

**Instituto de Engenharia de Sistemas e Computadores de
Coimbra**
Institute of Systems Engineering and Computers
INESC - Coimbra

Catarina Francisco, Lúcia Martins,
João Redol, Paulo Monteiro

**Multiservice Protection Algorithms
in IP Mobile Backhaul**

No.6

2011

ISSN: 1645-2631

Instituto de Engenharia de Sistemas e Computadores de Coimbra
INESC - Coimbra
Rua Antero de Quental, 199; 3000-033 Coimbra; Portugal
www.inescc.pt

Multiservice Protection Algorithms in IP Mobile Backhaul

June 7, 2011

Contents

1	Introduction	3
2	Previous work - DARMP and MODR	5
2.1	DARMP	5
2.2	MODR	6
3	Protection Mechanism	7
3.1	Protection with Multiservice Dynamic Alternative Routing with Multiple Protection paths (MDARMP)	8
3.2	Protection with Multiple Objective Dynamic Routing with Multiple Protection paths (MODRMP)	9
4	Study Environment	11
4.1	MODRMP	13
4.2	Results Analysis	13
4.2.1	Network A	13
4.2.2	Network B	22
5	Conclusion	28
	List of Figures	29
	List of Tables	30
	Bibliography	31

Chapter 1

Introduction

With the advent of higher-capacity third-generation (3G) radio access technology, mobile operators have launched additional services such as mobile email, videotelephony, audio and video streaming, and so on. In fact, the volume of data traffic in mobile networks has already surpassed that of voice traffic [5]. However, since the new services are broadband, they have the potential to generate more traffic with additional operational costs [3]. Traditional TDM/ATM environment will neither scale to the required bandwidth nor meet the cost reduction requirements and so mobile service providers are deploying IP/Ethernet in the backhaul to move as quickly as possible to an all-IP infrastructure. However, traditional IP technologies do not provide efficient reliability, manageability and network synchronization. To accomplish carrier-class service transport it is necessary to have carrier-class IP transport networks. MPLS appears as a solution to support the migration from legacy (TDM/ATM) to IP-based radio access networks (RANs) providing, at the same time, resiliency and OAM (Operation, Administration, and Maintenance) functions that can be used to ensure the reliability and traffic engineering capabilities of the mobile backhaul [6].

A major goal of Internet Traffic Engineering (TE) is to enable efficient and reliable network operation, while simultaneously enabling to maximize network resources utilization and traffic throughput [10]. In that sense, MPLS TE offers service providers the mechanisms to optimize their infrastructure by distributing traffic through explicit routing where paths can be calculated by appropriate algorithms.

To provide a carrier-class recovery (in 50 ms - the SONET time), IETF's MPLS working group has developed a local protection mechanism (FRR), where the node immediately upstream the failing facility redirects the affected traffic to the backup path. However, in order to enable a fast protection mechanism, current MPLS FRR approaches usually imply bandwidth reservation that leads to bandwidth waste when there are no failures. This may be particularly critical in a period of time in which capacity is becoming a scarce resource for 3G traffic volumes.

As mentioned before, mobile broadband networks support a variety of heterogeneous services which must be delivered in line with subscriber's expectations in terms of bandwidth, packet loss, delay, etc. The need of dealing with multiple and multifaceted QoS requirements leads to a potential advantage in the formulation of the optimization problems, in this network environment, as

multicriteria problems. Multicriteria formulations enable to take advantage of the trade-offs between the objective functions explicitly involved in the problem in order to choose in each case appropriate non-dominated solutions. A non-dominated solution, or a Pareto optimal solution, is a feasible solution such that there is no other feasible solution which improves one objective function without worsening the value of any other objective.

In [13], we have presented a multiple objective dynamic routing (MODR) method for telecommunication networks, extensively explained in [11, 12], which was adapted in order to obtain a suitable version for application to a realistic IP/MPLS network environment. Alternative routing is a routing scheme that allows a second-chance to a connection whose first-choice path does not have the available resources to meet its QoS requirements.

The use of dynamic alternative routing improves network survivability because of its ability to reroute traffic in congestion or failure situations [1]. In case of a link failure, the only problem this approach doesn't address is the traffic in progress which is lost. Traffic rescue can only be accomplished by recovery mechanisms where a pair of link-disjoint paths (primary and backup) are provided between each node pair.

In [7] we have proposed a local protection scheme to be used in association with a well-known alternative routing method (Dynamic Alternative Routing [9]) in order to route not only the newly incoming traffic but also the ongoing traffic over the failing link. This proposed method addressed single service networks, which is not the case of the nowadays mobile broadband networks. In this paper we are going to extend Dynamic Alternative Routing with Multiple Protection paths (DARMP) to multiservice networks, and to compare its performance with the previously proposed multiobjective dynamic alternative routing method here extended with a local protection mechanism of the same type of the one used in DARMP.

Chapter 2

Previous work - DARMP and MODR

2.1 DARMP

The previously proposed DARMP is based on Dynamic Alternative Routing (DAR) which behaves as follows: a connection is offered to the first-choice route and, if there are no available resources, the connection may overflow to a randomly chosen alternative route [9]. If this alternative route fails, a new alternative route to be used in future incoming requests is randomly selected from within a set of admissible alternative routes. This type of routing is particularly attractive because it is simple and based on local information and because of that it has been proposed for several network technologies [15, 4, 14], after being implemented by British Telecom in its telephone network. DAR was first proposed for fully-meshed networks where the first-choice path is the direct link between each pair of nodes. In an overload case, if alternative routing is not controlled, the network tends to be overtaken by second-choice traffic leading to a snow-ball effect where first-choice traffic has no chance to be routed, which leads to an increased congestion. To overcome this problem, a direct traffic protection mechanism has been developed where alternative paths are not allowed if the occupied bandwidth in each link achieves a previously tuned threshold value.

In [7] we have extended DAR to be applied in strongly meshed networks, i. e. networks where there are at least two paths between each pair of nodes, and we have proposed a local protection mechanism to be used with DAR in order to improve network performance in the case of a link failure without increasing links' bandwidth for protection. Dynamic alternative routing is mainly suitable for strongly or fully meshed networks where there is a set of admissible paths (instead of a single one) to be used dynamically for alternative routing. In the same way, in these types of networks, it is also possible to have a set of paths that may be used for local protection. This is the key idea behind our proposed local protection mechanism to be used in association with dynamic alternative routing. In case of a link failure, alternative routing can efficiently redirect new incoming traffic through the most appropriate alternative route and the ongoing traffic in the failed link is saved through the splitting of that traffic into a set

of pre-assigned backup paths (bypass tunnels).

2.2 MODR

MODR is a hierarchical multiobjective dynamic routing method the aim of which is to balance the traffic between all links in the network for all the services, trying not to benefit the more demanding service in terms of bandwidth and taking advantage of the available bandwidth in each link. This routing method leads in general to a good overall network performance with more carried traffic and less bandwidth denial rate for all the services, as compared with DAR [12]. This performance is mainly accomplished by a biobjective shortest path algorithm, which obtains the set of alternative paths to be updated in each time interval, and by a direct traffic protection mechanism, which selectively removes each alternative path for each traffic flow of each service.

The requirements for the use of dynamic alternative routing in a MPLS environment are explained in detail in [13].

Chapter 3

Protection Mechanism

We now present the main notation in order to explain in detail the multiservice protection mechanism as well as some features of the DAR and MODR dynamic alternative routing methods.

- G - undirected graph representing network topology. $G = (V, L)$, where V is the node set and L the link set.
- S - set of all services in the network.
- f_s - traffic flow of service type s from origin node v_o to destination node v_d , where $v_o, v_d \in V$ and $v_o \neq v_d$. This flow, in the context of this study, is characterized by: *i*) an effective bandwidth (bw_{f_s}); *ii*) a mean holding time (h_s) in minutes; *iii*) the flow connections' arrival rate λ_s . A number of connections belonging to traffic flow f_s are designated by c_{f_s} .
- bw_{k_s} - required bandwidth on link l_k by a call of service $s \in S$, which may be interpreted as its effective bandwidth in terms of number of circuits occupied.
- F_s - set of all traffic flows in the network for service s .
- $wr(f_s)$ - a loopless working path for traffic flow $f_s \in F$. It consists of a sequence of adjacent links such that first link is $l_1 = (v_o, v_i)$ and last link is $l_{|wr(f_s)|} = (v_j, v_d)$, where $v_o, v_i, v_j, v_d \in V$. $wr(f_s)$ corresponds to a LSP for traffic flow f_s whose bandwidth varies according to incoming connections requests.
- $wr_1(f_s)$ - a first choice working path for traffic flow f_s .
- $wr_2(f_s)$ - an alternative working path for traffic flow f_s , such that $|wr_2(f_s)| \leq |wr_1(f_s)| + 1$.
- $WR_t(f_s)$ - set of working paths which is used by traffic flow f_s at time t . $WR_t(f_s) = \{wr_1(f_s), wr_2(f_s)\}$.
- $\mathcal{D}(f_s)$ - routing domain for traffic flow f_s which encompasses the set of all possible paths from v_o to v_d .
- l_f - failing link at failure time instant t_f . $l_f = (v_k, v_l)$, where $v_k, v_l \in V$.

- $F_{l_f}^c(s)$ - the set of ongoing traffic flow f_s connections whose first or alternative path traverse the failing link l_f in failure time instant t_f .

$$F_{l_f}^c(s) = \sum_{f_s: l_f \in wr_1(f_s) \vee l_f \in wr_2(f_s)} c_{f_s}$$
- $b_{l_f}(s)$ - loopless bypass tunnel for the service s traffic in the link l_f . It consists of a sequence of adjacent links such that the first link is $l_1 = (v_k, v_i)$ and the last link is $l_{|b_{l_f}(s)|} = (v_j, v_l)$, where $v_k, v_i, v_j, v_l \in V$.
- $BD_{l_f}(s)$ - service type s bypass tunnel domain for link l_f such that $BD_{l_f}(s) = \{b_{l_f}^1(s), \dots, b_{l_f}^U(s)\}$, where U is the maximum number of bypass tunnels for each link.
- $prob_{l_f}^i(s)$ - probability of using the i^{th} bypass tunnel to protect $F_{l_f}^c(s)$ at time instant t_f such that $i = 1, \dots, U$. Let n_j , with $j = 1, 2$, be the number of paths $b_{l_f}(s) \in BD_{l_f}(s)$ such that $|b_{l_f}(s)| = j + 1$. Then $prob_{l_f}^i(s) = x/(j)$ with $n_1 \times x + n_2 \times x/2 = 1$.
- $pr_{l_f}(f_s)$ - an end-to-end path for a flow f_s resulting from the activation of local protection after the failure of link l_k . This path results from the union of the working path beginning at the origin node v_o until node v_k , followed by bypass tunnel until node v_l , and finally a sequence of nodes belonging to the original working path since node v_l until destination node v_d .

The multiple paths protection mechanism for multiservice networks consists in having a set of $BD_{l_f}(s)$ for each link l_f and for each service type s . $b_{l_f}(s) \in BD_{l_f}(s)$ has a probability $prob_{l_f}^i(s)$ of being used in the failure time instant.

Our methodology is explained in figure 3.1. In the advent of a failure of the link (B,E), LSPs that are established through that link are backed up by a set of bypass tunnels $BD_{BE}(s) = (BCE)_s, (BDE)_s, (BAE)_s, (BFE)_s$ with a probability $prob_{l_f}^i(s), i = 1, \dots, 4$. Regarding the new incoming connections to a given node, they will be carried by one of its alternative paths which may vary with the service, the destination node and over time.

It is important to remark that the use of alternative paths to carry new incoming requests allows the use of potentially smaller paths during link failure instead of the longer paths resulting from the local protection mechanism. For instance, if in failure time instant there exists traffic in path (EBD) and it is protected by (EFB), then the end-to-end path becomes (EFBD) which is longer than any of the alternative routes for node pair (ED) because in a fully meshed network any alternative path has at most two arcs. In addition, these end-to-end paths remain active until the end of the saved connections. This time is independent of the link recovery time.

3.1 Protection with Multiservice Dynamic Alternative Routing with Multiple Protection paths (MDARMP)

First, it is necessary to find and to store $\mathcal{D}(f_s)$, the set of admissible working paths (LSPs) that will be used by each service to carry traffic for each pair

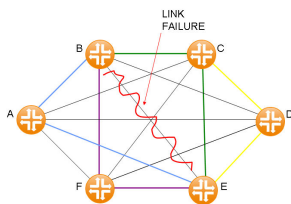


Figure 3.1: Fully meshed network with multi-path protection mechanism.

of nodes. These LSPs are chosen in ascending order of hop count metric and must comply simultaneously with 2 parameters: maximum number of admissible paths (MAP) and maximum number of hops in the path (MHP). In [14], the maximum number of admissible paths may have an optimal value which depends on the network and on the alternative routing scheme. The two previous mentioned parameters must then be adjusted according to each test network degree of connectivity and they are very important in order to prevent congestion due to the use of LSPs with high hop count. The admissible set of paths and their probabilities of being chosen are obtained as follows:

- $\mathcal{D}(f_s) = \{wr_1(f_s), wr_2(f_s) : wr_1(f_s) \text{ is a shortest path for } f_s \wedge |wr_2(f_s)| = |wr_1(f_s)| + j, j = 0, 1\}$.
- $|\mathcal{D}(f_s)| \leq MAP$
- Let n_j , with $j = 0, 1$, be the number of paths $wr_2(f_s) \in \mathcal{D}(f_s)$ such that $|wr_2(f_s)| = |wr_1(f_s)| + j$. Then $prob_{wr_2(f_s)} = x/(j+1)$ with $n_0 \times x + n_1 \times x/2 = 1$

Moreover, it must be found, for each link, the set of bypass tunnels that will be used to back up traffic in case of failure. These bypass tunnels must obey to the same parameters mentioned before for the working LSPs and their usage probabilities are given by $prob_{l_f}^i(s)$.

3.2 Protection with Multiple Objective Dynamic Routing with Multiple Protection paths (MODRMP)

The simplified MODR method presented in [13] allows to obtain the set of working paths for each traffic flow f_s at each time instant and relies on a heuristic for route selection based on two mechanisms: *i*) a biobjective shortest path algorithm (MMRA) which obtains an alternative path for each traffic flow; *ii*) a procedure that sequentially updates, in each time interval, only a subset of the available pairs of routes for each service. Because MMRA was designed for fully-meshed networks the first-choice paths were fixed over time. In this case,

however, we allow $wr_1(f_s)$ to be updated if there is more than one shortest-path in terms of hop count.

Moreover, MODR is a hierarchical multiple objective routing algorithm because the set of paths which is updated in each time interval attempts to find compromise solutions in terms of the network level objective functions (o. fs.), (aiming at maximizing network expected revenue W_T and minimizing the maximal service mean blocking probability B_{Mm}) and simultaneously in terms of the service level o. fs. (in order to minimize the service mean blocking probabilities B_{ms} and the maximal point-to-point blocking probability, B_{Ms} , for each service s).

Instead of W_T we are considering in this study the bandwidth denial rate concept BDR (which considers the overall ratio of the total admitted bandwidth to the total requested bandwidth), with the objective of considering the effect of having flows of widely different bandwidths [15].

It is important to note that network level metrics have priority over the service level ones.

Chapter 4

Study Environment

With this study we wish to compare a simple event-dependent routing approach (MDARMP) with a biobjective and centralized scheme (MODRMP) in order to evaluate the performance improvement that can be obtained with a more sophisticated routing method. A discrete-event OMNet++ simulator, developed for this study, was used to evaluate network performance. For our study it was assumed the following: all traffic flows are homogeneous Poissonian and independent and service times are negative exponentially distributed. For each simulation scenario, 10 independent simulation runs were performed, and results are within a 97.5% confidence interval.

The first test network used in our study is based on Network I in [15]. Network I is derived from a MPLS service provider network, it comprises 15 nodes, connected by 58 links, and all sources of traffic have direct links between them. In addition, three service models were implemented: fixed rate (FR), uniform fixed rate (UFR) and variable rate on-off model (VR). All these models require specification of the Erlang load to be generated and the flow duration. In our previous work [7], we have introduced DARMP which is a dynamic alternative routing algorithm with multiple paths protection in order to show that the combination of multiple paths to save ongoing flows and the existence of alternative paths to carry incoming traffic is an advantage in terms of network survivability in case of link failure. With that in mind, we have adjusted Network I to consider a single service network, in order to simplify our study. In our current study, we wish to extend our previous idea to a multiservice network. However, because several services may have conflicting requirements we will show that a more sophisticated multiservice and multi-objective routing algorithm achieves better performance than DARMP.

In [15] there were 4 defined services, and the ratio of the overall effective load of the traffic classes was given by 4.69(S1):4.58(S2):90.71(S3):0.02(S4), as derived from an actual service provider network. Because S4 represented only 0.02% of total traffic, we left this service out of our test environment, and we have considered the following traffic load distribution 4.69(S1):4.6(S2):90.71(S3).

Now, it is necessary to calculate the equivalent bandwidth for each service. The same line of thought as in [8] is followed in here to calculate each service bandwidth usage. Erlang's function $B(\lambda, C)$ gives us the blocking probability that occurs when Poisson traffic of intensity λ is offered to a link with capacity C . According to the inverse of Erlang-B formula (which gives us the number of

circuits needed to carry Poisson traffic λ with blocking probability at most B), for a low value of B , the bigger the value of the offered load and the closer it becomes of the number of circuits. The total capacity regarding active node pairs in Network I is 75573 Mbps. As such, we will make an assumption and consider that the offered load to the network is approximately 75573 Mbps. According to the ratio of the overall effective load, service 1, 2 and 3 are responsible for 3544.3737 Mbps, 3476.3580 Mbps and 68552.2683 Mbps, respectively.

Our mobile broadband backhaul tests networks were engineered with three services: voice calls ($h_1 = 1$ and $bw_{k1} = 1$), videotelephony ($h_2 = 3$ and $bw_{k2} = 30$) and high-quality streaming audio ($h_3 = 10$ and $bw_{k3} = 10$), where each circuit represents 12,2 Kbps.

As stated in [15], the most important aspect of the traffic is the distribution of effective load throughout the topology and not necessarily the actual loading levels of the network as a whole. Consequently, we have reduced the global traffic and capacities by a 27 order of magnitude, because the services that we have considered occupy much less bandwidth than the ones proposed in the original article which would lead to a much higher number of connection's requests to achieve the same load. However, the traffic load distribution was maintained.

Our model requires that we convert each link capacity (in Mbps) to the corresponding number of circuits. As such, considering that each circuit occupies the equivalent bandwidth of service 1 (12.2 kbps), the test network that we have used (Network A) is the one in 4.1.

O-D Pair	Cap	O-D Pair	Cap	O-D Pair	Cap	O-D Pair	Cap
1-2	2831	1-3	2831	1-5	5662	1-7	5662
1-8	5662	1-9	2831	1-10	2831	1-11	5662
1-13	5662	1-15	5662	2-3	5662	2-6	5662
2-7	2831	2-8	5662	2-9	5662	2-12	2831
3-5	2831	3-6	2831	3-7	8493	3-9	11324
3-10	5662	3-11	2831	3-13	2831	3-14	8493
3-15	2831	4-5	2831	4-8	5662	4-9	2831
4-10	2831	4-13	2831	5-7	8493	5-9	8493
5-11	5662	5-14	8493	6-7	2831	6-8	5662
6-10	2831	7-8	2831	7-11	2831	7-13	8493
7-14	2831	8-9	5662	8-10	2831	8-11	2831
8-12	5662	9-11	5662	9-13	11324	9-14	2831
10-11	2831	10-12	5662	10-15	2831	11-13	2831
11-14	8493	12-13	5662	12-15	5662	13-14	11324
13-15	2831	14-15	5662				

Table 4.1: Test Network A, in terms of circuits

Our original study was accomplished with test network A. Nevertheless, we would like to understand the impact of different topologies in our routing algorithms performance. As such, we used one more representative topology: a fully meshed network. Test network B is a 10 nodes fully meshed network with 45 links and it was chosen because DAR was designed for fully-connected circuit-switched voice networks. Network B ratio of the overall effective load of the traffic classes is given by $50(s_1):25(s_2):25(s_3)$. Notice that in mobile networks the voice calls (s_1) represent in many cases about 50% of the network load. Traffic was considered asymmetric, and link capacities and offered load were not

engineered by a specific algorithm. Instead, they were adjusted by simulation in order to obtain a close performance in terms of BDR for MODRMP, in a network situation where there is no failure. In conclusion, link capacities are the ones presented in table 4.2.

O-D Pair	Cap	O-D Pair	Cap	O-D Pair	Cap	O-D Pair	Cap	O-D Pair	Cap
1-2	1262	2-3	1292	3-5	1322	4-8	1592	6-8	1622
1-3	1502	2-4	1382	3-6	1322	4-9	1262	6-9	1292
1-4	1292	2-5	1262	3-7	1232	4-10	1262	6-10	1262
1-5	1322	2-6	1232	3-8	1682	5-6	1262	7-8	1592
1-6	1262	2-7	1352	3-9	1292	5-7	1292	7-9	1232
1-7	1292	2-8	1622	3-10	1322	5-8	1622	7-10	1262
1-8	1682	2-9	1382	4-5	1262	5-9	1262	8-9	1562
1-9	1322	2-10	1532	4-6	1262	5-10	1262	8-10	1622
1-10	1382	3-4	1322	4-7	1262	6-7	1292	9-10	1202

Table 4.2: Test Network B, in terms of circuits

It is important to remind that in neither of these two networks was protection against failures involved in network dimensioning.

Networks A and B were configured with MAP=8, MHP=4 and $U \leq 8$.

In each time instant, both MDARMP and MODRMP present a multi-path routing table for each service in each node: a first-choice path and an alternative path. Additionally, there will be a list with all admissible bypass tunnels (and also their usage probabilities), for each one of its adjacent links. Note that there is only one active alternative path in each time instant for each pair of nodes and for each service, while the set of bypass tunnels, $BD_{l_f}(s)$, is entirely used at the failure time instant.

4.1 MODRMP

In the case of this routing method a 30 seconds cycle update length was considered [2]. The reason for this value is that in mobile networks the voice traffic is very important and voice has a small average time duration (1 minute) when comparing to the remaining services. Consequently, it is more demanding in terms of the paths' update time interval which must be smaller.

4.2 Results Analysis

We want to validate that our centralized MODRMP routing algorithm which makes decisions based on periodically updated network status information presents a better performance than the event-dependent MDARMP routing scheme, not only in normal situations but also when a link failure occurs.

4.2.1 Network A

We begin our analysis with Network A. Regarding a normal network situation (in table 4.3), we can see that MODRMP presents in general better performance not only in terms of network global performance but also in terms of service performance. This can be easily explained because there are several links in this network that have no direct traffic and that are idle unless they are

used for alternative routing. Because MODRMP receives periodically updated information regarding the overall status of the network, it can take advantage of this situation. The ability to distribute the traffic in an uniform way is a paramount advantage when it comes to accommodate connections at risk in a failure situation as can be seen next.

Table 4.3: Network A - Performance when there is no failure

	NO Failure	
	MDARMP	MODRMP
Network	BDR	
	0.0086 ± 0.0016	0.0032 ± 0.0002
Network	B_{Mm}	
	0.0390 ± 0.0087	0.0202 ± 0.0014
	B_{ms}	
s=1	0.0013 ± 0.0006	$0.0003 \pm 2.9 \times 10^{-5}$
s=2	0.0390 ± 0.0087	0.0202 ± 0.0014
s=3	0.0179 ± 0.0041	0.0052 ± 0.0136
	B_{Ms}	
s=1	0.0284 ± 0.0116	0.0065 ± 0.0006
s=2	0.6980 ± 0.1731	0.3212 ± 0.0832
s=3	0.3321 ± 0.0682	0.0667 ± 0.0056

The purpose of this work is to validate the combined approach of our MODR routing algorithm with our previously proposed protection mechanism [7]. In that sense, we have done network simulations in failure conditions (with and without link protection activated) for MDARMP and MODRMP routing schemes.

Failure in the biggest link in terms of carried traffic and capacity

In tables 4.4, 4.5, 4.6 and 4.7 we can see the results obtained for Network A with a 5 minutes failure in link 3-9 (one of the biggest in terms of both carried traffic and capacity [8]), with and without protection). The 5 minutes failure may be the necessary time for a reboot.

Table 4.4: Network A - Network Performance with failure in link 3-9 and without activation of the protection mechanism

	NO Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.091 \times C$	$1.058 \times C \pm 0.089 \times C$
S_F	0	0
F_F	$C \pm 0.091 \times C$	$1.058 \times C \pm 0.089 \times C$
	During Failure time interval	
BDR	0.0139 ± 0.0008	0.0274 ± 0.0014
B_{Mm}	0.0391 ± 0.0223	0.0383 ± 0.0174
	After Failure Recovery	
$BDR, t = t_1$	0.0076 ± 0.0004	0.0031 ± 0.0008
$BDR, t = t_{10}$	0.0090 ± 0.0006	$0.0033 \pm 5.6 \times 10^{-5}$
$B_{Mm}, t = t_1$	0.0251 ± 0.0110	0.0139 ± 0.0065
$B_{Mm}, t = t_{10}$	0.0381 ± 0.0060	0.0218 ± 0.0023

O_F , S_F and F_F represent the total, saved and failed, respectively, ongoing traffic going through the failing link in the failure time instant. C and C_x represent the total and service x ongoing traffic that was carried by MDARMP

Table 4.5: Network A - Service performance with failure in link 3-9 and without activation of the protection mechanism

	NO Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
	F_F	
s=1	$C_1 \pm 0.0320 \times C_1$	$1.0171 \times C_1 \pm 0.0399 \times C_1$
s=2	$C_2 \pm 0.3714 \times C_2$	$1.2580 \times C_2 \pm 0.4004 \times C_2$
s=3	$C_3 \pm 0.1359 \times C_3$	$1.0472 \times C_3 \pm 0.0967 \times C_3$
	During Failure time interval	
	B_{m_s}	
s=1	0.0054 ± 0.0045	0.0261 ± 0.0008
s=2	0.0391 ± 0.0223	0.0383 ± 0.0174
s=3	0.0240 ± 0.0082	0.0332 ± 0.0056
	B_{M_s}	
s=1	0.3292 ± 0.2334	0.9168 ± 0.0223
s=2	0.7667 ± 0.2462	0.9000 ± 0.2262
s=3	0.6266 ± 0.1779	0.9652 ± 0.0303
	After Failure Recovery	
	$B_m, t = t_1$	
s=1	0.0012 ± 0.0008	0.0008 ± 0.0004
s=2	0.0251 ± 0.0110	0.0139 ± 0.0065
s=3	0.0162 ± 0.0041	0.0094 ± 0.0050
	$B_m, t = t_{10}$	
s=1	0.0012 ± 0.0004	$0.0002 \pm 7.6458 \times 10^{-5}$
s=2	0.0381 ± 0.0060	0.0218 ± 0.0023
s=3	0.0170 ± 0.0028	0.0054 ± 0.0010
	$B_{M_s}, t = t_1$	
s=1	0.0402 ± 0.0213	0.0386 ± 0.0195
s=2	0.7167 ± 0.2453	0.7000 ± 0.2501
s=3	0.4617 ± 0.1450	0.3547 ± 0.1501
	$B_{M_s}, t = t_{10}$	
s=1	0.0260 ± 0.0076	0.0055 ± 0.0021
s=2	0.7114 ± 0.0955	0.4167 ± 0.1609
s=3	0.3234 ± 0.0439	0.0913 ± 0.0228

routing method and that was traversing the failing link in the time instant that the failure has occurred. Considerer also the following time instant $t_y = t_f + 300 \times (y + 1)$, where 300 is the time duration of the failure (in seconds).

We begin by analyzing the situation where no protection is activated in none of the algorithms (tables 4.4 and 4.5). The analysis is done as follows: at the failure time instant, during the failure and at time instants after the failure recovery. Regarding the global network performance analysis (table 4.4), we can see that in failure time instant MODRMP has more traffic at risk than MDARMP, which comes in line with the fact that in a normal situation MODRMP presents a better performance which consequently results in having more carried traffic. During the failure it can be seen that MODRMP presents an increase of 700% in terms of BDR and 90% in terms of B_{Mm} , while MDARMP presents an increase of 60% in terms of BDR and the value for B_{Mm} maintains stable. The increase in the metric BDR for MODRMP is due to the fact that until a reasonable number of paths is updated according to the new network condition, many flows will be routed based on the previous status (no failure). Note that MDARMP reacts faster than MODRMP to a network congestion situation. However, if the failure was maintained for a longer period, MODRMP would again present better network global performance than MDARMP. It is important not to forget that even so MDARMP did not perform better than MODRMP as we are doing a biobjective analysis and B_{Mm} for MODRMP remains lower than for MDARMP.

Table 4.6: Network A - Network Performance with failure in link 3-9 and with activation of the protection mechanism

	With Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.091 \times C$	$1.058 \times C \pm 0.089 \times C$
S_F	$0.4337 \times C \pm 0.0878 \times C$	$0.7581 \times C \pm 0.0676 \times C$
F_F	$0.5663 \times C \pm 0.0878 \times C$	$0.2419 \times C \pm 0.0676 \times C$
	During Failure time interval	
BDR	0.0162 ± 0.0008	0.0282 ± 0.0014
B_{Mm}	0.0466 ± 0.0192	0.0437 ± 0.0203
	After Failure Recovery	
$BDR, t = t_1$	0.0080 ± 0.0005	0.0036 ± 0.0008
$BDR t = t_{10}$	0.0091 ± 0.0006	$0.0035 \pm 6.0224 \times 10^{-5}$
$B_{Mm}, t = t_1$	0.0265 ± 0.0107	0.0157 ± 0.0083
$B_{Mm} t = t_{10}$	0.0389 ± 0.0063	0.0217 ± 0.0022

Regarding the analysis some time after failure recovery, we can see that both algorithms present in $t = t_1$ an increase in their performances in both global metrics. This can be easily explained because upon link recovery there is more available capacity in the network and there is an increase in terms of traffic acceptance for paths using the prior failed link. Of course, after a certain amount of time, in this case in $t = t_{10}$, the metrics' values start returning to their original values. After link recovery, all MODRMP metric values are performing better than the ones achieved with MDARMP. Regarding service performance the same analysis applies, and can be consulted in table 4.5.

We now wish to validate the performance of our protection mechanism. As we can see in table 4.6, MODRMP has more traffic in danger in the failure time instant, however, it is still able to save almost twice the amount of traffic

Table 4.7: Network A - Service performance with failure in link 3-9 and with activation of the protection mechanism

	With Protection Mechanism Activated	
	MDARMP	MODRMP
In failure time instant		
	F_F	
s=1	$0.5195 \times C_1 \pm 0.0320 \times C_1$	$0.2927 \times C_1 \pm 0.0858 \times C_1$
s=2	$0.3871 \times C_2 \pm 0.4672 \times C_2$	$0.4516 \times C_2 \pm 0.4672 \times C_2$
s=3	$0.4195 \times C_3 \pm 0.1049 \times C_3$	$0.2865 \times C_3 \pm 0.1049 \times C_3$
	S_F	
s=1	$0.4805 \times C_1 \pm 0.0320 \times C_1$	$0.7073 \times C_1 \pm 0.0858 \times C_1$
s=2	$0.6129 \times C_2 \pm 0.4672 \times C_2$	$0.5484 \times C_2 \pm 0.4672 \times C_2$
s=3	$0.5805 \times C_3 \pm 0.1049 \times C_3$	$0.7135 \times C_3 \pm 0.1049 \times C_3$
During Failure time interval		
	B_{ms}	
s=1	0.0061 ± 0.0044	0.0261 ± 0.0007
s=2	0.0466 ± 0.0192	0.0437 ± 0.0203
s=3	0.0270 ± 0.0086	0.0338 ± 0.0057
	B_{Ms}	
s=1	0.3854 ± 0.2248	0.9168 ± 0.0223
s=2	0.8333 ± 0.2103	0.9000 ± 0.2262
s=3	0.5923 ± 0.1704	0.9652 ± 0.0303
After Failure Recovery		
	$B_m, t = t_1$	
s=1	0.0012 ± 0.0008	0.0008 ± 0.0005
s=2	0.0265 ± 0.0107	0.0157 ± 0.0083
s=3	0.0163 ± 0.0041	0.0099 ± 0.0048
	$B_m, t = t_{10}$	
s=1	0.0012 ± 0.0004	$0.0002 \pm 8.2079 \times 10^{-5}$
s=2	0.0389 ± 0.0063	0.0217 ± 0.0022
s=3	0.0169 ± 0.0028	0.0058 ± 0.0011
	$B_{Ms}, t = t_1$	
s=1	0.0402 ± 0.0204	0.0369 ± 0.0187
s=2	0.7167 ± 0.2453	0.7000 ± 0.2501
s=3	0.4728 ± 0.1415	0.3374 ± 0.1303
	$B_{Ms}, t = t_{10}$	
s=1	0.0260 ± 0.0075	0.0054 ± 0.0022
s=2	0.7137 ± 0.0958	0.4167 ± 0.1609
s=3	0.3255 ± 0.0432	0.0879 ± 0.0187

of MDARMP leading also to less than half of the lost traffic. In conclusion, because traffic is better distributed when MODRMP is used, in the advent of a failure, it is possible to protect more traffic in the failing link. Note that BDR is greater for MODRMP during the failure because MODRMP saves more traffic leading to a more occupied network. Regarding the network global performance after the failure recovery, we can see that there is a slight decrease of performance when comparing to the situation where no protection is implemented due to the increase of carried traffic resulting from the protection. Again, we can see that during the failure MDARMP presents lower BDR while MODRMP has lower B_{Mm} . On the other hand, after failure recovery, MODRMP is always better.

If we analyze the service performance metrics we can see that, in the failure time instant, MODRMP saves 47% more voice calls traffic and 20% more streaming audio (the less and more demanding services in terms of bandwidth, respectively), while MDARMP saves more 10% videophone traffic than MODRMP.

Failure in a median link in terms of carried traffic and capacity

We now present the simulation results from a failure in Network A in a median link in terms of carried traffic and capacity (link 1-5). As can be consulted in tables 4.8, 4.9, 4.10 and 4.11, the same line of thought and conclusions as for the failure in the biggest link (link 3-9) also stands for the median link.

Table 4.8: Network A - Network Performance with failure in link 1-5 and without activation of the protection mechanism

	Without Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.1349 \times C$	$0.9605 \times C \pm 0.0956 \times C$
S_F	0	0
E_F	$C \pm 0.1349 \times C$	$0.9605 \times C \pm 0.0956 \times C$
	During Failure time interval	
BDR	0.0153 ± 0.0011	0.0256 ± 0.0011
B_{Mm}	0.0409 ± 0.0191	0.0369 ± 0.0156
	After Failure Recovery	
$BDR, t = t_1$	0.0089 ± 0.0005	0.0018 ± 0.0001
$BDR, t = t_{10}$	0.0103 ± 0.0013	0.0033 ± 0.0002
$B_{Mm}, t = t_1$	0.0334 ± 0.0183	0.0122 ± 0.0073
$B_{Mm}, t = t_{10}$	0.0409 ± 0.0092	0.0215 ± 0.0034

Table 4.9: Network A - Service performance with failure in link 1-5 and without activation of the protection mechanism

	Without Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
	F_F	
s=1	$C_1 \pm 0.0676 \times C_1$	$0.9755 \times C_1 \pm 0.0613 \times C_1$
s=2	$C_2 \pm 1.0248 \times C_2$	$0.7222 \times C_2 \pm 0.4261 \times C_2$
s=3	$C_3 \pm 0.0806 \times C_3$	$0.9879 \times C_3 \pm 0.0842 \times C_3$
	During Failure time interval	
	B_{ms}	
s=1	0.0073 ± 0.0054	0.0252 ± 0.0010
s=2	0.0409 ± 0.0191	0.0369 ± 0.0156
s=3	0.0290 ± 0.0099	0.0272 ± 0.0039
	B_{Ms}	
s=1	0.2645 ± 0.2149	0.9141 ± 0.0107
s=2	0.9500 ± 0.1131	0.9999 ± 0.1010
s=3	0.6086 ± 0.1926	0.9208 ± 0.0520
	After Failure Recovery	
	$B_m, t = t_1$	
s=1	0.0016 ± 0.0015	0.0001 ± 0.0002
s=2	0.0334 ± 0.0183	0.0122 ± 0.0073
s=3	0.0201 ± 0.0025	0.0029 ± 0.0015
	$B_m, t = t_{10}$	
s=1	0.0014 ± 0.0006	$0.0001 \pm 6.7 \times 10^{-5}$
s=2	0.0409 ± 0.0092	0.0215 ± 0.0034
s=3	0.0190 ± 0.0041	0.0051 ± 0.0016
	$B_{Ms}, t = t_1$	
s=1	0.0388 ± 0.0295	0.0041 ± 0.0067
s=2	0.8333 ± 0.2384	0.6000 ± 0.2262
s=3	0.3769 ± 0.0342	0.1029 ± 0.0707
	$B_{Ms}, t = t_{10}$	
s=1	0.0284 ± 0.0090	0.0021 ± 0.0010
s=2	0.7759 ± 0.1170	0.3788 ± 0.1220
s=3	0.3168 ± 0.0212	0.0894 ± 0.0226

Table 4.10: Network A - Network Performance with failure in link 1-5 and with activation of the protection mechanism

	With Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.1349 \times C$	$0.9605 \times C \pm 0.0956 \times C$
S_F	$0.6044 \times C \pm 0.1628 \times C$	$0.6494 \times C \pm 0.0813 \times C$
F_F	$0.3956 \times C \pm 0.1628 \times C$	$0.3506 \times C \pm 0.0813 \times C$
	During Failure time interval	
BDR	0.0210 ± 0.0015	0.0257 ± 0.0011
B_{Mm}	0.0518 ± 0.0214	0.0369 ± 0.0156
	After Failure Recovery	
$BDR, t = t_1$	0.0088 ± 0.0005	0.0018 ± 0.0001
$BDR, t = t_{10}$	0.0103 ± 0.0013	0.0033 ± 0.0001
$B_{Mm}, t = t_1$	0.0305 ± 0.0121	0.0122 ± 0.0073
$B_{Mm}, t = t_{10}$	0.0404 ± 0.0093	0.0215 ± 0.0034

Table 4.11: Network A - Service performance with failure in link 1-5 and with activation of the protection mechanism

	With Protection Mechanism Activated	
	MDARMP	MODRMP
In failure time instant		
	F_F	
s=1	$0.4590 \times C_1 \pm 0.0676 \times C_1$	$0.4609 \times C_1 \pm 0.0626 \times C_1$
s=2	$0.4445 \times C_2 \pm 1.0248 \times C_2$	$0.4445 \times C_2 \pm 0.2513 \times C_3$
s=3	$0.3729 \times C_3 \pm 0.1429 \times C_3$	$0.3099 \times C_3 \pm 0.0463 \times C_3$
	S_F	
s=1	$0.5410 \times C_1 \pm 0.0676 \times C_1$	$0.5391 \times C_1 \pm 0.0626 \times C_1$
s=2	$0.5555 \times C_2 \pm 1.0248 \times C_2$	$0.5555 \times C_2 \pm 0.2513 \times C_3$
s=3	$0.6271 \times C_3 \pm 0.1429 \times C_3$	$0.6901 \times C_3 \pm 0.0463 \times C_3$
During Failure time interval		
	B_{ms}	
s=1	0.0113 ± 0.0068	0.0252 ± 0.0010
s=2	0.0518 ± 0.0214	0.0369 ± 0.0156
s=3	0.0352 ± 0.0066	0.0272 ± 0.0039
	B_{Ms}	
s=1	0.4056 ± 0.2070	0.9141 ± 0.0107
s=2	1.0000 ± 0.0000	1.0000 ± 0.0000
s=3	0.7488 ± 0.1566	0.9208 ± 0.0520
After Failure Recovery		
	$B_m, t = t_1$	
s=1	0.0016 ± 0.0015	0.0001 ± 0.0002
s=2	0.0305 ± 0.0121	0.0122 ± 0.0073
s=3	0.0198 ± 0.0022	0.0029 ± 0.0015
	$B_m, t = t_{10}$	
s=1	0.0014 ± 0.0006	$0.0001 \pm 7.2 \times 10^{-5}$
s=2	0.0404 ± 0.0093	0.0215 ± 0.0034
s=3	0.0189 ± 0.0042	0.0051 ± 0.0017
	$B_{Ms}, t = t_1$	
s=1	0.0467 ± 0.0383	0.0041 ± 0.0067
s=2	0.8333 ± 0.2384	0.6000 ± 0.2262
s=3	0.3917 ± 0.0372	0.1029 ± 0.0707
	$B_{Ms}, t = t_{10}$	
s=1	0.0287 ± 0.0090	0.0022 ± 0.0010
s=2	0.7759 ± 0.1170	0.3788 ± 0.1220
s=3	0.3091 ± 0.0304	0.0894 ± 0.0226

4.2.2 Network B

We now briefly present the results accomplished with Network B. In this fully-meshed network all admissible alternative paths have the same size (two arcs), and the challenge is to choose the alternative paths that adjust better to current network condition.

Table 4.12: Network B - Performance when there is no failure

	NO Failure	
	MDARMP	MODRMP
Network	0.0235 ± 0.0008	BDR $0.0042 \pm 5.6 \times 10^{-5}$
Network	0.0310 ± 0.0023	B_{Mm} 0.0055 ± 0.0002
s=1	$0.0002 \pm 3.2 \times 10^{-5}$	B_{ms} $1.2 \times 10^{-5} \pm 2.8 \times 10^{-5}$
s=2	0.0310 ± 0.0023	0.0055 ± 0.0002
s=3	0.0042 ± 0.0002	$0.0007 \pm 8.9 \times 10^{-5}$
s=1	0.0015 ± 0.0004	B_{Ms} 0.0002 ± 0.0001
s=2	0.0900 ± 0.0179	0.0244 ± 0.0087
s=3	0.0209 ± 0.0082	0.0070 ± 0.0026

Failure in the biggest link in terms of carried traffic and capacity

Here we present the results from the simulation of a failure in one of the biggest links in terms of carried traffic and capacity in Network B (link 1-8). As we can see in tables 4.12,4.13 and 4.15, MODRMP has better network global performance in all cases. Service performance results can be consulted in tables 4.14 and 4.16.

Table 4.13: Network B - Network Performance with failure in link 1-8 and without activation of the protection mechanism

	Without Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.093 \times C$	$1.038 \times C \pm 0.104 \times C$
S_F	0	0
F_F	$C \pm 0.093 \times C$	$1.038 \times C \pm 0.104 \times C$
	During Failure time interval	
BDR	0.0421 ± 0.0027	0.0337 ± 0.0010
B_{Mm}	0.0492 ± 0.0063	0.0337 ± 0.0045
	After Failure Recovery	
$BDR, t = t_1$	0.0287 ± 0.0037	0.0094 ± 0.0009
$BDR, t = t_{10}$	0.0239 ± 0.0006	0.0049 ± 0.0003
$B_{Mm}, t = t_1$	0.0354 ± 0.0133	0.0106 ± 0.0034
$B_{Mm}, t = t_{10}$	0.0294 ± 0.0015	0.0059 ± 0.0008

Table 4.14: Network B - Service performance with failure in link 1-8 and without activation of the protection mechanism

	Without Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
	F_F	
s=1	$C_1 \pm 0.038 \times C_1$	$0.994 \times C_1 \pm 0.032 \times C_1$
s=2	$C_2 \pm 0.137 \times C_2$	$1.041 \times C_2 \pm 0.144 \times C_2$
s=3	$C_3 \pm 0.095 \times C_3$	$1.036 \times C_3 \pm 0.097 \times C_3$
	During Failure time interval	
	B_{ms}	
s=1	0.0033 ± 0.0018	0.0253 ± 0.0013
s=2	0.0492 ± 0.0063	0.0337 ± 0.0045
s=3	0.0107 ± 0.0054	0.0264 ± 0.0066
	B_{Ms}	
s=1	0.1385 ± 0.0805	0.9118 ± 0.0094
s=2	0.4886 ± 0.1051	0.9221 ± 0.0515
s=3	0.2808 ± 0.1280	0.9612 ± 0.0503
	After Failure Recovery	
	$B_m, t = t_1$	
s=1	0.0004 ± 0.0004	$2.0 \times 10^{-5} \pm 4.6 \times 10^{-5}$
s=2	0.0354 ± 0.0133	0.0106 ± 0.0034
s=3	0.0051 ± 0.0025	0.0010 ± 0.0014
	$B_m, t = t_{10}$	
s=1	$0.0003 \pm 8.7 \times 10^{-5}$	$2.2 \times 10^{-5} \pm 1.6 \times 10^{-5}$
s=2	0.0294 ± 0.0015	0.0059 ± 0.0008
s=3	0.0039 ± 0.0008	0.0009 ± 0.0004
	$B_{Ms}, t = t_1$	
s=1	0.0150 ± 0.0116	0.0010 ± 0.0023
s=2	0.2844 ± 0.0745	0.2191 ± 0.0831
s=3	0.2344 ± 0.2169	0.0339 ± 0.0410
	$B_{Ms}, t = t_{10}$	
s=1	0.0108 ± 0.0066	0.0008 ± 0.0005
s=2	0.1110 ± 0.0126	0.0425 ± 0.0094
s=3	0.0775 ± 0.0670	0.0329 ± 0.0211

Table 4.15: Network B - Network Performance with failure in link 1-8 and activation of the protection mechanism

	With Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.093 \times C$	$1.038 \times C \pm 0.104 \times C$
S_F	$0.771 \times C \pm 0.084 \times C$	$0.8388 \times C \pm 0.0827 \times C$
F_F	$0.229 \times C \pm 0.084 \times C$	$0.1992 \times C \pm 0.0827 \times C$
	During Failure time interval	
BDR	0.0492 ± 0.0038	0.0368 ± 0.0007
B_{Mm}	0.0574 ± 0.0088	0.0389 ± 0.0042
	After Failure Recovery	
$BDR, t = t_1$	0.0297 ± 0.0030	0.0095 ± 0.0008
$BDR, t = t_{10}$	0.0242 ± 0.0006	0.0051 ± 0.0003
$B_{Mm}, t = t_1$	0.0366 ± 0.0116	0.0111 ± 0.0033
$B_{Mm}, t = t_{10}$	0.0296 ± 0.0018	0.0061 ± 0.0008

Table 4.16: Network B - Service performance with failure in link 1-8 and activation of the protection mechanism

		With Protection Mechanism Activated	
		MDARMP	MODRMP
In failure time instant			
F_F			
s=1	$0.1660 \times C_1 \pm 0.079 \times C_1$	$0.1330 \times C_1 \pm 0.074 \times C_1$	
s=2	$0.2329 \times C_2 \pm 0.1154 \times C_2$	$0.2054 \times C_2 \pm 0.083 \times C_2$	
s=3	$0.2274 \times C_3 \pm 0.1277 \times C_3$	$0.1912 \times C_3 \pm 0.098 \times C_3$	
S_F			
s=1	$0.8340 \times C_1 \pm 0.079 \times C_1$	$0.8610 \times C_1 \pm 0.074 \times C_1$	
s=2	$0.7671 \times C_2 \pm 0.1154 \times C_2$	$0.8356 \times C_2 \pm 0.083 \times C_2$	
s=3	$0.7726 \times C_3 \pm 0.1277 \times C_3$	$0.8448 \times C_3 \pm 0.098 \times C_3$	
During Failure time interval			
B_{ms}			
s=1	0.0036 ± 0.0019		0.0255 ± 0.0013
s=2	0.0574 ± 0.0088		0.0389 ± 0.0042
s=3	0.0109 ± 0.0060		0.0268 ± 0.0072
B_{Ms}			
s=1	0.1501 ± 0.0862		0.9134 ± 0.0095
s=2	0.5522 ± 0.0974		0.9373 ± 0.0402
s=3	0.2986 ± 0.1357		0.9612 ± 0.0503
After Failure Recovery			
$B_m, t = t_1$			
s=1	0.0003 ± 0.0004		0.0001 ± 0.0001
s=2	0.0366 ± 0.0116		0.0111 ± 0.0033
s=3	0.0049 ± 0.0035		0.0014 ± 0.0012
$B_m, t = t_{10}$			
s=1	$0.0003 \pm 8.5 \times 10^{-5}$		$2.9 \times 10^{-5} \pm 1.7 \times 10^{-5}$
s=2	0.0296 ± 0.0018		0.0061 ± 0.0008
s=3	0.0041 ± 0.0010		0.0010 ± 0.0004
$B_{Ms}, t = t_1$			
s=1	0.0129 ± 0.0129		0.0046 ± 0.0047
s=2	0.3000 ± 0.0905		0.1991 ± 0.0497
s=3	0.1795 ± 0.2096		0.0618 ± 0.0471
$B_{Ms}, t = t_{10}$			
s=1	0.0048 ± 0.0020		0.0010 ± 0.0006
s=2	0.1313 ± 0.0190		0.0425 ± 0.0083
s=3	0.0717 ± 0.0667		0.0383 ± 0.0232

Failure in a median link in terms of carries traffic and capacity

We now show the results from a failure simulation in a median link in terms of the same parameters (carried traffic and capacity) which is link 1-4. Results can be consulted in tables 4.17, 4.18, 4.19 and 4.20.

Table 4.17: Network B - Network Performance with failure in link 1-4 and without activation of the protection mechanism

	Without Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.1246 \times C$	$0.9615 \times C \pm 0.1248 \times C$
S_F	0	0
O_F	$C \pm 0.1246 \times C$	$0.9615 \times C \pm 0.1248 \times C$
	During Failure time interval	
BDR	0.0483 ± 0.0045	0.0327 ± 0.0018
B_{Mm}	0.0545 ± 0.0087	0.0318 ± 0.0046
	After Failure Recovery	
$BDR, t = t_1$	0.0252 ± 0.0023	0.0073 ± 0.0004
$BDR t = t_{10}$	0.0236 ± 0.0008	0.0048 ± 0.0003
$B_{Mm}, t = t_1$	0.0322 ± 0.0090	0.0087 ± 0.0024
$B_{Mm} t = t_{10}$	0.0288 ± 0.0019	0.0056 ± 0.0008

Table 4.18: Network B - Service performance with failure in link 1-4 and without activation of the protection mechanism

	Without Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
	F_F	
s=1	$C_1 \pm 0.1012 \times C_1$	$0.9924 \times C_1 \pm 0.1041 \times C_1$
s=2	$C_2 \pm 0.1772 \times C_2$	$0.9516 \times C_2 \pm 0.1638 \times C_2$
s=3	$C_3 \pm 0.1670 \times C_3$	$0.9842 \times C_3 \pm 0.1642 \times C_3$
	During Failure time interval	
	B_{ms}	
s=1	0.0029 ± 0.0027	0.0243 ± 0.0013
s=2	0.0545 ± 0.0087	0.0318 ± 0.0046
s=3	0.0133 ± 0.0058	0.0259 ± 0.0064
	B_{Ms}	
s=1	0.1838 ± 0.1065	0.9150 ± 0.0166
s=2	0.6755 ± 0.0885	0.9302 ± 0.0344
s=3	0.3480 ± 0.1361	0.9653 ± 0.0549
	After Failure Recovery	
	$B_m, t = t_1$	
s=1	0.0004 ± 0.0003	$2.0 \times 10^{-5} \pm 4.6 \times 10^{-5}$
s=2	0.0322 ± 0.0090	0.0087 ± 0.0024
s=3	0.0037 ± 0.0019	0.0006 ± 0.0007
	$B_m, t = t_{10}$	
s=1	$0.0003 \pm 6.3 \times 10^{-5}$	$1.3 \times 10^{-5} \pm 1.0 \times 10^{-5}$
s=2	0.0288 ± 0.0019	0.0055 ± 0.0008
s=3	0.0037 ± 0.0009	0.0008 ± 0.0003
	$B_{Ms}, t = t_1$	
s=1	0.0129 ± 0.0083	0.0010 ± 0.0023
s=2	0.2813 ± 0.0754	0.1377 ± 0.0391
s=3	0.2369 ± 0.2160	0.0359 ± 0.0423
	$B_{Ms}, t = t_{10}$	
s=1	0.0059 ± 0.0050	0.0008 ± 0.0008
s=2	0.1254 ± 0.0306	0.0401 ± 0.0077
s=3	0.0750 ± 0.0672	0.0318 ± 0.0214

Table 4.19: Network B - Network Performance with failure in link 1-4 and with activation of the protection mechanism

	With Protection Mechanism Activated	
	MDARMP	MODRMP
	In failure time instant	
O_F	$C \pm 0.1246 \times C$	$0.9615 \times C \pm 0.1248 \times C$
S_F	$0.7297 \times C \pm 0.1041 \times C$	$0.7357 \times C \pm 0.0932 \times C$
F_F	$0.2703 \times C \pm 0.1041 \times C$	$0.2643 \times C \pm 0.0932 \times C$
	During Failure time interval	
BDR	0.0560 ± 0.0044	0.0348 ± 0.0019
B_{Mm}	0.0650 ± 0.0086	0.0344 ± 0.0045
	After Failure Recovery	
$BDR, t = t_1$	0.0269 ± 0.0026	0.0072 ± 0.0003
$BDR, t = t_{10}$	0.0238 ± 0.0007	0.0050 ± 0.0004
$B_{Mm}, t = t_1$	0.0337 ± 0.0094	0.0088 ± 0.0025
$B_{Mm}, t = t_{10}$	0.0290 ± 0.0016	0.0057 ± 0.0009

Table 4.20: Network B - Service performance with failure in link 1-4 and with activation of the protection mechanism

	With Protection Mechanism Activated	
	MDARMP	MODRMP
In failure time instant		
	F_F	
s=1	$0.1141 \times C_1 \pm 0.0573 \times C_1$	$0.1084 \times C_1 \pm 0.0654 \times C_1$
s=2	$0.2863 \times C_2 \pm 0.1695 \times C_2$	$0.2944 \times C_2 \pm 0.1100 \times C_3$
s=3	$0.2559 \times C_3 \pm 0.1375 \times C_3$	$0.2087 \times C_3 \pm 0.1445 \times C_3$
	S_F	
s=1	$0.8859 \times C_1 \pm 0.0573 \times C_1$	$0.8916 \times C_1 \pm 0.0654 \times C_1$
s=2	$0.7137 \times C_2 \pm 0.1695 \times C_2$	$0.7056 \times C_2 \pm 0.1100 \times C_3$
s=3	$0.7441 \times C_3 \pm 0.1375 \times C_3$	$0.7913 \times C_3 \pm 0.1445 \times C_3$
During Failure time interval		
	B_{ms}	
s=1	0.0037 ± 0.0025	0.0243 ± 0.0013
s=2	0.0650 ± 0.0086	0.0344 ± 0.0045
s=3	0.0168 ± 0.0061	0.0267 ± 0.0069
	B_{Ms}	
s=1	0.0025 ± 0.1166	0.9150 ± 0.0166
s=2	0.6739 ± 0.0618	0.9432 ± 0.0363
s=3	0.4263 ± 0.1779	0.9653 ± 0.0549
After Failure Recovery		
	$B_m, t = t_1$	
s=1	0.0005 ± 0.0003	$2.0 \times 10^{-5} \pm 4.6 \times 10^{-5}$
s=2	0.0337 ± 0.0094	0.0088 ± 0.0025
s=3	0.0041 ± 0.0020	0.0004 ± 0.0006
	$B_m, t = t_{10}$	
s=1	$0.0003 \pm 7.3 \times 10^{-5}$	$1.3 \times 10^{-5} \pm 8.9 \times 10^{-5}$
s=2	0.0290 ± 0.0016	0.0057 ± 0.0009
s=3	0.0041 ± 0.0008	0.0008 ± 0.0004
	$B_{Ms}, t = t_1$	
s=1	0.0171 ± 0.0107	0.0010 ± 0.0023
s=2	0.3088 ± 0.0870	0.1353 ± 0.0365
s=3	0.1738 ± 0.1058	0.0215 ± 0.0331
	$B_{Ms}, t = t_{10}$	
s=1	0.0077 ± 0.0051	0.0009 ± 0.0008
s=2	0.1162 ± 0.0137	0.0399 ± 0.0053
s=3	0.0685 ± 0.0260	0.0290 ± 0.0226

Chapter 5

Conclusion

In this paper we have presented a multiobjective dynamic alternative routing scheme now extended with a previous proposed local protection mechanism for the multiservice case (MODRMP) in order to provide carrier-grade resilience in mobile broadband backhaul networks. Our approach needs no bandwidth reservation because, at the failure time instant, it saves, on average, by 70% – 80% of the traffic in danger (which in real networks would correspond to traffic flows belonging to classes of service previously recognised as more important). As we have already stated, this is a critical constraint because this type of networks is already struggling to cope with current 3G traffic volumes. In addition, we have shown that a multiobjective approach achieves the best performance when several services with different requirements have to share the same resources.

List of Figures

3.1 Fully meshed network with multi-path protection mechanism. . .	9
--	---

List of Tables

4.1	Test Network A, in terms of circuits	12
4.2	Test Network B, in terms of circuits	13
4.3	Network A - Performance when there is no failure	14
4.4	Network A - Network Performance with failure in link 3-9 and without activation of the protection mechanism	14
4.5	Network A - Service performance with failure in link 3-9 and without activation of the protection mechanism	15
4.6	Network A - Network Performance with failure in link 3-9 and with activation of the protection mechanism	16
4.7	Network A - Service performance with failure in link 3-9 and with activation of the protection mechanism	17
4.8	Network A - Network Performance with failure in link 1-5 and without activation of the protection mechanism	19
4.9	Network A - Service performance with failure in link 1-5 and without activation of the protection mechanism	20
4.10	Network A - Network Performance with failure in link 1-5 and with activation of the protection mechanism	20
4.11	Network A - Service performance with failure in link 1-5 and with activation of the protection mechanism	21
4.12	Network B - Performance when there is no failure	22
4.13	Network B - Network Performance with failure in link 1-8 and without activation of the protection mechanism	22
4.14	Network B - Service performance with failure in link 1-8 and without activation of the protection mechanism	23
4.15	Network B - Network Performance with failure in link 1-8 and activation of the protection mechanism	23
4.16	Network B - Service performance with failure in link 1-8 and activation of the protection mechanism	24
4.17	Network B - Network Performance with failure in link 1-4 and without activation of the protection mechanism	25
4.18	Network B - Service performance with failure in link 1-4 and without activation of the protection mechanism	26
4.19	Network B - Network Performance with failure in link 1-4 and with activation of the protection mechanism	26
4.20	Network B - Service performance with failure in link 1-4 and with activation of the protection mechanism	27

Bibliography

- [1] J. Ash. *Traffic Engineering and QoS Optimization of Integrated Voice & Data Networks*. The Morgan Kaufmann Series in Networking. Elsevier, 2007.
- [2] P. Chemouil, J. Filipiak, and P. Gauthier. Performance issues in the design of dynamically controlled circuit-switched networks. *IEEE Communications Magazine*, (10):90–95, October 1990.
- [3] Inc Cisco Systems. Architectural considerations for backhaul of 2g/3g and long term evolution networks. Technical Report C11-613002-00, Cisco Systems, Inc, 2010.
- [4] M. Conte. *Dynamic Routing in Broadband Networks*. Klumwer Academic Publishers, 2003.
- [5] Ericsson. Mobile data traffic surpasses voice, March 2010.
- [6] IP/MPLS Forum. Mpls in mobile backhaul networks framework and requirements technical specification. Technical report, IP/MPLS Forum, 2008.
- [7] Catarina Francisco, Lúcia Martins, João Redol, and Paulo Monteiro. In proceedings of 2nd International Workshop on Reliable Network Design and Modeling, RNDM 2010. In *Proceedings of the IEEE*, 2010.
- [8] Catarina Francisco, Lúcia Martins, João Redol, and Paulo Monteiro. A previous study on Dynamic Alternative Routing with local protection paths in MPLS networks. Technical Report ISSN:1645-2631, INESC-Coimbra, May 2010.
- [9] R. Gibbens. *Dynamic Routing In Circuit-Switched Networks: The dynamic alternative routing strategy*. PhD thesis, University of Cambridge, 1988.
- [10] IETF Network Working Group, RFC 2702, Q. Awduche, J. Malcolm, J. Agogbua, M. O’Dell, and J. McManus. Requirements for traffic engineering over MPLS, September 1999.
- [11] L. Martins, J. Craveirinha, J. Clímaco, and T. Gomes. On a bi-dimensional dynamic alternative routing method. *European Journal of Operational Research - Special Issue on Advances in Complex Systems Modeling*, 166(3):828–842, 2005.
- [12] L. Martins, J. Craveirinha, and J. Clímaco. A new multiobjective dynamic routing method for multiservice networks: Modelling and performance. *Computational Management Science*, 3(3):225–244, July 2006.

- [13] Lúcia Martins, Catarina Francisco, João Redol, José Craveirinha, J. Clímaco, and Paulo Monteiro. *NETWORKING 2009*, volume 5550 of *Lecture Notes in Computer Science*, chapter Evaluation of a Multiobjective Alternative Routing Method in Carrier IP/MPLS Networks (Work in Progress), pages 195–206. Springer Berlin / Heidelberg, 2009.
- [14] D. Medhi and I. Katib. Adaptive alternate routing in wdm networks and its performance tradeoffs in the presence of wavelength converters. In *Optical and Switching Networks*, March 2009.
- [15] S. Srivastava, B. Krithikaivasan, C. Beard, and D. Medhi et al. Benefits of traffic engineering using qos routing schemes and network controls. *IEEE Computer Communication Magazine*, 27:387–399, 2004.