

AGEP: Um Esquema de Gerenciamento de Falhas em Redes Ópticas

Alisson Barbosa de Souza, Antônio Sérgio de S. Vieira, Jéssyca Alencar L. e Silva, Ana Luiza B. de P. Barros, Gustavo Augusto L. de Campos¹, Joaquim Celestino Júnior, Laure W. N. Mendouga

LARCES – Laboratório de Redes de Computadores e Segurança

¹LACONI - Laboratório de Computação Natural e Inteligente
Universidade Estadual do Ceará (UECE)
Av. Paranjana, 1700 – Itaperi - 60740-903 – Fortaleza

{alisson, sergiosvieira, jessyca, analuiza, gustavo, celestino, laure}@larces.uece.br

Abstract. *One of the ways to offer QoS in optical networks, in a policy based environment, is to use route protection policies. For each signed contract, the network administrator defines the type of protection (1:1, 1+1 or 1:n) through service classes (Gold, Silver, Bronze). However, the pre-planned backup routes can be inadequate to guarantee the SLA (Service Level Agreement). In case of failure, there is no way to guarantee the chosen protection route will meet the client requirements. In this paper, a method for choosing the best backup route is proposed through Genetic Algorithms and PBM, called AGEP.*

Resumo. *Uma das formas de oferecer QoS (Quality of Service) em redes ópticas, em um ambiente gerenciado por políticas, é utilizando políticas de proteção de rotas. Para cada contrato firmado, o administrador de rede define o tipo de proteção (1:1, 1+1 ou 1:n) através de classes de serviço (Gold, Silver e Bronze). Entretanto, os caminhos de backup pré-planejados podem ser inadequados para satisfazer o SLA (Service Level Agreement) contratado. Em caso de falha, não há como garantir que o caminho de proteção escolhido atenderá satisfatoriamente as exigências do cliente ou mesmo da aplicação utilizada. Neste artigo, é proposto um método de escolha de melhor caminho de backup através de Algoritmos Genéticos e PBM, denominado AGEP.*

1. Introdução

Com o advento de redes ópticas de alta capacidade de transmissão, como DWDM (*Dense Wavelength Division Multiplexing*), diversos autores têm afirmado não ser necessário utilizar mecanismos de gerência inteligente dos recursos da rede e que somente a capacidade de transmissão da fibra óptica, junto com equipamentos fotônicos, seria suficiente para garantir Qualidade de Serviço (QoS). De forma diferente, outros defendem que mesmo utilizando esta tecnologia, sempre surgirão aplicações capazes de consumir os recursos oferecidos, sendo necessário, portanto, o uso de mecanismos de QoS. O fato é que a popularidade de certas aplicações (e.g., Vídeo-conferência, VoIP,

IPTV) e o surgimento de novos serviços geram grande demanda por recursos, causando sobrecarga e piorando o desempenho da rede.

Segundo [ISO/IEC 1995], [Ivanovici 2006] e [Beuran 2003], a QoS é determinada pelo grau de satisfação do usuário em relação a um serviço específico, sendo que cada serviço possui diferentes exigências (e.g., largura de banda, tempo de resposta, variação do atraso, descarte). De maneira a assegurar uma QoS em nível de aplicação, um usuário ou empresa estabelecem um acordo em nível de serviço SLA, através de um contrato. Neste contexto, a rede óptica é uma importante aliada na oferta de recursos, porém sua grande capacidade de transmissão não necessariamente assegura o pleno atendimento destas exigências.

Como exemplo real da necessidade de mecanismos que cumpram o SLA podemos citar o uso de aplicações de Telemedicina, especificamente a cirurgia à distância. Nesta situação, um médico cirurgião poderá estar operando um paciente utilizando um robô ligado à Internet equipado com um bisturi elétrico. Qualquer falha na transmissão dos comandos de movimentação do robô pode ser fatal, sendo fundamental utilizar técnicas que permitam atender os requisitos dessas aplicações.

Esses requisitos são inseridos via SLA, através de políticas, e são garantidos através dos mecanismos de tradução dessas políticas em especificações em níveis de serviços (SLS) e no final, na implementação dos mecanismos presentes num sistema computacional e que compõem uma rede de computadores, que deve estar sempre disponível.

Uma das formas de garantir essa disponibilidade é utilizando políticas de proteção de rotas. Para cada contrato firmado, o administrador de rede define o tipo de proteção (1:1, 1+1 ou 1:n) em função de classes de serviço (*Gold*, *Silver* e *Bronze*) [Papadimitriou 2001] a serem ofertadas às aplicações usuárias. Entretanto, os caminhos de backup pré-planejados podem ser inadequados para satisfazer o SLA contratado. Em caso de falha, não há como garantir que o caminho de proteção escolhido atenderá satisfatoriamente às exigências do cliente ou mesmo da aplicação utilizada, pois esta escolha não leva em conta a qualidade (taxa de erro de bit e tipo de proteção dos enlaces) do caminho de proteção.

Neste artigo, é proposto um método de escolha de melhor caminho de backup através de Algoritmos Genéticos (AG) e PBM, denominado AGEP. O uso de meta-heurísticas para resolver este tipo de problema vem amplamente sendo utilizado. Uma das vantagens é o baixo tempo gasto na procura de uma solução próxima da ótima [Wang 2005].

O restante deste artigo segue organizado da seguinte maneira: na Seção 2, são apresentados os trabalhos relacionados. A Seção 3 exhibe as considerações iniciais, discorrendo sobre cada tópico coberto. O Esquema de Proteção AGEPE, que é objeto deste artigo, é apresentado na Seção 4. Em seguida, a Seção 5 mostra as simulações e os resultados. Por fim, a Seção 6 apresenta as principais conclusões e contribuições deste trabalho.

2. Trabalhos Relacionados

A ocorrência de falhas em redes ópticas necessita de soluções rápidas, pouco onerosas e eficazes. Nesse sentido, atualmente diversos trabalhos têm sido realizados utilizando meta-heurísticas.

O uso de algoritmos genéticos é explorado em [Wang 2005], onde se busca maximizar a taxa de restauração de caminhos de *backups* pré-planejados. No método AGEPE, apesar de utilizar AG de forma semelhante, utiliza-se conversão total de comprimentos de ondas e outras métricas (BER e Tipo de Proteção) para escolha do caminho de proteção mais adequado.

Em [Celestino 2005] é descrito um novo esquema de engenharia de tráfego baseado em um método reativo de balanceamento de carga para controle de congestionamento em redes MPLS (*Multiprotocol Label Switching*), utilizando técnicas de lógica difusa e aprendizado baseado em algoritmos genéticos. No AGEPE também se utiliza AG, porém, o mecanismo reativo não está relacionado ao congestionamento do tráfego e sim ao valor de taxa de erro de bit de um caminho de proteção.

No trabalho aqui proposto, utiliza-se AG para a escolha de uma rota de proteção quase ótima usando como parâmetros de escolha de rota o BER (*Bit Error Rate*) e os tipos de proteção de cada enlace. Além disso, PBM (*Policy Based Management*) é utilizado para gerenciar a rede e diferenciar o tratamento dado, no momento de uma quebra de requisito, para cada classe de serviço.

3. Considerações Iniciais

3.1. Redes Ópticas

As redes ópticas são utilizadas para tentar atender a demanda crescente de recursos na Internet e a necessidade de garantir QoS às aplicações. A transmissão de dados em um ambiente óptico envolve diversos dispositivos, tais como: terminais, amplificadores e comutadores ópticos.

Os terminais ópticos são compostos por adaptadores de sinais óticos e multiplexadores (OADM) com a função de multiplexar e demultiplexar comprimentos de onda. Amplificadores ópticos recuperam os sinais atenuados durante a propagação. Comutadores ópticos (OXC *Optical Crossconnect*) aprovencionam os caminhos da rede de forma automatizada, comutar e/ou converter comprimentos de onda das inúmeras portas da entrada à saída e possibilitar novas rotas em situações de falha.

Os caminhos de proteção em redes ópticas podem ser: (1) Proteção 1+1, aloca-se uma rota de proteção para o caminho principal e a mesma informação trafega por cada um. No nó de egresso, o sinal com melhor qualidade é selecionado e então encaminhado; (2) Proteção 1:1, o caminho de proteção, em condições de não-falha do caminho principal, pode ser utilizado para transportar tráfego extra. Sendo que, em caso de falha, ele é utilizado somente pelo tráfego do caminho principal; (3) Proteção 1:n, semelhante a Proteção 1:1, em condições de não-falha, o caminho de proteção pode ser utilizado para transportar tráfego extra. A diferença é que neste método, n caminhos compartilham a mesma proteção.

Neste trabalho, a proteção requerida para fornecer a QoS necessária para as aplicações é simulada através do GLASS (GMPLS *Lightwave Agile Switching Simulator*) [GLASS 2007].

3.2. Gerenciamento Baseado em Políticas

Gerenciar redes tem se tornado uma tarefa muito complexa devido ao grande número de equipamentos envolvidos, sua heterogeneidade (e.g. diferentes OXCs e OADMs), diversificação de tráfegos e suas exigências e a necessidade de prover QoS e segurança. Ela deixou de ser uma tarefa de configuração de equipamentos, para ser vista como uma operação de negócios, através de acordos de níveis de serviço, conhecidos como SLAs (*Service Level Agreements*).

Tornam-se, assim, necessárias a automatização e a configuração dos elementos envolvidos, bem como o controle da própria rede de maneira a prover a QoS acordada. Assim, foi proposto um novo paradigma pelo IETF/DMTF (*Internet Engineering Task Force e Distributed Management Task Force*), visando à cobertura desses problemas, denominado Gerenciamento de Redes Baseado em Políticas (*Policy-Based Network Management – PBNM*) [Verma 2000].

O LARCES desenvolve nos últimos anos, uma plataforma genérica para gerenciamento de redes baseado em políticas (LARCES_PBM) [Celestino 2006]. Esta plataforma é baseada na proposta do IETF, tem sido testada exaustivamente e foi usada neste trabalho para a validação do esquema de proteção.

3.3. Algoritmos Genéticos

Os Algoritmos Genéticos (AG), propostos por John Holland nos anos 60, são algoritmos probabilísticos que oferecem mecanismo de busca adaptativo e paralelo. Embora não encontrem o ponto ótimo, eles se aproximam da solução ótima e de forma mais rápida do que utilizando técnicas convencionais de pesquisa exaustiva ponto-a-ponto [Wang 2005].

Baseados na teoria da evolução de Darwin, de acordo com a qual somente os indivíduos mais adaptados irão sobreviver, os AG iniciam com uma população de indivíduos, que são os cromossomos (cadeia de bits que representa uma solução possível para o problema), gerados aleatoriamente, representando as configurações iniciais de um problema.

Em seguida é feita a avaliação de cada um (aplicação da função objetivo) e são selecionados os “melhores” (escolha daqueles cuja função de custo atinge o ponto ótimo). A probabilidade de um cromossomo ser selecionado é proporcional à sua aptidão. Para visualizar este método considere um círculo dividido em n regiões (tamanho da população), onde a área de cada região é proporcional à aptidão do indivíduo. Coloca-se sobre este círculo uma "roleta" com n cursores, igualmente espaçados. Após um giro da roleta a posição dos cursores indica os indivíduos selecionados. Este método é denominado amostragem universal estocástica [Medeiros 2006].

Os indivíduos sofrem cruzamento (*crossover*), o qual ocorre da seguinte forma: a lista de indivíduos selecionados é embaralhada aleatoriamente criando-se, desta forma,

uma segunda lista, chamada lista de parceiros. Cada indivíduo selecionado é então cruzado com o indivíduo que ocupa a mesma posição na lista de parceiros. Um novo cromossomo é gerado permutando-se a porção inicial de um cromossomo com a porção final do outro [Miranda 2007].

Os indivíduos também sofrem mutação, que é utilizada para garantir uma maior varredura do espaço de estados e evitar que o algoritmo genético convirja muito cedo para mínimos locais. A mutação altera o valor de um gene de um indivíduo sorteado aleatoriamente com uma determinada probabilidade, denominada probabilidade de mutação, ou seja, vários indivíduos da nova população podem ter um de seus genes alterado aleatoriamente, correspondente às perturbações, a fim de criar uma nova população [Viana 1998].

O processo é repetido até que uma condição de parada seja satisfeita. O indivíduo com maior aptidão é a solução para o problema.

4. Descrição do Esquema de Gerenciamento de Falhas

O problema da escolha do melhor caminho de *backup* em uma rede óptica pode ser de difícil solução e pode consumir bastantes recursos computacionais na procura de uma solução exata. A idéia fundamental consiste em buscar boas soluções para o problema, embora não se assegure encontrar uma solução ótima [Wang 2005].

Dizer que um serviço possui uma rota de *backup* pré-definida não é garantia de que, em caso de falha, esta rota atenda as especificações definidas no SLA. Também não se pode afirmar que seus valores de BER são adequados para determinada classe de serviço. Um caminho protegido (1+1, 1:1 ou 1:n) garante que em caso de falha o tráfego será encaminhado, porém, a taxa de erros de bit (BER) do caminho de proteção não é considerada, penalizando a QoS oferecida a aplicação. Então, torna-se necessário um mecanismo de procura de caminho de *backup* quase ótimo para tentar atender estas exigências.

A fim de solucionar este problema, é proposto neste artigo um esquema de gerenciamento de falhas de rotas de *backup* em rede ópticas utilizando GA e o LARCES_PBM [Celestino 2006] (Figura 1).

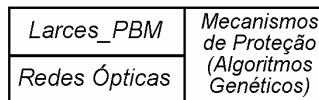


Figura 1. Arquitetura proposta

O uso do LARCES_PBM é de fundamental importância no monitoramento dos enlaces. O disparo do cálculo de escolha do melhor caminho de proteção só é feito caso a comparação dos parâmetros atuais do enlace com os valores definidos no SLA não seja satisfatória. Tal comparação e disparo são feitos pelo LARCES_PBM, através do PEP. Os aparelhos ópticos têm que estar configurados para reportar a não satisfação do SLA e para notificar a alteração da rota de proteção, caso seja necessário. O LARCES_PBM faz a comunicação com o simulador GLASS, que implementa o módulo de redes ópticas da figura 1, para trocar informações a respeito do estado da rede e

informações de aplicação de política e está sempre pronto para engatilhar o AG para escolha da melhor rota de proteção.

Neste trabalho, considerou-se as políticas de proteção para as classes de serviço, especificadas através do LARCES_PBM, com o intuito de atender as exigências de aplicações VoIP (*Voice over IP*), IPTV (*IP Television*), transação eletrônica e tráfego comum. Seguindo o proposto em [Pinart 2007] foram definidos os valores necessários para a associação entre a classe de serviço e o nível de exigência requerido, de maneira a atender SLAs em redes ópticas, conforme a Tabela 1. Segundo [Krishna 2005], o tempo máximo de restauração de uma falha pode variar segundo três classes de serviço: *platinum* (50ms), *gold* (50-100ms) e *silver* (1-10s). Neste artigo, o tempo gasto para escolha do melhor caminho de proteção para as quatro classes de serviço é de no máximo 100ms. Este valor foi escolhido através de testes onde se constatou que este valor era suficiente para o método convergir a uma solução próxima da ótima.

Classe de Serviço	Gold	Silver	Bronze	Best-Effort
BER	$\leq 10^{-8}$	$\leq 10^{-7}$	$\leq 10^{-6}$	$> 10^{-6}$
Serviço	VoIP	IPTV	Transação Eletrônica	Tráfego Comum

Tabela 1. Valores de BER segundo políticas de proteção.

A Figura 2 representa um diagrama de seqüência do esquema de proteção. A figura indica as relações entre o LARCES_PBM, o simulador GLASS e o cálculo da rota de proteção.

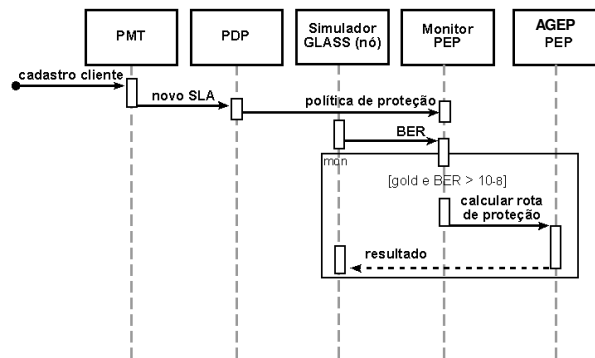


Figura 2. Diagrama de seqüência do esquema de proteção

Através do PMT (*Policy Management Tool*), cadastra-se o cliente e sua respectiva classe de serviço no repositório de políticas. Depois de estabelecida uma conexão entre o PEP (*Policy Enforcement Point*) e o PDP (*Policy Decision Point*), o último envia uma decisão de política de proteção ao primeiro.

A Figura 3 apresenta a aplicação da política de proteção. A mensagem recebida pelo PEP contém informações sobre o cliente e sua classe de serviço (1). Utilizando o protocolo OSPF-TE (*Open Shortest Path First – Traffic Engineering*) identifica-se o enlace que o cliente utiliza como rota de proteção (2). Desta forma, o monitor verifica constantemente o valor da taxa de erros de bit do enlace no dispositivo (3), caso este valor não atenda a exigência da classe de serviço (e.g. $BER > 10^{-8}$) do cliente (4), o monitor requisita ao método AGEP o cálculo de um caminho de proteção adequado (5).

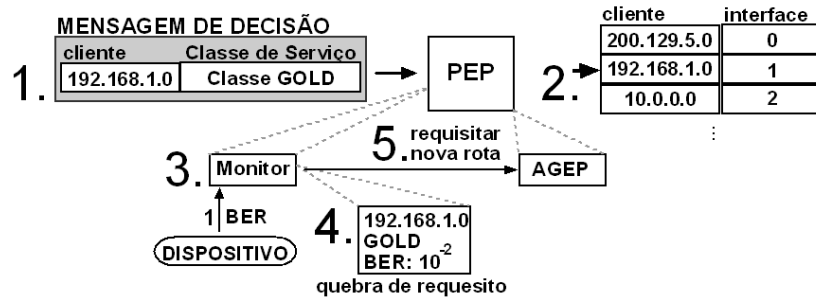


Figura 3. Exemplo de Política de Proteção

Para realizar a comunicação entre o LARCES_PBM e o GLASS, adicionou-se uma classe à biblioteca de recursos do simulador (merlin2.jar) que funciona como um PEP. Esta classe utiliza o protocolo de comunicação COPS-PR (*Common Open Policy Service for Policy Provisioning*) para troca de mensagens com o ambiente externo. Também existe uma função que monitora o valor de BER do dispositivo (gatilho) e chama o método AGEPE caso aconteça uma quebra de requisito.

Os cromossomos no AGEPE representam possíveis rotas completas e não têm tamanho fixo. Os genes representam os enlaces. Cada gene tem associado a ele o tipo de proteção e o valor de BER. A primeira geração da população é criada aleatoriamente e é constituída de n indivíduos (rotas), contendo soluções válidas e inválidas.

Existem vários parâmetros (seção 4.2) que influenciam a eficácia do algoritmo genético. Neste artigo, a função de *fitness* exerce papel fundamental na escolha das melhores soluções. Contudo, a ligação direta entre nível de adaptação e probabilidade de reprodução pode, às vezes, causar alguns problemas. Por exemplo, ao trabalhar em um problema cuja solução leve em conta vários critérios com parâmetros opostos, a escolha do critério de aptidão de uma solução pode não ser clara. Dessa forma, na construção da função de *fitness*, não é importante somente a escolha dos elementos, ou seja, dos parâmetros associados a ela, mas também dos pesos a serem atribuídos a cada um deles.

4.1. O Cálculo da Função de *Fitness*

O cálculo de aptidão do cromossomo incorpora na função de *fitness* a contribuição de cada um de seus genes. Para cada gene, duas métricas são consideradas: (1) o valor da taxa de erro de bit (BER) e (2) o tipo de proteção, que pode ser *ONLY*, *SHARED* e *NEVER*.

Considerando a primeira métrica, quanto maior for o valor de BER, menor será a contribuição do gene na aptidão do cromossomo. Para obter a participação da segunda métrica no cálculo da aptidão dos cromossomos, é necessário definir pesos que reflitam como cada tipo de proteção irá influenciar na aptidão.

O enlace com proteção *ONLY* é exclusivo, seus recursos não podem ser compartilhados com outros clientes. Neste caso, cromossomos que possuem esta característica em algum de seus genes, podem não ser boas escolhas. Definiu-se então, que esta característica influenciará negativamente na aptidão do cromossomo. No enlace com proteção *SHARED*, os recursos são compartilhados com outros clientes, conseqüentemente, genes com esta característica influenciarão positivamente no cálculo

da *fitness*. Finalmente, no caso de enlaces sem proteção, ou seja, *NEVER*, os recursos podem ser melhor utilizados para proteção de um caminho principal, assim terão contribuição mais positiva no cálculo da *fitness*.

Dentro deste contexto, uma rota terá uma qualidade muito alta, ou seja, será ótima, se ela for constituída de enlaces cujos valores de BER forem baixos e valores de proteção forem *NEVER*. No outro extremo, uma rota terá uma qualidade muito baixa se os valores de BER forem altos e os de proteção forem *ONLY*. No caso de rotas inválidas o valor da *fitness* deve ser zero, ou seja, o cromossomo não tem aptidão para participar do processo de seleção de pares, por representar uma rota infactível.

4.1.1 Abordagem de Pesos

O valor de aptidão de cada gene em um cromossomo é calculado em uma única etapa. Leva-se em consideração os valores de BER e proteção do enlace descrito no gene e os valores de importância, pesos, desses atributos na obtenção da qualidade da rota. Inicialmente considera-se um valor inicial $k > 0$ para a *fitness* e a cada iteração do algoritmo genético, incrementa-se os valores de cada enlace em função dos valores dos atributos naquela iteração. Por fim, o resultado daquela iteração é reduzido em 80% com o intuito de penalizar as maiores rotas. O valor da porcentagem de penalização foi definido experimentalmente, onde a probabilidade de seleção de uma boa rota foi usada como critério de avaliação. A penalização previne que uma rota inferior com uma grande quantidade de enlaces seja escolhida, pois assim, sua *fitness* pode ser superior ao valor da *fitness* de uma boa rota que possua poucos enlaces. A Expressão (1) especifica a função de *fitness* de um cromossomo:

$$fitness = k + \sum_{i=1}^n ((\alpha \cdot f(ber_i) + (1 - \alpha) \cdot g(prot_i)) * 0.2) \quad (1)$$

onde $\alpha \in [0,1]$ e α é determinado para avaliar os diferentes resultados das situações em que é dada maior prioridade ao BER ($\alpha > 0.5$), ao Tipo de Proteção ($\alpha < 0.5$), ou nenhuma prioridade aos dois parâmetros ($\alpha = 0.5$); k é uma constante usada para evitar que o valor da *fitness* não seja negativo; n representa o número de genes no cromossomo. A Função 1 define $f(ber_i)$ e a Função 2 define $g(prot_i)$.

$$f(x) \begin{cases} 1, x < 0 \\ 0, x > 1 \\ 1-x, 0 \leq x \leq 1 \end{cases}$$

Função 1. Função de BER

$$g(x) \begin{cases} -0.98, x = ONLY \\ 0.2, x = SHARED \\ 0.98, x = NEVER \end{cases}$$

Função 2. Função de Proteção

Portanto, dependendo do valor de α , a função *fitness* fornece maior prioridade, maior peso, para os valores de BER ou para os tipos de proteção.

4.2. Parâmetros de Configuração do Algoritmo Genético

Um dos aspectos mais importantes na estratégia dos Algoritmos Genéticos é a correta configuração dos seus parâmetros. Como tais parâmetros dependem muito do tipo do problema, não existe nenhuma metodologia genérica [Fernandez 2003]. Devem-se levar em conta também os recursos computacionais disponíveis e os tempos de execução relacionados ao problema.

4.2.1. Tamanho da População

Com uma população pequena, a probabilidade de escolha de uma solução próxima da ideal é menor, pois o número de indivíduos (possíveis soluções) é reduzido. Porém, tem-se a vantagem de utilizar menos recursos computacionais. Uma população grande fornece uma cobertura maior do espaço de busca aumentando a chance de escolha de uma solução ideal ou muito próxima da ideal. Entretanto, tal população requer longos tempos e maiores recursos computacionais mesmo em problemas simples.

Normalmente, usa-se um tamanho de população proporcional à quantidade de genes de um cromossomo [Fernandez 2003].

4.2.2. Máximo de Evoluções

Não existe um valor ideal para o número máximo de evoluções. Cada problema possui suas próprias restrições, e assim, um valor adequado deve ser escolhido tendo em vista estas restrições. No método AGEP, a principal restrição do problema é o tempo necessário para localizar uma boa solução. No problema estudado utilizou-se no máximo 30 evoluções.

Após 30 evoluções, a média da *fitness* dos 20 melhores indivíduos permanece a mesma. Não há razão para produzir novas gerações, tendo em vista que o melhor indivíduo continua se repetindo através das gerações. Além disso, este valor previne que o tempo de resolução ultrapasse os 100 ms de restrição.

4.2.3. Taxa de *Crossover*

Determina a probabilidade de ocorrer um cruzamento. Em termos de busca, a taxa de *crossover* permite ao algoritmo genético explorar áreas desconhecidas. Um valor baixo pode restringir o campo de busca dificultando a localização de uma solução próxima da ideal. Com uma taxa muito alta, novas soluções serão introduzidas na população mais rapidamente. Porém, soluções com bons valores de *fitness* poderão ser substituídas mais rapidamente, desperdiçando boas oportunidades de achar a solução “ótima”.

As figuras 4, 5 e 6 apresentam um exemplo hipotético de *crossover* utilizado no método AGEP. A Figura 4 indica a Rota 1, que passa pelos enlaces 0-5-7 . A Figura 5 mostra a Rota 2, que é constituída pelos enlaces 1-3-7 . Na figura 6 é apresentada a rota resultante do *crossover* entre as rotas 1 e 2. Nem sempre o *crossover* irá gerar uma rota válida.

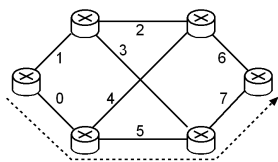


Figura 4. Rota 1

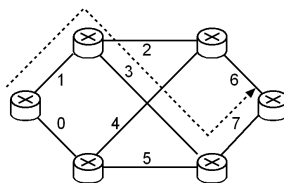


Figura 5. Rota 2

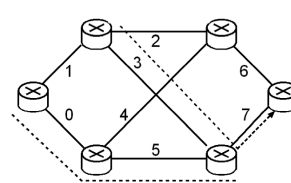


Figura 6. *Crossover* entre Rota 1 e 2

4.2.4. Taxa de Mutação

Uma baixa taxa de mutação diminui a possibilidade de incluir novos cromossomos na população, resultando em restringir o espaço de busca. Uma taxa muito alta torna, praticamente, a busca do algoritmo genético uma busca aleatória. Muitos trabalhos sugerem usar um valor entre 0,1% e 5% [Fernandez 2003]. Na figura 7, é apresentado um exemplo hipotético de mutação de rota utilizado. A rota original era 1-2-6. Após a mutação foi obtida uma nova rota constituída dos enlaces 1-3-7.



Figura 7. Mutação

4.2.5. Método de Seleção Natural

O método de Seleção Natural utilizado foi o *BestChromossomeSelector* que seleciona os n melhores cromossomos para gerar a próxima população. Desta forma, a busca convergiu mais rapidamente a soluções sub-ótimas do que utilizado o método de seleção por roleta.

5. Simulação, Resultados e Análise

Nesta seção é apresentada a simulação do esquema proposto e os resultados obtidos. Como parâmetros de análises, foram avaliados: a qualidade do caminho de proteção; a capacidade de atender os requisitos da aplicação; o tamanho da rota; e o tempo despendido na busca da solução.

Nesse trabalho, a proteção requerida para fornecer a QoS necessária para as aplicações é executada através de um simulador. Dentre diversos simuladores atualmente existentes (e.g., MARBEN, NS, OpNet) o que apresentou melhor adequação à nossa proposta foi o GLASS [GLASS 2007]. Alguns dos outros simuladores são pagos e os demais não têm todos os protocolos necessários implementados. Além disso, o código do AGEF foi desenvolvido em Java e para facilitar, decidiu-se usar um simulador na mesma linguagem. No GLASS é possível adicionar ou modificar protocolos, simular eventos de falhas e visualizar o resultado do roteamento. A única restrição é não poder variar o valor de BER durante a simulação, sendo necessário definir uma quebra de requisito (alto valor de BER) antes do início da simulação.

Foi utilizado o *framework* de Algoritmos Genéticos JGAP [Meffert 2007] (*Java Genetic Algorithms Package*) que fornece todos os mecanismos básicos dos princípios evolucionários.

5.1. Topologia

Os testes foram realizados no cenário da rede dos Estados Unidos, que é composto por 19 nós e 31 enlaces. Cada enlace tem o nível de proteção especificado (*Only, Shared, Never*) e um respectivo valor de BER. (Figura 8).

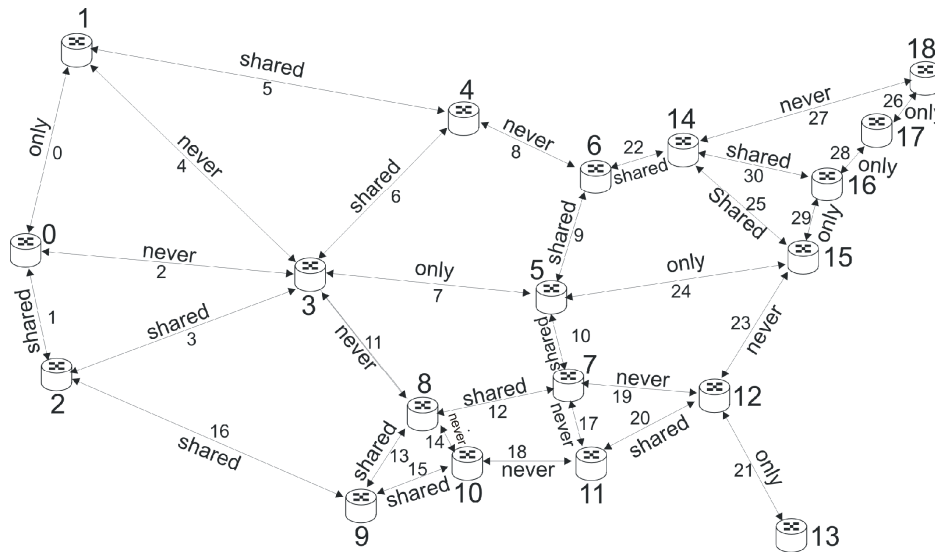


Figura 8. Topologia utilizada nos testes

Neste cenário, os valores de BER (10^{-8}) dos enlaces 1 a 30 são adequados para fornecer qualidade de serviço para as aplicações *GOLD*, *SILVER* e *BRONZE*. Já o enlace 0 possui um alto valor de BER (10^{-2}). Nos nós (1), (2), (3), (6), (7), (9), (10), (12), (15), (16) e (18) encontram-se os PEPs, possibilitando monitorar todos os enlaces no ambiente simulado.

O Caminho 0-5-8-22-27 é utilizado como caminho de *backup* por um cliente que contratou um serviço *GOLD* que utiliza aplicações VoIP. Após configuradas as políticas de proteção, é detectado, através do monitor (nó 1), que o valor de BER do enlace 0 não satisfaz o SLA do cliente.

Após detectar a quebra de requisito é solicitado ao método AGEP encontrar um caminho de proteção adequado.

5.2. Resultados e Análises

Para obtenção dos resultados e posterior análise, os parâmetros do algoritmo genético assumiram os seguintes valores: máximo de evoluções = 30, taxa de mutação = 0,1%, taxa de *crossover* = 50%, tamanho da população = 256 cromossomos [Fernandez 2003]. Esses valores foram definidos através de testes. A análise foi feita levando em conta o tempo (<100ms) para localizar boas soluções. O critério de parada do algoritmo leva em consideração o número máximo de evoluções ou a média da *fitness* dos indivíduos de uma geração, ou seja, as evoluções terminam sempre que a média da *fitness* dos vinte melhores cromossomos é igual ou superior a 99,95% do valor da *fitness* do melhor indivíduo.

Na parada por média da *fitness*, foram realizadas em média oito evoluções para a obtenção de uma solução e o tempo necessário ficou dentro de uma faixa de 3 a 81 ms. Quando o critério de parada foi igual a trinta evoluções, o tempo necessário para encontrar uma solução ficou numa faixa entre 63 e 141 ms. Esse tempo pode não ser bom para o caso de redes ópticas, já que algumas vezes ele ultrapassa os 100 ms.

A Figura 10 destaca os resultados da Abordagem de Pesos. Os valores de α foram sendo alterados (0.01-0.99) e três rotas diferentes foram avaliadas. A rota 0-4-11-14-18-17-19-23-25-27 tem a pior *fitness*, a rota 2-3-16-13-14-18-17-19-23-25-27 tem um valor médio de *fitness* e a rota 2-11-14-18-17-19-23-25-27 tem o melhor valor de *fitness*. O Gráfico representa a porcentagem de escolha de rota em função de α . As Figuras 11 a 13 também foram obtidas a partir das variações dos valores de α (0.1, 0.5 e 0.9) e utilizaram os dois critérios de parada. Para cada geração de um determinado valor de alfa foram realizados 1000 testes, os gráficos mostram a média de *fitness* dos 1000 testes.

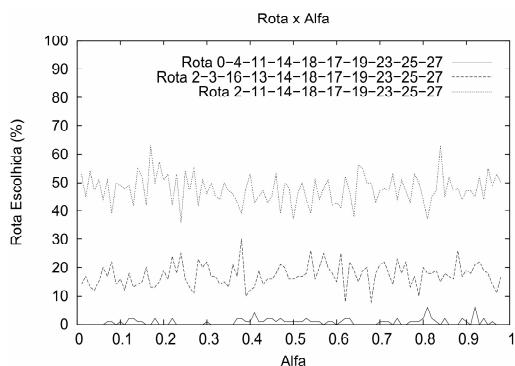


Figura 10. Porcentagem de escolha da rota em função de α (0.01-0.99)

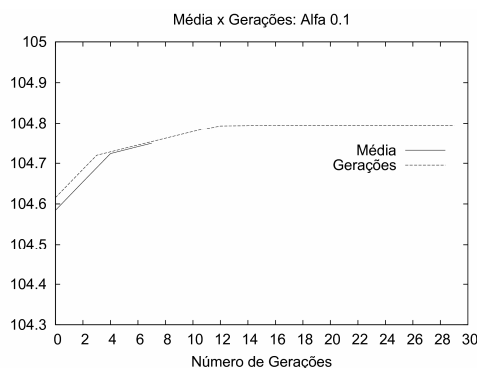


Figura 11. Média da *Fitness* x Número de Gerações (α 0.1)

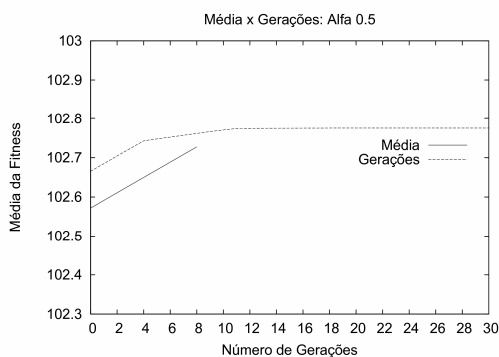


Figura 12. Média da *Fitness* x Número de Gerações (α 0.5)

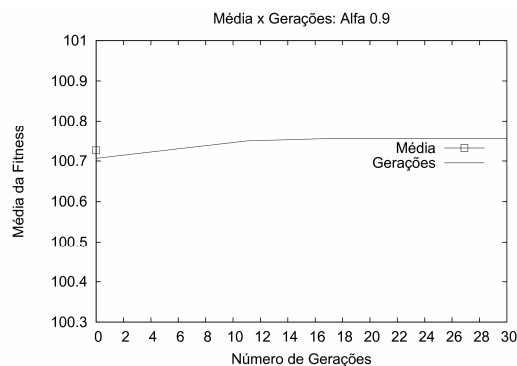


Figura 13. Média da *Fitness* x Número de Gerações (α 0.9)

O critério de parada mais adequado, em nosso problema, é o da média dos valores de *fitness* dos indivíduos em uma geração. Tal critério indica que em uma geração existem vários indivíduos aptos e assim, aumenta a probabilidade de uma rota ótima ou quase ótima ser escolhida. Seu resultado foi bastante adequado tendo como tempo máximo para resolução do problema 81 ms.

Com um baixo valor de α dá-se mais importância ao tipo de proteção e as rotas com altos valores de BER têm mais probabilidade de serem escolhidas. Com um valor um pouco mais alto de α , dá-se mais importância ao valor de BER e há mais probabilidade das rotas com enlaces *ONLY* ou *SHARED* serem escolhidas.

As Figuras 11 a 13 demonstram que, atribuindo-se um valor de importância maior para o tipo de proteção, a média de *fitness* de uma população varia bastante, devido aos diferentes tipos de proteção de enlace presentes na topologia. Quanto maior a importância dos valores de BER, mais homogênea vai se tornar a média de *fitness* de uma população devido aos valores de BER da topologia serem bastante semelhantes.

6. Conclusão

O artigo descreve um esquema de proteção de falhas em rotas de backup (AGEP) em redes ópticas através do uso de algoritmos genéticos. A proteção nestas redes é um problema complexo e tem merecido atenção, dado à falta de recursos que possam permitir a criação de caminhos de proteção. Portanto, neste trabalho, fez-se uso de um esquema baseado em algoritmo genético, de maneira a permitir que um novo caminho de proteção só seja requisitado quando a rota de *backup* estiver na iminência de não fornecer a QoS acordada através de SLAs.

O uso do AGEPE com critério de parada sendo um valor mínimo para a média de *fitness* dos indivíduos em uma geração proporciona achar, rapidamente, uma solução que satisfaça ou quase satisfaça o SLA e assim realizar um gerenciamento autônomo da rede.

Nas soluções propostas através de uma rota de *backup* pré-selecionada para determinado tráfego pode acontecer dessa rota possuir valores de BER muito altos e, assim, descumprir o SLA, o que é evitado em nossa proposta. O AGEPE faz com que uma rota de *backup* esteja sempre pronta para atender o SLA requisitado pelo cliente, caso haja uma falha no caminho principal.

A utilização das métricas BER e tipo de proteção permite a escolha do caminho de proteção mais adequado para determinado cliente. O AGEPE fornece soluções rápidas, pouco onerosas e eficazes.

Como atividade futura para esse trabalho, pretende-se usar outros parâmetros próprios de redes ópticas para qualificação de um enlace utilizando uma abordagem fuzzy de penalização da aptidão do cromossomo. Além disso, desenvolver uma classe de eventos para simular dentro do GLASS variações em tempo real do valor de BER e testar também outras meta-heurísticas para a solução desse problema.

7. Referências

- Wang, Y., et. al. (2005), “Improved Genetic Algorithm to Solve Preplanned Backup Path on WDM Networks”, Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA’05).
- Krishna, M., Sivalingam et. al. (2005), “Emerging Optical Network Technologies: Architectures, Protocols and Performance”, Springer, ISBN 038722582X, pág. 358.
- Viana, V. (1998), “Meta-heurísticas e programação paralela em otimização combinatória”, UFC Edições, Fortaleza.
- Fernandez, M. P., et. al. (2003), “Implementação de Políticas de Gerenciamento com Lógica Fuzzy e Algoritmo Genético Visando à Melhoria da Qualidade de Serviço (QoS)”, XXI SBRC, 2003, Natal. Anais do SBRC’2003. p. 185-200.

- Celestino, Jr., et al. (2005), "IntelliDyLBA: Um Esquema de Balanceamento de Carga para Redes MPLS com Aprendizado Desassistido baseado em Lógica Difusa e Algoritmos Genéticos", XXIII SBRC, Fortaleza.
- Miranda, M. N. (2007), "Algoritmos Genéticos: Fundamentos e Aplicações", <http://www.gta.ufrj.br/~marcio/genetic.html>.
- GLASS (GMPLS Lightwave Agile Switching Simulator), <http://www.antd.nist.gov/glass>, acessado em novembro de 2007.
- Meffert, K. (2007), "Java Genetic Algorithms Package", <http://jgap.sourceforge.net/>, acessado em novembro de 2007.
- Pinart, C. (2007) "Alternatives for in-service BER estimation in all-optical networks: towards minimum intrusion", JOURNAL OF COMPUTERS, VOL. 2, NO. 3, MAY.
- ISO/IEC DIS 13236 (1995), "Information Technology – Quality of Service – Framework", ISO/OSI/ODP.
- Ivanovici, M., Beuran, R. (2006), "User-Perceived Quality Assessment for Multimedia Applications", OPTIM'06, vol. IV, Brasov, Romania, May 18-19, pp. 55-60.
- Beuran, R., et. al. (2003), "Network Quality of Service Measurement System for Application Requirements Evaluation", SPECTS'03, Montreal, Canada, July 20-24, pp. 380-387.
- Medeiros, A. V. (2006), "Modelagem de sistemas dinâmicos não lineares utilizando sistemas Fuzzy, algoritmos genéticos e funções de base ortonormal", Dissertação de Mestrado, UNICAMP, SP Janeiro.
- Celestino, Jr., et. al. (2006), "LARCES_PBM: Uma Ferramenta de Gerenciamento Baseado em Políticas para prover QoS", Salão de Ferramentas, XXIV SBRC, Curitiba/PR, maio/junho.
- Verma, D. C. (2000). Policy Based Network – Architecture and Algorithms. New Riders.
- Papadimitriou, D. (2001) "Enhanced LSP Services in Optical Networks", Internet Draft <draft-papadimitriou-enhanced-lsps-04.txt> , July.