Performance evaluation of minimum interference routing in network scenarios with protection requirements

Jose L. Marzo a,*, Eusebi Calle a, Pere Vilà a, Anna Urra b

a Institute of Informatics and Applications (IIiA), University of Girona, Campus Montilivi, 17071 Girona, Spain
b Cisco Systems Inc, 1414 Massachusetts Avenue, Boxborough, MA 0171, United States

Abstract

Minimum interference routing schemes are good options for achieving fewer working-path request rejections. They improve the vast majority of the current QoS routing proposals. However, when backup paths are added there is no guarantee of achieving a similar performance. In this paper, we analyze the suitability of these routing schemes in protected network scenarios. The main objective was to define the network scenarios in which the required performance can be achieved using only minimum interference. Some simulation results are presented to consider different network topologies and different routing schemes and to show the main drawbacks and advantages of using minimum interference schemes in protected network scenarios.

Keywords: Network protection; Minimum interference routing; QoS routing

1. Introduction

As networks grow and offer better quality of service, the consequences of a failure become more pronounced. Network reliability is therefore seen as a key requirement for new traffic engineered networks [1]. This involves new routing schemes that offer both high performance (in terms of the number of accepted connection requests) and suitable protection according to the defined requirements.

A minimum interference technique that increases the number of accepted paths in the network is proposed as one of the most effective techniques for improving online routing: the minimum interference routing algorithm (MIRA) [2]. MIRA identifies “critical” paths and avoids overloading them in order to minimize the future request rejection ratio. The identification is based on a pre-process phase of maximum flows. Although this family of algorithms improves previous QoS routing proposals, it involves long and complex computations. Some recent approaches, such as LMIR [3] and FMIRA [4], overcome this drawback by avoiding the maxflow computation. However, the most important minimum interference QoS online routing proposals do not include protection among their main objectives due to the very complex evaluation involved. Some preliminary proposals, which do consider protection in their objectives, have a high computational cost. One such example is an evolution of MIRA that uses dedicated 1+1 protection called minimum interference restorable routing [5] (MIRR).

However, 1+1 or 1:1 protection (dedicated protection) uses a large amount of spare restoration capacity; hence, it is not cost effective for most customer applications [6]. Significant reductions in spare capacity can be achieved by sharing this capacity across independent failures. The accuracy and performance of the shared backup schemes are based on the available network information. An initial proposal for computing shared backups is based on partial routing information (PIR). In [7], an in-depth analysis that compares different shared backup proposals is presented. Full information routing (FIR) schemes are proposed as...
the most effective mechanisms. FIR assigns a weight to each link based on the maximum capacity needed if a link of the protected path fails.

The main objective of this paper is to define situations in which minimum interference routing with protection can be effectively used. To do this, a comparison between some very well known routing proposals, such as widest shortest path (WSP), minimum interference routing and some techniques that offer effective shared backups, are presented.

2. Related work: minimum interference routing algorithms

In this section, the concept of minimum interference is introduced. An overview of some of the main current minimum interference proposals is also given.

2.1. The concept of minimum interference routing

Minimum interference schemes were introduced in the “minimum interface routing algorithm” (MIRA) [2] taking into consideration particular aspects of the MPLS architecture to design an online routing scheme. In this case, ingress and egress nodes are taken into account. Kodialam and Lakshman introduce the concept of interference and develop a multiple maxflow computation to determine the path of least interference.

The main idea of interference is to establish paths that do not interfere “too much” with future label switch path (LSP) setup requests and consider pre-established values of ingress–egress pairs. Fig. 1 shows an example of this “interference” effect. Consider the maximum-flow (maxflow) value I between a given ingress–egress (Source–Destination) pair (S1, D1). Note that the maxflow value I decreases whenever a bandwidth demand is routed between S1 and D1. The value of I can also decrease when an LSP is routed between another ingress–egress pair. The amount of interference on a particular ingress–egress pair, for example (S1, D1), is defined and an LSP is routed between another ingress–egress pair as the value of I decreases.

Existing LSP1 (S1, D1); LSP2 (S2, D2); and LSP3 are required between S3 and D3. If the MHA (minimum hop algorithm) is used, the route between (S3, D3) will be 1-2-3-4-5. This route produces a blocking path between S2 and D2 as well as between S1 and D1. In this example it is better to choose route 1-2-3-4-5 even though the path is longer.

The minimum interference path for an LSP between, for example (S1, D1), is the explicit route which maximizes the minimum maxflow between all other ingress–egress pairs.

In other words, this can be thought of as choosing a path between (S1, D1) which maximizes the minimum residual capacity between every other ingress–egress pair.

The objective might be to choose a path that maximizes a weighted sum of the maxflows between every other ingress–egress pair. This algorithm not only makes capacity available for the possible arrival of future demands, but also makes capacity available for rerouting LSPs if there are link failures.

Another concept introduced in minimum interference schemes is the concept of critical links. Critical links are links characterized by a decrease in the maxflow value of one or more ingress–egress pairs whenever an LSP is routed over them. This is the criteria for creating a weighted graph.

The path selection by shortest path computation is carried out using the well known Dijkstra or Bellman-Ford algorithms to compute the present explicit route. They do this by generating a weighted graph where the critical links have weights that are an increasing function of their criticality. The increasing weight function is chosen to defer loading the critical links whenever possible. The actual explicit route is calculated using a shortest path computation as in other routing schemes.

2.2. Minimum interference routing review

In this section a survey of the evolution of minimum interference routing schemes is introduced. Not all schemes are included. We focus only on some schemes that introduce new concepts such as those oriented to specific technologies (wireless or optical networks) and those reporting significant performance improvements.

Minimum interference routing was extended to include lightpath establishment (wavelength routing) as well as routing in the logical topology in the maximum open capacity routing algorithm (MOCA) [8]. The same authors proposed a version which included 1+1 protection. An evolution of MIRA using dedicated 1+1 protection is MIRR [5]. However, these algorithms include complex computations with long calculation times. In order to overcome this drawback, new proposals are introduced.

A first proposal without maximum-flow calculations is presented by Iliadis in simple MIRA (SMIRA) [9]. SMIRA uses a new procedure for obtaining the set of critical paths without maximum-flow computation, called k-widest shortest path 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 no maximum-flow calculations to obtain the critical links, is Wang, Su, and Chen’s (WSC) algorithm [10]. These algorithms are also proposed for MPLS-based network scenarios. Two enhanced proposals of SMIRA and WSC are presented in integrated SMIRA (SMIRA-I) [11] and light minimum interference routing (LMIR) algorithm [3].

Light minimum interference routing (LMIR) is one of the most recent proposals [3]. LMIR uses a modified Dijk-
3. Minimum interference and shared protection

We would like to investigate whether a suitable performance can be reached by using only minimum interference for selecting both the working and backup paths. With this in mind, first we have to select the most suitable minimum interference routing. As mentioned previously, techniques without maximum flow computation, such as the LMIR, can be used easily in real network scenarios. These techniques offer high performance without long computation time.

Dedicated protection (e.g., 1+1, or 1:1) typically uses a large amount of spare restoration capacity. Thus, some recovery schemes are not cost effective for most customer applications. Significant reductions in spare capacity can be achieved by sharing this capacity across multiple, independent failures.

In this paper, we use the concept of restoration overbuild to evaluate the resource consumption under protection utilization. Restoration overbuild is defined as the percentage of bandwidth allocated for backup paths divided by the percentage of bandwidth allocated for working paths. Dedicated protection schemes, such as 1+1, can easily exceed 100% of the extra resources to protect the working paths. In this paper, we focus on shared protection schemes in order to offer the maximum number of accepted requests when combining minimum interference routing for the working and backup paths.

Different, more or less accurately shared protection schemes are developed depending on the available network information. In [6], an in-depth analysis comparing different shared backup proposals is presented. Full information routing (FIR) schemes were proposed to be the most effective mechanisms. The main idea of FIR is based on assigning weight to each link based on the maximum bandwidth needed if any of the links of the protected path fail and if any of the network links fail.

In this section we review and formalize selection of the working path and backup path using LMIR and FIR techniques. In the next section these techniques are combined with well known QoS routing algorithms, such as the widest shortest path, in order to make comparisons.

Let \( G = (V, E) \) describe the given network, where \( V \) is the set of network nodes and \( E \) is the set of network links. Assuming that there is a set of distinguished node pairs \( P \), where each node belongs to \( V \), \( P \) can be thought of as the set of potential ingress-egress node pairs. Therefore, all requests are assumed to occur between these pairs. A generic element of this set \( P \) is denoted by \( (s, d) \). A setup request is defined by \( (s, d, r) \), where \( r \) specifies the amount of required capacity. For each request, a working path and a backup path have to be set up. If there is not sufficient capacity in the network for either the working or the backup path for the current request, the request is rejected. If the connection is accepted, all links on its working path will reserve units of capacity. For the backup path, the allocated capacity depends on the amount of capacity that can be shared in each of its links.

3.1. Selecting the working path

Let us assume that the working path is selected by applying the light minimum interference routing (LMIR) algorithm [3]. LMIR attempts to find the feasible paths with the lowest capacities out of all the \((s, d)\) pairs in order to determine the critical edges. Dijkstra’s algorithm is modified to find the paths with the lowest capacity to identify the critical edges. LMIR does not assume knowledge about future requests or about statistical traffic profiles.
Once the lowest capacity paths are identified, a weight is assigned to all the network links that have a capacity equal to or greater than the capacity required by the path, and other links are no longer considered. Finally, Dijkstra's algorithm is applied using the computed weights and thereby avoiding critical links. We refer the reader to [3] for more details.

### 3.2. Shared backup routing algorithm

Once the working path is calculated, the backup path, which must be link-disjointed from the working path, is computed. A possible approach for selecting the backup path is to use full information routing (FIR) techniques [7]. A weight, \( w_i \), is assigned to each network link \( i \) based on the maximum capacity needed if a link of the working path fails.

\[
\begin{align*}
    w_i &= \begin{cases} 
    \frac{\min(r, T[i] + r - R[i])}{C[i]} & \text{if } T[i] + r - R[i] > 0 \\
    \infty & \text{if } i \in WP \\
    0 & \text{if } T[i] + r - R[i] \leq 0 \\
    \end{cases}
\end{align*}
\]

where \( R[i] \) is the maximum capacity required in link \( i \) to restore all the failed paths if a network link fails; \( T[i] \) is the maximum capacity needed in link \( i \) if a link along the working path fails. All this information is available through OSPF extensions [17]. Afterwards, Dijkstra’s algorithm is used to select the backup path that minimizes \( \sum w[i] \).

### 4. Proposed schemes for evaluating the suitability of minimum interference routing with protection

In this section four routing algorithms are presented. The objective of this paper is to show that when using only minimum interference to compute both the working and the backup paths we can achieve a similar performance as in network scenarios without protection computation. The presented routing algorithms are based on a well known QoS routing algorithm (WSP) [18], a minimum interference algorithm (LMIR) and a method for selecting shared backup paths (FIR).

Table 2 summarizes the proposed algorithms.

1. Minimum interference – minimum interference routing (MM). This scheme only focuses on minimizing the interference. Both the working and the backup paths are evaluated using minimum interference techniques. LMIR, as explained in the previous section, is used as the minimum interference technique (Section 2.2). This algorithm is the target algorithm used to show that a suitable performance can be achieved by using minimum interference only. This algorithm does not consider bandwidth sharing in the backup path evaluation.

2. Widest shortest path – widest shortest path routing (WW). This objective of this scheme is not to account minimizing the interference. Moreover, backup paths are selected without the objective of sharing capacity. This algorithm uses the widest shortest path (WSP) [19] to compute both the working path and the backup path.

3. Widest shortest path full information routing (WF). This scheme selects the widest shortest working path and evaluates the backup path that reports the highest shareable capacity, using the FIR techniques described in Section 3.

4. Minimum interference full information routing (MF). This scheme combines the minimum interference to choose the working path and selects the backup path with the highest shareable capacity. Thus, LMIR is used to compute the working path, and FIR to compute the backup path (as explained in Section 3).

### Table 1

<table>
<thead>
<tr>
<th>Routing schemes</th>
<th>Year</th>
<th>Network scenario</th>
<th>Complexity (1)</th>
<th>Protection scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIRA</td>
<td>2000</td>
<td>MPLS</td>
<td>High</td>
<td>None</td>
</tr>
<tr>
<td>MOCA</td>
<td>2001</td>
<td>IP/MPLS over WDM</td>
<td>High</td>
<td>None</td>
</tr>
<tr>
<td>MIRR</td>
<td>2002</td>
<td>IP/MPLS over WDM</td>
<td>High</td>
<td>1+1</td>
</tr>
<tr>
<td>SMIRA</td>
<td>2002</td>
<td>MPLS</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>WSC</td>
<td>2002</td>
<td>MPLS</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>SMIRA_I</td>
<td>2004</td>
<td>Wireless-optical</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>LMIR</td>
<td>2004</td>
<td>MPLS</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>MIRO</td>
<td>2005</td>
<td>Optical</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>LCPF</td>
<td>2005</td>
<td>MPLS</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>A2F</td>
<td>2006</td>
<td>MPLS</td>
<td>Low</td>
<td>1+1</td>
</tr>
</tbody>
</table>

Historical evolution.

(1) High complexity means maximum-flow calculations are executed.
5. Simulation results

A set of simulations was carried out to determine the behavior of the above protection schemes in a dynamic scenario. For this set of experiments the NSF, KL, and European networks were also adopted to evaluate the algorithms’ performances in different network topologies and network loads. Further details about the topology features (diameter, node degree, number of nodes/links) can be found in Table 3 and Fig. 2. Each link is bi-directional. In the simulation experiments path requests arrived randomly at the same average rate for all ingress-egress node pairs. Paths arrived between each ingress-egress pair according to a Poisson process with an average rate \( \lambda \). Holding times were exponentially distributed with a mean of \( 1/\mu \). In this set of experiments four different network loads were evaluated: low, medium, high, and very high (\( \lambda/\mu = 25, 50, 75, \) and 100, respectively). Ten independent trials were executed over a window of 10,000 LSP requests. The allocated capacity for each path was uniformly distributed into 10, 20, and 30 capacity units.

The performance, when using only minimum interference for both working and backup paths (MM algorithm), is analyzed in Fig. 3a. In this case MM performs very well for low and medium network loads, with a very low request rejection. In the case of European and KL topologies, with similar network features (see Table 3), MM is always under 12% rejection. When using the NSF topology, the algorithm shows a dramatic increase in the request rejection ratio (especially in the case of high or very high network load). That is partly due to the physical network’s features: a very small diameter and network degree, compared to the European and the KL topologies. Moreover, minimum interference routing tends to select long paths, which is suitable for avoiding critical paths. This technique is very suitable in networks where it is easy to find more than one alternative path from the source to destination with a similar number of hops. This is not the case of NSF where only a few paths can be found from the source to destination. In networks, such as NSF and when adding backup paths, long paths increase the request rejection ratio dramatically. This effect is especially dramatic in the case of high network loads.

In order to compare this behavior, Fig. 3b shows the same experiment using WW. This algorithm focuses mainly on reducing the amount of resources (bandwidth) by selecting the shortest paths. In this case the performance for the KL and European topology is very similar to the MM experiment (MM is slightly better for low and medium loads), WW even outperforms MM in the NSF case. This can be partially explained in Fig. 5a. In this figure it can be observed that WW only needs 50% of the extra resources for protection, while MM uses more than 70%. This percentage is applicable throughout the experiment. However, for high network loads, as explained above, MM (minimum interference) selects longer paths than...
This, combined with NSF characteristics, is the reason for WW's better performance. We might initially conclude that MM slightly outperforms WW in the case of KL and European topologies. These topologies are suitable for minimum interference routing schemes. However, in topologies where minimum interference does not perform very well (without protection), introducing the computation of backup paths results in a worse performance result.

As can be seen, MM requires large amounts of resources for protection (70%, 74%, and 80% in Fig. 5a). This is because longer backup paths are used and shared capacity is used badly. In Fig. 5b, it can be observed that MM achieved, on average, a 15–20% lower level of sharing than WW. In the next set of experiments, techniques for reducing the amount of resources used for protection are analyzed.

In MF (Fig. 4a), a proposal to use more suitable backup computation techniques (in terms of shared capacity) combined with minimum interference is analyzed. This method (as expected), outperforms MM and WW, in the European and KL topologies. For high network loads the request rejection decreases from 12% in the case of MM to 1.8% in the case of combining minimum interference and the FIR techniques (MF). The main reason for this perfor-

![Fig. 3. Request rejection ratio study for different network loads and different network topologies: (a) the working and the backup paths are computed using LMIR (MM) and (b) the working and the backup paths are computed using WSP (WW).](image)

![Fig. 4. Request rejection ratio study for different network loads and different network topologies: (a) the working is computed using LMIR and the backup path is computed using FIR (MF) and (b) the working is computed using WSP and the backup paths are computed using FIR (WF).](image)

![Fig. 5. Average of (a) the restoration overbuild and (b) the level of sharing for different network topologies.](image)
management increase is that MF requires about 30% less extra resources for protection than MM. This 30% also reduces the request rejection ratio when the NSF topology is used.

In this case, MF is able to reduce the request rejection ratio (in the case of high network load) from 29% to 14%. However, compared to the results obtained in KL and European topologies for high loads, minimum interference (MF) has a persistently bad performance.

It is also interesting to compare MF with WF. This is done in Fig. 4b. WF selects shorter paths than MF. However, WF does not perform as well as our proposal (MF) for the European and KL topologies. In this case, the effect of minimum interference combined with FIR outperforms WF. However, in topologies such as the NSF case, WF, as in the above set of experiments, outperforms MF for higher and lower network loads.

6. Conclusions

In this paper, minimum interference routing schemes have been reviewed. A complete review of the main minimum interference schemes ordered according to complexity has also been presented. Once the main schemes were compared, light MIRA (LMIR) was selected as a suitable candidate for analyzing minimum interference when adding protection.

Results have shown that by using minimum interference routing to route the working and the backup paths (MM algorithm) a similar performance is obtained proportionally to the case of non-protection. This performance can be achieved for low and medium network loads, and with similar topologies (European and KL). For scenarios with high or very high network load demands or for network topologies with very specific characteristics (such as the NSF, with very low diameter and network degree), minimum interference routing performance dramatically decreases. This is due to the minimum interference method which avoids using shared links that are identified as critical. Due to this fact, minimum interference routing requires a very large amount of resources for protection compared to other routing techniques.

To overcome these problems, a new routing method was introduced into the analysis, which combines minimum interference routing and a shared backup scheme. In this case, results have shown that when the network load increases, the use of techniques focused on sharing backup paths (such as FIR) are able to reduce the number of request rejections, therefore making a more suitable use of the capacity for protection.

In summary, in this paper a first analysis of the suitability of using minimum interference routing schemes combined with protection has been introduced. This study is the first of its kind and more network scenarios can also be taken into account. These initial results have shown the feasibility of using minimum interference in network scenarios with high demands for reliability and request acceptance. This study can be enhanced by introducing other protection or restoration techniques, analyzing other minimum interference schemes, and including other network topologies. Furthermore, in this paper the first drawbacks and advantages of using minimum interference routing with protection have been identified.

Acknowledgements

This work was partially supported by the Spanish Research Council (TEC2006-03883/TCM) and the Generalitat de Catalunya (Grant SGR-00296).

References


Please cite this article in press as: J.L. Marzo et al., Performance evaluation of minimum interference routing ..., Comput. Commun. (2007), doi:10.1016/j.comcom.2007.05.044
Jose´ L. Marzo is a senior lecturer in the Department of Electronics, Computer Science and Automatic Control of the University of Girona, Spain. He received his Ph.D. degree in Industrial Engineering from the University of Girona in 1997. From 1978 to 1991, he was with Telefonica, as head of the engineering department and head of the planning and programming office in Girona. 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 heads the Broadband Communications and Distributed Systems research group. He has coordinated the participation of this research group in various national and Spanish research projects.

Eusebi Calle is an associate lecturer in the University of Girona. He has been working in the Department of Electronics, Computer Science and Automatic Control for the last 8 years. He is a member of the Broadband Communications and Distributed Systems research group (BCDS) at the Institute of Informatics and Applications. He has a Ph.D. in Computer Science from the University of Girona (2004). His research interests are in the fields of routing, protection, and performance evaluation of communication networks, MPLS and GMPLS. He has co-authored over 30 papers in journals and international conferences.

Pere Vila has been a Computer Science researcher and associate lecturer in the Department of Electronics, Computer Science and Automatic Control of the University of Girona (Spain) since 1998, where he is a member of the Broadband Communications and Distributed Systems research group (BCDS) at the Institute of Informatics and Applications. He has a Ph.D. in Computer Science from the University of Girona (2004). His research interests are in the fields of management and performance evaluation of communication networks, distributed network management based on intelligent agents, MPLS and GMPLS. He has coordinated the participation of this research group in various national and Spanish research projects.

Anna Urra is a researcher at CISCO Systems in Boston. She recently got her Ph.D. in Computer Science (2006) from the University of Girona (Spain) in the Department of Electronics, Computer Science and Automatic Control, where she was working as a member of the Broadband Communications and Distributed Systems research group (BCDS) at the Institute of Informatics and Applications. Her research interests are in the fields of routing, protection, and performance evaluation of communication networks, MPLS and GMPLS. She has worked on several national projects of the Spanish Ministry of Education and Science and has carried out research stays at Georgia Institute of Technology (Atlanta) and at the University of Strathclyde (Glasgow).