A Management Scheme of SRLG-Disjoint Protection Path

Alisson Barbosa de Souza, Ana Luiza de B. de P. Barros, Antônio Sérgio de S. Vieira, Gustavo Augusto L. de Campos, Jéssyca Alencar L. e Silva, Joaquim Celestino Júnior, Joel Uchôa, Laure W. N. Mendouga
Computer Networks and Security Laboratory (LARCES)
Natural and Intelligent Computation Laboratory (LACONI)
State University of Ceará (UECE)
{alisson, analuiza, sergiosvieira, gustavo, jessyca, celestino, joel, laure}@larces.uece.br

***Abstract*—With the emergence of new applications and requirements it became necessary to create new monitoring and reactive configuration mechanisms to try to meet the SLAs (*Service Level Agreements*). In WDM (*Wavelength Division Multiplexing*) optical networks, one way of trying to fulfill these agreements is by using pre-established protection paths. However, despite guaranteeing that traffic will be rapidly routed to its protection path in case of failure, there is no guarantee that the latter will be capable of meeting the contracted SLA in accordance with the bit error rate of its links. In this article we propose a scheme for monitoring and selecting the SRLG (*Shared Risk Link Group*) protection path disjointed from the main path using Genetic Algorithms, Fuzzy Logic in a PBM (*Policy Based Management*) platform denominated GAFUDI.**

I. Introduction

With the advent of high transmission capacity optical networks, such as WDM (*Wavelength Division Multiplexing*), several authors have stated that it is not necessary to use intelligent management mechanisms for the network resources, and that just the transmission capacity of the optical fibre, together with the photonic devices, would be enough to guarantee Quality of Service (QoS). Differently, other authors defend the idea that, even with the use of this technology, applications will always appear that are capable of consuming the resources offered, requiring, therefore, the use of QoS mechanisms. The fact is that the popularity of certain applications (e.g., Videoconferencing, VoIP, IPTV) and the appearance of new services generate great demand of resources, causing an overload and aggravating network performance.

According to [1], [2] and [3], QoS is determined by the degree of satisfaction of the user regarding a specific service, and each service has different requirements (e.g., bandwidth, response time, delay variation, discard rate). In order to assure application level QoS, a user or business establishes an SLA (*Service Level Agreement*) by means of a contract. In this context the optical network is an important ally in offering resources due to its large transmission capacity, which does not necessarily assure full compliance with these requirements.

One way of attempting to meet the standards of the client's application is to ensure the survival of the network by means of mechanisms that allow its continuous operation, through the definition of protection policies. For each SLA established the network administrator defines a type of protection (1+1, 1:1, 1:n) according to the classes of service (*Gold*, *Silver* and *Bronze*). However, in case of failure, there is no manner of guaranteeing that the backup path will meet the client's requirements, or even those of the application in use, because the choice of this path does not take into account bit error rate and the type of link protection, among other things.

This article proposes a scheme for monitoring and selecting the SRLG (*Shared Risk Link Group*) protection path disjointed from the main path using *Fuzzy* Logic and Genetic Algorithms (GA) within a PBM architecture denominated GAFUDI.

The remainder of this article is organized as follows: in Section II related works are presented; Section III unfolds the initial considerations, discussing each topic covered; the definition of the problem is introduced in Section IV; the Protection Scheme is presented in Section V; next, Section VI details considerations on Genetic Algorithms and *Fuzzy* Logic; simulation, results and analysis are shown in Section VII; finally, the last Section presents the main conclusions and contributions of this work.

II. Related Works

Selecting the pairs of main and disjoint backup paths is approached in [4]. In this article the algorithm used is based on the Bhandari and Bellman-Ford algorithms. Differently from the proposal of the GAFUDI scheme, the selection of the paths does not take into account BER (*Bit Error Rate*) metrics and type of protection, whose objective is to guarantee quality of the traffic that may flow through the backup path.

In [5] sufficient conditions were developed to locate SRLG failures (that can affect more than one path). It also sought a form of minimizing the number of monitors on the network without affecting the reporting of such failures. Techniques were used for the transformation of graphs such that an SRLG failure should affect only a single combination of paths and cycles. However, in this article, monitoring according to the Quality of Service (QoS) for different applications and clients is not conducted. There is no concern in attending the requirements of QoS should there be a failure in the main path.

In [6] the backup path is managed in such a way as to guarantee that traffic flowing along its protection line will meet the client's SLA. Choice of the adequate protection path is carried out by use of genetic algorithms according to BER metrics and type of protection.

In [7] there is improved probability of choosing the best protection route and an improvement in the fitness function of the genetic algorithm. In this new fitness function the monitored BER measurements are evaluated through Fuzzy Logic and make the sets of values less restrictive. As in [6], the problem of the SRLG disjointed from the main path is not taken into consideration.

This article describes a scheme for monitoring and selecting a protection path using Fuzzy Logic and Genetic Algorithms in a PBM platform. GAFUDI's objective is to comply with the SLA by delivering due QoS. In order to meet these requirements the following metrics were taken into consideration: bit error rate (BER), type of protection, the SRLG disjointed from the main path and path size. Furthermore, implementation of the genetic algorithm was directed to the resolution of the problem of searching for a protection path so as to diminish search time and improve the quality of the solution found.

III. Initial Considerations

A. Optical Networks

Optical networks are used to try to meet the growing demand of Internet resources and the need to guarantee QoS for the applications. Data transmission in an optical environment involves several devices (terminals, amplifiers and optical switches).

B. Protection Schemes

Protection routes in optical networks can be: (1) 1+1 Protection, a protection path is assigned to the main path, and the same information flows through both. In the egress node the signal with better quality is selected and then forwarded; (2) Protection 1:1, under non-failure conditions of the main route the protection route can be used to carry extra traffic. Whereas, in case of failure it is used only by main route traffic; (3) Protection 1:n, similar to Protection 1:1, under non-failure conditions the protection path can be used to transport extra traffic. The difference is that, in this method, the paths share the same protection.

C. Management of Optical Networks

Managing networks has become a very complex task due to the large quantity of equipment involved, their heterogeneity, traffic diversification, different demands and the need to supply QoS and security. Furthermore, in optical networks, due to the high capacity of the links, a failure could potentially lead to enormous quantities of lost data.

In order to simplify administration, monitoring and configuration of the network's simulated elements (OXCs), Policy-Based Management was used through the LARCES_PBM tool (Management Platform for different types of networks - including optical networks) [8].

D. Genetic Algorithms and Fuzzy Logic

Genetic Algorithms are probabilistic algorithms that offer adaptive search mechanisms. Its use is recommended in the resolution of NP-complete problems, thus striving to minimize the computational effort necessary. They are based on Darwin's Theory of Evolution in which only the most adapted individuals survive.

Fuzzy Logic extends Traditional Logic. The groups are labeled qualitatively (using linguistic terms, such as: tall, warm, active, small, near) and the elements of these sets are characterized by variation of the degree of pertinence (a value that indicates the degree to which an element belongs to a set). Thus, by being less restrictive, *Fuzzy* Logic can be considered as more adequate for handling imprecise information [9].

E. SRLG

SRLG defines risk groups that share the same physical resources on the network (nodes, links, conduits, power sources). In the case of failure of one of these elements the entire group shall be affected.

Establishing a disjoint SRLG protection route involves calculating disjoint SRLG routes, with the objective of avoiding that a failure in the main path should also affect the protection path. Some links with the same SRLG are represented in 1.

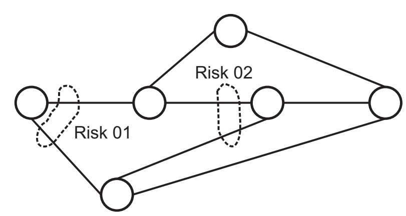

Fig. 1. Shared Risk Links

The problem of disjoint SRLG paths is NP-complete, hence it is solved by metaheuristics.

IV. Defining the Problem

For some applications there are levels of quality requirements that must be respected in order not to jeopardize their service. For applications like VoIP (*Voice over IP*), for example, even if a few voice packets are lost and there is a tolerable limit, it is important to try to guarantee that the data transmission rate remain continuous to avoid some or many interruptions in the conversation between the users. On WDM optical networks any impairment of a service may be related to its bit error rate (BER). In [11], BER value intervals for some applications (VoIP, IPTV, Electronic Transaction and Normal Traffic) were associated to classes of service. (Tabela I).

Further to BER, another important metric to supply QoS is the type of link protection in a route. Thus, for the purposes of this work three types have been defined: *Never*, *Shared* or *Only*.

TABLE I
SERVICE CLASSES ACCORDING TO BIT ERROR RATES (BER).

Service Class	Gold	Silver	Bronze	Best-Effort
Bit Error Rate	10^{-8}	10^{-7}	10^{-6}	10^{-6}
Service	VoIP	IPTV	E-Commerce	Common Traffic

A link with *Only*-type protection is exclusive, in other words, it cannot be selected to compose the protection path of other clients on the network. However, at worst, this link may be chosen if no *Never* and *Shared*-type links are available, so as to guarantee the survival of the network. This type of protection is generally used for high priority traffic. The *Shared*-type link, on the other hand, can compose the protection path for several clients. Finally, a *Never*-type link is not reserved as part of a protection path for any client. Therefore, the best solution for a protection path is a route composed of *Never*-type links with BER values very close to zero. By the same token, the worst solution is a route just composed of *Only*-type links and BER values close to one.

V. DESCRIPTION OF THE PROPOSED SCHEME

The Protection Scheme is accomplished within a PBM platform called LARCES_PBM, however, this is not the only management architecture capable of benefiting from the GAFUDI scheme. A platform capable of monitoring and configuring the devices according to service level specifications can also be used. In this work, PBM was chosen both for facilitating the configuration and for monitoring the simulated devices [10]. Considering the problem previously defined, the scheme will undertake the attempt to guarantee full compliance of the services offered, and thus diminish the risk of breach of contract.

Among the alterations effected on the PBM platform, the development of two modules that were integrated to the PEP is worthy of note: (1) Monitoring Model, and (2) Search Module.

The Monitoring Module is responsible for verifying the BER value of the lambda of one fibre at every instant, comparing this value to the BER allowed for each client according to their class of service, and, if necessary, request the Search Module to calculate a new protection path. Figure 2 shows the consultation structure of the Monitoring Module used to identify a hindered client.

Each OXC can have one or more links, and each link has only one fibre and a fibre only one lambda. In Figure 2, in **LAMBDA1**, the present BER value and the link's type of protection are stored. At every instant this value is updated and compared to the value of the client's permitted rates.

The Search Module is charged with calculating a new protection route capable of accomplishing the SLA contracted by a client. In it, GA and *Fuzzy* Logic are used to search for a solution.

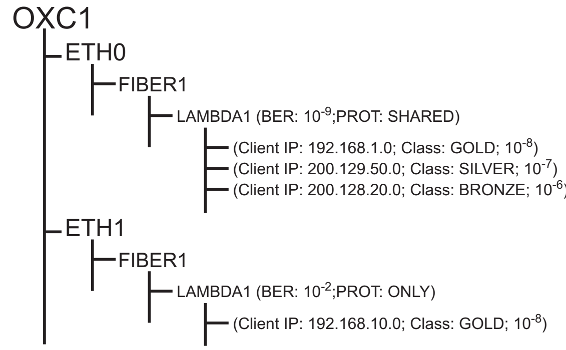

Fig. 2. Monitoring Module consultation structure

In general, the operation of the protection method can be better understood through Figure 3, where the fibres of links 0, 1 and 2 are monitored constantly and, should there be a breach of requirements, a high BER value, a new protection route is requested of the Search Module (I), finally, the RSVP-TE (Resource Reservation Protocol - Traffic Extension) (II) is requested to sinalize the route that was found.

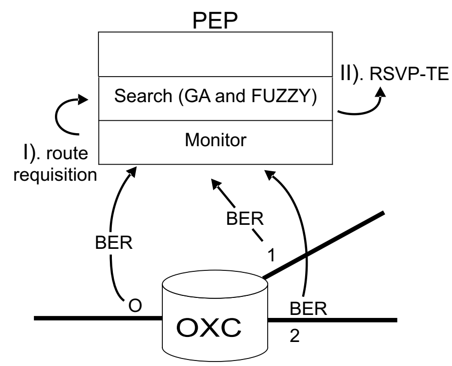

Fig. 3. Operation of the Protection Scheme

VI. GENETIC ALGORITHMS AND *Fuzzy* LOGIC

In an IP/WDM network, protection must be undertaken in the WDM layer, since it provides restoration time (time between a failure and the recovery of the protection route), lower than in the IP layer. This time is an important criterion for analysis of the recovery mechanisms [11].

Network operators consider that restoration should be undertaken in 50 ms, at most [13]. However, the proposal of this article does not consist of restoring a main optical path, but in restoring a backup path, as yet unused, in such a way that said path is capable of meeting the requirements of the client's applications. The worst case occurs when a failure in the main path happens at the same time that a high BER value is detected in the protection path. In this case, the ideal time span for the genetic algorithm to locate a good protection route should be inferior to 50 ms.

In the resolution of the problem, the physical topology of the optical network was mapped as a non-oriented connected graph $G = (V, E, S)$, where $V = \{v_i \mid i = 1, 2, ..., n\}$

represents the set of nodes (OXC), $E = \{e_{ij} \mid v_i, v_j \in V\}$ the set of fibres, where e_{ij} is the fibre that connects v_i to v_j, and in each fibre there is only one λ available. $S_i = \{s_j \mid j = 1, 2, ..., n\}$ is the set of SRLGs in a fibre i. Furthermore, $\forall\ \lambda\ \exists$ *ber*, *prot*; onde *ber* $\in [0, 1]$ is the value of the BER and *prot* is the type of protection (*Never*, *Shared*, *Only*). It was also defined that $\forall\ e_{ij} \in E, \exists$ gene $w \in W$ constituted by ber_{ij}, $prot_{ij}$ and values i, j, therefore, a chromosome is a sequence of genes where the first gene is the origin of the route and the last is the destination.

In this work the proposal for the operation of the GA is conducted in two steps: (1) Readout and Filtration, (2) Evolutionary Methods and Stoppage Criterion.

In the first step, Readout and Filtration, the genes (links) that will not contribute to an adequate solution must be removed from the topology. In this way, genes will be removed that have a BER value greater or equal to 10^{-3}, that have the SRLG of the main path and the genes of the main route. Thus, it is possible to obtain advantages such as: lesser computational effort, and smaller time span in calculating a solution due to the reduced search space. Further, one eliminates the possibility of selecting SRLG routes joint to the main route. The operation of this phase is represented by Algorithm 1.

Input: Set of genes W, set of genes U of the main path
Output: Set W' containing only valid genes
$W' \leftarrow \emptyset$
$Y \leftarrow \emptyset$
foreach $u \in U$ **do**
    $Y \leftarrow Y \cup u.S$
end
foreach $w \in W$ **do**
    if $w.ber < 10^{-3}$ *and* $w \notin U$ *and* $w.S \cap Y = \emptyset$ **then**
        $W' \leftarrow W' \cup \{w\}$
    end
end

Algorithm 1: Readout and Filtration

For the second step we used the evolutionary methods (initial population, natural selection, crossover and mutation), commonly used in GA so that the search converges on an optimum solution. In that proposal to diminish search time two stoppage criteria were considered: the first takes into account the maximum number of evolutions, and the second the average fitness of the individuals in a generation. In the second case the search will be stopped when the average fitness of the individuals is equal to 99.99% of the fitness value of the best individual. Algorithm 2 presents the pseudo-code of the operation of the GA.

Input: Set of genes W', popSize, maxGen, crossRate, mutRate
Output: Set of genes K of the protection route
$P \leftarrow$ createInitialPopulation(W', popSize)
evaluate(P)
$Q \leftarrow \emptyset$
$K \leftarrow \emptyset$
$curGen \leftarrow 0$
while $curGen < maxGen$ **do**
    $Q \leftarrow$ naturalSelection(P)
    $Q \leftarrow$ crossover(P, crossRate)
    $Q \leftarrow$ mutation(P, mutRate)
    $P \leftarrow$ Q
    evaluate(P)
    $Q \leftarrow \emptyset$
end
$K \leftarrow$ bestIndividual(P)
return K

Algorithm 2: Operation of GA using the maximum number of evolutions as stoppage criterion

A. Evolutionary Mechanisms

The initial population directly influences in the time and quality of a solution. An initial population containing many invalid individuals may need many generations before a good solution is found. In this way search time may be quite high. To solve this problem a random method was developed of creating chromosomes of the initial population using a roulette. In this method each gene is added to the chromosome as the result of a lottery using a loaded roulette in which the *Never* and *Shared* links have a heavier weight, and the *Only* links are lighter. Initially the route's node of origin is selected and a roulette is created containing the links of that node. Seeking to select links with *Never* or *Shared*-type protection, weights were defined for each type of protection: *Never* (Weight 5), *Shared* (Weight 4) and *Only* (Weight 0.5). Figure 4 represents the idea of the roulette containing three links with the respective types of protection.

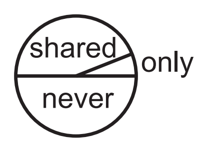

Fig. 4. Roulette used in the creation of the initial population

Afterwards a lottery is carried out to choose a link, thus creating a gene and adding it to the chromosome. All the links of that node are disabled so no links are selected that may lead back to the previous node, and the process is carried out again from the destination node of the chosen link. This is done until the destination of the route is found, or until there are no more enabled links. In Figure 5 the method of creation of a chromosome is detailed.

For this method two tests were undertaken. The first evaluates the quantity of valid and invalid individuals, and the second verifies the time spent in creating the chromosomes. In both tests population size varied from 2 to 1024 individuals. Figures 6 and 7 represent the first and second test, respectively.

In Figure 6, despite the existence of more invalid than valid individuals, the method proved adequate, since, as can be observed in Figure 7, the average time spent to create a

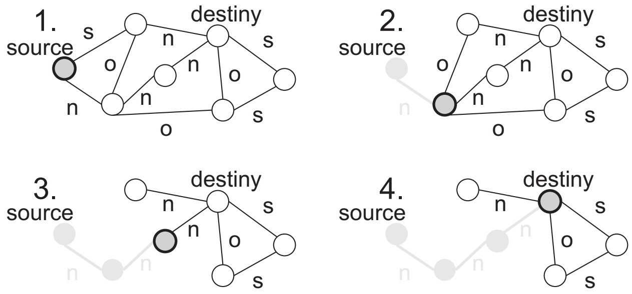

Fig. 5. Method of creating the random chromosome used in a roulette

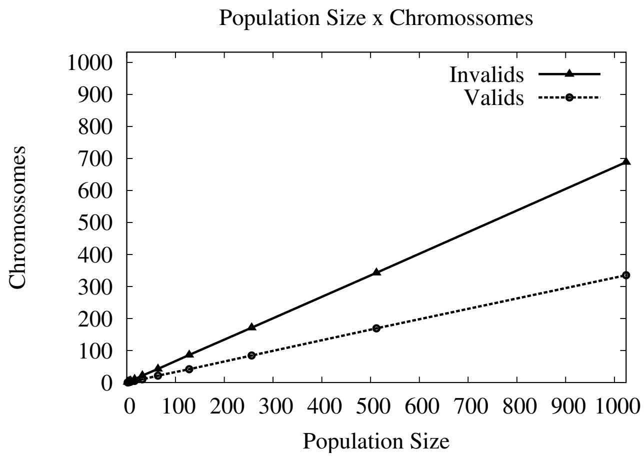

Fig. 6. Average quantity of valid and invalid chromosomes generated as a result of population size

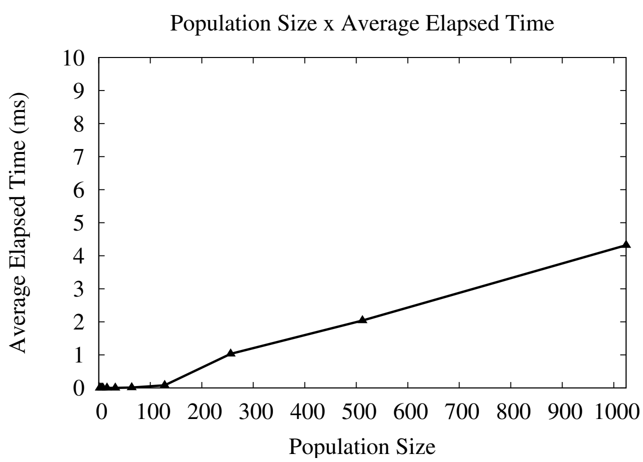

Fig. 7. Average time spent in creating the chromosomes as a result of population size

population with many individuals is low ($< 5ms$). Since time is a decisive factor in this problem, this method of creation was chosen.

The method used in the Natural Selection chooses the best adapted individuals to suffer mutation and crossover, with the objective of seeking new solutions. Selection is conducted using a roulette created from the fitness of the individuals in a generation, thus, the chromosomes with higher fitness values have a greater probability of being chosen.

For the crossover a gene G of one chromosome (C1) and a gene H of another (C2) are chosen randomly. Using the same idea for the creation of the chromosome of the initial population, one seeks to find a route from G to H (R1). The offspring chromosome (F1) by genes C1, G_1 to G_x, R1 and by the genes C2, H to H_n. Eventual ties that may be generated are removed and, if the offspring is not valid, the parent chromosome possessing the highest fitness value is returned. Figure 8.

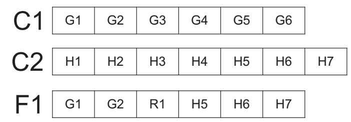

Fig. 8. Example of a crossover

The method used in the mutation is based on the crossover. Instead of conducting a crossover using different individuals, the same individual is used.

B. Fitness Function

This defines the aptitude of an individual in the solution of the problem. The higher the fitness value, the better the solution will be. In our proposal we define the following function:

$$fitness \leftarrow \frac{\sum_{i=1}^{n} \alpha f(ber_i) + (1-\alpha) g(prot_i)}{n} \frac{N}{n}$$

.

$$f(x) = defuzzy(x)$$

.

$$g(x) = \begin{cases} 0.70 & \text{, if} \quad x = NEVER \\ 0.29 & \text{, if} \quad x = SHARED \\ 0.01 & \text{, if} \quad x = ONLY \end{cases}$$

Where, for each chromosome, $\alpha \in [0, 1]$ defines the weight ascribed to the BER, that may vary between 0 and 1, and, consequently, the type of protection. Thus, to calculate Fitness, one of the metrics will have greater importance, n represents the quantity of genes of the chromosome and N the quantity of links in the topology, $f(ber_i)$ calculates the contribution of the BER of the gene using a defuzzifier [7], and $g(prot_i)$ the contribution of the type of protection of the gene in the fitness calculation. Note that to leave the fitness function inversely proportional to the size of the route, the average of the sum of the values of the genes is multiplied by $\frac{N}{n}$, thus, $n > 0$, the bigger the route the lower the fitness value.

VII. Simulation, Results and Analysis

This section presents the simulation of the proposed scheme and the results obtained. The evaluation criteria considered in the simulation were: BER values of the lambdas of the protection route, size and time spent in seeking a solution. The implementation of the protection scheme was carried out by a simulator. Among several presently existing simulators (e.g., MARBEN, NS, OpNet), the one most adequate to our proposal was the GLASS [14]. In it, protocols can be added or modified, failure events simulated, and the routing result visualized. The only restriction is not being able to vary the BER value during the simulation, making it necessary to define a requirement breach (high BER value) before starting the simulation.

Contrary to [7] and [6], that used the JGAP [15] (*Java Genetic Algorithms Package*) framework, that supplies all the basic mechanisms of the evolutionary principles, for the GA-FUDI scheme a new implementation of the genetic algorithm was done in order to reduce search time, improve the quality of the solution and simplify the code. Through comparative tests it was possible to identify that the new implementation obtains better results than those obtained with the framework.

To implement the Fuzzy Logic the FuzzyF [16] framework was used, allowing implementation time to be reduced, and addressed the needs of the route evaluation problem.

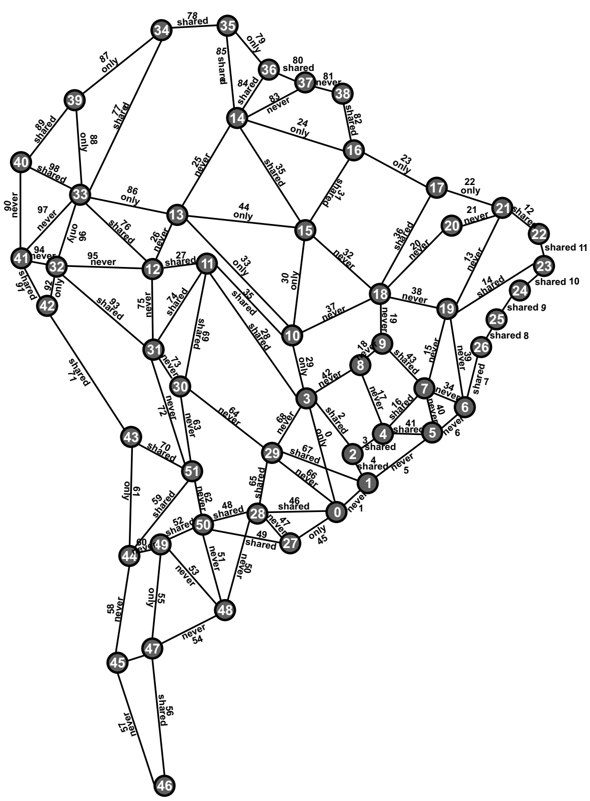

Fig. 9. Topology

The tests were undertaken using a hypothetical scenario of the South America network (Figure 9), which is composed of 52 nodes and 99 links. Each link has only one fibre, and each fibre one lambda that has its protection type (*Only, Shared, Never*) specified, and a respective BER value. Furthermore, 8 links were defined with lambdas with a high BER value ($> 10^{-3}$) and 2 links with SRLG joined to the links of the main path. Consequently, the complexity of the problem was increased to better evaluate the behaviour of the method. Tests were conducted using 192 and 256 chromosomes in the population and, for each population, 16 and 32 generations. In this way, good results were obtained for average rate of choice and average search time (Table II). These values were defined through tests that evaluated the time necessary to choose a route, and the rate of choice of the best solutions varying the value of α. 15500 tests were conducted for each combination.

TABLE II
TEST RESULTS.

Population Size	192		256	
Max Generations	16	32	16	32
Best Routes Average Choice (%)	35.3	36.3	39.8	39.9
Average Elapsed Time (ms)	40.4	67.2	62.2	108

In this scenario adequate BER values exist ($\sim 10^{-9}$) to supply quality of service to the classes *Gold*, *Silver* and *Bronze*, as well as inadequate values ($> 10^{-6}$). While the tests were conducted, an SLA for VoIP (Gold) applications were signed with a customer. The application data flow through nodes (51) (30) (29) (1) (2) (3) (10) (15) (16) (17) (21), that characterizes the main path, and there is a protection path through nodes (51) (50) (28) (0) (1) (5) (7) (19) (21), The search for a new protection route starts when, through the PEP (Monitoring Module) a high BER value for link (48) of node (50) is detected. Right away, the Search Module is requested to calculate a new protection route.

To evaluate the scheme, two types of graph were generated varying the value of α. The first shows the average rate of choice of route, and the second the average time of choice. 4 representative routes were chosen among all the paths generated, it being that the first two are the best solutions found, and the last two are less adequate solutions. Among the best routes, the path with links [72][74][28][42] [18][19][20][21] has good BER values, but it is made up of two links with *Shared*-type protection, and eight *Never* links. However, path [72][75][26][25][35][32][20][21] has seven *Never* links and only one link with *Shared*-type protection, but has worse BER values.

The tests were conducted varying the value of α (x axis) to determine which metric (BER or protection type) would bear more importance in the protection calculation.

In Figure 10 the test was conducted using 192 chromosomes in the population, and 16 generations. It is noted that the second best route, due to having more *Never*-type links, is chosen more times, because the value of α(0.2∼0.44) prioritizes the type of protection. When the value of α goes above 0.44, on average, the first route is chosen more times. This occurs because its links have better BER values. The average time of choice in this case remained below 50 ms, and the average rate of choice of the best routes was 35.35%.

Now, in Figure 11 the test was conducted using 192 chromosomes in the population and 32 generations. In this case it is noted that the difference between average rates of choice of the best routes diminished a bit, consequently, the rate of

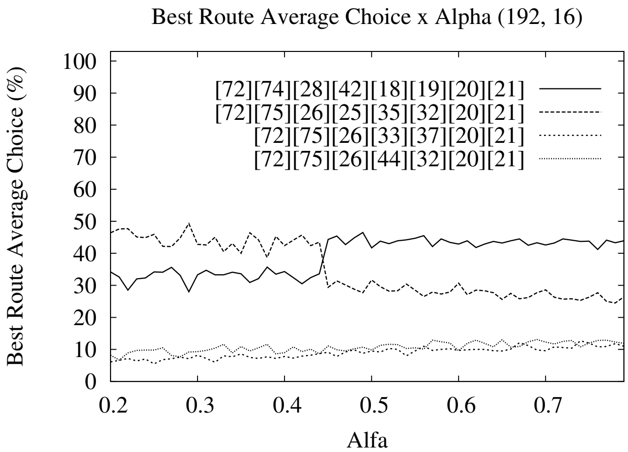

Fig. 10. Average rate of choice of good routes hinging on alpha (192 chromosomes and 16 generations)

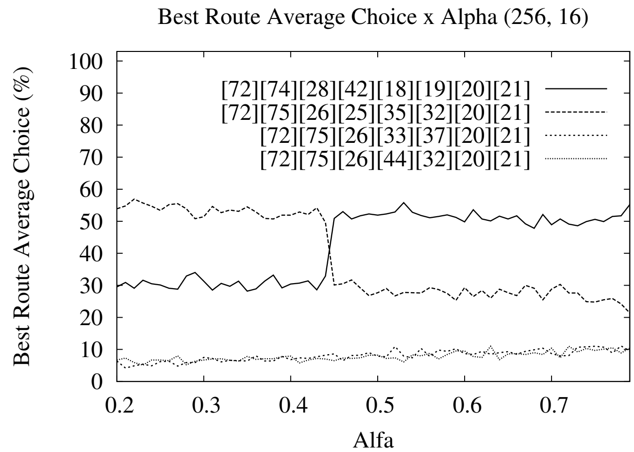

Fig. 12. Average rate of choice of good routes hinging on alpha (256 chromosomes and 16 generations)

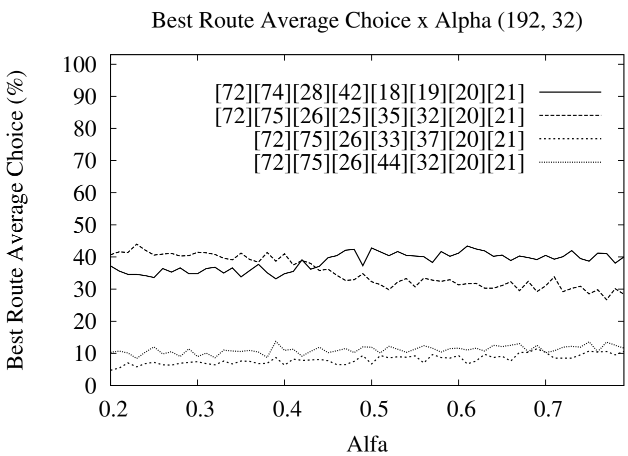

Fig. 11. Average rate of choice of good routes hinging on alpha (192 chromosomes and 32 generations)

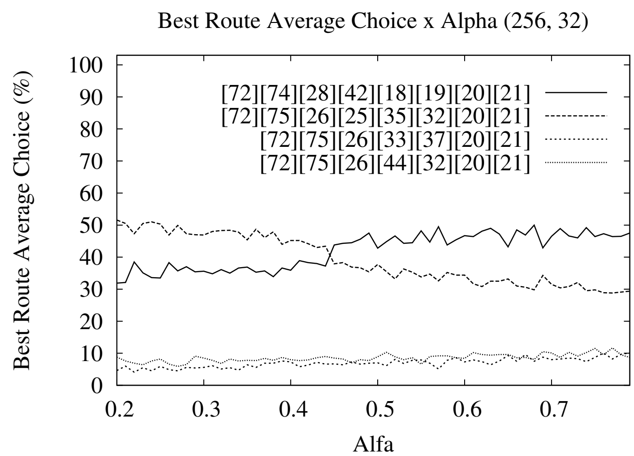

Fig. 13. Average rate of choice of good routes hinging on alpha (256 chromosomes and 32 generations)

choice of less adequate paths increased. This occurs because, for this quantity of chromosomes the number of generations is not adequate, therefore, for each new generation created, no improvement is observed in the search for a solution.

Figure 12 shows the results of the test conducted using 256 chromosomes in the population and 16 generations. With these values, excellent results were obtained for average rate of choice of the best routes (39.87%) in an average time slightly higher than 50 ms.

Finally, Figure 13 shows the results of the test using 256 chromosomes in the population and 32 generations. Here, despite obtaining the best average rate of choice of the best routes, the time spent exceeded 100 ms. Therefore, these configuration values of GA are not adequate.

Figure 14 shows average time spent on the choice using 192 and 256 chromosomes with 16 and 32 generations. With this, one can verify the influence of the size of the population and the number of generations in the operation of the algorithm. Therefore, it is up to the administrator to define what is best to solve his problem, to produce the solution rapidly, slightly diminishing the rate of choice of the best routes, or to risk a time span above 50 ms and obtain a better rate of choice.

VIII. Conclusions

The article describes a scheme for choosing the best SRLG Disjoint protection route in optical networks through the use of Genetic Algorithms with the support of *Fuzzy* Logic. Protection on these networks is a complex problem and has deserved attention due to the lack of resources available to allow the creation of protection paths. The use of GAFUDI allows quickly finding a solution that satisfies, or almost satisfies the SLA, and thus contributes to the survival of the network. Furthermore, it avoids that a failure in the main path should also affect the protection path. This proposal shows that the solutions were found in adequate time, and were satisfactory.

With the results obtained, one can conclude that, for this type of problem, the method of creating an initial population,

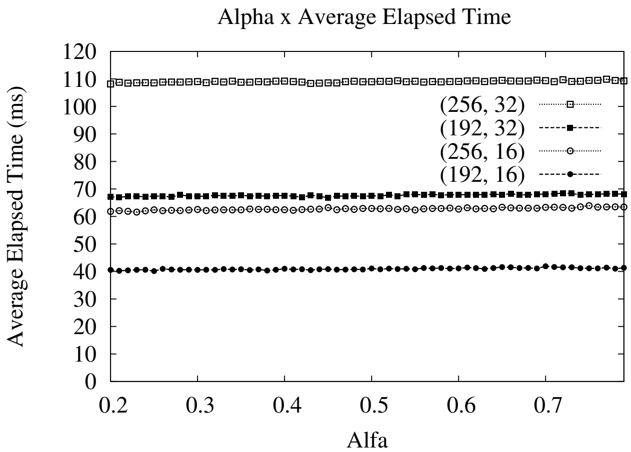

Fig. 14. Average choice time hinging on alpha.

mutation and crossover are decisive. The use of a random method of creating chromosomes turned out to be very adequate in respect of time spent. Furthermore, the variation of the value of α fulfils an important function in the choice of the solution. With this variation one can define which metric will have the decisive role. Since in this proposal the important thing is to guarantee that the links in the main path have low BER values, the ideal thing is that the value of α be higher than 0.44, according to the results obtained.

As future activities for this work, it is intended to test other metaheuristics for the solution of the problem presented. Use other parameters peculiar to optical networks to qualify a link. Apart from that, propose a solution for the problem of routing and wavelength assignment (RWA), each link containing more than one lambda, and develop a class of events to simulate, within GLASS, variations of BER values in real time.

Acknowledgments

The authors wish to thank the financial support obtained through the RNP-Rede Nacional de Pesquisa (the Brazilian National Research Network), within the Project Rede GIGA - FUNTEL.

References

[1] ISO-IEC-DIS 13236, *Information Technology - Quality of Service Framework*, ISO-OSI-ODP, Junho 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 Applications Requirements Evaluation*, SPECTS03, Montreal, Canada, July 20-24, 2003, pp. 380-387.

[4] X. Luo, B. Wang *Diverse Routing in WDM Optical Networks with Shared Risk Link Group (SRLG) Failures*, Proceedings of the 5th IEEE International Workshop on Design of Reliable Communication Networks (DRCN), October 16-19, 2005, Island of Ischia (Naples), Italy. (R)

[5] S. S. Ahuja, S. Ramasubramanian and M. Krunz, *SRLG Failure Localization in All-Optical Networks Using Monitoring Cycles and Paths*, INFOCOM 2008. The 27th Conference on Computer Communications, Phoenix-AZ, USA, 13-18 April 2008 Page(s):181 - 185.

[6] J. Celestino Jr. et al.,*GEAP: A Fault Management Scheme in Optical Networks*, The Fourth Advanced International Conference on Telecommunications (AICT), 2008, June 8-13, 2008 - Athens, Greece

[7] J. Celestino Jr. et al., *GAFUPA: Uma Proposta para Proteção em Redes Ópticas*, XXVI SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES - SBrT 08, 02-05 DE SETEMBRO DE 2008, RIO DE JANEIRO, RJ

[8] 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.

[9] S. Sandri e C. Correa, *Lógica Nebulosa*, Anais da V Escola de Redes Neurais, São José dos Campos, 1999, pp 073-090.

[10] Verma, D. (2000). *Policy-Based Networking: Architecture and Algorithms*, New Riders Publishing Thousand Oaks, CA, USA

[11] C. Pinart, *Alternatives for in-service BER estimation in all-optical networks: towards minimum intrusion*, JOURNAL OF COMPUTERS, VOL. 2, NO. 3, MAY 2007

[12] J. Vasseur, M. Pickavet, e P. Demeester, *Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*, 2004, Elsevier Inc.

[13] V. Souza, *Uma Arquitetura Orientada a Serviços para Desenvolvimento, Gerenciamento e Instalação de Serviços de Rede*, Dissertação de Mestrado, Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, SP, 2006.

[14] GMPLS Lightwave Agile Switching Simulator (GLASS), http://www.antd.nist.gov/glass, acessado em novembro de 2007.

[15] K. Meffert, *Java Genetic Algorithms Package* ,http://jgap.sourceforge.net/, acessaso 11-2007.

[16] Bittencourt, J. R.; Osório, F. S., *Fuzzy Logic Framework*, http://www.inf.unisinos.br/ jrbitt/fuzzyf/, acessado 02-2008.