem afetar a rede, e uma vez que a solução é implementada, o ataque não pode ser evitado ou pode será evitado com um custo bastante alto (se a rede for planejada totalmente protegida). Levando em consideração os efeitos de ataques indesejáveis, planejamos um roteamento que permite limitar a possível interferência desses ataques.*

1. Introdução

O planejamento de redes ópticas WDM transparentes é uma tarefa de grande complexidade. Esta complexidade surge não apenas pelo fato das redes serem de grande dimensão, o que torna muitas vezes o problema difícil ou intratável, mas também porque há uma grande quantidade de dados transmitidos em um único enlace de fibra. Logo, falhas em enlaces podem provocar perdas e inconveniências para as operadoras e usuários desta rede. Outro aspecto que deve ser observado é a qualidade do sinal, a qual pode ser degradada devido a efeitos inerentes a camada física. Por exemplo, a interferência entre canais (*crosstalk*) depende da utilização ou não de comprimentos de onda adjacentes em lightpaths que compartilham enlaces físicos [Deng *et al*, 2004]. Além disso, os efeitos de outras degradações, como a Modulação Cruzada de Fase (XPM- C*ross Phase Modulation*) e a Mistura de Quatro Ondas (FWM- *Four Wave*

Mixing) são altamente dependentes do uso de canais adjacentes ou próximos aos adjacentes, [Azodolmolky, 2009]. Portanto, evitar as interferências entre canais adjacentes, falhas, e ataques externos ou inerentes a rede são critérios importantes para planejar de forma eficiente redes WDM transparentes.

Diante disso, a solução do problema de Roteamento e Alocação de Comprimentos de Onda (*Routing and Wavelenght Assignmet*-RWA) tem uma influência importante no surgimento desses efeitos e na prevenção de falhas, pois selecionar uma rota, para um par origem-destino, e alocar comprimentos de onda para o *lightpath* dessa rota pode diminuir ou aumentar as degradações dos efeitos da camada física e também as chances de restauração em caso de falhas na rede. Então, o planejamento de redes ópticas transparentes deve ser capaz de considerar em suas decisões os efeitos e propriedades da camada física [Ramamurthy *et al*, 1999]. Nesse caso, as formulações matemáticas e algoritmos são conhecidos como IRWA ou ICBR (*Impairment Constraint Based Routing*) [Bastos Filho *et al*, 2009].

Nesse trabalho nós propomos um novo algoritmo heurístico, o ILR- *Iterative Load Routing*, para otimização do roteamento em redes ópticas transparentes. O principal objetivo desse algoritmo é minimizar os efeitos danosos que um efeito da camada física, conhecido como ataque *jamming* pode causar na rede.

Esse objetivo foi inspirado no trabalho proposto em [Skorin-Kapov *et al*, 2010). No referido trabalho um novo critério para o problema do roteamento de lightpaths na topologia física é usado na rede. Esse critério busca minimizar uma grandeza definida como *maxLAR*, que indica o máximo número de lightpaths que podem ser afetados por um ataque *jamming* (descritos na seção 3).

Para alcançar esse objetivo nós usamos uma abordagem que procura rotear os lightpaths atuais através de rotas físicas pouco usadas por outros lightpaths, ou seja, procuramos minimizar o compartilhamento de enlaces físicos por lightpaths. Isto difere da abordagem apresentada em [Assis *et al*, 2010], onde minimizamos os efeitos da alocação de comprimentos de ondas a pares fonte-destino já estabelecidos.

Este artigo está organizado da seguinte forma. Na seção 2 definimos mais detalhadamente topologia virtual e topologia física. Na seção 3 apresentamos o problema abordado neste artigo e uma heurística para solução do mesmo. Na seção 4 mostramos resultados numéricos para uma topologia de rede com 6 nós e, posterioremente, para uma rede de 30 nós, comparamos com alguns resultados de [Skorin-Kapov *et al*, 2010]. Finalmente, concluímos nosso artigo na seção 5.

2. Topologia Física e Topologia Virtual

Ao projetar uma rede óptica WDM é necessário estabelecer os lightpaths por onde o tráfego (geralmente medido em Gbps) será encaminhado [Assis *et al*, 2005]. Essa definição é feita através do VTD (*Virtual Topology Design*). Posteriormente, o RWA deve ser resolvido, ou seja, os lightpaths, previamente escolhidos, devem ser roteados por uma topologia física e comprimentos de onda devem ser alocados de forma adequada nesses lightpaths. Esse segundo processo deve obedecer às seguintes regras:

a) dois lightpaths podem compartilhar um mesmo enlace, porém, não podem ser associados ao mesmo comprimento de onda em um mesmo enlace físico.

b) se conversões de comprimento de onda não forem permitidas, o lightpath deve ser

associado ao mesmo comprimento de onda em todos os enlaces da rota.

Essas duas regras se aplicam a este trabalho. A Figura 1 ilustra uma arquitetura de uma rede óptica simples, formando uma topologia física, com os nós numerados de 1 a 6 e interconectados através de enlaces físicos (fibras ópticas) bidirecionais.

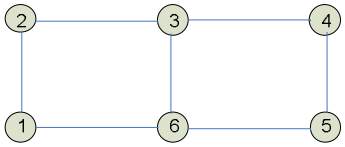


Figura 1. Topologia física

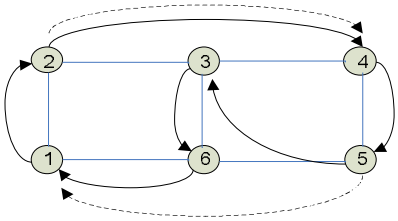


Figura 2. Topologia virtual

O projeto de topologia virtual envolve a definição dos caminhos virtuais para o encaminhamento dos dados entre um par de nós (fonte e destino). Todos os nós da rede se comunicam através dos caminhos virtuais. Se na topologia virtual um nó não estiver conectado diretamente (conectado virtualmente) com o nó destino, então os dados serão conduzidos por várias rotas virtuais até chegarem ao seu destino. Pode-se visualizar isto na Figura 2, onde, o nó 3 não tem uma conexão direta (caminho virtual) para o nó 1. Então o tráfego originado em 3 terá que passar por dois caminhos virtuais: de 3 para 6 e de 6 para 1 para chegar ao seu destino, o nó 1. A quantidade de lightpaths utilizados, também é chamada de saltos virtuais (*virtual hops*). No exemplo anterior, houve a utilização de dois lightpaths, então se diz que ocorreram dois saltos virtuais. Coincidentemente, também ocorreu a passagem por dois enlaces físicos. Neste exemplo, limitamos para 2 o número de enlaces físicos que um lightpath pode percorrer. O número máximo de enlaces físicos que um lightpath pode percorrer é denotado por *H* e o número de comprimentos de onda disponíveis para planejar a rede é denotado por *W*. Neste artigo nós iremos gerar uma Topologia Virtual, a partir de uma demanda de tráfego, que será a entrada do problema em estudo.

3. Segurança em Redes Ópticas

Nos últimos anos vários estudos foram iniciados no intuito de investigar fatores de segurança em redes ópticas transparentes [Kim *et al*, 2010], [Ramaswami, 2010]. Novos métodos de ataque e de detecção de ataque surgiram decorrentes das particularidades inerentes às redes ópticas. Além disso, alguns tradicionais métodos estão sendo re-estudados.

No ataque *jamming*, o atacante injeta um sinal para reduzir a capacidade do receptor de interpretar os dados transmitidos ou o atacante explora o *crosstalk* em componentes ópticos, injetando um sinal de comprimento de onda diferente do usado na banda de comunicação, porém dentro da banda passante do componente.

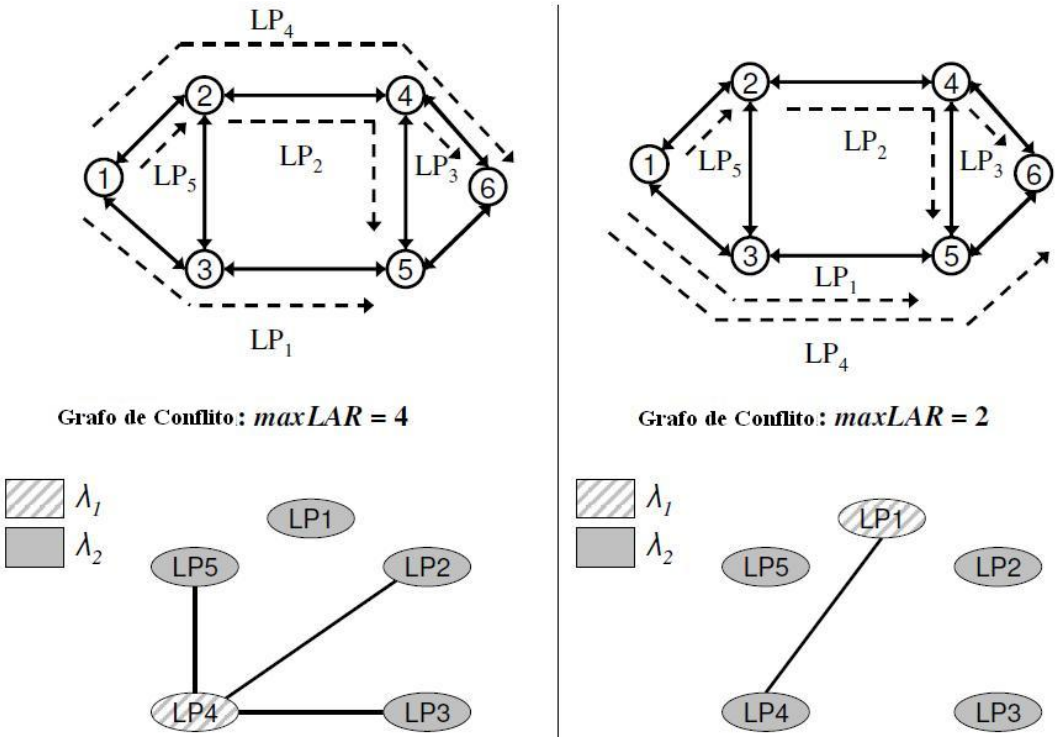
Além do ataque *jamming*, nas redes WDM transparentes, a qualidade do sinal é degradada devido às restrições da camada física. Essas restrições dependem das características físicas das fibras usadas, mas algumas dessas restrições também variam de acordo com a utilização da rede. Por exemplo, a interferência entre canais, a modulação cruzada de fase (XPM) e a mistura de quatro ondas (FWM) não dependem

unicamente das características da fibra, mas também da utilização de outros comprimentos de onda no mesmo enlace, ou seja, de lightpaths que compartilham o mesmo enlace físico [Azodolmolky *et al*, 2009]. Portanto, neste caso, temos que levar em consideração como o roteamento irá interferir na solução do RWA. Logo, todos esses efeitos podem ser minimizados através de uma nova estratégia com uma nova função objetivo. Um exemplo do problema e uma proposta para solucioná-lo são apresentados nas próximas subseções.

3.1 Minimizando o Raio de Ataque

Para minimizar o raio de ataque e os efeitos provocados por uma possível falha, nós definimos uma variável chamada *maxLAR*. Na rede há um conjunto de lightapths, então o *maxLAR* é definido como o número máximo de lightpaths que um lightpath deste conjunto pode atacar. Ele indica se o lightpath em análise compartilha enlaces físicos com os outros lighpaths do conjunto. Isso difere da abordagem de balanceamento de carga, pois o *maxLAR* considera quantos lightpaths compartilham enlaces físicos e não o número de lightpaths roteados ao longo de cada enlace físico em uma rota. Ou seja, consideramos o número máximo de lightpaths que serão interrompidos em caso de diversos cenários de ataque na camada física. Se um sinal de interferência é injetado em um lightpath, ele pode interromper, além dele mesmo, os lightpaths com os quais compartilha enlaces físicos. Isso pode decorrer da concorrência entre os ganhos dos amplificadores de sinal e também da interferência inter-canal em fibras. Nós assumimos que apenas o sinal de ataque inicial pode causar efeitos *crosstalk*, ou seja, que os lightapths posteriormente atacados não adquirem capacidade para realizar novos ataques.

Logo, nosso principal objetivo para o problema RWA é minimizar o *maxLAR* atendendo toda a demanda de tráfego (em termos de lightpaths). Um objetivo secundário é reduzir o congestionamento (ou seja, o número máximo de lightpaths roteados através de qualquer enlace físico). O *maxLAR* de uma configuração de roteamento é também um limite superior no congestionamento, assim, minimizando a *maxLAR*, também minimizamos o pior caso de congestionamento. Note que um aspecto de congestionamento é que ele representa o número máximo de lightpaths interrompido em caso de corte de fibra ou mal funcionamento ao longo de qualquer outro componente do enlace. Assim, minimizar o congestionamento pode minimizar a necessidade de mudança de rota em caso de falhas, o que pode ser um benefício adicional de nossa abordagem.



a) b)

Figura 3. Estratégias de Roteamento

Um exemplo de dois diferentes roteamentos para uma demanda de cinco lightpaths é mostrado na Fig. 3 para uma rede de 6 nós. As duas soluções de roteamento têm um congestionamento L=2 e podem ser realizadas usando dois comprimentos de onda. Entretanto o *maxLAR* na primeira solução é 4 (Fig.3.(a)), enquanto que na segunda solução o *maxLAR* é 2 (Fig. 3.b). Ou seja, um ataque *jamming* iniciado no lightpath 4 na primeira solução de roteamento, poderia interrromper os lightpaths 2, 3, 4, e 5. Já na segunda solução de rotemaneto, um ataque *jamming* em qualquer lightpath poderia interromper no máximo 2 lightpaths (incluindo o próprio lightpath de início do ataque). Observe que para incluir o lightpath de início de ataque, o valor do *maxLAR* é sempre acrescido de 1. Logo, apesar dos dois esquemas de roteamento usarem o mesmo número de comprimentos de onda *W*, o mesmo número de *hops H*, e terem o mesmo congestionamento; o segundo esquema poderia reduzir significamente a interrupção causada pelo ataque *jamming* sem nenhum custo extra ao planejamento. Logo, a nova formulação matemática para o RWA é descrita informalmente abaixo com uma nova função objetivo (As formulações tradicionais têm objetivos descritos em [Zang *et al*, 2000]).

Min *maxLAR*

sujeito a:

- os enlaces virtuais, gerados a partir de uma matriz de tráfego são entradas do problema;

- o número total de comprimentos de onda usados é no máximo *W*;
- todos os nós na topologia virtual têm *Ri* arcos de entrada (número de receptores) e *Ti* arcos de saída (número de transmissores) como entrada do problema.
- *Attack radius constraints* de [Skorin-Kapov *et al*, 2008] são adicionadas a formulação do RWA.

A formulação MILP(*Mixed Integer Linear Programming*) detalhada do problema pode ser encontrada em [Skorin-Kapov *et al*, 2008] ou [Skorin-Kapov *et al*, 2010].

3.2 Algoritmo Heurístico

A formulação MILP só é viável para redes de pequena dimensão. Logo, nós propomos a heurística abaixo, chamada ILR (*Iterative Load Routing*) para solucionar o problema descrito anteriormente.

Heurística ILR

Passo 1: rotei a topologia virtual sobre a topologia física pelo método clássico do menor caminho.

Passo 2: Ache o lightpath com o *maxLAR* e remova-o do roteamento.

Passo 3: Defina *sumLOAD* como a soma das cargas de cada link físico ao longo do caminho no qual o lightpath removido estava roteado.

Passo 4: Ache entre todos os possíveis caminhos para o lightpath removido aquele com a menor soma das cargas de seus links físicos, nós chamamos essa soma de *minLOAD*.

Passo 5: *se sumLOAD > minLOAD*

então

re-rotei o lightpath removido sobre caminho com *minLOAD* e volte ao passo 2.

caso contrário

re-rotei o lightpath removido no mesmo caminho no qual ele estava roteado antes.

Passo 6: Ache o próximo lightpath em ordem decrescente de LAR, remova ele do roteamento e volte ao passo 3. Se todos os lightpaths tiverem sido testados sem voltar ao passo 2, então o algoritmo está encerrado.

Nota: – A idéia por trás dessa heurística é que re-roteando os lightpaths sobre conjuntos de links físicos menos congestionados nós podemos reduzir consideravelmente o *maxLAR*. Para aumentar a eficiência da heurística, nós acrescentamos uma restrição: o roteamento resultante após o re-roteamento de cada lightpath só passa a ser uma possível saída do algoritmo se o *maxLAR* não tiver aumentado, caso contrário a saída não se altera.

4. Simulação e Resultados Numéricos

Para validar a formulação proposta consideramos a rede pequena (Figura 1). Também contemplamos uma rede maior, a rede de 30 nós, a *Europe Network* [Inkret, 2003], que devido à complexidade é planejada apenas por meio de heurística e de SP (Shorthest Path).

A) Redes pequenas

Primeiro, nós testamos a heuristic ILR e o MILP de [Skorin-Kapov *et al*, 2008] que tem o objetivo de minimizar o *maxLAR*. Nós usamos o *solver* CPLEX 10.0 para o MILP e o MATLAB 8.0 para a heurística. Para criar os lightpaths , nós geramos 15 matrizes de tráfego diferentes usando o método sugerido em [Banerjee *et al*, 2000], onde uma Fração *F* do tráfego é uniformemente distribuído entre [0, C/ *a*] enquanto que o tráfego remanescente é uniformemente distribuído sobre [*0,C.Ƴa*]. Aqui *C* representa

a capacidade do lightpath, *a* é um inteiro qualquer maior ou igual a 1 e Υ representa a taxa média de intensidade de tráfego entre os pares fonte-destino com maiores e menores valores. Aqui nós usamos os seguintes valores C = 1250, a = 20, Υ = 10, and F = 0.7, como em [Banerjee *et al*, 2000]. Para obter a topologia virtual nós obtemos lightapths em ordem decrescente de tráfego com no máximo 3 transmissores e 3 receptores em cada nó, ou seja, Ti=Ri=3.

Nós fizemos comparações entre o desempenho do algoritmo, o da formulação exata e o do tradicional algoritmo do menor caminho *Shortest Path Routing* – SP [Dijkstra, 1959]. Além da métrica *maxLAR*, também comparamos o desempenho da nossa heurística com relação a outras grandezas usadas em [Skorin-Kapov *et al*, 2010], são elas:

- *AverageLAR*, que indica o número médio de lightpaths que podem ser afetados num ataque;

- *Congestion*, que indica o número máximo de lightpaths roteados sobre qualquer caminho físico e;

- *AverageLOAD*, que indica a carga média dos caminhos físicos.

Os resultados das comparações para a rede de 6 nós é mostrado nas figuras 4,5,6 e 7 abaixo. Nas figuras a nossa heurística é denotada como ILR (*Iterative Load Routing*), o algoritmo do menor caminho é denotado como SP (*Shortest Path*) e a formulação exata é denotada como MILP (*Mixed Integer Linear Programming*). Nós fizemos 15 comparações para cada grandeza, de modo a obter um resultados mais seguros.Podemos constatar, com base na observação das figuras, que a nossa heurística se mostrou bastante eficiente na redução do *maxLAR*, obtendo também bons resultados em relação as demais grandezas, em alguns casos se apresentando melhor até mesmo do que a formulação exata, como na grandeza *AverageLOAD* mostrado na figura 7.

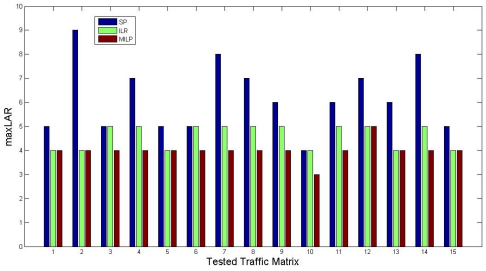


Figura. 4. maxLAR

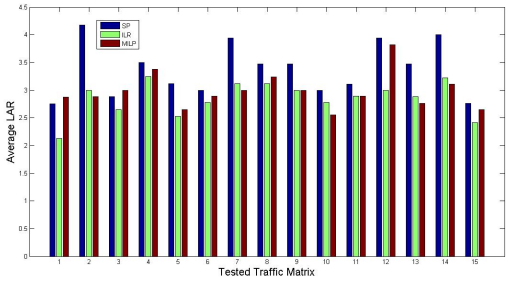


Figura. 5. Average LAR

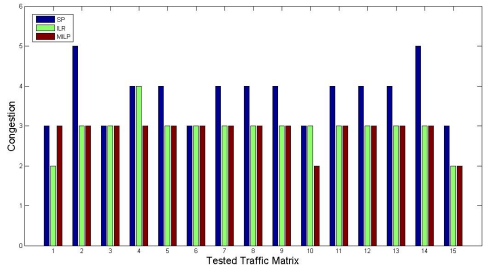


Figura. 6. Congestion

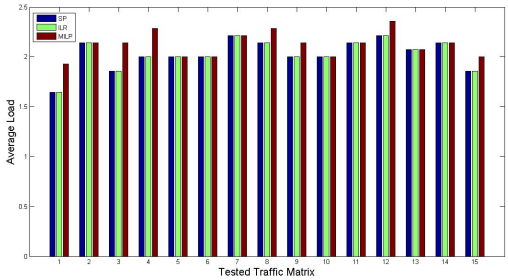


Figura. 7. Average Load

B) Redes Grandes

A heurística ILR mostrou-se muito eficaz para a topologia de 6 nós. Para avaliar o seu desempenho em problemas maiores, nós simulamos a mesma numa rede de 30 nós [Inkret *et al*, 2003].O conjunto de lightpaths foram criados utilizando o mesmo método descrito acima para a rede seis nós, mas com 10 transmissores e receptores por nó, ou seja, *Ti=Ri=10*. Nós também comparamos com o SP. Os resultados para o *maxLAR*, *AverageLAR*, *Congestion* e *AverageLoad* são mostrados nas Figs. 9, 10, 11 e 12, respectivamente.

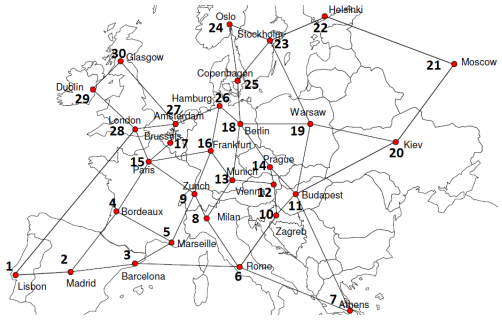


Figure. 8. Large Network

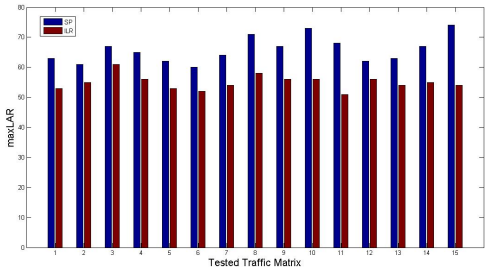


Figura. 9 maxLAR

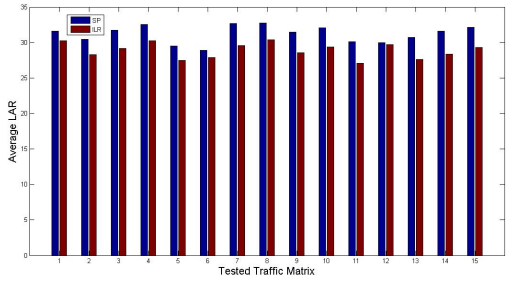


Figura.10 Average LAR

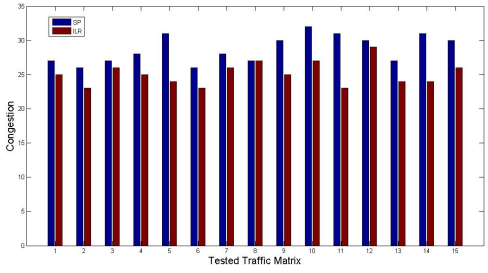


Figura. 11 Congestion

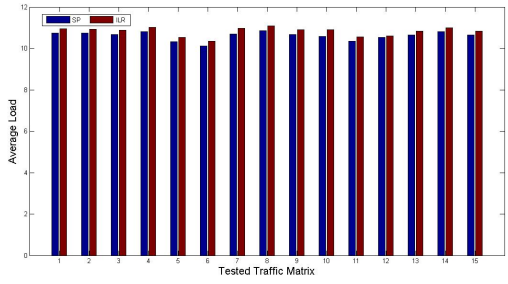


Figura. 12 Average Load

Podemos ver na Figura 9 que a heurística ILR superou significativamente SP em relação a métrica *maxLAR*. Por exemplo, no caso 11, um ataque jamming poderia interromper aproximadamente 50 lightpaths na solução obtida com a ILR e aproximadamente 70 com a solução via SP. Com relação ao congestionamento, podemos ver na figura. 11 que o algoritmo ILR tem o melhor desempenho em todos os casos, enquanto SP obtém valores de congestionamento muito superiores. A métrica *AverageLoad* (e, proporcionalmente, o comprimento médio dos lightpath em termos de saltos) é mostrado na figura. 12. Nela, podemos ver que, como esperado, o SP dar melhores resultados, mas os resultados do ILR estão próximos.

Devemos relembrar que o congestionamento é o limite superior de números de comprimentos de onda necessários em uma rede conversora de comprimentos de onda e que o *maxLAR* é o limite superior no número de comprimentos de onda necessários em redes ópticas conversoras ou não de comprimentos de onda. Logo, em nossas simulações consideramos que após o roteamento o planejador sempre terá disponível *maxLAR*=*W* comprimentos de onda, o que permitirá fazer alocação de comprimentos de onda em qualquer dos dois tipos de redes ópticas. Estratégias de alocação de comprimentos de ondas que minimizem o valor escolhido para *W*, após o roteamento, podem ser obtidas facilmente em [Zang *et al*, 2000] e [Skorin-Kapov, 2007].

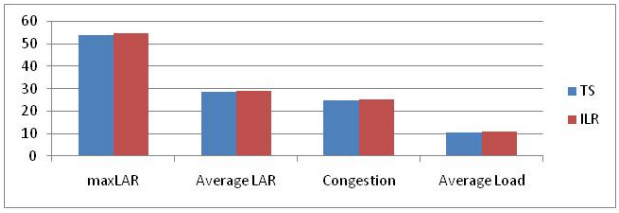


Figura. 13. Average of 15 test cases for each measure with the ILR and TS [1]

A Figura 13 compara os valores médios das 15 simulações para cada métrica utilizando ILR e a heurística Tabu Search –TS proposta por [Skorin-Kapov *et al*, 2010]. Nós podemos observar que TS obtém resultados um pouco melhores, entretanto o custo computacional é elevado e isto será assunto para um próximo artigo.

5. Conclusões

Os experimentos computacionais demonstram claramente que a heurística proposta apresenta uma melhora em relação às estratégias tradicionais de roteamento, quando queremos evitar ataques. Essa melhora vem do fato de que a heurística seleciona as rotas de modo a otimizar a carga nos enlaces percorridos de uma fonte para o destino ou o balanceamento do tráfego na rede. É fato que as redes transparentes sofrem ataques, inerentes aos dispositivos ou ataques externos indesejáveis. Portanto, o planejamento da rota e a alocação de comprimentos de onda levando em conta esses fatores pode ajudar os planejadores e operadores de rede a oferecer uma melhor QoS aos clientes. As perdas inerentes aos componentes ópticos (amplificadores, comutadores ópticos, multiplexadores, demultiplexadores etc) que afetam a qualidade do sinal serão objetos de estudos futuros, assim como o estudo de redes maiores e análise de complexidade, para assim termos uma formulação e heurísticas mais robustas.

Agradecimentos

Ou autores gostariam de agradecer à Fundação de Amparo à Pesquisa do Estado da Bahia-FAPESB pelo apoio financeiro.

Referências

K.D.R. Assis ; SANTOS, Alex Ferreira dos ; SAVASINI, Marcio S. ; GIOZZA, William . Projeto de Topologia Virtual em Redes Ópticas: Uma Abordagem para Evitar Interferências entre Canais. In: WGRS - XV Workshop de Gerência e Operação de Redes e Serviços, 2010, Gramado-RS. XV Workshop de Gerência e Operação de Redes e Serviços, SBRC-2010, 2010. v. 1. p. 87-100 (2010).

Assis, K.D.R., Waldman, H., Giozza, W.: Optical Networks: A Complete Design. IEEE COMSOC SBRT Spec. Join. Iss. J. COMMUN. INF. SYS. 20, 81–95 (2005).

Azodolmolky, Siamak., Klinkowski , Mirosław., Marin, Eva., Careglio , Davide., Pareta , Josep Solé., Tomkos, Ioannis "A survey on physical layer impairments aware routing and wavelength assignment algorithms in optical networks" Computer Networks, vol. 53 pp. 926–944. (2009).

Banerjee, D., Mukherjee, B.:Wavelength-Routed Optical Networks: Linear Formulation, Resource Budgeting Tradeoffs, and a Reconfiguration Study. IEEE ACM Trans. Net. 8, 598–607 (2000).

Bastos Filho, C. J. A. ; Chaves, D. A. R. ; Silva, F. S. F. ; Carvalho, R. V. B. ; Pereira, H. A. ; Martins-Filho, J. F. "Wavelength Assignment Optimization for All-Optical Networks Using Evolutionary Computation" XXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, v.1. pp 31-44, Recife/PE (2009).

Deng, T., Subramaniam, S. e Xu, J., "Crosstalk-Aware are Wavelength Assignment in Dynamic Wavelength Routed Optical Networks", *Broadnets 2004*. First International Conference on Broadband Networks.(2004).

Dijkstra, E.W.: A Note on Two Problems in Connection with Graphs. Num. Math. 1,269–271 (1959).

Inkret, R., Kuchar, A., Mikac, B.: Advanced Infrastructure for Photonic Networks Extended Final Report of COST Action 266. Faculty of Electrical Engineering and Computing, University of Zagreb, pp. 1921, Zagreb (2003).

Kim, Y., Lee, H.: On Classifying and Evaluating the Effect of Jamming Attacks. ICOIN (2010).

Ramamurthy Byrav, Debasish Datta, Helena Feng, Jonathan P. Heritage, and Biswanath Mukherjee "Impact of Transmission Impairments on the Teletraffic Performance of Wavelength-Routed Optical Networks" Journal of Lightwave Technology, Vol. 17, Issue 10, pp. 1713 (1999).

Ramaswami, R. Optical Networking Technologies: What Worked and What Didnt. IEEECommun Mag. 132–139 (2007).

Skorin-Kapov, N.: Routing andWavelength Assignment in Optical Networks Using Bin Packing Based algorithms. Euro. J. Oper. Res. 177, 1167–1179 (2007).

Skorin-Kapov, N.: MILP Formulation for Routing Lightpaths for Attack-Protection in TONs. Proc. NAEC. 55–62 (2008).

Skorin-Kapov, N., Chen, J., Wosinska, L.: New Approach to Optical Networks Security: AttackAware Routing andWavelength Assignment. IEEE. ACMTran. Net. 18, 750–760 (2010).

Zang, H., Jue, J., Mukherjee, B.: A Review of Routing and Wavelength Assignment Approaches for Wavelength Routed Optical WDM Networks. Opt. Net. Mag. (2000).