SRLG Connection Provisioning in WDM Network: A Review

Karamjit Kaur, Anil Kumar*
Department of ECE, Amity University Haryana
Maneasar, Gurgaon, India

Abstract—The optical fiber technology has completely revolutionized the telecom industry by its properties like low error rates, long transmission distance, less inter signal interference and high signal security. The invent of WDM technology has played a crucial role in increasing the data carrying capacity of the network. The major concern of these networks is the risk of link failure that may result in huge loss of data. Thus, special attention is paid to provide backup path protection for failure like control plane failure, link failure, shared risk link group failure. The present paper focus on the eminent research wok reported on the field of SRLG failure & provision of backup path protection in this scenario.

Keywords—WDM Networks, link failure, backup path, SRLG.

I. INTRODUCTION

Optical fiber is a revolutionary means of transmission. Its low error rates, transmission capacity, and immunity to noise are considered to be responsible for growing popularity. More and more optical fiber networks are linking to other networks and being used in big corporate networks. Networks like these must work 24×7 to support applications that require unbroken processing, such as applications in airline companies, hospitals, banks, supermarkets, and many others. WDM (Wavelength Division Multiplexing) technology allows optical networks to support speed close to terabits per second, and consequently any interruption could lead to the loss of enormous quantities of data, thus harming the applications. In order to avoid these problems, safe and reliable protection techniques are necessary. One of the techniques implemented in optical networks to guarantee uninterrupted service is the use of protection paths. In this technique alternative routes (protection paths) are employed so that, in case of any failure along the main-path, the flow remains undamaged because traffic is quickly redirected to the protection path [1].

A network which contains many network components of both hardware and software can incur failures due to one (or even multiple) of its contained components. Ranging from the largest to the smallest and from hardware to software, network failures can be categorized as control plane failure, Sub network failure, Network card failure, Link failure, Shared Risk Link Group (SRLG) failure. SRLG failure is a generic concept to define all types of network failures whenever a common SRLG incurs a failure [2]. Here a shared risk link group can be a fiber link, node, sub network, or control plane, etc. SRLG defines a concept that multiple different services may suffer from a common network failure if they are sharing a common failure risk. Such risks can be a fiber link, a man-hole, an operational center, etc. The consequence of the failure of the common risk is that all the services that share the risk would be affected or even totally interrupted. The examples of SRLGs include fiber conduit that contains multiple fibers if cut will affect all the traffic carried by the fibers within the conduit; or an operational center, which can be shut down due to some disasters like fire, storm, etc. All the traffic that traverses the center or starting or ending at the center would be affected; or may be the whole regional sub network. The example for this could be that the sub network is laid in a region that is invulnerable to disasters like earthquakes.

In addition, the SRLG concept is network layer-related. A link or node that is an SRLG for its upper layer services can also share a shared risk link group in a lower layer. Meanwhile, this wavelength channel shares a fiber with all the other wavelengths contained within the fiber; the fiber is a common SRLG of all these wavelengths. The layered SRLG relationship is transferred from upper layers to lower layers [3]. A transport network is also divided into a data plane and a control plane [4]. The control plane provides control functionality to administrate the data plane. The failure of the control plane would lose the control of the whole data plane; thus, control plane is also considered as a type of SRLG for all the services carried on the data plane. To enable network services to survive from SRLG failures, many survivable network design approaches have been developed [5]. A common key principle for SRLG protection in these approaches is to set up a pair of SRLG-disjoint routes respectively for the working and protection paths. For the link SRLG, one can find a pair of working and protection routes that do not share any common links; for the node SRLG, it can find a pair of routes that do not share any common nodes, and for the sub network SRLG, it can ensure that a pair of working and protection routes do not traverse any common sub networks. With the advent of high transmission capacity optical networks, such as WDM (Wavelength Division Multiplexing), applications like videoconferencing and the appearance of new services always generate great demand of resources, causing an overload thereby worsening network performance. Quality of service depends upon arising requirements of services according to the specific task they perform. Some may require higher bandwidth, while for the other response time, delay variation, discard rate may be more important.

In order to assure application level quality of service, a user or businesses is required to sign a Service Level Agreement (SLA). In order to meet the standards required, it is necessary to ensure the survival of the network by means of mechanisms that allow its continuous operation, through the definition of protection policies. Protection is a proactive procedure, in which the backup resource is reserved during the setup of the working light-path, can be employed to overcome such failure. A light-path that carries traffic during normal operation is known as a working path, when a working path fails, the traffic is switched to the backup path. Working path and backup path should be diverse so that no single failed link can affect both paths. In order to maintain the required SLA, protections are classified in three types as 1+1, 1:1, 1: N. In 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. In 1:1 protection, 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. For 1: N protection, 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.

In WDM optical networks, one way of trying to fulfil 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. 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 quality of service and security. So, 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 [5]. In optical networks, due to the high capacity of the links, a failure could potentially lead to enormous quantities of lost data. So, 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.

Considerable theoretical work has been done in the field of shared risk link group disjoint path protection, where different authors have reported different conclusions employing different techniques. Few of the prominent findings have been reported in brief according to the input element used by them.

An efficient path restoration algorithm for distributed path selection which supports fast end to end path based connection restoration in an Automatically Switched Optical Network (ASON) [6]. The author proposed a new path restoration algorithm with SRLG constraint to handle single-link failures in Generalized Multi-Protocol Label Switching (GMPLS)-Based ASON, whose restoration paths are pre-computed and stored in the routing table at each node [7]. The proposed RSGA can efficiently find physically disjoint Label Switched Paths (LSP) by modifying network topology and Dijkstra's algorithm. The numerical simulations show the RSGA can significantly improve resource utilization, and reduce blocking ratio. As specified in [8] the control plane (CP) of ASON is based on GMPLS. Actually, we can say that the survivability of ASON is mainly the survivability of CP. Protection and restorations are the key techniques to improve network survivability. In order to recover successfully, service and restoration LSPs must be physical disjoint. To demonstrate the efficiency of RSGA, the resources utilization and blocking ratio is evaluated with the well-known restoration path selection algorithm shortest path restoration (SPR) [8]. According to the simulation results, the RSGA uses bandwidth more efficiently than traditional SPR, since it keeps accurate information about the amount of reserved bandwidth that must be reserved on each link in the network to restore any single link failure. Also, algorithm represents a potentially significantly cost saving solution to network providers, and its blocking ratio is lower than SPR.

The problem of shared path protection algorithm in survivable WDM optical networks is reported in [9], taking into consideration differentiated reliability under shared-risk-link-group constraint. A subset of network links that share the risk of failure at the same time are said to be in a common SRLG. Rather than the conventional complete SRLG-disjoint shared path protection, a heuristic partial SRLG-disjoint shared path protection algorithm based on the concept of SRLG conditional failure probability is introduced to provide differentiated reliability protection [10]. According to the concept of differentiated reliability, each connection in the layer under consideration is guaranteed a minimum reliability degree or equivalently a maximal failure probability required by the client application. In order to avoid the simultaneous failure of both work path and backup path in this condition [11], a straightforward way is to find two paths which are not only link-disjoint but also SRLG-disjoint. Generally, it classifies the optical network topology into two layers: the logical layer and the physical layer. The logical layer presents the logical connective relationship among the nodes. It contains optical links (the logical connection of two nodes) and optical switch nodes. The physical layer presents the fiber topology (more generally the physical resource) of the optical network. It contains fiber spans (e.g. fiber, cable, tunnel); optical switch nodes and fiber span nodes. An optical link in logical layer presents a connection which may traverse several fiber spans in the physical layer. In order to identify the risk, it assign a unique shared risk link group identity (SRLG-ID) to each fiber span in the physical layer; each optical link in the logical layer is assigned an SRLG-list, which contains all the SRLG-IDs of the fiber spans traversed by the link. After all the links are assigned SRLG-lists, it is possible to implement various routing algorithms in the logical layer [12]. A light-path is also associated with an SRLG-list, which contains all the SRLG-IDs of the links traversed by the path. Two paths are said to be SRLG-disjoint if there is no common SRLG-ID in both SRLG-lists of the two paths.

In the algorithm, the *K*-shortest paths algorithm is adopted to compute the working path. We first compute *K*-shortest paths as the candidate working paths. For each candidate working path, it prunes all the links and nodes along the path in the graph. Then it use Dijkstra's algorithm to compute another shortest path [13]. The full wavelength convertible capacity for each node is allowed. Once a connection request comes, *K*-shortest path is calculated as the candidate working paths. Then for each candidate working path, the corresponding candidate backup path is calculated. At last, from the candidate path pairs, the best candidate working and backup path are selected as the final decision. It is assumed that all nodes in the network are equipped with wavelength converters. The request will be rejected immediately if the algorithm cannot find the proper paths, so there is not waiting queue. The bandwidth of every request is supposed to be one wavelength. The performance of the algorithm is evaluated in terms of blocking probability and backup resource utilization ratio in the dynamical conditions. The backup resource utilization ratio in the paper is defined as the mean backup bandwidths allocated for protecting a unit working bandwidth, because it suppose that the bandwidth request of every connection is the full bandwidth of a wavelength channel, the mean proportion between the backup paths' hops (excluding the shared part) and the working paths' hops can be considered as the backup resource utilization ratio.

Although many mature heuristic algorithms have been proposed to find link disjoint paths, most of them can't be simply extended to find SRLG disjoint paths. There are only a few heuristic algorithms and Integer Linear Programming (ILP) which have been proposed to find SRLG disjoint paths. But the ILP-based solution is extremely time consuming and becomes infeasible for a large network size. Accordingly, the APF-based heuristic algorithms, which are easily carried out, are widely applied. However, it is the major challenge in using these APF-base heuristic algorithms that once a primary path is established, it may not be able to find a SRLG disjoint backup path, even though there does exist a pair of SRLG disjoint paths in the network. This is the so-called trap problem when finding SRLG disjoints paths using APF. In addition, considering the traffic of network always arrive dynamic and leave randomly, it is required to dynamic establish and release connections for them. So the dynamic traffic assignment scheme has more practical significance. Furthermore, among path protection schemes, shared path protection has higher network bandwidth utilization than dedicated path protection, but the primary paths and the backup paths aren't allowed to share the common bandwidth in any case.

A protection scheme entitled Mixed Shared Multi-Paths Protection (MSMPP) is proposed in [14]. Mixed shared multi-paths protection can not only effectively avoid traps, but also, differing from previous shared path protection scheme, make the primary path, when it doesn't work, share its bandwidth with the backup paths, so that the network bandwidth utilization is enhanced. Simulation results show that the performance of mixed shared multi-paths protection is better than shared path protection. In the paper, two critical problems i.e. trap problem and shared problem are discussed. If an algorithm can't find a pair of SRLG disjoint paths between a given source node and destination node pair, this algorithm falls into a trap. According to the definition of trap problem, one can classify the traps into real traps and avoidable traps. Real trap means there does not exist any SRLG disjoint paths for a given source node and destination node pair.

Two open issues of avoiding failures in path determination caused by traps and maximizing bandwidth sharing are discussed in [15]. Integer linear programming (ILP)-based approach, on the other hand, is not feasible for large SRLG networks. Also, an efficient shared SRLG protection scheme based on trap avoidance (TA) is presented that can achieve a bandwidth efficiency that is nearly as high as other schemes based on ILP. In shared SRLG protection, the objective is to find a pair of SRLG-disjoint paths for any given request such that the total bandwidth consumption for all requests is minimized, taking into consideration that the two or more backup paths can share backup bandwidth as long as their corresponding working paths do not fail at the same time. Compared to ILP and some other existing algorithms, the proposed algorithm runs much faster [16], and yet falls into few traps and achieves the same bandwidth efficiency. This algorithm is designed mainly for shared SRLG protection with dynamic routing, although it is also applicable for static routing. In order to verify that the algorithm is also near-optimal in terms of bandwidth efficiency when used in dynamic routing, performance of several ILP formulations for shared SRLG protection with dynamic routing is compared. It is shown that it can outperform existing heuristics algorithms [17], including the well-known shortest path algorithm, significantly in terms of trap avoidance performance and running time.

The problem of dedicated path-protection in wavelength-division multiplexed mesh networks with waveband switching functionality under shared risk link group constraints is considered in [18]. Two dedicated path protection schemes are proposed, namely the (Protecting-wave Band-At-wave Band-Level) PBABL scheme and the (Mixed-Protection-At-wave Band-and-Wavelength-Level) MPABWL scheme. The protecting-wave band-at-wave band-level scheme protects each working waveband-path through a backup waveband-path. The mixed-protection-at-wave band-and-wavelength-level scheme protects each working waveband-path by either a backup waveband-path or multiple backup light paths. Heuristic algorithms adopting random optimization technique are proposed for both the schemes. The performance of the two protection schemes is studied and compared. Simulation results show that both the heuristics can obtain optimum solutions and the mixed-protection-at-wave band-and-wavelength-level scheme leads to less switching and transmission costs than the protecting-wave band-at-wave band-level scheme. To reduce the provisioning costs in the optical domain of a WDM network, waveband switching (WBS) was introduced to group a specific set of wavelengths into a waveband at an optical cross connect (OXC). The cost is represented by the total number of occupied waveband-links and wavelength-links in provisioning the connection requests.

For the protecting-wave band-at-wave band-level scheme, each connection request is assigned with a working and backup path which are SRLG-diverse. A wavelength is assigned to each of the paths [19]. If the waveband grouping requirement is satisfied, the protecting-wave band-at-wave band-level scheme tries to set up a working waveband-path and a backup waveband-path under the condition that there are common free wavebands along both paths. MPABWL is similar to PBABL except that it allows a working waveband-path to be protected by several backup light paths. To obtain the optimum solution, mixed integer linear programming (MILP) can be applied for small networks. For medium and large networks, as the variables and constraints increase exponentially, it is difficult for the MILP approach to find the optimum solution given limited computational resources. Heuristic algorithms adopting random optimization technique are proposed for both the schemes. Moreover, the results show that the MPABWL heuristics lightly outperforms the PBABL heuristic in most cases [20].

Survivable traffic grooming (STG) is a promising approach to provide reliable and resource-efficient multi-granularity connection services in wavelength-division-multiplexing (WDM) optical networks. [21] study the STG problem in WDM mesh optical networks employing path protection at the connection level. Both dedicated-protection and shared-protection schemes are considered. Given network resources, the objective of the STG problem is to maximize network throughput. To enable survivability under various kinds of single failures, such as fiber cut and duct cut, one consider the general shared-risk-link-group (SRLG) diverse routing constraints [22]. Three efficient heuristics, namely separated survivable grooming algorithm (SSGA), integrated survivable grooming algorithm (ISGA), and Tabu-search survivable grooming algorithm (TSGA) are proposed. While SSGA and ISGA correspond to an overlay network model and a peer network model, respectively, TSGA further improves the grooming results from SSGA and ISGA by incorporating the effective Tabu-search (TS) method. Protection schemes can also be divided into dedicated-protection and shared-protection schemes [23], depending on whether resources can be shared among backup paths or not. In the two-layered grooming network, path protection can be applied at two different levels, namely protection at light path (PAL) and protection at connection (PAC) [24]. PAL is a coarse granularity protection scheme operating at aggregate (light path) level and PAC is a fine-granularity protection scheme operating at per-flow (connection) level.

In path protection, the backup path must not share a common resource with its primary path. This requirement prevents a single failure from affecting both the backup path and the primary path. In the paper, the static STG problem under SRLG constraints, with the objective of maximizing network throughput (or revenue) is studied. Various constraints taken into consideration include resource constraints, wavelength-continuity constraint [25], diverse-routing constraints and light path-capacity constraint. With SSGA, the SSTG problem is divided into two sub problems. One is the protection-aware virtual-topology design (PAVTD) problem, which involves establishing a virtual topology over the physical topology. The other one is the sub-wavelength-connection survivable-routing (SWCSR) problem, which involves packing the sub-wavelength connections on the light-paths in the virtual topology, with each connection having a primary path and a backup path. In ISGA, the provisioning of the light paths and connections are considered jointly. The objective is to accommodate as many connections as possible. New light paths are established to carry connections only when necessary. It is possible to establish a connection using only existing light paths or using a combination of existing and new light paths.

Tabu-search-based grooming algorithm is a meta-heuristic that defines general-neighbourhood search strategies to tackle difficult combinatorial optimization problems [26]. Comparing the results of the ILPs and the heuristics, one can see that heuristics obtain comparable, and even better, results than the ILPs. This is, in part, because most of the ILPs cannot obtain an optimal solution within 2 hours. Another reason may be that the heuristics achieve good results close to the optimal solutions. The running times of SSGA and ISGA are within 1 second and that of TSGA is also within a few seconds. Among the three heuristics, TSGA performs better than SSGA and ISGA due to the inherent reason that TSGA optimizes solutions obtained from SSGA and ISGA. The numerical results presented show that the computational complexity of the integer-linear-programming approach is too large, even for networks of small sizes [27]. This result implies that the integrated-routing approach is superior to the overlay routing approach in terms of resource efficiency.

M. Li and A scheme for monitoring and selecting the shared risk link group protection path disjointed from the main path using fuzzy logic and genetic algorithms within a PBM architecture denominated GAFUDI. GAFUDI's objective is to comply with the SLA by delivering due quality of service. In order to meet these requirements bit error rate, type of protection, the SRLG disjointed from the main path and path sizes are taken into consideration. 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. According to [28] the type of link protection in a route, avoiding the selection of paths that already have been reserved for other traffic flows is an important is another important issue to be considered after the required BER. Thus, three types have been defined: Never, Shared or Only. 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 [29]. 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. The implementation of the protection scheme was carried out by a simulator GLASS.

A method to try to assure that a pre-established alternative protection route is adequate in case of failure in the main path without lambda conversion is proposed in [30]. Commonly, network operators consider recovery time of a failure [31] to be 50 ms or less, raising difficulties in the search for an adequate solution. To solve this problem, exact algorithms, such as Dijkstra, may be inadequate because they only obtain a solution in reasonable computational time for small instances. In a network with many links, where each link may have many fibers, and each fiber has many lambdas, the time necessary to determine the best solution using an exact algorithm may surpass 50 ms by far. In general, to achieve the solution to this type of problem, meta-heuristics are employed, and while these do not guarantee the optimal, they offer low resolution time. This work uses genetic algorithms with the support of fuzzy logic, allowing the method to quickly reach a solution respecting the limit of 50 ms. the use of meta-heuristics, in this case and therefore cannot be resolved in polynomial time. The use of genetic algorithm provides a relatively simple manner of representing several metrics intrinsic to the problem, and comparing the solutions using a fitness value. Furthermore, several genetic algorithms configuration parameters (Mutation Rate, Crossover Rate, Stop Criterion, and Maximum Generations) can be used to find a solution that meets the requirements of our problem, such as a time period below 50 ms.

II. Conclusion

After going through the research work associated with protection using SRLG-link, it can be concluded that although the Integer Linear Programming (ILP) is an effective way in solving the various issues involved, but it is seldom used because of its time consuming attributes. Moreover, as the network size increase, the complexity in implementing algorithms increases, making the practical applications almost impossible. So most of research work associated suggests the implementation of various heuristic algorithms which selects the backup path depending on quality of service required like bandwidth, bit error rate, response time etc. One of the effective method of implementing disjoint link path protection is by using fuzzy logic.

Although considerable work is done for implementing fuzzy logic in system, it still have a great potential that need considerable efforts to be put in to design the state of art type system. The time constraint is the major issue involved. It is required that the processing time of system should be as small as possible, preferably less than 50 ms. 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, which should be taken into account by using fuzzy logic.

Moreover, features like required response time, bandwidth, wavelength and percentage reliability are peculiar to optical network to qualify a link, so should be considered accordingly. There is scope of implement if problem of routing and wavelength assignment (RWA) have more than one lambda is considered while implementing fuzzy logic. Further, most of the authors have considered the case of single link failure. Multiple-SRLG failure must also be taken into consideration for real time implementation. For betterment of the system, some more meta-heuristics algorithms can be implemented using fuzzy logic.

Also, it is observed that implementation of neural networks in the protection systems for optical networks are almost negligible. Applications of neural network will not only help in reducing the processing time but also improve the decision taking capability of the network. Additionally, further study is required to be carried out on SRLG-protection to consider the maintenance of protection path and the system for restoring the main path using fuzzy logic, which is equally important.

References

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

[2] Xu D, Xiong Y, Qiao C, Li G., "*Failure protection in layered networks with shared risk link groups*" IEEE Network2004;18:36–41.

[3] 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.

[4] Stephen S. Liu, "*A Systematic Approach to Develop and Manage SRLGs for Optical Transport Networks with Multi-Tier Resources*" NThA2.pdf, OSA / OFC/NFOEC 2010, IEEE 978-1-55752-884-1/10, 2010.

[5] Yueheng Sunet. et. al., "*An Evolutionary Approach for Survivable Network under SRLG Constraints*" IEEE 978-0-7695-3736-8/09, DOI 10.1109/ICNC.2009.739, pp. 122-126, 2009.

[6] YuanqiuLuo, Si Yin, Ting Wanget.et. al, "*Backup Path Multiplexing over Survivable GMPLS Networks*" NTuD2OSA 1-55752-830-6, 2007.

[7] Li DU, Yu LIANG, Xiaojuan LIU, *"A New Shared-Path Restoration Algorithm with SRLG constraint in ASON*" presented in 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. Digital Object Identifier: 10.1109/WiCom.2008.1038

[8] Bin Zhou and Hussein T. Mouftah, "*Adaptive Shortest Path Routing in GMPLS-based Optical Networks Using Fuzzy Link Costs*" CCECE 2004- CCGEI 2004, Niagara Falls, 0-7803-8253-6/04 IEEE, pp. 1553-1557, May 2004.

[9] Jin Cao, Lei Guo, Hongfang Yu et al., "*Partial SRLG-disjoint shared path protection with differentiated reliability in survivable WDM network*" Int. J. Electronics and Communication (AEÜ) 61, pp353 – 362,2007.

[10] Jin Cao, Lei Guo, Hongfang Yu, Lemin Li, "*Differentiated Reliable Partial SRLG-disjoint Shared Path Protection in Survivable WDM Network*" IEEE0-7803-9584-0/06, pp. 1887-1896, 2006.

[11] Xu Shao, Luying Zhou, Yixin Wang, "*Backup Re-provisioning after Shared Risk Link Group(SRLG) Failures in Survivable WDM Mesh Networks*" OThJ4.pdf,OSA 1-55752-830-6, 2006.

[12] Mohammad Javad Rostami Siavash Khorsandi Ali Asghar Khodaparast, "*CoSE: A SRLG-Disjoint Routing Algorithm*" Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07), 0-7695-2768-X/07, 2007.

[13] Q. Zhang, J. Sun, G. Xiao, and E. Tsang, "*Evolutionary algorithms refining a heuristic: A hybrid method for shared path protections in WDM networks under SRLG constraints*" IEEE Transactions on System, Man and Cybernetics, Part B,37(1), pp. 42–48, 2007.

[14] Zong-Li Tang, Xing-Ming Li, "*A Mixed Shared and Multi Paths Protection Scheme with SRLG Constraints*", Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 60-65, 2007.

[15] Dahai Xu, Yizhi Xiong, Chunming Qiao, and Guangzhi Li, "*Trap Avoidance and Protection Schemes in Networks With Shared Risk Link Groups*" Journal of Lightwave Technology, Vol. 21, No. 11, pp. 2683-2693,November 2003.

[16] Xubin Luo, Bin Wang, "*Diverse Routing in WDM Optical Networks with Shared Risk Link Group (SRLG) Failures*" IEEE0-7803-9439-9105, pp. 445-452, 2005.

[17] Lei Guo, "*A Novel Heuristic Method Based on Shared-Risk Link Groups (SRLG) Constraints in WDM Optical Networks*" ICACT2007, pp. 1569-1572, Feb. 12-14, 2007.

[18] Mengke Li and Byrav Ramamurthy, "*Survivable Waveband Switching in WDM Mesh Networks under Dedicated Path-Protection*" IEEE Globecom, 0-7803-9415-1/05, pp. 1874-1878, 2005.

[19] Daryoush Habibi, Viet Q. Phung and Hoang N. Nguyen, "*Minimizing the Number of Constraints for Shared Backup Path Protection (SBPP) in Shared Risk Link Group (SRLG) Optical Mesh Networks*" IEEE1-4244-1230-7/07, pp. 246-251, 2007.

[20] P. Datta and A. K. Somani, "*Diverse Routing for Shared Risk Resource Groups (SRRG) Failures in WDM Optical Networks*" BROADNETS'2004, San Jose CA USA, pp. 120-129, October 2004.

[21] Wang Yaoand Byrav Ramamurthy, "*Survivable Traffic Grooming With Path Protection at the Connection Level in WDM Mesh Networks*" pp-2846-2853,Journal of Lightwave Technology, Vol. 23, No. 10, October 2005

[22] Viet Q. Phung, Daryoush Habibi and Hoang N. Nguyen, "*On Diverse Routing for Shared Risk Link Groups (SRLGs) in Optical Mesh Networks*" IEEE1-4244-1230-7/07, ICON 2007, pp. 235-239.

[23] C. S. Ou, J. Zhang, H. Zang, L. H. Sahasrabuddhe, and B. Mukherjee, "*New and improved approaches for shared-path protection in WDM mesh networks*" Journal of Lightwave Technology, Vol. 22, No. 5,pp. 1223–1232, 2004.

[24] C. Ou, K. Zhu, B. Mukherjee, "*Traffic Grooming for Survivable WDM Networks – Shared Protection*" IEEE Journal on Selected Areas in Communications, vol. 21, no. 9, pp. 1367-1383, Nov. 2003.

[25] Ramamurthy S, Sahasrabuddhe L, Mukherjee B., *"Survivable WDM mesh networks"* IEEE/OSA J LightwaveTechnol2003;21:870–83.

[26] Pin-Han Ho et. al, "*A Novel Survivable Routing Algorithm for Shared Segment Protection in Mesh WDM Networks With Partial Wavelength Conversion*" IEEE Journal on Selected Areas in Communications, Vol. 22, No. 8, pp. 1548-1560, October 2004.

[27] Shen L, Yang X, Ramamurthy B., "*Shared risk link group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks*" IEEE/ACM Trans Networking 2005;13:918–31.

[28] Alisson Barbosa de Souza, Ana Luiza de B. de P. Barros, et al., "*A Management Scheme of SRLG-Disjoint Protection Path*" *2009 IFIP/IEEE* International Symposium on Integrated Network Management (IM 2009), pp.553-560, 2009.

[29] Guo L, Yu H, Li L.,"*A new path protection algorithm for meshed survivable wavelength-division-multiplexing networks*" In: Proceedings of ICN'05, Reunion Island, France,2005. p. 68–75.

[30] Alisson Barbosa de Souza, Ana Luiza de B. de P. Barros, "*Survivability on Optical Networks: Protecting the Protection*" presented in International conference on Ultra modern telecommunication and Workshops, 2009. Digital Object Identifier: 10.1109/ICUMT.2009.5345521.

[31] 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.