10-2005

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

Wang Yao
IEEE

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

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

Wang Yao, *Student Member, IEEE*, and Byrav Ramamurthy, *Member, IEEE*

Abstract—**Survivable traffic grooming (STG) is a promising approach to provide reliable and resource-efficient multigranularity 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 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 (TS) method. Numerical results show that the heuristics achieve comparable solutions to the ILP approach, which uses significantly longer running times than the heuristics.**

Index Terms—**Path protection, shared-risk link group (SRLG), survivability, tabu search (TS), traffic grooming, wavelength-division multiplexing (WDM).**

I. INTRODUCTION

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 optical carrier (OC)-192 (10 Gb/s). On the other hand, the bandwidth of a connection request [such as synchronous-optical-network (SONET) circuits, Internet Protocol (IP)/multiprotocol label switching (MPLS) label-switched paths] may be less than that, possibly OC-3 (155 Mb/s), or even lower. To make efficient use of the wavelength bandwidth, traffic grooming [1] is needed to pack connections at subwavelength 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 [2], [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. 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 connections together. It seeks to provide fault-recovery capability for connections and minimize the consumption of spare capacities in the network. With network service providers facing the pressure of generating revenues by providing reliable multigranularity connection services and reducing network-operation cost, we anticipate that STG will play an important role in future optical networks.

Protection is classified into link protection and path protection. Protection schemes can also be divided into dedicated-protection and shared-protection schemes, 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 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. In this paper, we focus on path protection at the connection level. We refer the interested readers to our earlier work [23] for the STG problem with protection at the lightpath 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. Shared-risk link group (SRLG) 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 an 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

The authors are with the Department of Computer Science and Engineering, University of Nebraska–Lincoln, Lincoln, NE 68588 USA (e-mail: wyao@cse.unl.edu; byrav@cse.unl.edu).

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 (MSHT) and maximizing resource utilization (MRU), were proposed to solve the problem efficiently. The works in [8] and [9] considered the static-routing and wavelength-assignment problems with path protection in wavelength-division-multiplexed (WDM) mesh networks without grooming capability.

Although traffic grooming and survivability have been studied extensively in the past decade, STG remains a relatively unexplored issue, only gaining attention recently. The work in [10] 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 [11] 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], [10], and [11], either node- or link-disjoint constraints were considered to solve the STG problem.

In this paper, we study the static STG problem under SRLG constraints, with the objective of maximizing 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 multigranularity 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 (TS) [20] method.

The rest of the paper is organized as follows. Section II formally states the STG problem under the SRLG constraints. Section III presents the two greedy heuristic grooming algorithms, SSGA and ISGA. Section IV presents the tabu-search-based grooming algorithm, TSGA. Section V presents numerical results from the ILPs, and the SSGA, ISGA, and TSGA heuristics. Section VI concludes the paper.
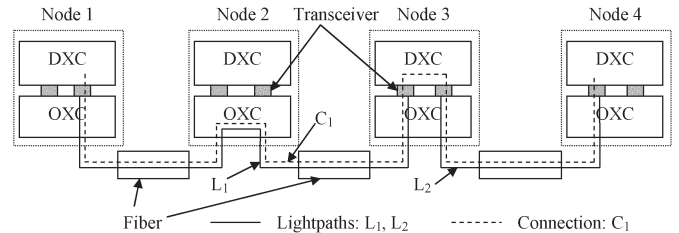

Fig. 1. Illustration of lightpaths and a connection in traffic grooming. Lightpath L_1 traverses fiber link (1, 2) and (2, 3), lightpath L_2 traverses fiber link (3, 4), and connection C_1 uses a two-hop path, including lightpaths L_1 and L_2.

II. PROBLEM DEFINITION

A wavelength-routed network (WRN) is deemed as a promising architecture for the core network of the next-generation Internet. 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 multigranularity subwavelength 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 an SONET over WDM optical network. Note that a lightpath uses a transmitter at the source node and uses a receiver at the destination node.

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.

1) Inputs:
   a) 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 $N = |V_p|$.
   b) 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 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 $48/3 = 16$.
   c) The number of transmitter and receiver pairs at each node is $\triangle_i (1 \leq i \leq N)$. In this study, we assume the transceivers are tunable to any wavelength operating on the fiber.
   d) The set of connection granularities supported in the network is X. For example, if a network with each wavelength operating at OC-48 supports connections at OC-3, OC-12, and OC-48, then $X = \{1, 4, 16\}$ after normalization.
   e) Connection requests represented as a set of $N \times N$ traffic matrices $\Lambda^x (x \in X)$.
   f) 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.

2) *Constraints*:

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

  b) *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.

  c) *Diverse-routing constraints*: The primary and backup paths of a connection must not share a common risk in the physical topology.

  d) *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 PAC level is to maximize bandwidth sharing without breaking the lightpath-capacity constraints.

3) *Objective*:

    To establish a virtual topology over the physical topology and to maximize the network throughput by effectively routing the connection over the virtual topology.

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 (but can be found in [24]). However, we will present the results of the ILP formulations in Section V.

III. GREEDY GROOMING HEURISTICS

The static routing-and-wavelength-assignment (RWA) problem is a well-known nondeterministic polynomial time (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 an RWA problem. The work in [6] and [7] proved that finding two SRLG-diverse paths between a node pair is NP-complete. Therefore, it is easy to see that the SSTG problem subject to the SRLG constraints is NP-hard. To efficiently solve an NP-hard problem, heuristics are needed.

Operationally, the two layers involved in traffic grooming can be managed separately or jointly, corresponding to an overlay or a peer-deployment model, respectively. For the overlay model, the routing of lightpaths over the physical topology and the routing of connections over the virtual topology are managed by two control planes. Therefore, the client layer (the virtual-topology layer) can only see lightpaths provided by the server layer (the physical-topology layer). The internal structure of the physical topology is invisible to the client-layer control plane. For the peer model, the two layers are managed by a single control plane. Therefore, the control plane has all the information about the two layers and the routing decisions of lightpaths and connections can be considered jointly.

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.   MSHT-PAVTD algorithm.

Corresponding to the two models, we propose two grooming algorithms, namely SSGA and ISGA.

A. Separate Survivable Grooming Algorithm (SSGA)

With SSGA, the SSTG problem is divided into two subproblems. 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 subwavelength-connection survivable-routing (SWCSR) problem, which involves packing the subwavelength connections on the lightpaths in the virtual topology, with each connection having a primary path and a backup path.

1) Protection Aware Virtual Topology Design (PAVTD): The VTD problem has been studied extensively in previous studies [12]–[15]. However, unlike the VTD problem studied in 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 the survivable routing of connections.

To solve the PAVTD problem, we propose the 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, the two times Dijkstra's risk-disjoint path (TTD-RDJP) algorithm (see Fig. 3) is a proposed algorithm for finding two risk-disjoint paths and DIJKSTRA is Dijkstra's algorithm for finding the shortest path. Note that for traffic of C units, MSHT-PAVTD establishes two risk-disjoint lightpaths in dedicated protection and establishes only one lightpath in shared protection. This is because for dedicated

---

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. TTD-RDJP algorithm.

protection, MSHT-PAVTD knows for sure that a connection will use two risk-disjoint paths. For shared protection, the resources are only reserved for backup paths and the backup paths can even share resources if their primary paths are risk disjoint. Therefore, establishing two lightpaths for a connection using shared protection might be overprovisioning. In addition, because the shared protection is at the connection level, it might be more resource efficient to address the risk-disjoint routing constraints in the SWCSR problem, so that backup-path resource sharing can be exploited with more flexibility. Because only one lightpath is established and a connection will use two risk-disjoint paths, the corresponding residual bandwidth is subtracted by $C/2$ in shared protection.

2) TTD-RDJP Algorithm: The MSHT-PAVTD heuristic requires a risk-disjoint path-selection algorithm. Suurballe's algorithm [16] is a well-known algorithm for finding edge- or node-disjoint paths with minimum cost. However, Suurballe's algorithm cannot be used to find risk-disjoint paths. The work in [17]–[19] tries to find a pair of risk-disjoint paths with the least cost. We propose the TTD-RDJP selection algorithm based on a three-step algorithm proposed in [17].

3) Subwavelength-Connection Survivable Routing (SWCSR): The SWCSR problem involves finding two risk-disjoint paths in the virtual topology for each connection to serve as the primary path and the 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) is subject to and $R_p(i, j)$ be the set of risks a lightpath (i, j) is subject to. Then $R_p(i, j)$ is the union of the risk sets of the fiber links it uses, as follows:

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

We propose the large-traffic-first (LTF-SWCSR) algorithm (see Fig. 4) to solve the SWCSR problem. The LTF-SWCSR algorithm also uses the RDJP algorithm. Note that MSHT-PAVTD uses the RDJP algorithm to find RDJPs in the physical

---

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. LTF-SWCSR algorithm.

topology for lightpaths, while LTF-SWCSR uses the RDJP algorithm to find risk-disjoint paths in the virtual topology for connections. Therefore, the link-bundled auxiliary graph (LBAG) G in LTF-SWCSR only includes lightpath edges.

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 in step 1 of TTD-RDJP.

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

where $f_{m,n}$ is the fiber length of link (m, n), B_r is the bandwidth requested by the connection, $B_a(i, j)$ is the free bandwidth on lightpath (i, j). Equation (2) is also used in step 2 of TTD-RDJP when dedicated protection is used.

When the shared-protection scheme is used, backup connections can share bandwidth within a lightpath if their primary connections are risk disjoint. A lightpath has C channels. Depending on the usage, the channels can be classified into dedicated, spare, and free channels. 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. For a specific primary connection p, a spare channel c can be further classified as a sharable spare channel or a nonsharable 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.

To fully exploit the backup-bandwidth sharing to reduce spare-capacity consumption, a different link-weight function (3) is defined for lightpaths while searching for backup paths of connections in step 2 of TTD-RDJP. 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

---

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 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. 5. ISGA algorithm.

possible. Only if the amount of sharable spare channels is not enough, does it assign free channels to the backup connection.

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

(3)

where $l_{i,j} = \sum_{(m,n) \in (i,j)} f_{m,n}$, $B_s(i,j,p)$ is the amount of sharable spare bandwidth on 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), and $\alpha(1 < \alpha < 1)$ 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.

B. 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 an LBAG [21].

Fig. 5 describes the ISGA heuristic grooming algorithm based on the LBAG model. The ISGA algorithm also uses the TTD-RDJP algorithm proposed in Section III-A. In ISGA, TTD-RDJP is used to calculate a pair of risk-disjoint paths in the auxiliary graph for a connection request. The SRLG information for lightpaths is handled in the same way as (1) in

SSGA. Also, the link weights of lightpath edges are handled in 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.

IV. Tabu-Search-Based Grooming Algorithm (TSGA)

TS [20] is a metaheuristic that defines general-neighborhood search strategies to tackle difficult combinatorial optimization problems. Suppose $f(x)$ is the objective function and X is the solution space that includes all solutions that satisfy 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 (e.g., number of iterations) is met.

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

x current solution;

x^* best solution already obtained;

$\tilde{N}(x)$ admissible subset of $N(x)$.

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.

TSGA is a grooming algorithm following the general TS procedure. It starts with an initial solution that can be obtained by either SSGA or ISGA. Then, it proceeds to an iterative optimization phase that 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 with 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 and backup paths 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
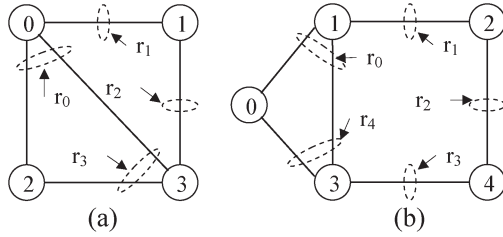
Fig. 6. (a) Network 1: Four-node network. (b) Network 2: Five-node network.

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.

$$g(c, p_1, p_2) = \begin{cases} \dfrac{V(c)}{\text{WPC}_{(p_1, p_2)}} - \text{Freq}(c) & \text{if add} \\ \dfrac{-V(c)}{\text{WPC}_{(p_1, p_2)}} - \text{Freq}(c) & \text{if drop} \end{cases} \quad (4)$$

where $g(c, p_1, p_2)$ is the move value of a connection c, p_1 and p_2 are the primary and backup paths assigned to a satisfied connection (in the drop operation) or the paths to be used for a blocked connection (in the add operation), $V(c)$ is the revenue value (or simply the bandwidth) of connection c, $\text{WPC}(p_1, p_2)$ is the weighted-path cost of path p_1 and p_2, and $\text{Freq}(c)$ is the frequency of the connection c 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.

V. 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. 6. 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.

A. ILP Versus Heuristics

For the small networks in Fig. 6, we assume that the capacity of a lightpath is two units and all connections request one unit of bandwidth.

TABLE I
THROUGHPUT OF ILP AND HEURISTICS: DEDICATED PROTECTION
(NET: NETWORK; REQ: TOTAL TRAFFIC AMOUNT REQUESTED;
W: NUMBER OF WAVELENGTHS; AND k: NUMBER OF SHORTEST PATHS)

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 II
THROUGHPUT OF ILP AND HEURISTICS: SHARED PROTECTION

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

We use CPLEX [22] to solve the ILPs. To reduce the complexity, 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.

Tables I and II show the network throughput of the ILPs and heuristics with dedicated protection and shared protection, respectively. For the ILP results, a number without an asterisk represents an optimal solution, a number with an asterisk represents the best solution obtained by CPLEX within 2 h, and a single asterisk means that no feasible solution is found within 2 h. Note that the optimality mentioned here is for the modified ILPs. From Tables I and II, we can see that for the modified ILPs, the accepted traffic fluctuates when k increases from 1 to 4. On 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 II, 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,
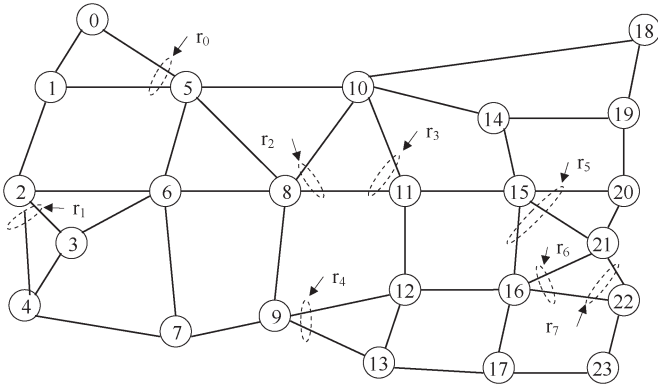
Fig. 7.   24-node network.

Fig. 8.   Comparison of heuristics.

results than the ILPs. This is, in part, because most of the ILPs cannot obtain an optimal solution within 2 h. 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 1 s 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 I and shared protection in Table II, it is obvious from the heuristic results that shared protection accommodates more connections than dedicated protection.

B. Heuristics Comparison

To compare the three heuristics, we apply them to a 24-node network, as shown in Fig. 7. In this scenario, we assume that the capacity of a lightpath is 16 units and there are two different connection granularities at one and four units, respectively. The total amount of traffic requested is 2208 units.

Fig. 8 shows the performance of SSGA, ISGA, and TSGA in terms of total accommodated traffic. As can be seen, ISGA accommodates more traffic than SSGA. For dedicated protection, ISGA has an average of about 50% improvement over SSGA when the number of wavelengths (W) is less than 18. After that, the improvement margin reduces. This is because ISGA has already accepted almost all the connection requests when $W \geq 18$. For shared protection, ISGA accepts an average of about 15% more traffic than SSGA when $6 \leq W \leq 12$. The difference between SSGA and ISGA is that SSGA separates the routing decision of lightpaths and connections into two phases, while ISGA focuses on the routing of connections by considering lightpath routing as an auxiliary outcome of the connection path-selection result. 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 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.

Fig. 8 also shows that TSGA has an average of about 5% improvement over ISGA when $W \leq 18$ for dedicated protec-
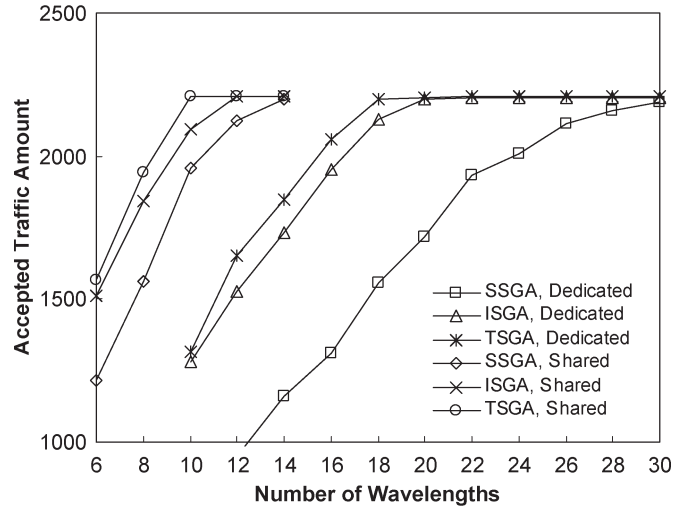
tion and $6 \leq W \leq 10$ for shared protection. However, as W increases, the improvement margin reduces rapidly to zero. Although this is, in part, because of the reduced improvement space as the throughput increases close to the total requested bandwidth, it also substantiates the fact that ISGA is quite effective.

Comparing the two schemes, it is clear that shared protection is much more resource efficient than dedicated protection, as shared protection with TSGA uses about ten wavelengths to accept all the connection requests, while dedicated protection with TSGA uses about 18 wavelengths to achieve the same objective.

Fig. 9 compare the running times of the three grooming algorithms. As can be seen, ISGA has a slightly larger running time than SSGA and their running times generally increase with W. TSGA has a much longer running time than both SSGA and ISGA, especially when W is relatively small. This is because when W is large, even SSGA and ISGA can satisfy most of the connections. Therefore, the space left for improvement is small and the TS optimization process exits after a few iterations without much improvement. On the other hand, when W is relatively small, the TS can improve the objective value fairly easily. Therefore, the optimization process might go through many iterations and use more running time. This observation is substantiated by looking at Figs. 8 and 9 simultaneously. When the improvement in throughput becomes trivial ($W \geq 20$ for dedicated protection and $W \geq 12$ for shared protection), the running time of TSGA also drops significantly.

VI. CONCLUSION

In this paper, we addressed the survivable-traffic-grooming (STG) problem under the shared-risk-link-group (SRLG)-diverse routing constraints in optical wavelength-division multiplexing (WDM) mesh networks employing path protection at the connection level. We showed with numerical results that the computational complexity of the integer-linear-programming (ILP) approach is too large, even for networks of small sizes. On the other hand, integrated survivable grooming algorithm (ISGA) performs much better than separated survivable
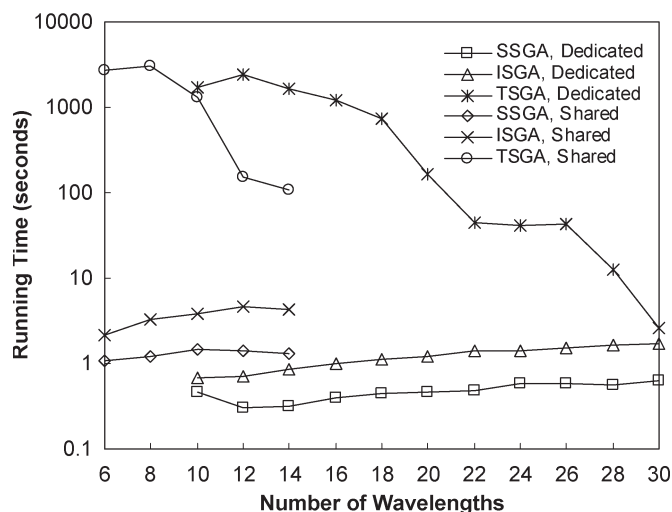
Fig. 9. Running-time comparison of heuristics.

grooming algorithm (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. Tabu-search survivable grooming algorithm (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 (TS) method.

REFERENCES

[1] K. Zhu and B. Mukherjee, "Traffic grooming in an optical WDM mesh network," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 1, pp. 122–133, Jan. 2002.

[2] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks—Part I: Protection," in *Proc. IEEE Information Communications (INFOCOM)*, New York, Mar. 1999, pp. 744–751.

[3] Y. Xiong, D. Xu, and C. Qiao, "Achieving fast and bandwidth-efficient shared-path protection," *J. Lightw. Technol.*, vol. 21, no. 2, pp. 2683–2693, Feb. 2003.

[4] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks—Part II: Restoration," in *Proc. IEEE Integrated Circuits Conf.*, Vancouver, Canada, Jun. 1999, pp. 2023–2030.

[5] C. Ou, K. Zhu, and B. Mukherjee, "Traffic grooming for survivable WDM networks—shared protection," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 9, pp. 1367–1383, Nov. 2003.

[6] G. Ellinas, E. Bouillet, R. Ramamurthy, J. Labourdette, S. Chaudhuri, and K. Bala, "Routing and restoration architectures in mesh optical networks," *Opt. Netw. Mag.*, vol. 4, no. 1, pp. 91–106, Jan./Feb. 2003.

[7] J. Hu, "Diverse routing in optical mesh networks," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 489–494, Mar. 2003.

[8] H. Zang, C. Ou, and B. Mukherjee, "Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints," *IEEE/ACM Trans. Netw.*, vol. 11, no. 2, pp. 248–258, Apr. 2003.

[9] L. Shen, X. Yang, and B. Ramamurthy, "Shared Risk Link Group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 4, pp. 918–931, Aug. 2005.

[10] S. Thiagarajan and A. Somani, "Traffic grooming for survivable WDM mesh networks," *Opt. Netw. Mag.*, vol. 3, no. 3, pp. 88–98, May/Jun. 2002.

[11] J. Fang and A. K. Somani, "Enabling subwavelength level traffic grooming in survivable WDM optical network design," in *Proc. IEEE Global Telecommunications (GLOBECOM)*, San Francisco, CA, Dec. 2003, vol. 5, pp. 2761–2766.

[12] R. Ramaswami and K. N. Sivarajan, "Design of logical topologies for wavelength-routed optical networks," *IEEE J. Sel. Areas Commun.*, vol. 14, no. 5, pp. 840–851, Jun. 1996.

[13] R. M. Krishnaswamy and K. N. Sivarajan, "Design of logical topologies: A linear formulation for wavelength-routed optical networks with no wavelength changers," *IEEE/ACM Trans. Netw.*, vol. 9, no. 2, pp. 186–198, Apr. 2001.

[14] D. Banerjee and B. Mukherjee, "Wavelength-routed optical networks: Linear formulation, resource budgeting tradeoffs, and a reconfiguration study," *IEEE/ACM Trans. Netw.*, vol. 8, no. 5, pp. 598–607, Apr. 2000.

[15] R. Dutta and G. N. Rouskas, "A survey of virtual topology design algorithms for wavelength routed optical networks," *Opt. Netw. Mag.*, vol. 1, no. 1, pp. 73–89, Jan. 2000.

[16] J. W. Suurballe, "Disjoint paths in a network," *Networks*, vol. 4, pp. 125–145, 1974.

[17] G. Li, B. Doverspike, and C. Kalmanek, "Fiber span failure protection in mesh optical networks," in *Proc. SPIE Optical Networking and Communications (OptiComm)*, Denver, CO, Aug. 2001, pp. 130–141.

[18] C. Xin, Y. Ye, S. Dixit, and C. Qiao, "A joint lightpath routing approach in survivable optical networks," *Opt. Netw. Mag.*, vol. 3, no. 3, pp. 23–32, May/Jun. 2002.

[19] P. H. Ho, J. Tapolcai, and H. T. Mouftah, "Diverse routing for shared protection in survivable optical networks," in *Proc. IEEE Global Telecommunications (GLOBECOM)*, San Francisco, CA, Dec. 2003, vol. 5, pp. 2519–2523.

[20] F. Glover and M. Laguna, *Tabu Search*. Boston, MA: Kluwer, ISBN 0-7923-9965-X, Jul. 1997.

[21] W. Yao and B. Ramamurthy, "A link bundled auxiliary graph model for constrained dynamic traffic grooming in optical WDM mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 8, pp. 1542–1555, Aug. 2005.

[22] *ILOG CPLEX*. Mountain View, CA: ILOG, Inc. [Online]. Available: http://www.ilog.com/products/cplex/

[23] W. Yao and B. Ramamurthy, "Survivable traffic grooming in WDM mesh networks under SRLG constraints," in *Proc. IEEE Int. Conf. Communications (ICC)*, Seoul, Korea, May 2005, pp. 1751–1755.

[24] W. Yao, "Traffic grooming in next-generation optical WDM mesh networks," Ph.D. dissertation, Dept. CSE, Univ. Nebraska, Lincoln, 2005.

Wang Yao (S'02) received the B.E. degree in cryogenic engineering and M.E. degree in computer science from the Beijing University of Aeronautics and Astronautics, Beijing, China, in 1997 and 2000, respectively. He is currently pursuing the Ph.D. degree in computer science in the Department of Computer Science and Engineering, University of Nebraska–Lincoln (UNL).

Before he joined UNL, he had worked with Huawei Technologies for one year at Huawei Beijing Research Center, Beijing, China, as a Senior Software Engineer. His research interests include networking and distributed computing, optical communication networks, and wireless networks.

Byrav Ramamurthy (S'97–A'98–M'03) received the B.Tech. degree in computer science and engineering from the Indian Institute of Technology, Madras, India, in 1993. He received the M.S. and Ph.D. degrees in computer science from University of California (UC), Davis, in 1995 and 1998, respectively.

Since August 2003, he has been an Associate Professor in the Department of Computer Science and Engineering, University of Nebraska–Lincoln (UNL). His research areas include optical networks, wireless networks, network security, distributed computing, and telecommunications.

Prof. Ramamurthy was a recipient of the Indian National Talent Search scholarship and was a fellow of the Professors for the Future program at UC, Davis. He is a recipient of the UNL Research Council Grant-in-Aid Award for 1999 and the College of Engineering and Technology Faculty Research Award for 2000. He served as a Guest Co-editor for a special issue of IEEE Network magazine on *Optical Communication Networks*. He served as a Member of the Technical Program Committees for the IEEE Conference on Computer Communications (INFOCOM), IEEE Global Telecommunications Conference (GLOBECOM), Opticomm, International Conference on Communications (ICC) and International Conferences on Computer Communications and Networks (ICCCN) conferences. From 2001–2003, he served as the Founding Secretary of the IEEE ComSoc Optical Networking Technical Committee (ONTC).