Minimum Interference Routing with Fast Protection

Eusebi Calle, Anna Urra, and Jose L. Marzo, Universitat de Girona, Spain

Geng-Sheng (G. S.) Kuo, National Chengchi University

Hai-Bo Guo, Beijing University of Posts and Telecommunications

ABSTRACT

One of the most effective techniques offering QoS routing is minimum interference routing. However, it is complex in terms of computation time and is not oriented toward improving the network protection level. In order to include better levels of protection, new minimum interference routing algorithms are necessary. Minimizing the failure recovery time is also a complex process involving different failure recovery phases. Some of these phases depend completely on correct routing selection, such as minimizing the failure notification time. The level of protection also involves other aspects, such as the amount of resources used. In this case shared backup techniques should be considered. Therefore, minimum interference techniques should also be modified in order to include sharing resources for protection in their objectives. These aspects are reviewed and analyzed in this article, and a new proposal combining minimum interference with fast protection using shared segment backups is introduced. Results show that our proposed method improves both minimization of the request rejection ratio and the percentage of bandwidth allocated to backup paths in networks with low and medium protection requirements.

INTRODUCTION

As networks grow, offering better quality of service (QoS), the consequences of a failure become more pronounced. Network reliability is therefore seen as a key requirement for new traffic engineered networks [1]. The main goal of a routing algorithm is to find a feasible path (i.e., a path with enough bandwidth and efficient resource utilization). In addition, routes selected by using QoS routing must have sufficient resources for the requested QoS parameters. Routing algorithms can be categorized into *static* and *dynamic* algorithms depending on the type of routing information used for computing paths. Static algorithms use network information that does not change with time, while dynamic ones use the current state of the network (link load, blocking probability, etc.). The dynamic routing algorithms can be invoked either *online* (on demand) or *offline* (precomputed) depending on the instant when this computation is applied. In the online routing algorithms path requests are attended to one by one, while offline routing ones do not allow new path route computation without recomputing all the requests. This article is focused on dynamic online routing.

Traditional QoS routing algorithms use two different objective functions to optimize network performance: the shortest path should be selected for minimizing the number of hops, and the least loaded path should be selected for load balancing. These improvements are not easy to achieve using only a single routing algorithm since the two objectives are difficult to reach simultaneously. In [2] a Widest-Shortest Path (WSP) algorithm was proposed where both criteria are mixed. The WSP algorithm first selects the path with the minimum hop count among all feasible paths; then, if more than one path is eligible, the one with maximum reservable bandwidth (MRB) is chosen. The MRB of a path is the minimum of the available bandwidth of all links on the path. Shortest-Widest Path (SWP) [2] uses the opposite criterion to the WSP (i.e., the first criterion is to select suitable paths with the MRB), and if more than one is feasible, the one with the minimum hop count is selected. In other words, WSP gives highest priority to resource utilization, SWP to balancing the network load.

There is a third objective to be considered: minimization of the number of connection request rejections, which is also called blocking probability. In recent literature there are some proposals that use the capabilities of multiprotocol label switching (MPLS) networks for QoS routing schemes. Major MPLS QoS routing schemes use the ingress-egress node information to develop minimum interference routing algorithms (MIRAs), which were introduced in [3]. These algorithms improve the previous QoS routing proposals. In this article a complete review of the main MIRAs is made. Most of the current approaches do not consider protection in their objectives. This objective together with other novel ones, such as adaptation to the optical layer, is taken into account to create a new set of MIRAs.

0163-6804/06/$20.00 © 2006 IEEE

The rest of this article is organized as follows. A complete review of the latest MIRAs is made. The failure recovery phases are reviewed. We present the basics of the proposed Minimum Interference with Fast Protection (MIFP) routing schemes. A set of routing algorithms that are used to evaluate the performance of the MIFP schemes is described. The simulation scenarios and performance results are presented and conclusions are made.

The objectives of this novel proposal are to reduce request rejection by using minimum interference, improve resource utilization for protection using shared backups, and consider both MPLS and the optical layer in order to avoid protection duplications

A Survey of Minimum Interference Routing Algorithms

In this section an overview of the main MIRAs is made. Table 1 summarizes the major aspects of each MIRA.

The first MIRA was introduced by Kodialam [3]. The aim of this MIRA is that a new connection must follow a path that interferes as little as possible with a path which may be critical for satisfying future requests. The idea is to identify those "critical" paths to minimize the future request rejection ratio. This identification is based on a preprocess phase of maximum minimum (maxmin) flow computation to generate a weighted graph in which Dijkstra is used to select the path. The MIRA was proposed for MPLS-based network scenarios. It was also extended to include establishing lightpaths (wavelength routing) as well as routing in the logical topology in the Maximum Open Capacity Routing Algorithm (MOCA) [4]. The same authors proposed a version to include 1+1 protection. An evolution of MIRA using dedicated 1+1 protection is Minimum-Interference Restorable Routing (MIRR) [5]. However, these algorithms include complex computation with large calculation times. In order to overcome this drawback, new proposals have been made.

The first proposal without maximum-flow calculations was presented by Iliadis in Simple MIRA (SMIRA) [6]. SMIRA uses a new procedure to obtain the set of critical paths without maximum-flow computation, called k-WSP, under bottleneck elimination. This procedure identifies a set of critical paths by using a WSP algorithm (an alternative is to use SWP). Another similar procedure, in terms of not using maximum flow calculations to obtain the critical links, is Wang, Su, and Chen's (WSC) algorithm [7]. These algorithms were also proposed for MPLS-based network scenarios. Two enhanced proposals of SMIRA and WSC were presented in Integrated SMIRA (SMIRA-I) [8] and the Light Minimum Interference Routing (LMIR) algorithm [9]. LMIR is one of the most recent proposals [9]. It uses a modified Dijkstra algorithm to identify the paths with least capacity. These paths are used to identify the critical links. The number of critical paths is a key factor in this algorithm. With five critical paths they achieve the highest performance, improving the computation in some network scenarios by 40 percent with respect to MIRA and WSC. Previous proposals are oriented to static topologies. A new proposal in the wireless optical dynamic network scenario was introduced in SMIRA-I. SMIRA-I extends SMIRA to compute the critical weight for each actual link and potential link (dynamic scenario).

However, major QoS online routing proposals that use minimum interference do not consider protection in their main objectives due to the added complexity. Some preliminary proposals that consider protection in their objectives have high computational cost. For instance, MIRR uses 1+1 protection. 1+1 achieves good results reducing recovery time; however, it has large resource consumption. Consequently, in 1+1 protection there is a trade-off between the minimization of the failure recovery time and the restoration capacity. Usually the fastest recovery schemes (e.g., 1+1 or 1:1 protection) use a large amount of spare restoration capacity. Hence, this is not cost effective for most customer applications. Significant reductions in spare capacity can be achieved by sharing this capacity among independent failures. The accuracy and performance of the shared backup schemes are based on the available network information. A proposal of shared protection based on Partial Information Routing (PIR) was introduced in [10]; a Full Information Routing (FIR) scheme was proposed in [11]. FIR has higher performance than previous proposals wherever the required routing information is available. Otherwise, this lack of information can be overcome by using signaling techniques.

In this article new mechanisms for MIFP are proposed. The objectives of this novel proposal are to reduce request rejection by using minimum interference, improve resource utilization for protection (restoration overbuild) using shared backups, and consider both MPLS and the optical layer in order to avoid protection duplications (Table 1). In order to guarantee fast protection, segment protection and shared backups are combined, resulting in suitable fault recovery time and resource consumption.

Fast Protection

The failure recovery process starts when a failure occurs and finishes when the traffic is fully restored in the backup path. This process involves different phases: failure identification, failure notification, backup activation, traffic switchover, and so on. These phases are summarized in Table 2 in relation to the protection method. Some phases can be formalized and evaluated in terms of time, but most of them depend on the network (traffic) conditions and other circumstances such as a certain random component or the technology used. Some of these phases are identified as crucial in recovery time reduction. Both failure detection and identification depend completely on the network technology. For instance, in optical networks signal loss and the corresponding failure alarm are quickly executed and cannot easily be reduced. However, slow failure notification (in segment or path protection schemes) can involve a high

Routing scheme	Network scenario	Complexity[1]	Protection scheme	Restoration overbuild
MIRA	MPLS	High	None	
MIRR	IP/MPLS over WDM	High	1+1	High
MOCA	IP/MPLS over WDM	High	None	
SMIRA	MPLS	Low	None	
SMIRA_I	Wireless optical	Low	None	
WSC	MPLS	Low	None	
LMIR	MPLS	Low	None	
Proposed schemes	IP/MPLS over WDM	Low	1:*n*	Low

[1] High complexity means maximum-flow calculations are executed.

Table 1. *Minimum interference routing schemes.*

Recovery phase	Path-segment protection	Local protection
Failure detection	√(1)	
Failure identification	√	√
Failure notification	√	
New backup	(2)	(2)
Backup activation	√	√
Switchover	√	√
Complete traffic recovery	√	√
Initial working path recovery	(3)	(3)

(1) In path-segment protection LSP monitoring techniques or detection+failure_notification can be used.

(2) If there is no pre-established backup, the backup path is computed (routed and signaled) after the failure.

(3) Revertive mode: "The revertive mode requires the traffic to be switched back to a preferred path when the fault on that path is cleared" [12].

Table 2. *The failure recovery phases.*

number of packet losses. In a similar way, slow backup activation involves slow switchover activation, and consequently introduces a large delay in traffic recovery.

Consequently, failure indication signaling and backup activation messages must be sent as fast as possible in order to reduce the fault recovery time. Node and link delays must be considered in this analysis. Nodes introduce a delay proportional to the node processing time and buffering time. The links' delay is proportional to the propagation and transmission time. If the node processing and queuing delays are very small, which can be expected in future networks, the propagation time (and consequently the link length) can be identified as the major component to be reduced. Therefore, the failure impact can be reduced by selecting network-protected segments with minimum physical length.

Minimum Interference Routing with Shared Segment Protection

In this section the basis of the MIFP scheme is presented and discussed. The network scenario and problem formulation are also described.

Disjoint Path Computation

Network protection is usually based on establishing link-disjoint path pairs: the working path (WP) and backup path (BP). When a link failure occurs, the affected WPs switch traffic over to their respective BPs. One example of a disjoint path-pair routing algorithm was introduced by Suurballe [13]. Although Suurballe's algorithm is optimal and has polynomial computational complexity, it is only oriented to *dedicated protection*. Since resources are not shared in dedicated protection, there is poor resource utilization. *Shared protection* outperforms dedicated protection in terms of resource consumption, but in order to provide efficient resource consumption, the WP links must be known before BP computation [14]. Therefore, a two-step routing algorithm is necessary when shared protection is used.

Partially Protected Network

We present a novel proposal that considers the already protected links at lower layers (e.g., link 5–6 in Fig. 1). Thus, no extra resource is necessary at the MPLS layer against failure for links protected at lower layers (e.g., by a lightpath at the optical layer). Once the WP is selected, a partial disjoint path (PDP) is computed. The PDP may overlap protected links and the WP nodes. When the PDP overlaps the

WP, more than one BP (i.e., segment backup paths [SBPs]) can be established. Hence, when a PDP is computed, the protected links may not belong to the protected segment path, or belong to the protected segment path. Both cases are shown in Figs. 1a and 1b, respectively. In Fig. 1 two WPs are established sharing link 5–6 that is protected at the lower layer. The same PDP is used to protect both WPs. In the first case, the computed PDP overlaps WP_A and WP_B. This means that two SBPs, SBP_1 and SBP_2, are established between the protected segment paths 3–4–5 and 6–7 since link 5–6 is already protected. Moreover, the SBP bandwidth is shared in both cases (Figs. 1a and 1b) since shared link 5–6 need not be protected at the MPLS layer.

Shared risk link groups (SRLGs) refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links of the same SRLG may fail too. Links in the group have shared risk. As shown in Fig. 1b, both WP_A and WP_B belong to the same SRLG since they share link 5–6. In this case their backup path capacity is not sharable. However, this link is already protected at the lower layer; consequently, the SBP defined at the MPLS layer is negligible to protect link 5–6 in case of a failure. Therefore, in the multilayer scenario considered in this approach, the two data paths are link-disjoint if their respective unprotected (at the lower layer) links do not belong to the same SRLG.

Network Scenario

Let $G = (V, E)$ describe the given network, where V is the set of network nodes, and E is the set of network links. Each link $(i,j) \in E$ has an associated L_{ij} physical length; R_{ij} residual bandwidth; S_{ij}^{uv} total bandwidth reserved to protect link (u,v); and T_{ij} the total backup bandwidth allocated in link (i,j). Note that S_{ij}^{uv} is equal to 0 when the link (u,v) is protected at the lower layer, and

$$T_{ij} = \max_{(u,v)\in E} (S_{ij}^{uv}).$$

Assume that there is a set of node pairs P as the set of potential ingress-egress node pairs. Hence, all connection setup requests occur between these pairs. A generic element of this set is denoted (s, d). A setup request is defined by (s, d, b), where b denotes the required amount of bandwidth.

Partial Disjoint Path Computation

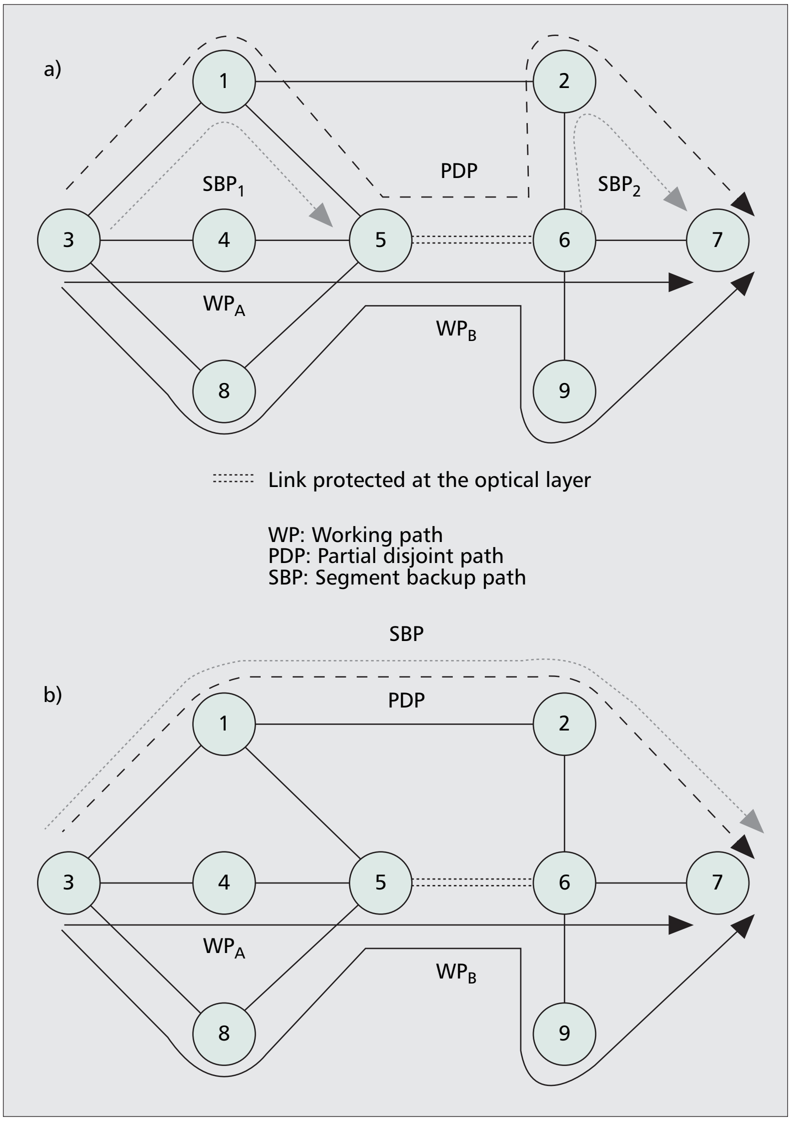
A PDP is computed in order to identify the necessary segment backup paths to protect the WP, as presented earlier. Therefore, a weight w_{ij} is assigned to each link according to the following expression:

$$w_{ij} = \begin{cases} 0 & \text{if } (i,j) \in WP \text{ and } p_{ij} = 1 \\ c_{ij} & \text{if } (i,j) \notin WP \text{ and } p_{ij} = 0 \text{ and } R_{ij} + T_{ij} - A \ge b \\ \infty & \text{otherwise} \end{cases} \quad (1)$$

where A is the maximum necessary capacity if one of the unprotected WP links fails; c_{ij} is the cost assigned to link (i,j) according to the routing objectives; and p_{ij} is 1 if link (i,j) is protected at the lower layer, 0 otherwise. Once the weight is assigned the PDP is computed. This is done using a variation of Dijkstra's algorithm called *PartialDisjointPath* (Algorithm 1).

In this algorithm *Cost(v)* is a vector that contains the path cost from s to v; *Pred(v)* contains v's predecessor node; and *WPlast(v)* contains the last WP node visited before treating node v. Q represents the list of adjacent vertices which were not yet visited. Function min_cost(Q) returns the element $u \in Q$ with the lowest *Cost(u)*, and *adjacent(u)* represents the adjacency list of vertex u.

Once the PDP is computed, the BP links are identified. Only the links of the PDP, which do not belong to the WP, are the backup links. Other links are considered unprotected at the MPLS layer since they are protected at the lower layer. The reserved bandwidth will depend on the amount of bandwidth that may be shared in each backup link and the links that are protected at the MPLS layer.



■ **Figure 1.** *MPLS protection when the PDP: a) overlaps protected links at the optical layer; b) does not overlap the protected links at the optical layer.*

```
For all $v \in$ V do
    $Cost(v) = \infty$
    $Pred(v)$ = null
    WPlast(v)= s
  $Cost(s) = 0$;
  Q ← s
  while (Q) do
    u ← min_cost(Q)
    for all $v \in adjacency(u)$ do
        if ( $Cost(u)+w_{uv} < Cost(v)$ ) then
            if ($v \in WP$ ) then
                  WPlast(v)= v
            else  WPlast(v)= WPlast(u)
            Pred(v) = u
            Cost(v)= Cost(u)+$w_{uv}$
            Q ← v
```

■ **Algorithm 1.** *PartialDisjointPath.*

Routing scheme	Working path	Backup path		
		PDP	Link cost based on	Protection method
MIFP	LMIR	✓	FIR	Segment
MI	LMIR	✓	LMIR	Segment
FP	WSP	✓	FIR	Segment
FIR	WSP	✘	FIR	Global
SP	WSP	✘	WSP	Global

■ **Table 3.** *Proposed routing schemes.*

Minimum Interference with Fast Protection Routing Algorithm

For each connection request, a WP has to be set up, and a BP must also be set up if the WP has at least one link to be protected. Thus, the proposed novel MIFP routing algorithm is divided into two steps:

- *WP computation*. The WP routing algorithm minimizes the resource consumption based on the minimum interference criterion. LMIR has been chosen to compute the WP. If there is sufficient bandwidth in the network for the WP of the current request, it is accepted and all links in the WP will reserve b units of bandwidth. Otherwise, the request is rejected.
- *BP computation*. Once the WP is known, a PDP is computed, based on the PDP routing algorithm, in order to identify the segment backup paths necessary to protect the WP. The BP routing algorithm aims at maximizing the shared bandwidth, i.e., reducing the resources used for protection. Full Information-based routing [7] is chosen to assign the link cost. Therefore,

$$c_{ij} = \begin{cases} 0 & \text{if } T_{ij}+b-A \le 0 \\ \min(b, T_{ij}+b-A) & \text{if } T_{ij}+b-A > 0 \end{cases}. \qquad (2)$$

If there is no sufficient bandwidth ($c_{ij} = 0$) in the network for the BP of the current request, the connection is rejected. Otherwise, the request is accepted. The reserved bandwidth will depend on the amount of bandwidth that may be shared in each backup link and the links that are protected at the MPLS layer.

Minimum Interference Routing Algorithms

In this section the routing algorithms used for performance evaluation later are described. A brief discussion of the necessary routing information is also presented.

Minimum Interference Routing Algorithms

In order to compare the performance of our proposed algorithm, MIFP, described earlier, two variations have been used. These approaches include either the minimization of the minimum interference or fast protection in order to explore MIFP when just one objective is considered (Table 3).

MIFP Minimum Interference (MI) — In order to compare our proposal, a routing algorithm that only aims to minimize interference is proposed. Thus, this algorithm differs from the proposed MIFP by assigning the link cost, c_{ij}, based on the LMIR algorithm [9].

MIFP Fast Protection (FP) — This scheme does not consider minimizing the interference; it differs from the proposed MIFP by computing the WP using the WSP routing algorithm.

Two existing algorithms in the literature are also considered. These algorithms do not compute partial disjoint path or segment protection. The global protection is applied without aiming to minimize the interference. They are:

Full Information Routing (FIR) — In this case minimizing the restoration capacity is achieved by using FIR [11] to compute the BP, whereas the WP is computed by using WSP.

Shortest Path (SP) — This scheme computes both the WP and BP using the WSP routing algorithm [2].

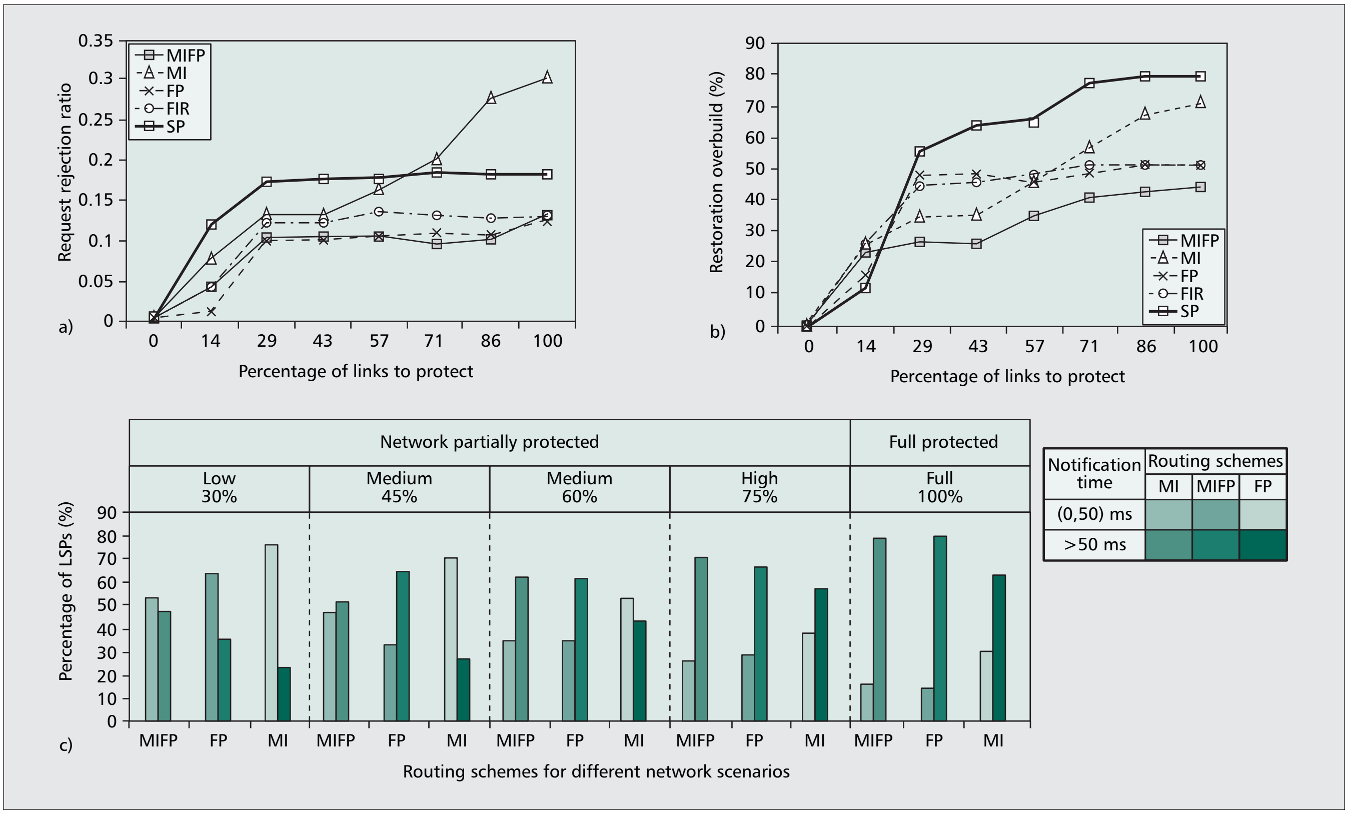
Routing Information

Open Shortest Path First (OSPF) or Intermediate System-Intermediate System (IS-IS) can be used to distribute link state information by flooding for all routing schemes. The information required (e.g., the MRB used by WSP) is available in the current Generalized MPLS (GMPLS) OSPF and IS-IS extensions. Other information, such as the total reserved restoration resources over all network links used by the FIR algorithms to compute shared backups, can be obtained by signaling [11].

Performance Evaluation

Network Topology and Traffic Requests

For this set of experiments the KL topology described in [3, 5, 9, 10] has been used. The capacity of the links is 12 and 48 units, scaled by 10 in order to experiment with thousands of LSPs. Each link is bidirectional (i.e., it acts as



■ **Figure 2.** *a) Request rejection ratio; b) restoration overbuild; c) notification time analysis for different network scenarios.*

two unidirectional links of that capacity). There are 15 nodes and 28 links.

In the simulation experiments, label switched path (LSP) requests arrived randomly at the same average rate for all ingress-egress node pairs. The main objective was to determine the behavior of various protection schemes in a dynamic scenario. LSP requests arrive between each ingress-egress pair according to a Poisson process with an average rate λ, and the holding times are exponentially distributed with a mean value of 1/μ. In this set of experiments, λ/μ = 150. Ten independent trials were calculated over a window of 10,000 LSP setup requests. The requested bandwidth for LSPs is uniformly distributed into one, two, or three units.

Figures of Merit

To evaluate the algorithm's performance, three figures of merit were used in the experiments: the *request rejection ratio*, *restoration overbuild* (percentage of bandwidth used as a BP), and *failure notification time*. In order to compute the failure notification time, a link length was assigned randomly between 200 and 1000 miles for each network link. Different network scenarios with diverse protection requirements, expressed in terms of number of links to protect at the MPLS level, were used.

Simulation Results

Request Rejection Ratio and Restoration Overbuild — Figure 2a shows that the proposed algorithms, MIFP and FP, present better behavior than algorithms MI, FIR, and SP. Using only minimum interference routing when 1:*n* protection is required (e.g., MI) results in very low performance, particularly when the network protection requirements increase. In Fig. 2a the MI request rejection ratio dramatically increases from 40 percent of network protection requirements. This is due to the fact that MI is unable to find shared capacity when network protection requirements are medium or high. For full protection (100 percent) MI is up to three times worse than other non-MI techniques, such as FP. In Fig. 2b algorithms that only aim to minimize the restoration overbuild (i.e., FIR and FP) present similar behavior through the experiment. However, our proposed method, MIFP, outperforms these algorithms by combining both minimum interference and a sharing-oriented BP computation.

Failure Notification Time — Figure 2c shows the quality of protection in terms of the percentage of protected LSPs with an approximated failure notification time less than or equal to 50 ms and the percentage of LSPs with a failure notification time greater than 50 ms. The percentage of large failure notification time segments (higher than 50 ms) was compared with low failure notification time segments (less than 50 ms). This 50 ms threshold is just a heuristic selection; there is no direct relation with the 50 ms restoration time of some physical transmission system technologies. The failure notification time was analyzed for diverse network protection requirements using our proposed routing schemes: MIFP, FP and MI. The FIR and SP algorithms were not considered since they just use the global/path protection to compute the backup path.

For building Fig. 2c, maximum notification times were used as the approximate average of the restoration times of each algorithm. This measure provides an approximate range of the notification time between end nodes of a particular protected segment based on the failure recovery constraint described earlier.

Figure 2c shows that both MIFP and FP algorithms offer a similar failure notification time through the experiment for medium and full protection except for low (30 percent) and medium (45 percent) protection. For low protection, the number of LSPs with a notification time longer than 50 ms is 50 percent for MIFP, while FP accumulates less LSPs with a notification time longer than 50 ms (35 percent). Thus, FP offers a better failure notification time than MIFP. However, for 45 percent medium protection, MIFP reports a better failure notification time. For total network protection (path protection) both algorithms report a high percentage of LSPs with a long propagation time. Therefore, only fast protection is suitable for the low-medium level of protection in terms of number of links to be protected. The MI algorithm reports better performance through the experiment. It accumulates more LSPs with failure notification time less than 50 ms. MI sets up more segment backup paths in order to protect the WP using a high amount of resources. However, as a result of the large amount of resources used to protect the BP, MI has a high request rejection ratio (Fig. 2a).

The quality of protection is only analyzed in terms of failure notification time. However, traffic differentiation is expected in future networks. In previous work, such as [15], a characterization of differentiated services (DiffServ) classes according to their protection requirements (including failure recovery time) was made. Not all the classes must be deployed over fast protected LSPs, only a small percentage of them. Figure 2c shows the percentage of LSPs with fast protection (failure recovery time) that could be set up using the analyzed algorithms. For instance, for partial protection (45 percent) using MIFP nearly 50 percent of LSPs with fast protection could be set up, while for full protection only 20 percent could be found. This figure and the previous one help us decide which routing algorithm to use whenever differentiated traffic services are required.

The proposed methods have shown that the fast-protected paths with low resource consumption can be achieved, even in network scenarios with full network protection requirements.

Conclusions

Using the minimum interference concept improves the efficiency of classic QoS routing algorithms, such as WSP. However, some implementations like MIRA are too complex to be practical. LMIR overcomes this drawback with a similar practical performance. However, these algorithms do not consider network protection as an objective; although in [5] 1+1 protection techniques are used, the high resource consumption makes this inapplicable in a generalized manner. Full information and backup sharing methods provide better resource utilization. The presented results show that the minimum interference paradigm is not efficient enough to establish protection without high resource consumption (i.e., using shared backup paths). In this case techniques that combine minimum interference for WP selection and sharing oriented algorithms for BP selection, such as the proposed MIFP, provide a lower request rejection ratio and better resource utilization.

Moreover, the level of protection for the proposed algorithms was analyzed. In this way an approximate range for the recovery time has been proposed based on the notification time of the failure. When traffic differentiation is applied, the selected paths should offer a certain quality of protection, such as a maximum failure recovery time. The proposed methods have shown that the fast-protected paths with low resource consumption can be achieved, even in network scenarios with full network protection requirements.

Acknowledgment

Part of this work was supported by the National High Technology Research and Development Program of China (863 Program) under Grant 2002AA122032 and the National Science Foundation Council of China under Grant 60272053. Part of this work was supported by the National Science Council of Taiwan under Grant NSC 92-2416-H-004-017. This work was partially supported by the EU COST 293 and the Spanish Research Council (CICYT) under contract TIC2003-05567. This work of A. Urra was also supported by the Catalan Department of Universities, Research and Information Society (DURSI) and European Social Funds.

References

[1] D. Awduche *et al.*, "Requirements for Traffic Engineering over MPLS," IETF RFC 2702, Sept. 1999.

[2] R. Guerin, D. Williams, and A. Orda, "QoS Routing Mechanisms and OSPF Extensions," *Proc. GLOBECOM 1997*.

[3] M. Kodialam and T. V. Lakshman, "Minimum Interference Routing with Applications to MPLS Traffic Engineering," *Proc. INFOCOM 2000*.

[4] M. Kodialam and T. V. Lakshma, "Integrated Dynamic IP and Wavelength Routing in IP over WDM Networks," *Proc. INFOCOM 2001*, Apr. 2001, pp. 358–66.

[5] K. Kar, M. Kodialam, and T. V. Lakshman, "Routing Restorable Bandwidth Guaranteed Connections using Maximum 2-Route Flows," *Proc. INFOCOM 2002*.

[6] Illias Iliadis and Daniel Bauer, "A New Class of Online Minimum-Interference Routing Algorithm," *Proc. Networking 2002*, *LNCS*, vol. 2345, May 2002, pp. 959–71.

[7] Bin Wang, Xu Su, and C. L. P. Chen, "A New Bandwidth Guaranteed Routing Algorithm for MPLS Traffic Engineering," *Proc. ICC 2002*, 2002, pp. 1001–05.

[8] F. Sun and M. Shayman, "Minimum Interference Algorithm for Integrated Topology Control and Routing in Wireless Optical Backbone Networks," *Proc. ICC 2004*.

[9] G. B. Figueiredo, N. L. S. Fonseca, and J. A. S. Moneiro, "A Minimum Interference Routing Algorithm," *Proc. ICC 2004*.

[10] M. Kodialam and T. V. Lakshman, "Dynamic Routing of Bandwidth Guaranteed Tunnels with Restoration," *Proc. INFOCOM 2000*.

[11] G. Li *et al.*, "Efficient Distributed Path Selection for Shared Restoration Connections," *Proc. INFOCOM 2002*.

[12] V. Sharma *et al.*, "Framework for Multi-Protocol Label Switching (MPLS)-Based Recovery," IETF RFC 3469.

[13] R. Bhandari, *Survivable Networks: Algorithms for Diverse Routing*, Kluwer, 1999.

[14] P.-H. Ho *et al.*, "On Achieving Optimal Survivable Routing for Shared Protection in Survivable Next-Generation Internet," *IEEE Trans. Reliability*, vol. 53, no. 2, June 2004.

[15] J. L. Marzo *et al.*, "QoS Online Routing and MPLS Multilevel Protection: A Survey," *IEEE Commun. Mag.*, Oct. 2003.

Biographies

Eusebi Calle received his doctorate degree in computer science from the University of Girona (UdG), Spain, in 2004. Since 1998 he has been a member of the research and teaching staff in the Broadband Communications and Distributed System Group of UdG, where he develops his research in GMPLS fault management and QoS routing. He has co-authored several papers in international journals and international conferences. He is also part of the Computer Department in the Education Department at Girona and a member of the Institute of Informatics and Applications at UdG.

Anna Urra received an M.Sc. degree in computer science from UdG in 2002, where she currently is pursuing a Ph.D. degree. Since 2003 she has been with the Broadband Communications and Distributed System Group of UdG. Her research interests include multilayer survivability, optical networks, network management, and QoS routing.

Jose L Marzo is an associate professor at the Electronics, Informatics and Automatics Department of UdG. He received his doctorate degree in industrial engineering from UdG in 1997. From 1978 to 1991 he was with Telefonica de Espana, where he had different responsibilities such as head of the engineering department, and head of the planning and programming office, among other technical tasks. His research interests are in the fields of management and performance evaluation of communication networks, network management based on intelligent agents, MPLS and GMPLS, and distributed simulation. He leads a research group on broadband communications and distributed systems (BCDS). He serves on the editorial board of *International Journal of Communications Systems*. He has co-authored several papers published in international journals and presented at leading international conferences.

G. S. Kuo (gskuo@ieee.org) currently is a professor at National Chengchi University, Taiwan. From 2001 to 2002 he was Editor-in-Chief of *IEEE Communications Magazine*. Currently, he is Area Editor of Network Architecture for *IEEE Transactions on Communications*, ComSoc Representative to *IEEE Internet Computing*, and Regional Editor for Asia of *European Transactions on Telecommunications*.

Hai-Bo Guo obtained his B.S. and Ph.D. degrees, both in communications engineering, from Beijing University of Posts and Telecommunications (BUPT) in 1999 and 2005, respectively. From 2002 to 2005 he worked at National Key Laboratory of Switching and Networking Technologies in BUPT as a Ph.D. student. His research interests include resource management and media access control in future wireless networks, mobile IP, next-generation network control plane, GMPLS, and EPON-based optical access networks. Currently, he serves as a Ph.D. patent examiner in communication fields at the State Intellectual Property Office of P.R. China.

IEEE Communications Magazine
Call for Papers
Network & Service Management Series

IEEE Communications Magazine announces the creation of a new series on Network and Service Management. The series will be published twice a year, in April and October, with the first issue planned for October 2005. It intends to provide articles on the latest developments in this well-established and thriving discipline. Published articles are expected to highlight recent research achievements in this field and provide insight into theoretical and practical issues related to the evolution of network and service management from different perspectives. The series will provide a forum for the publication of both academic and industrial research, addressing the state of the art, theory and practice in network and service management. Both original research and review papers are welcome, in the style expected for IEEE Communications Magazine. Articles should be of tutorial nature, written in a style comprehensible to readers outside the speciality of Network and Service Management. This series therefore complements the newly established IEEE Electronic Transactions on Network & Service Management (eTNSM). General areas include but are not limited to:

* Management models, architectures and frameworks
* Service provisioning, reliability and quality assurance
* Management functions
* Management standards, technologies and platforms
* Management policies
* Applications, case studies and experiences

The above list is not exhaustive, with submissions related to interesting ideas broadly related to network and service management encouraged.

IEEE Communications Magazine is read by tens of thousands of readers from both academia and industry. The magazine has also been ranked the number one telecommunications journal according to the ISI citation database for year 2000, and the number three for year 2001. The published papers will also be available on-line through Communications Magazine Interactive, the WWW edition of the magazine. Details about IEEE Communications Magazine can be found at http://www.comsoc.org/ci/.

Schedule for the First Issue

Manuscripts due: March 30, 2005
Acceptance notification: June 30, 2005
Manuscripts to publisher: July 30, 2005
Publication date: October 2005

Series Editors

Prof. George Pavlou
Center for Communication Systems Research
Dept. of Electronic Engineering
University of Surrey
Guilford, Surrey GU2 7XH, UK.
e-mail: G.Pavlou@eim.surrey.ac.uk

Dr. Aiko Pras
Center for Telematics and Information Technology
Dept. of Electrical Engineering, Mathematics and Computer Science
University of Twente
P.O. Box 217, 7500 AE Enschede, The Netherlands.
e-mail: a.pras@utwente.nl