GAFUPA: Uma Proposta para Proteção em Redes Ópticas

Alisson Barbosa de Souza, Ana Luiza B. de P. Barros, Antônio Sérgio de S. Vieira, Gustavo Augusto L. de Campos[1], Jéssyca Alencar L. e Silva, Joaquim Celestino Júnior, Laure W. N. Mendouga
LARCES – Laboratório de Redes de Computadores e Segurança
[1]**LACONI** – Laboratório de Computação Natural e Inteligente
Universidade Estadual do Ceará (UECE)

***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. Entretanto, os caminhos de proteção podem ser inadequados para satisfazer o SLA (*Service Level Agreement*). Em caso de falha, não há como garantir que o caminho de proteção escolhido atenderá as exigências do cliente ou mesmo da aplicação utilizada. Neste artigo, é proposto um método de escolha de melhor caminho de proteção através de Algoritmos Genéticos, Lógica *Fuzzy* e PBM, denominado GAFUPA.**

***Palavras-Chave* - Redes Ópticas, Esquema de Proteção, Algoritmo Genético, Lógica *Fuzzy*, PBM.**

***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 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 choosen protection route will meet the client requirements. In this paper, a method for choosing the best backup route is proposed through Genetic Algorithms, *Fuzzy* Logic and PBM, called GAFUPA.**

***Keywords* - Optical Network, Protection Schema, Genetic Algorithm, Fuzzy, PBM.**

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

Segundo [1], [2] e [3], 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 (*Service Level Agreement*), 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.

Este trabalho foi parcialmente financiado com recursos do Projeto RNP-GIGA-FUNTEL

Nesta proposta, os requisitos de QoS são inseridos via SLA, através de políticas, e são traduzidos em SLS (*Service Level Specification*). Estas especificações são utilizadas na configuração de dispositivos que compõem uma rede para então garantir disponibilidade e tentar fornecer os requisitos da aplicação.

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 das classes de serviço (*Gold, Silver e Bronze*) a serem ofertadas às aplicações usuárias [4]. Entretanto, os caminhos de proteção 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 proteção através de Algoritmos Genéticos (AG), Lógica *Fuzzy* e PBM (*Policy Based Management*), denominado GAFUPA.

O restante deste artigo segue organizado da seguinte maneira: na Seção II, são apresentados os trabalhos relacionados. A Seção III exibe as considerações iniciais, discorrendo sobre cada tópico coberto. O Esquema de Proteção GAFUPA, que é objeto deste artigo, é apresentado na Seção IV. Em seguida, a Seção V exibe os parâmetros de configuração do AG. Os resultados são exibidos na Seção VI. Por fim, a Seção VII apresenta as principais conclusões e contribuições deste trabalho.

II. TRABALHOS RELACIONADOS

A recuperação de falhas em redes ópticas necessita de soluções rápidas, pouco onerosas e eficazes. Nesse sentido, atualmente, diversos trabalhos têm sido realizados utilizando metaheurísticas [5] devido ao baixo tempo gasto na procura de uma solução próxima da ótima [6].

O uso de algoritmos genéticos é explorado em [6], onde se busca maximizar a taxa de restauração de rotas de proteção pré-planejadas. No método GAFUPA, 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 [7] descreve-se 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. Neste artigo também se utiliza AG e Lógica *Fuzzy*, porém, o mecanismo reativo não está relacionado ao congestionamento do tráfego, e sim ao valor de taxa de erro de bit de uma rota de proteção.

No trabalho proposto, utiliza-se AG, com apoio da Lógica *Fuzzy*, para a escolha de uma rota de proteção quase ótima usando como parâmetros de escolha 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.

III. Considerações Iniciais

A. 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 (terminais, amplificadores e comutadores ópticos).

As rotas de proteção em redes ópticas podem ser: (1) Proteção 1+1, é alocado um caminho de proteção para o caminho principal e a mesma informação trafega através dos dois. No nó de egresso, o sinal com melhor qualidade é selecionado e então encaminhado; (2) Proteção 1:1, a rota de proteção, em condições de não-falha da rota principal, pode ser utilizada para transportar tráfego extra. Sendo que, em caso de falha, ela é utilizada somente pelo tráfego da rota principal; (3) Proteção 1:n, semelhante à 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.

B. Gerenciamento Baseado em Políticas

Gerenciar redes tem se tornado uma tarefa muito complexa devido ao grande número de equipamentos envolvidos, sua heterogeneidade, diversificação de tráfegos e suas exigências e a necessidade de prover QoS e segurança. O gerenciamento deixou de ser uma tarefa de configuração de equipamentos, para ser visto como uma operação de negócios, através de acordos de níveis de serviço conhecidos como SLAs.

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 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*) [8].

O LARCES (Laboratório de Redes de Computadores e Segurança) desenvolve nos últimos anos, uma plataforma genérica para gerenciamento de redes baseado em políticas (LARCES_PBM) [9]. Esta plataforma é baseada na proposta do IETF, tem sido testada exaustivamente e foi usada neste trabalho em conjunto com o simulador GLASS (*GMPLS Lightwave Agile Switching Simulator*) [10] para a validação do esquema de proteção em redes ópticas.

C. Algoritmos Genéticos

Os Algoritmos Genéticos (AG) 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 [6].

Baseados na teoria da evolução de Darwin, de acordo com a qual somente os indivíduos mais adaptados irão sobreviver, os AGs 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 indivíduo (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 [11].

Os indivíduos sofrem cruzamento (*crossover*). Assim, um novo cromossomo é gerado permutando-se a porção inicial de um cromossomo com a porção final de outro [12].

Os indivíduos também sofrem mutação. 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 [13].

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

D. Lógica Fuzzy

A teoria da probabilidade pode ser utilizada para representar formalmente informações em ambientes de tomada de decisão estocásticos. Diz-se que ela representa a incerteza associada à aleatoriedade dos eventos. Por sua vez, teoria dos conjuntos nebulosos procura representar a incerteza associada à informação vaga, imprecisa. Ela foi desenvolvida por Lofti Zadeh e publicada inicialmente em 1965 [14].

A Lógica *Fuzzy* é uma extensão da Lógica Clássica para lidar com os conceitos ambíguos e nebulosos, que dão origem às proposições nebulosas como, por exemplo, "o tempo de resposta atual é alto". Neste caso, dependendo do valor do tempo de resposta atual esta proposição nebulosa poderá assumir um dos valores verdade (grau de verdade) presentes no intervalo [0, 1], e não somente os valores 0 ou 1 que são possíveis na Lógica Clássica. Quem decide o valor verdade é a pessoa responsável por declarar o conceito vago, ou seja, no exemplo o valor de tempo de resposta alto.

Com a incorporação do conceito de "grau de verdade", a teoria dos Conjuntos *Fuzzy* estende a teoria dos Conjuntos Tradicionais. Os grupos são rotulados qualitativamente (usando termos lingüísticos, tais como: alto, morno, ativo, pequeno, perto) e os elementos destes conjuntos são caracterizados variando o grau de pertinência (valor que indica o grau em que um elemento pertence a um conjunto). Dessa forma, por ser menos restritiva, a Lógica *Fuzzy* pode ser considerada mais adequada para o tratamento de informações imprecisas [14].

IV. Descrição do Esquema de Gerenciamento de Falhas

O problema da escolha do melhor caminho de proteção em uma rede óptica pode ser de difícil resolução e, geralmente, requer grandes custos computacionais para encontrar a solução ótima. A idéia fundamental consiste em buscar boas soluções para o problema, embora não se assegure encontrar uma solução ótima [6].

Dizer que um serviço possui uma rota de proteção 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, podendo penalizar a QoS oferecida à aplicação. Então, torna-se necessário um mecanismo de procura de rota de proteção quase ótima para tentar atender estas exigências.

A fim de solucionar este problema, é proposto um esquema de gerenciamento de falhas em rede ópticas utilizando AG, Lógica *Fuzzy* e o LARCES_PBM [9].

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 [15], foram definidos os valores necessários para a associação entre a classe de serviço e o nível de BER requerido, de maneira a atender os SLAs em redes ópticas, conforme Tabela I. O tempo gasto para escolha da melhor rota de proteção para as quatro classes de serviço é de no máximo 100ms. Este valor foi escolhido através de testes onde se constatou que ele era suficiente para o método convergir a uma solução próxima da ótima.

TABELA I
VALORES DE BER SEGUNDO POLÍTICAS DE PROTEÇÃO.

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

A proteção requerida para fornecer a QoS necessária para as aplicações é simulada através do GLASS. A Figura 1 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.

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.

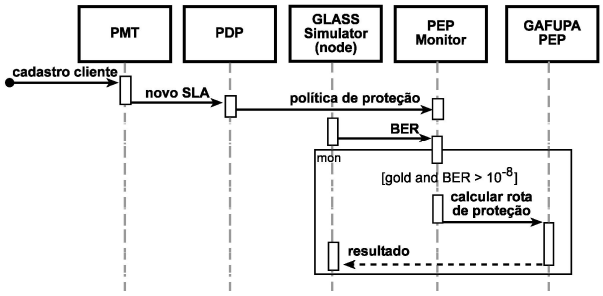

Fig. 1. Diagrama de seqüência do esquema de proteção.

A Figura 2 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 identifica-se o enlace pertencente ao caminho de proteção que o cliente utiliza (2). Desta forma, o monitor (PEP) verifica constantemente o valor da BER do enlace no dispositivo (3), caso ele não atenda a exigência da classe de serviço (e.g. BER>10^{-8}) do cliente (4), o monitor requisita ao método GAFUPA o cálculo de uma rota de proteção adequada (5).

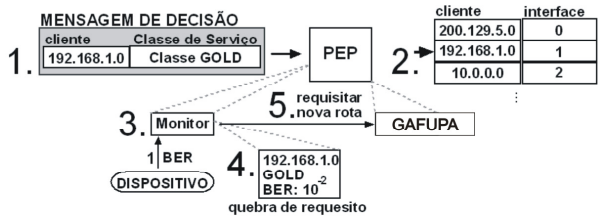

Fig. 2. Exemplo de Política de Proteção.

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 GAFUPA caso aconteça uma quebra de requisito.

Os cromossomos no GAFUPA representam possíveis rotas e os genes, 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 V) que influenciam a eficácia do algoritmo genético. Neste artigo, a função de *fitness* exerce um 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 leva em conta vários critérios com parâmetros opostos, alguns que aumentem a *fitness* e outros que diminuam, 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. Além destas noções, utilizou-se Lógica *Fuzzy* para calcular adequadamente o valor de contribuição de BER na *fitness* do indivíduo.

A. 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) 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, os 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.

O valor de aptidão de cada gene em um cromossomo é calculado em uma única etapa. Levam-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. 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. Por último, o valor da *fitness* do cromossomo é somado a uma constante k positiva suficientemente grande com o intuito de se obter sempre valores positivos. A Expressão (1) especifica a função de *fitness* de um cromossomo:

$$fitness = k + \sum_{i=1}^{n}((\alpha.f(ber_i) + (1-\alpha).g(prot_i)).0,2) \quad (1)$$

onde $\alpha \in [0,1]$ denota qual métrica possui o maior grau de importância, BER ou tipo de proteção; k assegura que o valor da fitness seja positivo; n representa o número de genes no cromossomo. A Função (2) define $g(prot_i)$. Para a função $f(ber_i)$, dois métodos foram considerados. O primeiro método utiliza a formulação apresentada na Função (3).

$$g(x) = \begin{cases} -0.98, & se\ x = ONLY; \\ 0.2, & se\ x = SHARED; \\ 0.98, & se\ x = NEVER. \end{cases} \quad (2)$$

$$f(x) = \begin{cases} 1, & se\ x < 0; \\ 0, & se\ x > 1; \\ 1-x, & se\ 0 \le x \le 1. \end{cases} \quad (3)$$

O segundo método utiliza Lógica *Fuzzy* e o sistema de inferência de Mamdani [14] para a função $f(ber_i)$, assim, o valor de contribuição de BER pode ser melhor avaliado mesmo existindo uma pequena variação dos valores de taxa de erro de bit nos enlaces.

Seis conjuntos triangulares lingüísticos foram definidos para representar o valor de BER de um enlace: (1) *Low*, (2) *Medium*, (3) *High*, (4) *Very High*, (5) *Very Very High* e (6) *Very Very Very High*. A área de abrangência dos conjuntos foi definida de acordo com [15]. A Figura 3 apresenta a definição destes conjuntos nebulosos para o caso em que os mesmos são utilizados para incrementar o valor de *fitness* $f(ber_i)$ em função do valor de ber_i. A Figura 4 apresenta o conjunto de regras empregado para estabelecer a relação entre BER e incremento.

O processo de adaptação de $f(ber_i)$ inicia com a leitura do valor atual da variável ber_i. Dependendo do método de inferência que se deseja utilizar, valores reais podem passar por um fuzzificador, que produzirá um valor nebuloso correspondente. Este trabalho empregou o método de inferência de Mamdani. Neste caso, para cada uma das regras na base da Figura 4, o valor de ber_i deve produzir um valor real intermediário, denominado limiar de disparo, e inferir um valor de incremento correspondente. O valor de incremento real em $f(ber_i)$, ou seja, o valor de contribuição da BER de um gene no cálculo da *fitness*, é resultado de duas operações: agregação envolvendo os valores inferidos a partir de cada uma das regras, obtendo-se um único valor nebuloso; e defuzzificação deste valor, obtendo-se um valor real de incremento.

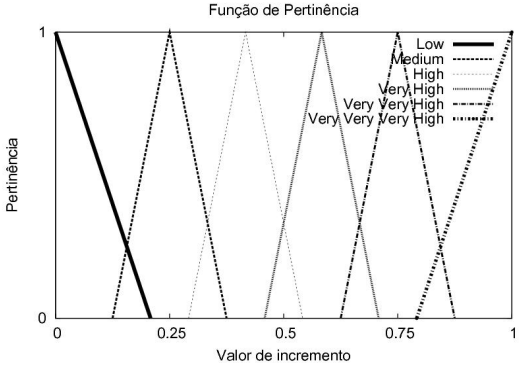

Fig. 3. Função de Pertinência.

```
if BER is VERY VERY VERY HIGH then
  INCREASE FITNESS is LOW
if BER is VERY VERY HIGH then
  INCREASE FITNESS is MEDIUM
if BER is VERY HIGH then
  INCREASE FITNESS is HIGH
if BER is HIGH then
  INCREASE FITNESS is VERY HIGH
if BER is MEDIUM then
  INCREASE FITNESS is VERY VERY HIGH
if BER is LOW then
  INCREASE FITNESS is VERY VERY VERY HIGH
```

Fig. 4. Base de Regras (2º Método).

O uso de Lógica *Fuzzy* foi justificado segundo análises comparativas utilizando as duas abordagens. A dimensão da topologia de testes foi aumentada para 51 nós e 99 enlaces e os valores de BER sofreram pouca variação entre si. O teste da figura 5 analisa a quantidade em que as melhores rotas são escolhidas para diferentes pares origem-destino, para isso basta alterar a origem, ou o destino, ou ambos. Em nosso caso, definiu-se um destino único enquanto que a origem da rota era trocada a cada teste. Assim, verificou-se a porcentagem de escolha da melhor rota de proteção. A Figura 5 exibe os resultados conseguidos.

Fica claro que a abordagem *Fuzzy* consegue em média resultados melhores mesmo aumentando o número de possibilidades de soluções.

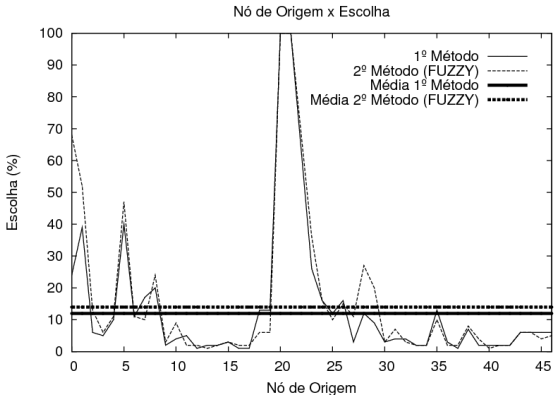

Fig. 5. Comparativo entre os dois métodos.

V. 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 [12]. Os recursos computacionais disponíveis e os tempos de execução relacionados ao problema também devem ser levados em conta.

Com uma população pequena, a probabilidade de selecionar uma solução próxima da ótima é pequena, já que o número de indivíduos (possíveis soluções) é reduzido. Por outro lado, requer menos esforços computacionais. Uma grande população fornece uma grande cobertura do espaço de busca, aumentando as chances de escolher uma solução ideal. Entretanto, tal população requer maiores esforços computacionais mesmo para problemas simples.

Normalmente, usa-se um tamanho de população proporcional à quantidade de genes de um cromossomo [12].

Não há um valor ideal pré-definido para o número máximo de evoluções. Cada problema tem suas próprias restrições. No

método GAFUPA, considerou-se como restrição do problema, o tempo para achar uma boa solução.

Concernente a busca feita pelo AG, a taxa de *crossover* permite a exploração de áreas desconhecidas. Um valor baixo para a taxa de *crossover* pode restringir a área de cobertura da busca e tornar mais difícil a busca por uma solução boa. Com um valor muito alto, novas soluções são introduzidas à população mais rapidamente. Entretanto, soluções com altos valores de *fitness* podem ser substituídas mais facilmente, desperdiçando boas oportunidades para encontrar a solução ótima.

No *crossover* é selecionado um par de rotas e a partir destas rotas é obtida uma nova rota. A nova rota é constituída de alguns enlaces da primeira rota e de outros enlaces da segunda rota.

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 5,0% [12].

Na mutação são escolhidos aleatoriamente alguns enlaces da topologia. Tais enlaces são usados para substituir outros enlaces de uma rota já definida. Depois da substituição é obtida uma nova rota.

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

VI. Simulação, Resultados e Análise

Nesta seção, é apresentada a simulação do esquema proposto, os resultados obtidos e uma comparação entre as duas abordagens de cálculo da função de BER: com e sem Lógica *Fuzzy*. 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 gasto na busca da solução.

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 [10]. Nele é possível adicionar ou modificar protocolos, simular eventos de falhas e visualizar o resultado do roteamento. Especificamente, no simulador são implementados o protocolo OSPF-TE e o CR-LDP (sinalização). Para estabelecer uma nova rota, passa-se, explicitamente, como parâmetro todo o percurso da rota ao protocolo CR-LDP. Após a devida sinalização, o OSPF-TE se encarrega de fazer o 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 [16] (Java *Genetic Algorithms Package*), que fornece todos os mecanismos básicos dos princípios evolucionários.

Para Lógica *Fuzzy*, utilizou-se o *framework Fuzzy*F [17], que permitiu reduzir o tempo de implementação e atender às necessidades do problema de avaliação das rotas.

Os testes foram realizados utilizando um cenário hipotético da rede RNP no Brasil que é composto por 27 nós e 36 enlaces. Cada enlace tem o nível de proteção especificado (*Only*, *Shared*, *Never*) e um respectivo valor de BER. (Figura 6).

Neste cenário, os valores de BER (~10^{-8}) dos enlaces 1 a 35 são adequados para fornecer qualidade de serviço para as classes GOLD, SILVER e BRONZE. Já o enlace 29, que faz parte do caminho de proteção, possui um alto valor de BER (10^{-2}). Nos nós (RS), (PR), (MS), (SP), (RJ), (BA), (ES), (AC), (RR), (MT), (DF), (AP), (AL), (PB), (CE) e (TO) encontram-se os PEPs, possibilitando monitorar todos os enlaces no ambiente simulado.

O caminho 1-0-29-30-31-23-22 é utilizado como proteção por um cliente que contratou um serviço GOLD para utilizar com aplicações VoIP.

Em um dado instante, é detectado, através do PEP, que o valor de BER do enlace 29 não satisfaz o SLA do cliente. Após detectar a quebra de requisito é solicitado ao método GAFUPA encontrar uma rota de proteção adequada.

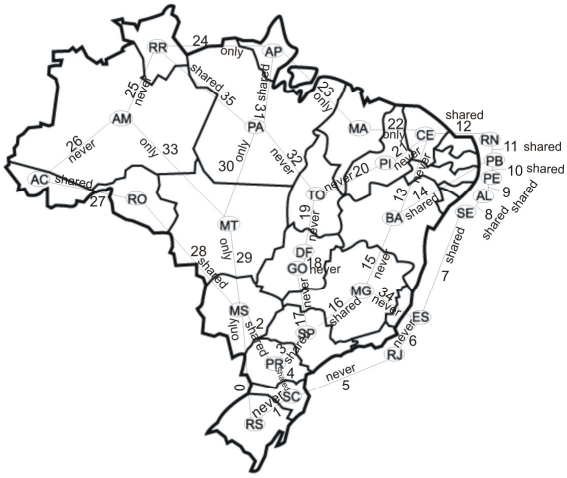

Fig. 6. Topologia utilizada nos testes (em um dado instante).

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 = 512 cromossomos. Estes valores foram obtidos experimentalmente. As análises foram feitas levando em conta os tempos para encontrar boas soluções (<100ms). Como a população tem um número de cromossomos adequado, ela contém boa porção das possíveis rotas de proteção de um tráfego. Desse modo, não houve necessidade de colocar uma taxa de mutação alta, tendo em vista que uma rota mutante, muito provavelmente, já estaria na população anterior.

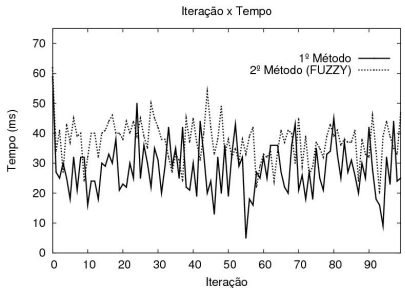

Fig. 7. Variação do tempo utilizando os dois métodos.

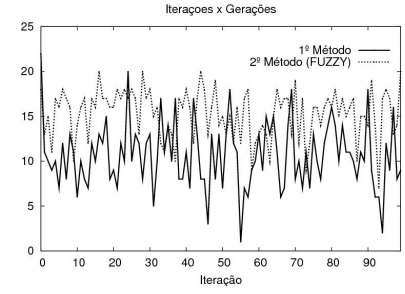

Fig. 8. Variação do número de evoluções utilizando os dois métodos.

O critério de parada do algoritmo leva em consideração 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 99,99% do valor da *fitness* do melhor indivíduo.

Desta forma, foram realizadas em média dez evoluções para a obtenção de uma solução utilizando a primeira abordagem e em média 15 evoluções na segunda. O tempo necessário ficou dentro de uma faixa de 10ms a 80ms para as duas abordagens. Este tempo está dentro do esperado (algumas vezes melhor do que o esperado) visto que o tempo para encontrar a solução não ultrapassa os 100 ms.

A Figura 7 mostra a variação de tempo gasto para achar a solução utilizando as duas abordagens. Os tempos mostraram-se bem semelhantes. Os resultados obtidos com Lógica *Fuzzy* foram um pouco piores devido à maior complexidade do algoritmo. Entretanto, os resultados nunca ultrapassam os 100ms. A Figura 8 compara o número de evoluções gasto para encontrar a solução utilizando os dois métodos. O segundo método, por ser mais sensível a variações de BER, necessitou de mais evoluções na busca de uma solução.

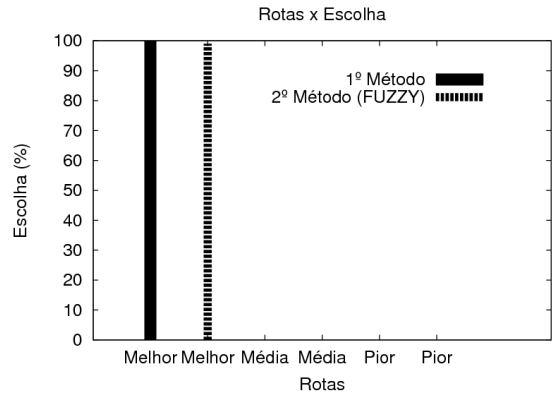

Fig. 9. Porcentagem de escolha de rotas com e sem lógica *fuzzy*.

A Figura 9 mostra a probabilidade de escolha entre três rotas (melhor solução, solução média e pior solução). A melhor rota possui o maior valor de *fitness*. Em todos os testes realizados a melhor rota foi escolhida pelos dois métodos.

Por último, constatou-se que atribuindo 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.

Apesar dos resultados das duas abordagens serem semelhantes, a segunda oferece a vantagem de ser menos restritiva quanto à classificação de uma métrica em conjuntos lingüísticos. Um valor pode pertencer parcialmente a um conjunto médio e pertencer parcialmente ao conjunto alto. Assim, torna-se mais adequado para tratar informações fornecidas. Outra vantagem em utilizar Lógica *Fuzzy*, é a possibilidade de tratar múltiplos critérios de entrada, mesmo com métricas inversamente proporcionais quanto ao aumento ou à diminuição do valor da *fitness*, extraindo uma saída concisa de alteração do seu valor.

VII. Conclusão

O artigo descreve um esquema de escolha de melhor rota de proteção (GAFUPA) em redes ópticas através do uso de algoritmos genéticos com apoio da lógica *fuzzy*. A proteção nestas redes é um problema complexo e tem merecido atenção, devido à falta de recursos que possam permitir a criação de caminhos de proteção.

O uso do GAFUPA proporciona achar, rapidamente, uma solução que satisfaça ou quase satisfaça o SLA e assim realizar um gerenciamento autônomo da rede.

Nos métodos propostos, demonstrou-se que as soluções foram encontradas em tempo hábil e eram satisfatórias. A escolha do segundo método (*Fuzzy*) mostrou ser mais adequada por possuir uma maior probabilidade de escolha da melhor rota de proteção.

Como atividades futuras para esse trabalho, pretende-se testar outras metaheurísticas para a solução do problema apresentado. Usar outros parâmetros próprios de redes ópticas para qualificação de um enlace e selecionar rotas com enlaces SRLG disjuntos aos da rota principal. Além disso, propor uma solução para o problema de roteamento e atribuição de lambda (RWA) [18] e desenvolver uma classe de eventos para simular dentro do GLASS variações em tempo real do valor de BER.

Agradecimentos

Os autores gostariam de agradecer o apoio financeiro obtido através da Rede Nacional de Pesquisa (RNP), dentro do Projeto Rede GIGA - FUNTEL.

Referências

[1] ISO-IEC-DIS 13236, "Information Techlonogy - Quality of Service – Framework", ISO-OSI-ODP, Julho de 1995.
[2] M. Ivanovici e R. Beuran, "User-Perceived Quality Assessment for Multimedia Applications", OPTIM06, vol. IV, Brasov, Romania, May 18-19, 2006, pp. 55-60.
[3] R. Beuran et al., "Network Quality of Service Measurement System for Application Requirements Evaluation", SPECTS03, Montreal, Canada, July 20-24, 2003, pp. 380-387.
[4] D. Papadimitriou, "Enhanced LSP Services in Optical Networks", draft-papadimitriou-enhanced-lsps-04.txt, 07-2001.
[5] M. Dorigo, "Conference Publications", http://www.metaheuristics.org/ index.php?main=2&sub=23, acessado 11-2007.
[6] Y. Wang et al, "Improved Genetic Algorithm to Solve Preplanned Backup Path on WDM Networks", AINA05, 2005.
[7] J. Celestino Jr. et al., "IntelliDyLBA: Um Esquema de Balanceamento de Carga para Redes MPLS com Aprendizado Desassistido baseado em Lógica Difusa e Algoritmos Genéticos", XXIII SBRC, 2005, Fortaleza.
[8] D. C. Verma, (2000). Policy Based Network - Architecture and Algorithms, New Riders.
[9] J. Celestino Júnior et al., "LARCES_PBM: Uma Ferramenta de Gerenciamento Baseado em Políticas para prover QoS", Salão de Ferramentas, XXIV SBRC, Curitiba/PR, maio/junho de 2006.
[10] GMPLS Lightwave Agile Switching Simulator (GLASS), http://www.antd.nist.gov/glass, acessado em novembro de 2007.
[11] A. V. de Medeiros, "Modelagem de sistemas dinâmicos não lineares utilizando sistemas Fuzzy, algoritmos genéticos e funções de base ortonormal", Dissertação de Mestrado, UNICAMP, SP 01-2006.
[12]M. N. de Miranda, "Algoritmos Genéticos: Fundamentos e Aplicações", http://www.gta.ufrj.br/ marcio/genetic.html, acessado 11-2007.
[13] V. Viana, "Metaheurísticas e programação paralela em otimização combinatória", UFC Edições, Fortaleza, 1998.
[14] S. Sandri e C. Correa, "Lógica Nebulosa", Anais da V Escola de Redes Neurais, São José dos Campos, 1999, pp 073-090.
[15] C. Pinart, "Alternatives for in-service BER estimation in all-optical networks: towards minimum intrusion", JOURNAL OF COMPUTERS, VOL. 2, NO. 3, MAY 2007.
[16] K. Meffert, "Java Genetic Algorithms Package", http://jgap.sourceforge.net/, acessaso 11-2007.
[17] J. R. Bittencourt e F. S. Osório, "Fuzzy Logic Framework", http://www.inf.unisinos.br/jrbitt/fuzzyf/, acessado 02-2008.
[18] V. T. Le, X. Jiang, S. Horiguchi, Y. Inoguchi, "A new fitness function for GA-based dynamic RWA algorithms in optical WDM networks", Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on, Volume 2, 2005.