

Design of Survivable Optical Virtual Private Networks (O-VPNs)

Anwar Haque

School of Computer Science
University of Waterloo Ontario, Canada, N2L 3G1
ahaque@bcr.uwaterloo.ca

Pin-Han Ho

Dept. of Electrical and Computer Engineering
University of Waterloo, Ontario, Canada, N2L 3G1
pinhan@bcr.uwaterloo.ca

Abstract

This paper tackles the resource allocation problem for optical networks supporting Virtual Private Networks (O-VPNs), in which working and spare capacity are allocated in the networks for satisfying a series of traffic matrices corresponding to each O-VPN. Based on the $(M:N)^n$ protection architecture defined in Generalized Multi-Protocol Label Switching (GMPLS), we propose two novel Integer Linear Program (ILP) models, namely ILP-I and ILP-II, aiming to initiate a graceful compromise between the capacity efficiency and computation time without losing the ability of addressing QoS requirements in each O-VPN. Experiment results show that in terms of capacity efficiency, a significant improvement is achieved by ILP-I compared to ILP-II at the expense of higher computation time. Although ILP-II is outperformed by ILP-I, it can handle the situation with an arbitrary size of O-VPNs. We conclude that the proposed ILP models yield a scalable solution for the capacity planning in the survivable optical networks supporting O-VPNs based on the $(M:N)^n$ protection architecture.

1. Introduction

Optical Virtual Private Networks (O-VPNs) are well-recognized as one of the killer applications of the future Internet market and have gained increasing acceptance due to the economic benefits and maturing technology [5]. An O-VPN extends enterprises' private intranets across public networks (such as the Internet and metropolitan areas networks), which provides secure private interconnections essentially through private tunnels supported by Wavelength Division Multiplexing (WDM) transmission [9]. Figure 1 illustrates the O-VPN architecture of interest in this study, where three VPNs share the public network through the corresponding access nodes A, B, C, and D. The public network consists of several switch nodes interconnected by multi-wavelength WDM links, while the access nodes serve as an interface between the

optical domain and the user domain. Since the customers may address different QoS requirements upon their private networks, the public network must be able to support heterogeneous services with stringent demands on security/data-integrity and accommodate connections with mixed characteristics. This leads to a fact that the networks supporting O-VPNs are more vulnerable to any failure and attack. This threat is further highlighted by the nature of all-optical WDM networks with absolute data transparency through ultra high-speed transmission. Thus, survivability has been well-recognized as one of the most important objectives for the design of O-VPNs such that any unexpected interruption upon the working traffic can be restored in a short time.

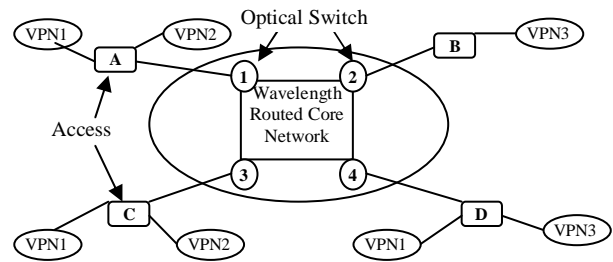


Figure 1. O-VPN architecture [8]

To achieve network survivability, the most commonly seen approach is to allocate spare capacity for the working capacity such that the affected working traffic can be restored by switching over to the protection paths which are Shared Risk Link Group (SRLG) [2,3,4] disjoint from the corresponding working paths. The design premise for protection is straightforward, however, to develop an effective scheme that can be both capacity-efficient and computation-efficient has long been an open question. The most difficult problem is to make the schemes scalable with the network size and the amount of traffic. In addition, the dependency between the working paths and the corresponding spare capacity in case shared protection is adopted has complicated the whole problem [3]. A significant amount of research efforts has been addressed on the topic of achieving network survivability [1-4,6,10-22] for general IP and WDM networks in which a single domain and uniform service requirements are assumed.

The research specifically upon the protection for O-VPN has been rarely reported. Due to the heterogeneity of O-VPNs and the huge computation complexity, the most intuitive approach for allocating working and spare capacity in such networks is to group the working capacity and to conduct optimization upon each group. Each group of connections is called a *protection group* where a specific protection scheme can be arranged.

One of the solutions for the resource allocation problem in networks with O-VPNs is to formulate the task into an Integer Linear Programming (ILP) model where all the traffic demands for the VPNs in the networks are jointly considered. Nonetheless, this approach simply suffers from a scalability problem as the network size and the traffic demands increase. The fact that each O-VPN may address different QoS survivability requirements further complicates the problem when a single ILP is formulated. Thus, a compromise between computation complexity and performance is desired such that the design can be applied to different network design scenarios. One of the most commonly adopted ideas is to divide the traffic demands into different protection groups. Similar ideas are taken by the $(M:N)^n$ protection architecture [1,2] defined in Generalized Multi-Protocol Label Switching (GMPLS) standard signaling protocol, where the network contains n protection groups each supporting N working paths protected by M protection paths. The advantages of grouping network demands are numerous which includes the improvement of scalability in computation and signaling efforts, the easy manipulation of QoS and survivability metrics, and less dissemination of link-state in case a distributed control is taken [1,2].

A short review is conducted as follows on the recently reported survivable routing schemes. Without considering grouping, work on path shared protection has been extensively reported in the past few years [6,10-21]. The study in [11] formulates the resource allocation problem into a single ILP, which imposes a constraint that every S-D pair can only issue traffic flows along a pre-defined physical route to minimize the computation complexity. Even so, the solving of the ILP formulation may still be subject to scalability problems as the network size grows. In [21], the study addresses the routing and wavelength-assignment problem in a network with path protection under duct-layer constraints, where off-line algorithms for static traffic are developed to combat single-duct failures. The authors divided the whole ILP formulation into separate routing and wavelength assignment problems and solved them by using an ILP solver and heuristics. One of the key issues worth mentioning is that the dividing of the ILP can bear little physical meanings in terms of QoS and survivability requirements in a practical network. The study in [18] addresses the problem that the logical topology (determined by the connection requests) is mapped to the physical topology such that a single failure

would not disconnect the network. The resultant fact is that every S-D pair can possess at least one link-disjoint path-pair. The problem is formulated into an ILP and is verified by comparing with some other counterpart routing proposals, such as shortest path first and greedy routing schemes. On the other hand, grouping of network resources has been considered in the studies in [1-5,22]. The study in [3] elaborates this idea by grouping working paths with a relatively diverse distribution in the network topology and shows simulation results comparing different grouping policies: Most-diverse, Most-overlapped, and Randomly-distributed. An analysis is given to the performance versus computation complexity. In [5], working paths are grouped such that the optimization is interleaved into multiple sub-processes, each of which is calculated sequentially to reduce the total computation complexity. The studies for specifically designing O-VPNs in optical networks can be seen in [5] and [8] where authors develop ILPs and heuristics to establish lightpaths in the O-VPNs and consider delay as a QoS performance metric. However, these works do not address the survivability requirements. To our knowledge, the survivability issue in the design of networks with O-VPNs has never been addressed.

Based on the idea of grouping traffic demands, in this paper we propose two ILP models, namely ILP-I and ILP-II, which provide a solution to the allocation of working and spare capacity for multiple O-VPNs. ILP-I optimizes the task of resource allocation by taking each O-VPN as a protection group, while the ILP-II breaks down each O-VPN into multiple small protection groups where all the working paths in each protection group are mutually link-disjointedly routed. To our knowledge, there is no reported research considering link-disjointedness of working paths as the grouping policy. This novel grouping policy not only achieves scalability, but also helps balancing the network traffic [22]. In ILP-I, instead of considering all the traffic demands in the optimization, an ILP is developed to optimize the resource allocation in each O-VPN, where sharing of spare resource among different O-VPNs is not allowed so as to reduce the computation complexity and to serve for any possible security reason. The result is derived by solving n ILPs sequentially if there are n O-VPNs in the network. With ILP-II, each O-VPN is further divided into multiple protection groups such that the working paths are link-disjointedly routed in each protection group. The motivation of introducing ILP-II is to overcome the scalability problem that may arise in the ILP-I scheme when the amount of traffic demands in each O-VPN is large such that the ILP-I would be subject to intolerably lengthy computation in solving the ILP formulation. Since the number of working paths that are mutually link-disjoint is limited in a protection group, it is expected that the scalability in ILP-II can be guaranteed. In addition to

load-balancing, the link-disjointedness of working paths in a protection group can further address an upper bound on the number of affected working paths due to a single failure [22]. We will investigate the performance and the computation complexity of each model.

The rest of the paper is organized as follows. Section 2 introduces the proposed ILP-I and ILP-II models. Section 3 shows the experiment results. Section 4 concludes the paper.

2. Proposed Schemes

Let the network be denoted as $G(V,E)$, where V and E are the set of nodes and directional links in the network, respectively. Let G contain n O-VPNs, and the i -th O-VPN support a traffic pattern defined in a traffic matrix T^i given in advance, where $1 \leq i \leq n$. Thus, each O-VPN is modeled as a group of working and protection lightpaths interconnecting a specific group of nodes according to the corresponding traffic matrix. The design objective is to minimize the total number of wavelength channels used for establishing the working and their corresponding protection paths in each O-VPNs for achieving 100% restorability, where the shared protection is adopted in each O-VPN and the single failure scenario is assumed. We also assume that the number of wavelength channels available on each link is limited and sparse wavelength conversion capability is present.

2.1 ILP-I

ILP-I is designed to optimally allocate the working and spare capacity in each O-VPN such that the total number of wavelength channels required for the working and protection paths is minimized. ILP-I follows the $(M:N)^n$ architecture where n represents the number of O-VPNs in the network, each of which has N working paths (i.e. N traffic entries) protected by M protection paths. Suppose n O-VPNs, denoted as O-VPN ^{i} where $i = 1 \dots n$, need to be established on a physical topology $G(V,E)$. With ILP-I, each of the n O-VPNs is considered as an individual protection group in which protection paths may share spare capacity, and the ILP formulation for allocating the working and protection paths in each O-VPN is solved using CPLEX [7].

Let $x_{i,j}^{k,\lambda}$ be a binary variable that takes on a value of 1 if working path k goes through link (i,j) using wavelength λ , and 0 otherwise. Let $y_{i,j}^{k,\lambda}$ indicates whether wavelength λ is used by protection path k on link (i,j) . This binary variable takes on a value of 1, if wavelength is used, 0

otherwise. Let $z_{i,j}^\lambda$ indicates whether wavelength λ is used by any protection path on link (i,j) , which takes on a value of 1 if the wavelength channel is used, and 0 otherwise. ILP-I is formulated as follows:

Minimize:

$$\sum_{i,j} \sum_k \sum_\lambda x_{i,j}^{k,\lambda} + \sum_{i,j} \sum_\lambda z_{i,j}^\lambda \quad (1)$$

Subject to:

$$\sum_j \sum_\lambda x_{i,j}^{k,\lambda} - \sum_i \sum_\lambda x_{i,j}^{k,\lambda} = \begin{cases} 1, & \text{if } i = src \\ -1, & \text{if } i = dst \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

$$\sum_j \sum_\lambda y_{i,j}^{k,\lambda} - \sum_i \sum_\lambda y_{i,j}^{k,\lambda} = \begin{cases} 1, & \text{if } i = src \\ -1, & \text{if } i = dst \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

$$x_{i,j}^{k,\lambda} = \sum_{i'} x_{j,i'}^{k,\lambda}; j \neq src, j \neq dst, j \in W \quad (4)$$

$$y_{i,j}^{k,\lambda} = \sum_{i'} y_{j,i'}^{k,\lambda}; j \neq src, j \neq dst, j \in W \quad (5)$$

$$\sum_k x_{i,j}^{k,\lambda} + y_{i,j}^{k,\lambda} \leq 1; \forall k \quad (6)$$

$$\sum_\lambda x_{i,j}^{k,\lambda} + \sum_\lambda y_{i,j}^{k,\lambda} + \sum_\lambda y_{j,i}^{k,\lambda} \leq 1 \quad (7)$$

$$\sum_k \sum_\lambda x_{i,j}^{k,\lambda} + \sum_k \sum_\lambda y_{i,j}^{k,\lambda} \leq \lambda^{MAX} \quad (8)$$

$$y_{i,j}^{k,\lambda} \leq z_{i,j}^\lambda \quad (9)$$

$$\sum_k \sum_{\lambda'} (y_{i,j}^{k,\lambda} + x_{i',j'}^{k,\lambda'} - 1) \leq 1 \quad (10)$$

Eq. (1) is the target function aiming to establish working-protection path pairs such that the total number of wavelength channels used is minimized by the maximum sharing of protection resource. Eq. (2) and Eq. (3) address the flow conservation constraint (i.e., satisfying traffic demands in the network) for the working and protection paths to ensure the end-to-end connectivity.

Eq. (4) and (5) ensure the wavelength continuity constraint for working and protection path respectively, where W is the set of nodes without wavelength conversion capability. Eq. (6) ensures that a particular wavelength λ on link (i,j) can only be used either by a working path k or by a protection path k or can be shared by protection paths. Eq. (7) ensures that a working path and its corresponding protection path are always link-disjointly routed. Eq. (8) limits the number of wavelength channels available on link (i,j) where λ^{MAX} is a constant. Eq. (9) ensures the maximum sharing of spare capacity among protection paths. Eq. (10) ensures that if a wavelength λ is shared by two or more protection paths on link (i,j) , their corresponding working paths are all link-disjointly routed.

If there are n O-VPNs to be set up over $G(V,E)$, ILP-I would be applied to each of these n O-VPNs sequentially to allocate working and protection resources in a single step. Flowchart in Figure 1 explains this scheme:

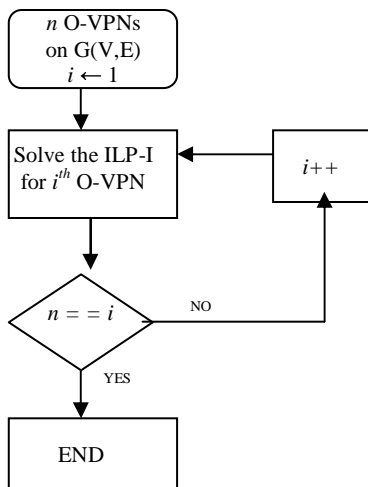


Figure 2. Applying ILP-I scheme on multiple O-VPNs

2.2 ILP-II

The computation time taken by ILP-I is exponentially increased as the number of connections defined in each O-VPN is increased. This section proposed ILP-II for the purposes of achieving a better scalability and load-balancing. Proposed ILP-II framework is based on $(M:N)^n$ architecture, where each of the n protection group has N link-disjoint working paths protected by M protection paths which has the following properties: (a) the number of working paths in each of the n protection groups is link-disjointly routed and thus well constrained; (b) it provides 100% intra-group spare capacity sharing while the inter-group sharing is not allowed to reduce the computation complexity and to serve for any possible security reason. Rather than simply defining each O-VPN

as a protection group, ILP-II allows each of the O-VPNs to be broken down into small protection groups based on the grouping policy, which is the requirement of link-disjointness for all the working paths in a protection group.

ILP-II works in two stages. In stage 1, source-destination pairs in the given traffic matrix are grouped into multiple protection groups. Figure 3 demonstrates the grouping algorithm that takes the traffic entries sequentially from the given traffic matrix and places them into appropriate protection groups.

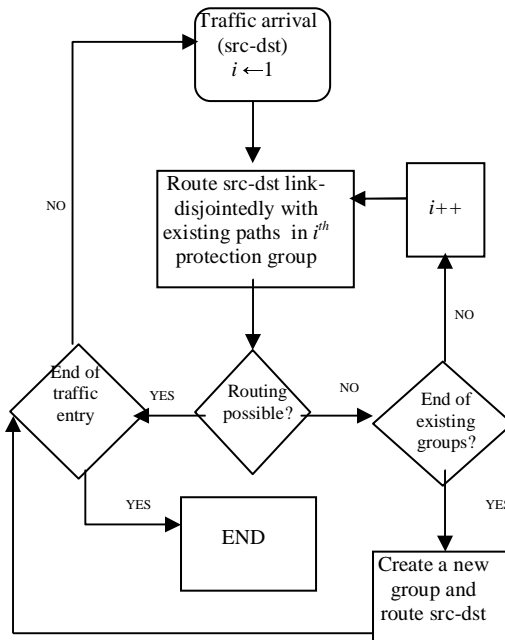


Figure 3. Dividing an O-VPN into multiple protection groups

Using this grouping algorithm, in Figure 4, A-B, A-C, B-D, C-B and D-C traffic can be accommodated in protection group $O-VPN^1_1$. Traffic A-D cannot be placed in the protection group $O-VPN^1_1$ and hence needs to be placed in a new protection group $O-VPN^1_2$. Thus an $O-VPN^1$ can be broken down into small protection groups (i.e., set of src-dst pairs) based on their working paths. Once the protection groups are created, in stage 2, ILP-II is applied to each of these protection groups sequentially to allocate working and protection resources in a single step. Figure 4 shows how $O-VPN^1$ is broken down into two protection groups $O-VPN^1_1$ and $O-VPN^1_2$ where the superscript and subscript represent O-VPN ID and protection group ID respectively.

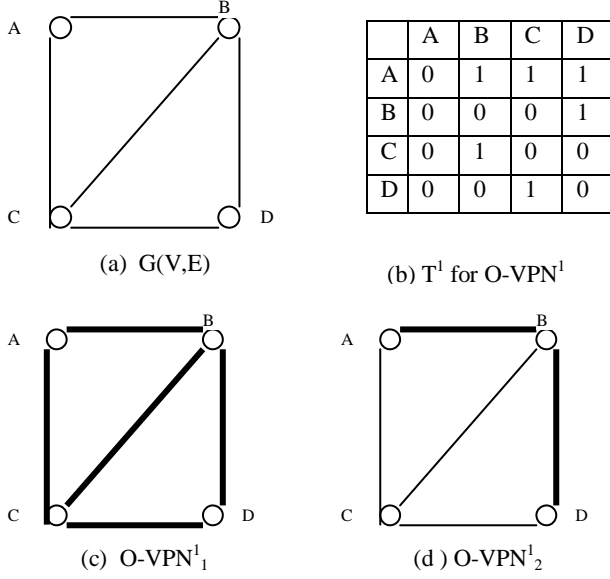


Figure 4. A single O-VPN is broken down into multiple protection groups

To add the link-disjoint constraint for enforcing the working paths to be link-disjointly routed with each other in each protection group, an extra constraint in Eq. (20) is added for ILP-II formulation.

Minimize:

$$\sum_{i,j} \sum_k \sum_{\lambda} x_{i,j}^{k,\lambda} + \sum_{i,j} \sum_{\lambda} z_{i,j}^{\lambda} \quad (11)$$

Subject to:

$$\sum_j \sum_{\lambda} x_{i,j}^{k,\lambda} - \sum_i \sum_{\lambda} x_{i,j}^{k,\lambda} = \begin{cases} 1, & \text{if } i = src \\ -1, & \text{if } i = dst \\ 0, & \text{otherwise} \end{cases} \quad (12)$$

$$\sum_j \sum_{\lambda} y_{i,j}^{k,\lambda} - \sum_i \sum_{\lambda} y_{i,j}^{k,\lambda} = \begin{cases} 1, & \text{if } i = src \\ -1, & \text{if } i = dst \\ 0, & \text{otherwise} \end{cases} \quad (13)$$

$$x_{i,j}^{k,\lambda} = \sum_{i'} x_{j,i'}^{k,\lambda}; j \neq src, j \neq dst, j \in W \quad (14)$$

$$y_{i,j}^{k,\lambda} = \sum_{i'} y_{j,i'}^{k,\lambda}; j \neq src, j \neq dst, j \in W \quad (15)$$

$$\sum_k x_{i,j}^{k,\lambda} + y_{i,j}^{k,\lambda} \leq 1; \forall k \quad (16)$$

$$\sum_{\lambda} x_{i,j}^{k,\lambda} + \sum_{\lambda} y_{i,j}^{k,\lambda} + \sum_{\lambda} y_{j,i}^{k,\lambda} \leq 1 \quad (17)$$

$$\sum_k \sum_{\lambda} x_{i,j}^{k,\lambda} + \sum_k \sum_{\lambda} y_{i,j}^{k,\lambda} \leq \lambda^{MAX} \quad (18)$$

$$y_{i,j}^{k,\lambda} \leq z_{i,j}^{\lambda} \quad (19)$$

$$\sum_k x_{i,j}^{k,\lambda} + \sum_k x_{j,i}^{k,\lambda} \leq 1, \forall (i,j) \quad (20)$$

Eq. (20) in the above formulation is a constraint ensuring the link-disjointness of all the working paths in a protection group. Flowchart in Figure 5 explains ILP-II scheme.

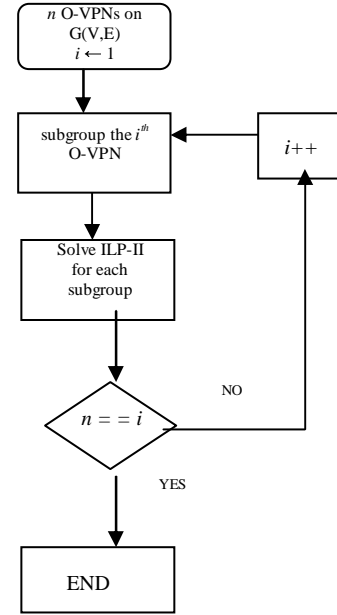


Figure 5. Applying ILP-II scheme on multiple O-VPNs

3. Results and Discussions

The simulation is conducted on 8 different mesh networks [11,13] as shown in Figure 6, which are chosen as representatives of typical mesh topologies. CPLEX linear optimizer [7] is used to solve ILP-I and ILP-II, running on a SUN Ultra Enterprise server. The performance metrics taken in this study are the total number of wavelengths taken by working and protection paths and the computation time. The following assumptions are made in simulation: (a) without loss of

generality, every connection request is a single lightpath that occupies a wavelength channel as traversing through the corresponding links; (b) since the objective of this study is to compare the performance of ILP-I and ILP-II in terms of capacity utilization and computational complexity, some constraints in ILP-I and ILP-II are relaxed to avoid the connection blocking. This relaxation includes keeping the number of wavelength channels along each link very high and assuming that each link has a full wavelength conversion capacity; (c) the traffic demand (i.e., source-destination nodes of the connections) in each O-VPN follows a uniform distribution; (d) each node can serve as an ingress or egress node of the network. Dijkstra's shortest path algorithm (in terms of hop counts) is adopted as a routing scheme in implementing a grouping algorithm and implementing a dedicated protection. A dedicated protection is implemented for the purpose of comparison.

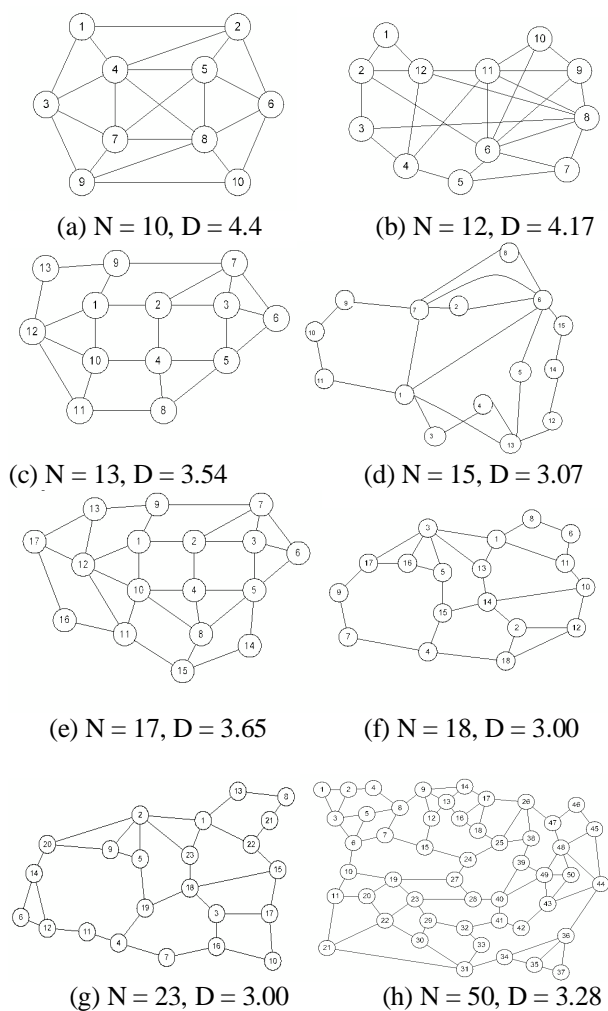


Figure 6. The 8 network topologies adopted in the simulation [11,13].

We classify whether an O-VPN is small, medium or large based on the number of connections it requires. For each of the 8 network topologies, three traffic matrices with different number of connections (25, 50, and 100 which correspond to small (S), medium (M), and large (L) O-VPN respectively) were generated following a uniform distribution, as listed in Table 1.

Table 1. Small, medium and large O-VPNs

VPN Type	Number of Connections
SMALL (S)	25
MEDIUM (M)	50
LARGE (L)	100

Table 2 shows the number of wavelength channels used by ILP-I and ILP-II for 8 different topologies. Table 3 provides the computation time (in seconds) taken by ILP-I and ILP-II for solving the cases with small, medium, and large O-VPNs on the 8 network topologies. Table 4 provides the total number of wavelengths used by ILP-I, ILP-II, and Dedicated Protection (DP) schemes and total computation time taken by ILP-I and ILP-II. From Table 4, it is clear that ILP-I and ILP-II required (53-60)% and (20-32)% less resources than of those taken by a dedicated protection, respectively, and that ILP-I outperforms ILP-II by (22-39)% in terms of the number of wavelength channels.

Table 2. Number of wavelengths used by ILP-I and ILP-II

N	Degree (D)	ILP-I (number of wavelengths)			ILP-II (number of wavelengths)		
		S	M	L	S	M	L
10	4.4	5	81	169	72	123	254
12	4.17	5	93	188	91	148	317
13	3.54	6	110	221	97	174	364
15	3.07	6	133	261	128	259	524
17	3.65	7	149	253	89	237	410
18	3.00	7	163	286	115	279	538
23	3.00	1	192	360	172	350	680
50	3.28	-	-	-	244	444	863

Table 3. Computation time for ILP-I and ILP-II

N	Degree (D)	ILP-I (seconds)			ILP-II (seconds)		
		S	M	L	S	M	L
10	4.4	86	280	352	65	831	1163
12	4.17	81	461	487	183	695	774
13	3.54	31	257	332	26	31	337
15	3.07	1	1	1	1	2	3
17	3.65	2861	2986	3172	80	227	513
18	3.00	55	58	72	19	35	208
23	3.00	26	27	37	13	21	57
50	3.28	-	-	-	235	1303	6481

Table 4. Total number of wavelengths and total computation time

N	Degree (D)	Total number of wavelengths			Total computation time (seconds)	
		ILP-I	ILP-II	DP	ILP-I	ILP-II
10	4.4	302	449	656	718	2059
12	4.17	340	556	738	1029	1652
13	3.54	394	635	855	620	394
15	3.07	462	911	115	3	6
17	3.65	472	736	100	9019	820
18	3.00	519	932	117	185	262
23	3.00	653	1202	149	90	91
50	3.28	-	1551	195	-	8019

The computation time for completing the task of resource allocation in each protection group using ILP-I and ILP-II varies according to the size of traffic demands in each protection group. From Table 3, it can be seen that no result can be obtained for the 50-node network with ILP-I in 10 hours. In all the other cases, ILP-I took approximately (0.02 – 48), (0.02 – 50), and (0.02 – 53) minutes for small, medium, and large O-VPNs, respectively. On the other hand, ILP-II took approximately (0.02 – 3), (0.03 – 14), and (0.05 – 19) minutes for network with small, medium, and large O-VPNs, respectively. ILP-II solved the case with the 50-node network with reasonable time while ILP-I failed to provide any result in 10 hours. It was also observed that the nodal degree of the network topology plays an important role on the computational complexity in solving the ILPs.

4. Conclusions

In this paper, we introduced a novel approach of resource allocation for static connection demand in survivable optical networks supporting Virtual Private Networks (VPNs). Based on the $(M:N)^n$ protection architecture defined in Generalized Multi-Protocol Label Switching (GMPLS), we formulate the off-line O-VPN survivability design problem into two Integer Linear Programming (ILP) models, namely ILP-I and ILP-II. The objective for our design is to initiate a graceful compromise between capacity-efficiency and computation complexity without losing the ability of addressing the QoS requirements of each O-VPN. ILP-I considers each O-VPN as a protection group and performs resource allocation according to the traffic matrix defined in each O-VPN separately. With ILP-II, on the other hand, each O-VPN is broken down into small protection groups where all the working lightpaths in a group are mutually link-disjointedly routed. Simulation was conducted on 8 mesh

topologies with different sizes of O-VPNs to examine ILP-I and ILP-II schemes. From the simulation results it was observed that ILP-I required (53-60)% less resources than a dedicated protection and ILP-I outperforms ILP-II by (22-39)% in terms of capacity usage. We also verified the scalability issue by addressing the time complexity for ILP-I and ILP-II, and found that the two schemes required similar computation time when the network size was small. However, ILP-II with a constant-sized grouping policy was seen more scalable when the network size and the amount of traffic demand were increasing. It is interesting to note that the nodal degree (i.e. number of links in the network) rather than the number of nodes has addressed a significant impact on the time complexity in solving the resource allocation problem with CPLEX. We conclude that ILP-I is a good candidate for providing survivability for O-VPNs when the size of the network and traffic demands of the VPNs are not very large. When the scalability issue and load balancing are concerned, ILP-II that requires the link-disjointedness with a fix-sized grouping policy would be a more effective approach.

5. References

- [1] D. Papadimitriou, E. Mannie, D. Brungard, S. Dharanikota, J. Lang, G. Li, B. Rajagopalan, and Y. Rekhter, "Analysis of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration)", *Internet Draft*, <draft-papadimitriou-ccamp-gmpls-recovery-analysis-03.txt>, working in progress, May 2003.
- [2] K. Sriram, D. Griffith, S. Lee, and N. Golmie, "Backup Resource Pooling in $(M:N)^n$ Fault Recovery Schemes in GMPLS Optical Networks", *Opticomm 2003*.
- [3] P. -H. Ho and H. T. Mouftah, "Reconfiguration of Spare Capacity for MPLS-based Recovery in the Internet Backbone Networks", *IEEE/ACM Transaction on Networking*, Vol. 12, No. 1, Feb. 2004.
- [4] P. -H. Ho and H. T. Mouftah, "A Framework of a Survivable Optical Internet using Short Leap Shared Protection (SLSP)", *IEEE Workshop on High Performance Switching and Routing (HPSR 2001)*, Dallas, May, 2001.
- [5] B. Ramamurthy and A. Ramakrishnan, "Design of Virtual Private Networks (VPNs) over Optical Wavelength Division Multiplexed (WDM) Networks", *SPIE Optical Networks Magazine*, Vol. 3, Issue 1, Jan./Feb. 2002.
- [6] P. -H. Ho and H. T. Mouftah, "On Optimal Diverse Routing for Shared Protection in Mesh WDM Networks", *IEEE Transactions on Reliability (to appear in March 2004)*.
- [7] CPLEX: An optimizer by ILOG Inc, url : www.ilog.com
- [8] Yang Qin, K. M. Sivalingam and Bo Li, "QoS for Virtual Private Networks (VPN) over Optical WDM Networks", *Optical Communications and Networking Conference*, (Dallas, TX), Oct. 2000.
- [9] M. W. Murhammer et. al, "A Guide to Virtual Private

- Networks”, Prentice Hall PTR, New Jersey, U.S.A, 1998
- [10] D. Xu, C. Qiao, and Y Xiong, “An Ultra-fast Shared Path Protection Scheme -- Distributed Partial Information Management, Part II”, *Proceedings IEEE International Conference on Network Protocols (ICNP 2002)*, Paris, France, Nov. 2002.
 - [11] Y. Liu, D. Tipper, and P. Siripongwutikorn, “Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing”, *Proceedings IEEE Infocom*, vol. 2, pp. 699-708, April 2001.
 - [12] D. Xu, Y. Xiong, and C. Qiao, “Protection with Multi-Segments (PROMISE) in Networks with Shared Risk Link Groups (SRLG)”, in *the 40th Annual Allerton Conference on Communication, Control, and Computing*, 2002.
 - [13] S. Ramamuthy and B. Mukherjee, "Survivable WDM mesh networks: Part I--Protection," *Infocom'99*, New York, Mar. 1999.
 - [14] K. Steigkitz, P. Weiner, and D. J. Kleitman, “The Design of Minimum-cost Survivable Networks”, *IEEE Transaction on Circuit Theory*, vol. 16, no. 4, pp. 445-460.
 - [15] B. V. Caenegem, W. V. Parys, F. D. Turck, and P. M. Demeester, "Dimensioning of Survivable WDM Networks", *IEEE Journal on Selected Areas in Communications (JSAC)*, no. 7, Sept. 1998, pp. 1146-1157.
 - [16] W. B. Ameur, “Constrained Length Connectivity and Survivable Networks”, *Networks*, vol. 36. no. 1, pp. 17-33.
 - [17] Y. Myung, H. Kim and D. Tcha, “Design of Communication Networks with Survivability Constraints”, *Management Science*, vol. 45, no. 2, pp. 238-252.
 - [18] E. Midiano and A. Narula-Tam, “Survivable Lightpath Routing: A New Approach to the Design of WDM-Based Networks”, *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 20, no. 4, May 2002, pp. 800-809.
 - [19] B. Zhou and H. T. Mouftah, “Spare Capacity Planning Using Survivable Alternate Routing for Long Haul WDM Networks”, *Proceedings of the Seventh IEEE International Symposium on Computers and Communications (ISCC 2002)*.
 - [20] R. R. Iraschko and W. D. Grover, “A Highly Efficient Path-Restoration Protocol for Management of Optical Network Transport Integrity”, *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 18, no. 5, May 2000, pp. 779-793.
 - [21] H. Zang, C. Qu, B. Mukherjee, "Path-Protection Routing and Wavelength Assignment (RWA) in WDM Mesh Networks Under Duct-Layer Constraints," *IEEE/ACM Transactions on Networking*, vol. 11, no. 2, April 2003.
 - [22] Anwar Haque, Pin-Han Ho, Raouf Boutaba, and James Ho, “Group Shared Protection (GSP): A Scalable Solution for Spare Capacity Reconfiguration in Mesh WDM Networks”, To appear in proceedings of the 47th IEEE Global Telecommunications Conference (Globecom 2004), Dallas, TX, November 2004