2004

Survivable Traffic Grooming with Path Protection at the Connection Level in WDM Mesh Networks

Wang Yao
University of Nebraska-Lincoln, wyao@cse.unl.edu

Byrav Ramamurthy
University of Nebraska-Lincoln, bramamurthy2@unl.edu

Proceedings. First International Conference on Broadband Networks, 2004. BroadNets 2004.
Digital Object Identifier: 10.1109/BROADNETS.2004.80
Publication Year: 2004 , Page(s): 310 - 319

Survivable Traffic Grooming with Path Protection at the Connection Level in WDM Mesh Networks

Wang Yao and Byrav Ramamurthy
Department of Computer Science and Engineering
University of Nebraska-Lincoln
E-mail: {wyao,byrav}@cse.unl.edu

Abstract

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. In this paper, we 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 the 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, we consider the general shared risk link group (SRLG) diverse routing constraints. We first resort to the integer linear programming (ILP) approach to obtain optimal solutions. To address its high computational complexity, we then propose three efficient heuristics, namely separated survivable grooming algorithm (SSGA), integrated survivable grooming algorithm (ISGA) and tabu search survivable grooming algorithm (TSGA). 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 method. Numerical results show that the heuristics achieve comparable solutions to the ILP approach, which uses significantly longer running times than the heuristics.

1. Introduction

The rapid increase of the Internet demands large volumes of bandwidth. Wavelength division multiplexing (WDM) technology has the potential to meet this need by allowing simultaneous transmission of traffic on multiple wavelengths in a fiber. A wavelength-routed network (WRN) based on WDM technology is deemed as a promising candidate for the core network of the next-generation Internet.

Traffic grooming addresses the gap between the bandwidth capacity of wavelengths and the bandwidth requirement of connections. With the improvement of optical technology, the capacity of a single wavelength reaches OC-192 (10Gbps). On the other hand, the bandwidth of a connection request (such as SONET circuits, IP/MPLS label switched paths) may be less than that, possibly OC-3 (155Mbps) or even lower. To make efficient use of the wavelength bandwidth, traffic grooming [1][2] is needed to pack connections at sub-wavelength granularities effectively onto wavelength channels.

Fault recovery capability is critical for optical networks, as a single failure may affect a large volume of traffic. There are generally two types of fault recovery mechanisms, namely protection [3] and restoration [4]. Protection aims at extremely fast recovery. The backup connection is established before the failure. Restoration, on the other hand, dynamically establishes a connection to recover from a failure after the failure occurs. Restoration, although relatively slow, uses less resource than protection. Note that irrespective of whether protection or restoration is used, spare capacity needs to be preplanned in order to provide survivability in optical networks.

Survivable traffic grooming (STG) addresses the provisioning and survivability of multi-granularity connections together in the optical networks with grooming capability. It seeks to provide fault recovery capability for connections and minimize the consumption of spare capacities in the network. With the network service providers facing the pressure of generating revenues by providing reliable multi-granularity connection services and reducing network operation cost, we anticipate that STG will play an important role in the future optical networks.

Protection is classified into link protection and path protection. In the two-layered grooming network, path protection can be applied at two different levels, namely protection at lightpath (PAL) and protection at connection (PAC) [5]. PAL is a coarse-granularity protection scheme operating at aggregate (lightpath) level and PAC is a fine-granularity protection scheme operating at per-flow (connection) level. On the other hand, PAL and PAC can be viewed as a segment protection scheme and an end-to-end path protection scheme respectively, because a lightpath is a concatenation of wavelength links and a connection is a concatenation of lightpaths. Comparing the two protection schemes, PAL is generally simpler in signaling due to its coarse-granularity nature. PAL also has relatively shorter fault recovery time because of its relatively short span. PAC, on the other hand, is more resource-efficient and flexible due to its fine-granularity nature. Moreover, as an end-to-end protection scheme, PAC may be good at preserving constraints imposed on individual connections, such as Quality of Service (QoS) constraints, traffic engineering (TE) constraints. In this paper, we focus on path protection at the connection level. We refer the interested readers to our earlier work [21] for the STG problem with protection at the lightpath level.

Protection schemes are further divided into dedicated protection and shared protection schemes depending on whether resources can be shared among backup paths or not. In dedicated protection, traffic is transmitted simultaneously over two disjoint paths and a switch is used at the receiving node to choose the better signal. In shared protection, the traffic is transmitted over the primary path at normal operation time and the backup paths can share common resources only if their primary paths are node (or link) disjoint. Shared protection offers better resource utilization at the cost of a longer recovery time.

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 primary path. Shared risk link group (SRLG) [6] is a set of links that share a common resource (risk) whose failure affects all the links in the set. In practice, the risk can be an optical cross-connect (OXC) node, a fiber or a duct. For example, if the risk is a duct, then all the fiber links buried into this duct belong to a SRLG corresponding to the duct.

To make the connections survivable after various failure scenarios such as fiber cut and duct cut, it is necessary to consider SRLG diverse routing constraints in the traffic grooming problem. The SRLG diverse routing constraint is more general than link-disjoint or node-disjoint constraints. It stipulates that the primary path and backup path of a connection must be risk-disjoint paths to guarantee survivability. In addition, for the shared path protection scheme, the backup paths can share resources only if their primary paths are risk-disjoint.

The static traffic grooming problem without considering survivability has been studied in [1]. An integer linear programming (ILP) formulation was presented to maximize network throughput when a fixed traffic pattern is given. Two heuristics maximizing single-hop traffic (MST) and maximizing resource utilization (MRU) were proposed to solve the problem efficiently.

The works in [9] and [10] considered the static routing and wavelength assignment problem with path protection in WDM mesh networks without grooming capability. The work in [9] considered the duct-layer constraints, a special case of the general SRLG constraints. Several ILP formulations and a heuristic algorithm were proposed to minimize the total number of wavelengths used on all the links in the network. The heuristic consists of three stages: compute a pair of duct-disjoint paths, assign wavelengths for the path pair and apply iterative optimization procedure to reduce the total number of wavelength links. The work in [10] considered the general SRLG constraints and models the survivable RWA problem as a revenue maximization problem and a capacity minimization problem. Besides the ILP formulations, a greedy heuristic and a tabu search heuristic were proposed.

Although traffic grooming and survivability are important issues for optical networks and have been studied extensively in the past decade, STG remains a relatively unexplored issue, only gaining attention recently. The work in [11] focused on the survivable grooming policies as to whether primary connections and backup connections should be groomed on the same lightpath. The work in [5] compared PAL and PAC in the WDM mesh grooming networks. Online heuristics were proposed to provision dynamically arriving connections. The work in [12] presented an ILP formulation of the STG problem to minimize the total number of wavelength links in WDM optical networks with path protection. In [5][11][12], either node or link disjoint constraints were considered to solve the STG problem.

In this work, we study the static STG problem under the SRLG constraints with the objective to maximize network throughput (or revenue). The generalized SRLG constraints subsume the node and link disjoint constraints considered in the earlier work within a single ILP formulation. In addition to the exact ILP solution approach, we propose three efficient heuristic grooming algorithms: separated survivable grooming algorithm (SSGA), integrated survivable grooming algorithm (ISGA) and tabu-search survivable grooming algorithm (TSGA). Both dedicated and shared path protection at the connection level are considered. Our work differs from previous work not only in that we consider the general SRLG constraints for multi-granularity subwavelength connections in the STG context, but also in that we design the grooming heuristics from the network architectural point of view. SSGA and ISGA are based on an overlay model and a peer model respectively. As both the overlay model and the peer model are two candidate deployment models for future optical WDM networks with grooming capability, SSGA and ISGA can compare the two models from the perspective of grooming algorithms. TSGA further improves the grooming results from SSGA and ISGA by incorporating an effective tabu search [18] method.

The rest of the paper is organized as follows. Section 2 formally states the STG problem under the SRLG constraints. Section 3 presents the two greedy heuristic grooming algorithms, SSGA and ISGA. Section 4 presents the tabu search based grooming algorithm TSGA. Section 5 presents numerical results from the ILPs, and the SSGA, ISGA, TSGA heuristics. Section 6 concludes the paper.

2. Problem Definition and Formulations

In WRNs, the physical topology is a set of OXC nodes connected by fiber links. A wavelength path is referred to as a lightpath, which may span several fiber links in the physical topology. A lightpath uses a wavelength on each fiber link along its path. All the lightpaths form the virtual topology. The multi-granularity connections are carried over the virtual topology. A connection may traverse several lightpaths along its path and takes a portion of the bandwidth of each lightpath it uses. Fig. 1 illustrates two lightpaths and a connection in a SONET over WDM optical network. Note that a lightpath uses a transmitter at the source node and uses a receiver at the destination node. Also, a connection must originate and end in the electronic domain, which is digital cross-connect (DXC) in this case. In IP over WDM networks, the DXCs in Fig. 1 are replaced with IP/MPLS routers.

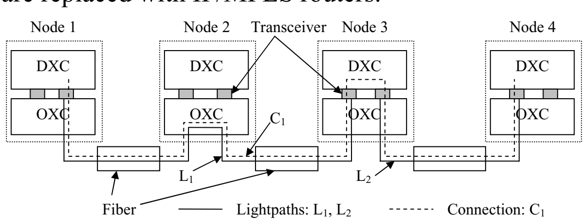


Fig. 1. Illustration of lightpaths and a connection in traffic grooming. Lightpath L_1 traverses fiber link (1,2) and (2,3), lightpath L_2 traverses fiber link (3,4), and connection C_1 uses a two-hop path using lightpaths L_1 and L_2.

The STG problem in WRNs under the SRLG constraints can be formally stated as follows. We assume the protection is provided at the connection level, that is, each connection has a primary path and a backup path.

- **Given**:

1). Physical topology represented as a unidirectional graph $G_p = (V_p, E_p)$, where V_p is a set of network nodes and $E_p \subset V_p \times V_p$ is the set of fiber links connecting the nodes. The number of nodes is $N = |V_p|$.

2). The set of wavelengths supported by each fiber is *W* and the capacity of each wavelength is *C*. We assume that the same set of wavelengths is deployed on every link. The capacity of a wavelength is normalized to an integer *C* (called the grooming factor) based on the smallest grooming granularity in the network. For example, if one wavelength supports an *OC*-48 channel, and the smallest grooming granularity is *OC*-3, then *C* equals 48/3=16.

3). The number of transmitter and receiver pairs at each node is Δ_i for $1 \le i \le N$. In this study, we assume the transceivers are tunable to any wavelength operating on the fiber.

4). Connection requests, represented as a set of $N \times N$ traffic matrices $\Lambda^x (x \in X)$. where X is the set of low-speed connection granularities. For example, *X*={1, 4, 16}. $\Lambda^x_{s,d}$ represents the number of connection requests of *OC-x* granularity from nodes *s* to *d*.

5). SRLG information, represented as a set of SRLGs. Each SRLG is identified by a risk number *r* and comprises of all the links affected by the risk.

- **Constraints**:

1). Resource Constraints: To establish a lightpath over a path, there must have at least one wavelength available on each of the links in the path. Besides, there must have at least one free transmitter and one free receiver at the source node and destination node of the path respectively.

2). Wavelength Continuity Constraint: We assume no wavelength conversion capability in the network. Therefore, a lightpath must use the same wavelength on all links in its path.

3). Diverse Routing constraints: The primary path and backup path of a connection must not share a common risk in the physical topology.

4). Lightpath Capacity Constraint: The total bandwidth of all the connections carried over a lightpath must not be larger than the bandwidth of a lightpath. Notice that backup connections may share bandwidth if shared protection is used. Actually, one focus of shared protection at connection level is to maximize bandwidth sharing without breaking the lightpath capacity constraints.

- **Objective:**

The objective is to establish a virtual topology over the physical topology and maximize the network throughput by effectively routing the connection over the virtual topology. The virtual topology can be represented as a unidirectional graph $G_v = (V_v, E_v)$, where $V_v = V_p$ and $E_v \subset V_v \times V_v$ is the set of lightpaths established over the physical topology G_p.

We formulate the above STG problem as two ILP problems, one for dedicated protection and the other for shared protection. Due to the page limit, the ILP formulations are not presented here (can be found in [22]). However, we will present the results of the ILP formulations in section 5.

3. Greedy Grooming Heuristics

The static RWA problem is a well-known NP-complete problem. The traffic grooming problem is also NP-complete, as RWA is a special case of the traffic grooming problem. By forcing each connection requesting the whole capacity of a lightpath and only allowing connections to travel one hop (lightpath), the traffic grooming problem can be transformed into a RWA problem. The work in [7] and [8] proved that finding two SRLG-diverse paths between a node pair is NP-complete. Therefore, it is easy to see that the STG problem subject to the SRLG constraints is NP-hard. To efficiently solve a NP-hard problem, heuristics are needed.

Operationally, the two layers involved in the traffic grooming can be managed separately or jointly, corresponding to an overlay or a peer deployment model respectively. Depending on the deployment models, there are generally two approaches to address the traffic grooming problem. For the overlay model, the routing decisions in the two layers are considered independently. Each layer has its own routing algorithms. For the peer model, an integrated grooming algorithm is needed in the control plane to provision both lightpaths and connections.

Corresponding to the two approaches, we propose two grooming algorithms, namely separate survivable grooming algorithm (SSGA) and integrated survivable grooming algorithm (ISGA).

3.1. Separate Survivable Grooming Algorithm (SSGA)

With SSGA, the STG problem is divided into two subproblems. One is protection aware virtual topology design (PAVTD) problem, which is to establish a virtual topology over the physical topology. The other one is subwavelength connection survivable routing (SWCSR) problem, which is to pack the subwavelength connections on the lightpaths in the virtual topology, with each connection having a primary path and a backup path.

Virtual topology design (VTD) problem has been studied extensively in the previous studies [13]-[15]. However, unlike the VTD problem studied in the previous studies, where a single traffic pattern matrix specifies the estimated traffic bandwidth needed between each node pair, the PAVTD problem designs a virtual topology to carry connection-oriented subwavelength channels in multiple granularities, which are specified in multiple matrices. Moreover, in the PAVTD problem, the virtual topology is designed to carry connections that are protected. Therefore, spare capacity needs to be planned in the virtual topology to support survivable routing of connections.

To solve the PAVTD problem, we propose the maximizing single-hop traffic (MSHT-PAVTD) heuristic grooming algorithm which tries to establish lightpaths between node pairs having the largest amounts of traffic. Fig. 2 shows the general procedure of the PAVTD heuristic. In MSHT-PAVTD, TTD-RDJP (see next section) is a proposed algorithm to find two risk-disjoint paths and DIJKSTRA is Dijkstra's algorithm to find the shortest path.

The MSHT-PAVTD heuristic requires a risk-disjoint path selection algorithm. Suurballe's algorithm is a well-known algorithm to find edge or node disjoint paths with minimum cost. However, Suurballe's algorithm cannot be used to find risk-disjoint paths. The work in [16]-[17] tries to find a pair of risk-disjoint paths with the least cost. We propose the two times Dijkstra's risk-disjoint path (TTD-RDJP) selection algorithm based on a three-step algorithm proposed in [16].

Algorithm MSHT-PAVTD

Input: Connection requests $\Lambda^x (x \in X)$, physical topology G_p, wavelength and transceivers, and *SRLG* information.
Output: A virtual topology G_v.

1) Sum the traffic matrix set to form a single residual traffic matrix Λ^*, where $\Lambda^*_{s,d} = \sum_{x \in X} (\Lambda^x_{s,d} \times x)$ represents the total bandwidth needed from node s to d.

2) **while** (not all the elements of Λ^* are zero)
    Select the node pair (s', d') with the maximum residual bandwidth in matrix Λ^*. Ties are broken arbitrarily.
    if (dedicated protection)
        if (TTD-RDJP(G_p, s', d', p_1, p_2))
            Establish two lightpaths from s' to d' on risk-disjoint paths p_1 and p_2.
        $\Lambda^*_{s,d} \leftarrow \Lambda^*_{s,d} - C$.
    else if (shared protection)
        if (DIJKSTRA(G_p, s', d', p))
            Establish a lightpath from s' to d' on path p.
        $\Lambda^*_{s,d} \leftarrow \Lambda^*_{s,d} - C/2$.

Fig. 2. The MSHT-PAVTD algorithm.

Algorithm TTD-RDJP(G, s, d, p, b)

Input: Source node s, destination node d, topology G, usage of wavelengths and transceivers, and *SRLG* information.
Output: Risk-disjoint paths p and b, if successful; return NULL, otherwise.
1) Update the link weights of G according to the current state of the network, and run Dijkstra's algorithm to select the shortest path as path p.
2) **if** (p)
    Delete any link in G that share at least one risk with the any link in p.
    if (shared protection)
        Update the link weights of G again according to the current state of the network and the path p.
    Run Dijkstra's algorithm again on G to select the shortest path as the path b.
    if (b)
        return (p, b).
3) **return** NULL.

Fig. 3. The TTD-RDJP algorithm.

Algorithm LTF-SWCSR

Input: Connection requests $\Lambda^x(x\in X)$, virtual topology G_v, and *SRLG* information.
1) Sort all the connection requests in a list Q in non-increasing traffic amount order.
2) **while** (the list Q is not empty)
    Get and remove the connection request (s, d, x, y) from the head of Q.
    if (TTD-RDJP(G_v, s, d, p_1, p_2))
        if (dedicated protection)
            Establish a primary connection and a backup connection from s to d on risk-disjoint paths p_1 and p_2 respectively.
        else if (shared protection)
            Establish a connection from s to d on path p_1 and reserve bandwidth on path p_2.
    else
        Block the connection request (s, d, x, y).

Fig. 4. The LTF-SWCSR algorithm.

The SWCSR problem needs to find two risk-disjoint paths in the virtual topology for each connection to serve as primary path and backup path respectively. As the SRLG information is originally defined for fiber links in the physical topology, SWCSR needs to derive the SRLG information for lightpaths in the virtual topology.

Let $R_l(m,n)=\{r:(m,n)\in r\}$ be the set of risks a link (m,n) subject to and $R_p(i,j)$ be the set of risks a lightpath (i,j) subject to. Then $R_p(i,j)$ is the union of the risk sets of the fiber links it uses, as shown in (1).

$$R_p(i,j)=\bigcup_{(m,n)\in(i,j)}R_l(m,n)\,. \tag{1}$$

We propose the large traffic first (LTF-SWCSR) algorithm to solve the SWCSR problem. The LTF-SWCSR algorithm also uses the TTD-RDJP algorithm in Fig. 3. Note that MSHT-PAVTD uses TTD-RDJP to find risk-disjoint paths in the physical topology for lightpaths, while LTF-SWCSR uses TTD-RDJP to find risk-disjoint paths in the virtual topology for connections.

TTD-RDJP is an adaptive algorithm in that it updates the link weights of the network according to the current network state. Equation (2) defines the link weight function $C_p(i,j)$ for a lightpath (i,j). $C_p(i,j)$ is used as a lightpath metric while searching for primary paths of connections.

$$C_p(i,j)=\begin{cases}\sum_{(m,n)\in(i,j)} l_{m,n} & \text{if } B_a(i,j)\ge B_r\\ \infty & \text{otherwise}\end{cases}, \tag{2}$$

where B_r is the bandwidth requirement of the connection, $B_a(i,j)$ is the free bandwidth on the lightpath (i,j).

When shared protection scheme is used, backup connections can share bandwidth within a lightpath if their primary connections are risk-disjoint. Generally, we can evenly divide the bandwidth of a lightpath into C channels. Each channel has a bandwidth equal to the smallest the grooming granularity. Depending on the usage, the channels can be classified into three categories, namely dedicated, spare and free channels (see Fig. 5). A channel is dedicated if it is assigned to a primary connection. A channel is a spare channel if it is assigned to a backup connection. The channels not assigned to any connections are free channels. When a primary connection p is specified, a spare channel c can be further classified as a sharable spare channel or a non-sharable spare channel depending on whether p is risk-disjoint with all the primary connections whose backup connections share the spare channel c. If they are risk-disjoint, then c is sharable to p; otherwise, c is not sharable to p. Note that for the dedicated protection scheme, all spare channels are not sharable.

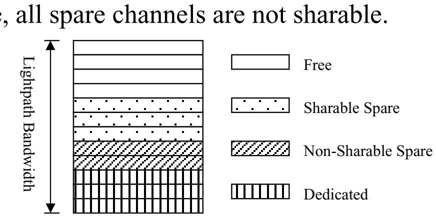


Fig. 5. Classification of channels within a lightpath.

To fully exploit the backup bandwidth sharing to reduce spare capacity consumption, a different link weight function is defined for lightpaths while searching for backup paths of connections. As shown in (3), the backup lightpath weight $C_b(i,j,p)$ also depends on the primary connection p. With (3), the grooming algorithm tries to assign as many sharable spare channels to a backup connection as possible. Only if the amount of sharable spare channels is not enough, does it assign free channels to the backup connection.

$$C_b(i,j,p)=\begin{cases}\alpha\times\sum_{(m,n)\in(i,j)} l_{m,n} & \text{if } B_s(i,j,p)\ge B_r\\ (\beta+\alpha(1-\beta))\sum_{(m,n)\in(i,j)} l_{m,n} & \text{if } B_s(i,j,p)+B_a(i,j)\ge B_r \text{ and } B_s(i,j,p)<B_r\\ \infty & \text{otherwise}\end{cases},(3)$$

where $B_s(i,j,p)$ is the amount of sharable spare bandwidth on the lightpath (i,j) with respect to the primary connection p, $\beta=1-B_s(i,j,p)/B_r$ is the ratio of the newly reserved bandwidth ($B_r-B_s(i,j,p)$) to the bandwidth requirement (B_r), α ($0<\alpha<1$) is a parameter to weight sharable bandwidth. By making α a number smaller than 1, we encourage the grooming algorithm to choose paths using sharable channels instead of free channels. On the other hand, α should not be set too small to avoid using too many sharable channels unnecessarily. Note that for dedicated protection, $B_s(i,j,p)\equiv 0$ regardless of the primary connection p, because all spare bandwidths are not sharable.

3.2. Integrated Survivable Grooming Algorithm (ISGA)

In ISGA, the provisioning of the lightpaths and connections are considered jointly. The objective is to accommodate as many connections as possible. New lightpaths are established to carry connections only when necessary. It is possible to establish a connection using only existing lightpaths or using a combination of existing and new lightpaths.

ISGA is based on a link bundled auxiliary graph (LBAG) [19]. In LBAG model, the auxiliary graph is constructed as a two-layered graph. The two layers are called the physical layer and the lightpath layer respectively. For each node in the network, there are two nodes, one in each layer, in the auxiliary graph. The two nodes are called the physical node and the virtual node respectively.

There are three categories of edges in an LBAG. The edges in the physical layer are wavelength edges representing the wavelength links in the physical topology. The edges in the lightpath layer are lightpath edges representing the lightpaths in the virtual topology. The edges between the lightpath layer and the physical layer are transceiver edges representing the transceiver resources. Specifically, an edge from the lightpath layer to the physical layer is a transmitter edge and an edge from the physical layer to the lightpath layer is a receiver edge. Fig. 6 shows an example of an LBAG. Note that no lightpath edge exists in Fig. 6 (b) because no lightpath has been established.

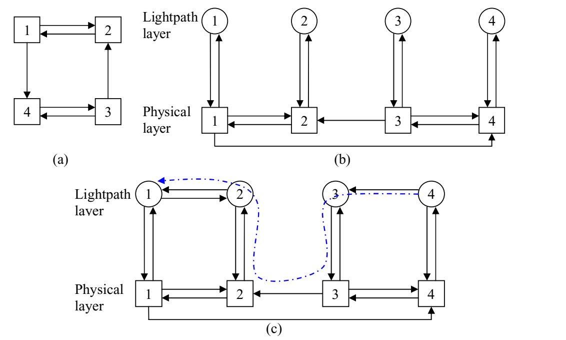


Fig. 6. (a) Physical topology of a network. (b) Auxiliary graph. (c) A path in the auxiliary graph.

A valid path in the LBAG should always begin and end in the lightpath layer. Once the path enters the physical layer through a transmitter edge, it implies a new lightpath needs to be established. The source node of the new lightpath is the node whose transmitter the transmitter edge represents. Finally the path will enter the lightpath layer again through a receiver edge. The node whose receiver the receiver edge represents is the destination node of the new lightpath. A path may have multiple sub-paths alternating in the physical layer and the lightpath layer. Therefore, multiple new lightpaths may need to be established. Fig. 6 (c) shows a path from node 4 to node 1 in the auxiliary graph. If a connection is to be routed on this path, a new lightpath from node 3 to node 2 must be established first. Then the connection can be routed on the three-hop path using the lightpaths 4-3, 3-2 and 2-1.

Algorithm ISGA

Input: Connection requests $\Lambda^x(x\in X)$, physical topology G_p, wavelength and transceivers, and *SRLG* information.
Output: A virtual topology G_v and the connections established over G_v.
1) Initialize the LBAG G_a according to the physical topology.
2) Sort all the connection requests in non-increasing traffic amount order in a list Q.
3) **while** (the list Q is not empty)
  Get and remove the connection request (s, d, x, y) from the head of Q.
  if (TTD-RDJP(G_a, s, d, p, b))
    for each physical layer sub-path p_s in p or b **do**
      Establish a new lightpath on p_s.
    if (dedicated protection **)**
      Establish a primary connection and a backup connection for the request on paths p and b respectively.
    else if (shared protection)
      Establish a primary connection on path p and reserve bandwidth on backup path b for the request.
  else
    Block the connection request.

Fig. 7. The ISGA algorithm.

Fig. 7 describes the ISGA heuristic grooming algorithm based on the LBAG model. The ISGA algorithm also uses the TTD-RDJP algorithm proposed in Section IV.A. In ISGA, TTD-RDJP is used to calculate a pair of risk-disjoint paths in the auxiliary graph for a connection request. The link weights of lightpath edges are handled the same way as (2) and (3) in SSGA. For a wavelength edge, its weight is the length of the corresponding fiber link. However, if there are no available wavelengths on the link, its weight is set to ∞. The weight of a transceiver edge is set as a fixed number if there are available transceivers on the corresponding node; otherwise, it is set to ∞ as well.

4. Tabu Search based Grooming Heuristic (TSGA)

Tabu search (TS) [18] is a meta-heuristic that defines general neighborhood search strategies to tackle difficult combinatorial optimization problems. An optimization problem can usually be characterized as a maximization (or minimization) problem subject to some constraints. Suppose $f(x)$ is the objective function and X is the set of solutions that satisfies all the constraints. The neighborhood $N(x)$ of a solution x is the subset of X that can be reached from x by a single transformation called a move. The TS optimization process iterates from one solution to another until a predefined termination criterion is met. TS uses short-term memory (tabu list) to avoid cycling back to previously visited solutions and uses long-term memory to generate quality moves. TS can break local optimal traps by allowing non-improving moves.

A general TS procedure (for a maximization problem) is as follows.

x the current solution.

x^* the best solution already obtained.

$\tilde{N}(x)$ the admissible subset of $N(x)$. $\tilde{N}(x) = \{x' \in N(x):\ x \to x' \textit{ not in tabu or allowed by aspiration}\}$

1. Choose an initial solution x_0. Set $x = x_0, x^* = x_0$. Initialize TS memory (including tabu lists and aspiration conditions).
2. Select the best move $x' \in \tilde{N}(x)$.
3. If $f(x') > f(x^*)$, then set $x^* = x'$.
4. Update TS memory.
5. If the termination criterion is satisfied, exit. Otherwise, set $x = x'$ and go to step 2.

The commonly used termination criteria in TS are:

- $\tilde{N}(x) = \varnothing$, i.e., the neighborhood set has been explored completely.
- The objective reaches a pre-specified threshold value or optimum value.
- The number of iterations reaches the maximum allowed value.
- The number of successive iterations without improving $f(x^*)$ reaches a specified number.

TSGA is a grooming algorithm following the general TS procedure. It starts with an initial solution which can be obtained by either SSGA or ISGA. Then it proceeds to an iterative optimization phase which keeps changing the current solution by executing the selected move. At any time, a solution comprises of a set of satisfied connections and a set of blocked connections. TSGA is also based on the LBAG model. Once the initial solution is obtained, an LBAG is constructed using the network state information.

In TSGA, a move is defined as either an add operation or a drop operation. For an add operation, a previously blocked connection request is satisfied by successfully finding a pair of risk-disjoint paths for the connection in the LBAG. Similar to ISGA, new lightpaths may be included in the paths and need to be established. Because a connection is satisfied, the objective function value (throughput or revenue) increases from the last iteration. For a drop operation, a satisfied connection is disconnected and all the bandwidth it uses along its primary path and backup path is released. After the connection is disconnected, if a lightpath is not used by any other connections, it is also disconnected and all its resources are released. The objective function value decreases after the drop operation. Note that we can only perform an add operation on a blocked connection and perform a drop operation on a satisfied connection.

To select the best move from $\tilde{N}(x)$, we define the move value of a connection as (4). The move with the largest move value is selected in each iteration.

$$g(C_{s,d}^{x,y}, p_1, p_2) = \begin{cases} \dfrac{V_{s,d}^{x}}{WPC(p_1, p_2)} - freq(C_{s,d}^{x,y}) & \textit{if add} \\ \dfrac{-V_{s,d}^{x}}{WPC(p_1, p_2)} - freq(C_{s,d}^{x,y}) & \textit{if drop} \end{cases}, \quad (4)$$

where $g(C_{s,d}^{x,y}, p_1, p_2)$ is the move value of a connection (s,d,x,y), p_1 and p_2 are the primary path and backup path assigned to a satisfied connection (in drop operation) or the paths to be used for a blocked connection (in add operation), $V_{s,d}^{x}$ is the revenue value (or simply the bandwidth) of a *OC-x* connection between (s,d), $WPC(p_1, p_2)$ is the weighted path cost of path p_1 and p_2, $freq(C_{s,d}^{x,y})$ is the frequency of the connection (s,d,x,y) being selected in the previous best moves.

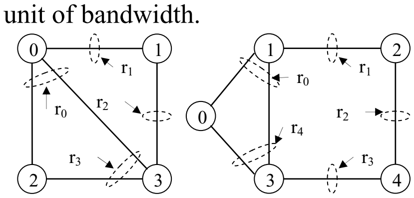
To prevent the search from being trapped in a small portion of the search space, TSGA uses two diversification techniques to force the search to go into unexplored search spaces. One technique is restart diversification. TSGA uses the solutions obtained from SSGA and ISGA respectively as initial solutions and runs the TS procedure twice. The other technique is continuous diversification. The frequency function is incorporated into the move value function as in (4), thus making the less frequently selected moves more favorable than the more frequently selected moves.

5. Numerical Results

In this section, we present numerical results to illustrate the performance of the ILP formulations and heuristics. We first apply the ILP formulations and heuristics to two small networks shown in Fig. 8. Then we apply the heuristics to a 24 node network and examine its results. In the following figures, we assume that the fiber links covered by a dashed circle belong to the same SRLG. We also assume that the networks have adequate grooming capability (enough transceivers) at every node. The traffic matrices are randomly generated. Note that the traffic units are normalized by being divided by the smallest grooming granularity in the network.

5.1. ILP vs Heuristics

For the small networks in Fig. 8, we assume that the capacity of a lightpath is 2 units and all connections request 1 unit of bandwidth.



(a) (b)

Fig. 8. (a) Network 1: a 4-node network. (b) Network 2: a 5-node network. The links covered by a dashed circle belong to the same SRLG.

We use CPLEX [20] to solve the ILPs presented in section III. Because of the large number of variables and constraints involved in the above ILPs, CPLEX fails to obtain feasible integer solutions for small networks shown in Fig. 8 within two hours. To make the ILPs solvable, we reduce the number of variables and constraints in the ILPs by restricting the path selection of lightpaths and connections. Specifically, the path of a lightpath is restricted to be from a pair of the shortest risk-disjoint paths between the two end nodes and the path of a connection is also restricted to be from the *k*-shortest paths. With these additional constraints, a large number of variables can be eliminated or replaced.

Table II and Table III show the results of the ILPs and heuristics with dedicated protection and shared protection respectively. For the ILP results, a number without asterisk represents an optimal solution, a number with asterisk represents the best solution obtained by CPLEX within two hours, and a single asterisk means that no feasible solution is found within two hours. Note that the optimality mentioned here is for the modified ILPs.

TABLE II
Dedicated protection at connection level: Network throughput from ILP, SSGA, ISGA and TSGA. (NET: Network, REQ: The total amount of traffic requested, W: Number of Wavelengths, *k*: Number of shortest paths a connection can use)

NET	REQ	W	Modified ILP			SSGA	ISGA	TSGA
			k=1	*k*=2	*k*=4			
1	12	1	4	4	4	4	4	4
1	12	2	8*	8*	8*	8	5	8
1	12	3	10*	9*	11*	10	9	11
1	12	4	11*	12	12	11	12	12
2	19	1	4	4	4	4	4	4
2	19	2	7*	5*	*	7	6	7
2	19	3	7*	8*	*	10	8	12

TABLE III
Shared protection at connection level: Network throughput from ILP, SSGA, ISGA and TSGA. (NET: Network, REQ: The total amount of traffic requested, W: Number of Wavelengths, k: Number of shortest paths a connection can use)

NET	DEM	W	Modified ILP			SSGA	ISGA	TSGA
			k=1	*k*=2	*k*=4			
1	12	1	4	4*	2*	2	4	4
1	12	2	8*	3*	*	9	5	12
1	12	3	8*	9*	7*	8	11	12
1	12	4	11*	11*	12	8	12	12
2	19	1	4	2*	2*	6	4	6
2	19	2	5*	*	*	8	6	18
2	19	3	*	*	*	13	13	19

From Table II and Table III, we can see that for the modified ILPs, the accepted traffic fluctuates when *k* increases from 1 to 4. On the one hand, the accepted traffic should increase as *k* increases. This is because the solution space of an ILP with a smaller *k* is included in the solution space of the ILP with a larger *k*. This trend is more or less reflected in the two tables. For example, in Table I, when *k* increases from 1 to 4 in network 1 with three wavelengths, the accepted traffic increases from 10 to 11, although optimal solutions are obtained in neither cases. On the other hand, when *k* increases, the time complexity of the ILPs also increases. Therefore, within a certain time limit, an ILP with a larger *k* may explore a smaller portion of its solution space than an ILP with a smaller *k*. This is especially obvious for relatively larger networks with more wavelengths. For example, in Table III, the ILPs with *k* =2 and *k*=3 only obtain feasible integer solutions when the number of wavelengths is one, which is worse than the solution of the ILP with *k*=1. Comparing the results of the ILPs and the heuristics, we can see that heuristics obtain comparable and even better results than the ILPs. This is in part because most of the ILPs cannot obtain optimal solution within two hours. Another reason may be that the heuristics achieve good results close to the optimal solutions. Although not shown here, the running times of SSGA and ISGA are within one 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. Comparing dedicated protection in Table II and shared protection in Table III, it is obvious from the heuristic results that shared protection accommodates more connections than dedicated protection.

5.2. Heuristics Comparison

To compare the three heuristics, we apply them to a 24 node network, as shown in Fig. 9. In this scenario, we assume that the capacity of a lightpath is 16 units and there are two different connection granularities at 1 unit and 4 units respectively. The total traffic amount requested is 2208.

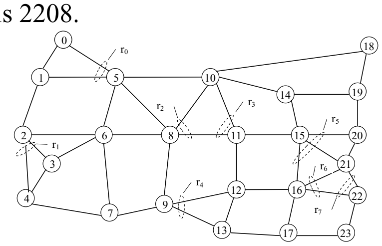


Fig. 9. A 24-node network. The fiber links covered by a dashed circle belong to the same SRLG. Any fiber link not covered in any dashed circle is a SRLG by itself.

Fig. 10 shows the performance of SSGA, ISGA and TSGA with dedicated protection in terms of total accommodated traffic. From Fig. 10, we can see that ISGA accommodates more traffic than SSGA. ISGA has an average of about 50% improvement over SSGA when the number of wavelengths is less than 18. After that, the improvement margin reduces. This is because ISGA has already accepted almost all the connection requests when the number of wavelengths is larger than 18. The difference between SSGA and ISGA is that SSGA separates the routing decision of lightpaths and connections in two phases while ISGA focuses on the routing of connections by considering lightpath routing as an auxiliary outcome of the connection path selection result. It finds the path with the minimum cost and only establishes a lightpath when it is included in the minimum cost path. SSGA tries to satisfy as many connections as possible with a single new lightpath for each one, and then routes the rest of the connections using the residual bandwidth on the established lightpaths. On the other hand, ISGA tries to balance the use of new lightpaths and existing lightpaths from the beginning. It finds the path with the minimum cost and only establishes a lightpath when it is included in the minimum cost path. The simulation results show that the strategy of ISGA is more efficient than that of SSGA.

From Fig. 10, we can also see that TSGA has an average of about 5% improvement over ISGA when the number of wavelengths is 18 or less. However, as the number of wavelengths increases, the improvement margin reduces rapidly to zero. Although this is in part because of the reduced improvement space as the throughput increases close to the total requested bandwidth, it also substantiates the fact that ISGA is quite effective.

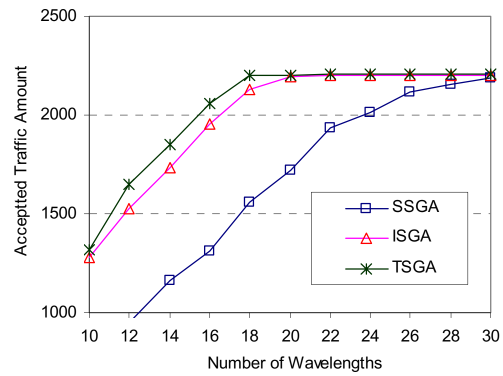


Fig. 10. Heuristics with dedicated protection.

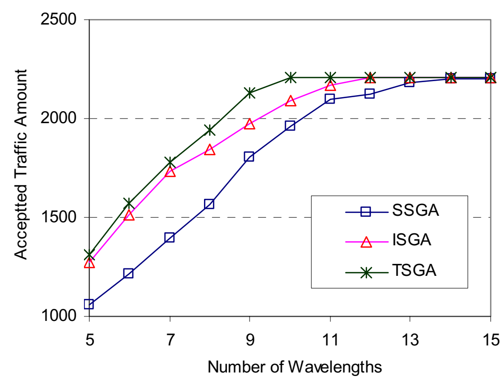


Fig. 11. Heuristics with shared protection.

Fig. 11 shows the performance of SSGA, ISGA and TSGA with shared protection. Comparing Fig. 11 with Fig. 10, it is clear that shared protection is much more resource-efficient than dedicated protection, as shared protection with TSGA uses about 10 wavelengths to accept all the connection requests while dedicated protection with TSGA uses about 18 wavelengths to achieve the same objective. Fig. 11 also shows that ISGA performs better than SSGA for the shared protection scheme, accepting an average of about 15% more traffic when the number of wavelengths is between 5 and 12. Still, TSGA provides an average of about 5% improvement over ISGA in terms of the amount of the accepted traffic with the number of wavelengths in the range of 5 to 10.

6. Conclusions

In this paper, we addressed the static STG problem under the SRLG-diverse routing constraints in optical WDM mesh networks employing path protection at the connection level. We presented two ILP formulations for the survivable traffic grooming problem, one for dedicated path protection and the other for shared path protection. We also proposed three efficient heuristic grooming algorithms, namely SSGA, ISGA and TSGA.

We showed with numerical results that the computational complexity of the ILP approach is too large even for networks of small sizes. On the other hand, ISGA performs much better than SSGA, with an average of 50% and 15% improvement in network throughput while using dedicated protection and shared protection respectively. This result implies that the integrated routing approach is superior to the overlay routing approach in terms of resource-efficiency. TSGA further improves the grooming results from ISGA by an average of about 5% at the cost of longer running time, which is required by the additional iteration optimization phase guided by the tabu search method.

7. Acknowledgment

This work was supported in part by the U. S. National Science Foundation grants (ANI-0074121 and EPS-0091900) and the UNL Program of Excellence PRISM Priority initiative.

8. References

[1] K. Zhu, B. Mukherjee, "Traffic Grooming in an Optical WDM Mesh Network," *IEEE Journal on Selected Areas in Communications*, vol.20, no.1, Jan. 2002.

[2] A. Lardies, R. Gupta, R. A. Patterson, "Traffic Grooming in a Multi-layer Network," Optical Network Magazine, May/Jun. 2001.

[3] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks—Part I: Protection," in *Proc. IEEE INFOCOM*, pp. 744-751, Mar. 1999.

[4] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks—Part II: Restoration," in *Proc. IEEE Integrated Circcuits Conf.*, pp. 2023-2030, Jun. 1999.

[5] 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.

[6] J. Strand, A. Chiu, R. Tkach, "Issues for routing in the optical layer," *IEEE Communications Magazine*, vol. 39, pp. 81-87, Feb. 2001.

[7] G. Ellinas, E. Bouillet, R. Ramamurthy, J. Labourdette, S. Chaudhuri, K. Bala, "Routing and Restoration Architectures in Mesh Optical Networks," *Optical Networks Magazine*, vol. 4, no. 1, pp. 91-106, Jan./Feb. 2003.

[8] J. Hu, "Diverse Routing in Optical Mesh Networks," *IEEE Transactions on Communications*, vol. 51, no. 3, pp. 489-494, Mar. 2003.

[9] 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, pp. 248-258, Apr. 2003.

[10] L. Shen, X. Yang, B. Ramamurthy, "Shared Risk Link Group (SRLG)-diverse Path Provisioning under Hybrid Service Level Agreements in Wavelength-routed Optical Mesh Networks: Formulation and Solution Approaches," in *Proc. of SPIE OptiComm 2003*, Dallas, TX, Oct. 2003.

[11] S. Thiagarajan, A. Somani, "Traffic Grooming for Survivable WDM Mesh Networks," *Optical Network Magazine*, vol. 3, no. 3, pp. 88-98, May/Jun. 2002.

[12] J. Fang, A. K. Somani, "Enabling Subwavelength Level Traffic Grooming in Survivable WDM Optical Network Design," *in Proc. of IEEE Globecom* 2003, vol. 5, pp. 2761-2766, San Francisco, CA, Dec. 2003.

[13] R. Ramaswami, K. N. Sivarajan, "Design of Logical Topologies for Wavelength-Routed Optical Networks," *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 5, Jun. 1996.

[14] R. M. Krishnaswamy, K. N. Sivarajan, "Design of Logical Topologies: A Linear Formulation for Wavelength-Routed Optical Networks with No Wavelength Changers," *IEEE/ACM Transactions on Networking*, vol. 9, no. 2, Apr. 2001.

[15] R. Dutta, G. N. Rouskas, "A Survey of Virtual Topology Design Algorithms for Wavelength Routed Optical Networks," *Optical Networks Magazine*, vol. 1, no. 1, pp. 73-89, Jan. 2000.

[16] G. Li, B. Doverspike, C. Kalmanek, "Fiber Span Failure Protection in Mesh Optical Networks," in *Proc. of SPIE OptiComm 2001*, Denver, CO, Aug. 2001.

[17] P. H. Ho, J. Tapolcai, H. T. Mouftah, "Diverse Routing for Shared Protection in Survivable Optical Networks," in *Proc. of IEEE Globecom* 2003, vol. 5, pp. 2519-2523, San Francisco, CA, Dec. 2003.

[18] F. Glover, M. Laguna, "Tabu Search," Kluwer Academic Publishers, ISBN 0-7923-9965-X, Jul. 1997.

[19] W. Yao, B. Ramamurthy, "Constrained Dynamic Traffic Grooming in Optical WDM Mesh Networks with Link Bundled Auxiliary Graph Model," *in Proc. IEEE HPSR 2004*.

[20] ILOG CPLEX, ILOG Inc., Mountain View, California, [Online]. Available: http://www.ilog.com/products/cplex/.

[21] W. Yao, B. Ramamurthy, "Survivable Traffic Grooming in WDM Mesh Networks under Shared Risk Link Group (SRLG) Constraints: Path Protection at the Lightpath Level", *in submission*.

[22] W. Yao, B. Ramamurthy, "Survivable Traffic Grooming in WDM Mesh Networks: An Integer Linear Programming Approach," Dept. Computer Science and Eng., UNL, Tech. Report, Feb. 2004. [Online]. Available: http://www.cse.unl.edu/~wyao/pub/SurGroomILP.pdf.