

Adaptive FAR: Improving availability through the knowledge of connection-holding time

Luis Velasco, Salvatore Spadaro, Jaume Comellas, Gabriel Junyent

Optical Communications Group, Universitat Politècnica de Catalunya (UPC), Barcelona Spain
{luis.velasco, spadaro, comellas, junyent}@tsc.upc.edu

Abstract— The average increment and the increasing variability of the traffic to be carried by ASON/GMPLS transport networks will require on-demand bandwidth provisioning in the near future. In this scenario dynamic routing based on traffic engineering techniques is a key issue.

This paper deals with dynamic routing in ASON/GMPLS networks based on using network failures information. We define three routing strategies which differ in the use of failure information. Their performance is evaluated by simulation in terms of request blocking probability and availability.¹

I. INTRODUCTION

The introduction of intelligence in Automatically Switched Optical Networks (ASON) [1] using a GMPLS control plane [2] allows provisioning of optical channels (lightpath or path) in seconds. Client network layers (IP, SDH, etc) can request optical connections to the optical network through the User Network Interface (UNI) [3].

The fast bandwidth provisioning open new opportunities related to better resource utilization, delivery of new services, such as bandwidth on demand, and a range of traffic engineering mechanisms [4]. Optical transport networks provide a huge amount of bandwidth in each path connecting two main locations. Currently, since the bandwidth requested by clients is usually much lower than the paths capacity, in order to increase the bandwidth utilization of the paths it is necessary to perform grooming of different client layer demands between locations.

But this scenario is rapidly changing, the traffic to be carried by today's backbone networks increases very rapidly mainly due to the massive use of internet and multimedia applications. Indeed, the mismatch between transport capacity and the requested bandwidth by the clients is falling down and the need to establish paths in an on-demand way as switched connections is rising.

Up to now, the holding time of the connections has not been considered as relevant information for routing, due to may not be known in advance. A closer look at bandwidth-leasing markets [5] show that customer lease large bandwidth, but for a limited period of time, e. g., a year. Actually, new applications need a huge amount of bandwidth between two locations for a given period of time. Examples of these applications are HDTV, Grid computing, Tele-immersion, massive data transfer for backup or storage purposes, etc. Thus, it is reasonable to

expect that network operators could know in advance the holding time of connections in optical backbone networks, mainly based on service-level agreements or contracts with customers [6]. There are previous works in the literature based on the knowledge of the connection holding time [7].

Switched connections are more sensible to failures in the network than permanent connections because they are on-demand requested when they are really needed and often will require the highest level of availability. The way to improve availability in optical transport networks is by means of recovery (protection or restoration) schemes. So, a lot of effort has been made to create, compare, develop, etc. different recovery schemes [8].

In a dynamic routing scenario, in order to increase the availability, it is necessary to periodically update routing tables to avoid congestion and failures for new path requests, allowing dynamic routing based on traffic engineering techniques to find the best route in the network. In an ASON/GMPLS based network, this information can be advertised by OSPF TE LSAs [9].

This paper compares three different diverse routing strategies based on a general diverse routing algorithm. The strategies differ as to whether failure information is taken into account for diverse routing or not. More over, we introduce a holding-time-aware diverse routing algorithm that improve paths's availability [10][11]. The performance is evaluated through simulation in terms of request blocking probability and availability.

Two different network topologies are used in order to compare the performance. The difference lies in the nodal degree average of the network, and hence the degree of meshedness. These two topologies have been chosen based on the study presented in [12].

The rest of the paper is organized as follows. Section 2 provides background on segment protection, the influence of failure information on diverse routing and availability. In Section 3 we describe the simulation scenario. In Section 4 we present the performance evaluation of the strategies. Section 5 draws the conclusions.

II. FAILURE AWARE DIVERSE ROUTING

A. End to end protection vs. segment protection

A survivable network [13] has to be based on a biconnected graph where at least two node-disjoint routes between every pair of nodes exist. In such networks, a 1+1 protected path consists on two fully disjoint routes between origin and destination nodes (end-to-end protection). Sometimes, either when the network is not fully deployed in an area or the utilization of some spans

¹ This work has been partially funded by NoE e-Photon/ONe+ project (FP6-IST-027497).

in the network is high or there are failed spans, it is not possible to find a fully disjoint path pair. In these cases, the best protection option is protecting where possible (i.e., segment protection). Fig.1 a-b illustrates both concepts. Note that in segment protection other nodes in addition to the end nodes perform protection switching (nodes B2 and B3 in Fig.1 b).

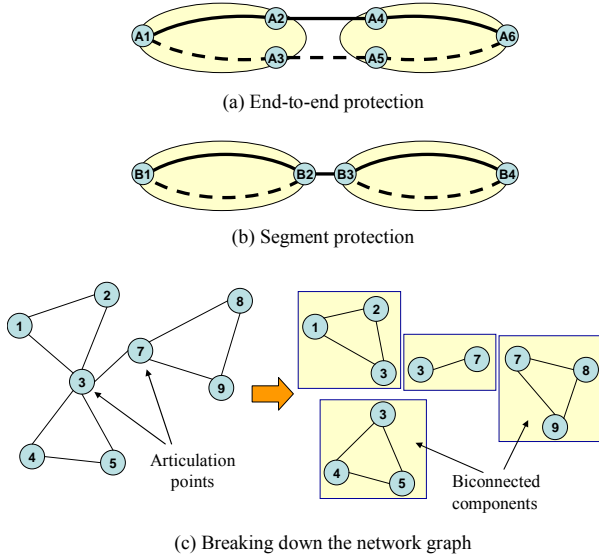


Figure 1. End-to-end vs. segment protection

In order to implement segment protection the graph representing the network has to be broken down in its *biconnected components* finding the nodes whose single failure would partition the graph into two separate subgraphs. These nodes are called *articulation points* (Fig. 1-c).

B. Influence of failure information on Diverse Routing

In a dynamic network scenario, the computation of protected paths has to take into account the global status of the network in order to know which resources are available to be used. Besides the availability of network resources (resources which are not being used by any path in the network) we suggest to take into account also its failure state.

Fig. 2a illustrates a network with a failed span between nodes 2 and 3. Let us suppose that a request comes at node 1 to establish a protected path towards node 4. One option at the routing phase is to choose the route without taking into account the failures in the network (The failure on the link between node 2 and 3 is not taken into account). We called it as *Failure Independent Routing* (FIR) algorithm (Fig. 2b). In this option if the failed span is repaired but the span connecting nodes 4 and 5 fails, the protected path will continue working.

In this paper we define the Failure Driven Routing (FDR) algorithm (Fig. 2c). The routing algorithm takes into account the failures in the network at the moment the request is triggered. If the failed span is repaired but the span connecting nodes 4 and 5 fails, the protected path will be down with only one failed resource.

If the holding time of the switched lightpath is very short the probability of having two consecutive failures

affecting the path is very low, so taking into account failures guarantees the path will be working once established. On the other hand, if the holding time of the lightpath is very long the probability that the path will be affected by two consecutive failures is higher, but paths have no guarantee of being in the working state at the time of establishment.

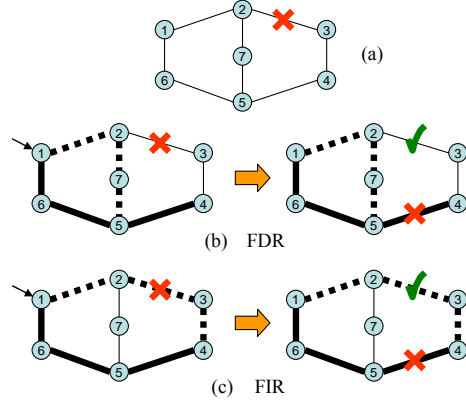


Figure 2. Influence of failure information on diverse routing

FIR strategy will use the same resources independently of the failures in the network, as not failure information is considered. However, FDR strategy can use more resources than FIR looking for a route without failed spans, or fewer resources than FIR if a disjoint route can not be found, as we will explain.

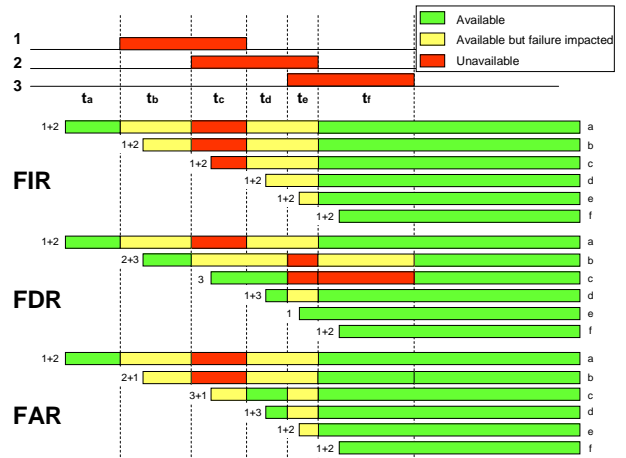


Figure 3. Behavior of routing strategies with failures

In Fig. 3 there are three available disjoint routes between source and destination. Route 2 uses more resources than Route 1 but fewer resources than Route 3. Some failures impact the routes in the time. In this scenario depending on the moment the diverse path is requested (t_a, \dots, t_g) FIR and FDR diverse routing strategies will choose different routes. We have designed a new diverse routing strategy selecting the best of FIR and FDR strategies or choosing a better combination of routes. We call this new strategy Failure Aware Routing (FAR). We will describe FAR strategy using the scenario described in Fig. 3.

- Incoming request in t_a and in t_f will result in the same routes using whatever strategy (paths a and f). Routes chosen are 1 and 2 as both are available

and use fewer resources. In fact FIR will always use routes 1 and 2.

- Incoming requests in t_b and in t_d will use different routes depending on the strategy. FDR will choose routes 2 and 3. FAR will choose routes 2 and 1. Comparing the result of the three strategies, path chosen by FDR present the same period of unavailability than the path chosen by FIR and FAR, but the unavailability of FDR's path is some time after FIR's and FAR's path unavailability periods. Therefore, short duration paths will present a better availability using FDR strategy.
- Incoming requests in t_c will use different routes depending on the strategy. FDR strategy will use only the route 3, as is the only route available at this moment, resulting in an unprotected path. On the other hand, FIR's path is unavailable when it establish. In this case the results of FIR and FDR strategies can be improved choosing routes 3 and 1 as FAR strategy do. A similar situation appears for incoming requests in t_c .

As shown, for very short holding times FDR strategy will present higher availability. This way, we propose a new holding-time-aware strategy, choosing between FAR and FDR strategies in function of the expected holding time of the connection request. We call this as *Adaptive Failure Aware Routing* (AFAR).

In the next Section, the three routing strategies, FIR, FDR and AFAR, are described in detail.

C. Routing algorithms

C.1 Failure Independent Routing (FIR)

Failure Independent Routing (FIR) algorithm compute the path route taking into account only the occupation of the spans in the network. Each time a path request arrives to a node FIR strategy creates a new network view locating the biconnected components of the network. For each biconnected component it constructs a new shortest path tree based on the min-hop criterion executing Modified Dijkstra algorithm. To compute the route of a disjoint path, Shortest Disjoint Path Pair Algorithm is used to calculate the disjoint path pair in each biconnected component. Connecting the segments the complete segment disjoint path pair is calculated. A more detailed description of these algorithms can be found in [13].

C.2 Failure Driven Routing (FDR)

The difference with the previously explained strategy is that Failure Driven Routing strategy includes span failure state in order to construct the network view. This way, incoming path requests will be routed through working spans avoiding failed spans.

C.3 Adaptive Failure Aware Routing (FAR)

Listing 1 contains AFAR pseudocode. In this strategy the working path is forced to use working spans while the protecting path is allowed to use failed spans for short and long holding times or forcing to use working spans for very short holding times. This way, all paths are guaranteed to be working when established and choose the shortest route for the protecting path in order to assure the best route when the failures in the network will be repaired. For very short holding times AFAR algorithm

will prevent from the use of in failure resources. We will find the holding time limit through simulation experiments.

Listing 1. FAR PSEUDOCODE

```

Create Network View (Failure Aware)
Look for single path to destination (pl_a)
If (holding time > holding time limit)
    Create Network View (not Failure Aware)
Else
    Create Network View (Failure Aware)
For each segment in pl_a
    Look for disjoint path in the biconnected component
    disjoint end-to-end path_a += segment disjoint path

```

In order to develop this strategy it is important to review Modified Dijkstra algorithm to avoid cycles on the graph with net negative cost. Such cycles can appear when using Shortest Disjoint Path Pair Algorithm with a path ($p1$) built from a network view that had taken into account the failures in the network, to obtain a path ($p2$) from a network view that does not have taken into account the failures in the network. The modification implemented first check rescanned nodes to detect a possible cycle with net negative cost.

D. Availability

An important issue when comparing different routing strategies in optical networks is path availability. Generally speaking, availability is the probability that a system will be found in the operating state at a random time in the future. Steady state availability can be expressed as:

$$A = \frac{\text{UpTime}}{\text{UpTime} + \text{DownTime}} \equiv \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}, \quad (1)$$

where:

- *MTTR*: Mean time to repair, the expected time needed to repair the item.
- *MTTF*: Mean time to failure, the expected time to the next failure of the item, following completion of the repair. MTTF is usually expressed in hours or in FITs, number of failures in 10^9 hours.

In this paper we assume the figures presented in Table 1 for MTTF and MTTR [14].

TABLE 1 MTTF AND MTTR TYPICAL VALUES

Tx failure rate	10,867 FITs
Rx failure rate	4,311 FITs
Plug-replacement Equipment MTTR	2 hours
Fiber-optic cable MTTR	12 hours
Fiber-optic cable failure rate	311 FITs/Km

As illustrated, the component with highest failure rate is optical cable, so the availability of a path provisioned over a number of spans with no recovery mechanism can be accurately estimated as:

$$A_{\text{path}} \cong 1 - \sum_i U_{\text{link}}^P(i), \quad (2)$$

where $U_{link}^p(i)$ is the physical unavailability of the i th link in the path.

Therefore, in this paper we confine our study to cable cuts analysis. The results thus derived can be adapted to equipment failure analysis.

III. SIMULATION SCENARIO

In order to compare the three different routing strategies, we have built an event-driven ad-hoc network simulator. The simulation scenario consists of a reference network, in which events are being executed.

In the simulation model we assume that each node maintains global network state information for routing and this information is periodically updated. In the following subsections we describe in detail the simulation scenario we adopted.

A. Traffic model

While telephonic (voice) traffic is mainly exchanged between locations that are geographically close, the exchange of internet traffic is much less related to the distance.

In our simulation, traffic is modeled using the approach of Dwivedi and Wagner [15]. This model differentiates between three traffic types: voice traffic, transactions data traffic (business IP traffic) and Internet traffic (IP traffic not related to business). The resulting total traffic between locations A and Z is derived as the sum of the previous component patterns.

According to [12] telephonic traffic intensity is inversely proportional to the distance between origin and destination (D_{A-Z}), transactions traffic intensity is inversely proportional to the square root of the distance, and Internet traffic is independent of the distance.

$$Telephonic_{A-Z} = \frac{C_v}{D_{A-Z}} \quad (3)$$

$$Transactions_{A-Z} = \frac{C_t}{D_{A-Z}^{1/2}} \quad (4)$$

$$Internet_{A-Z} = C_i \quad (5)$$

Constants (C_v , C_t and C_i) include parameters like population, number of non-production business employees, number of internet hosts and an estimation of traffic growth.

In this paper we assumed a mixture of traffic with 30% telephonic traffic, 50% transactions traffic and 20% of Internet traffic arriving to each location and all traffic demands are for protected paths.

B. Reference Networks

In the simulation experiments, we have investigated the behavior of routing strategies over two different network topologies. These two topologies have been chosen based on the study presented in [12] for a pan-European fiber-optic backbone network evaluated in terms of cost of the network design and availability of the connections of the different traffic types. Both topologies connecting the same largest European cities are illustrated in Fig.4.

The topology called Ring Topology (RT) is a sparse topology, while the Triangular Topology (TT) is highly meshed, in fact it consists of little triangles.

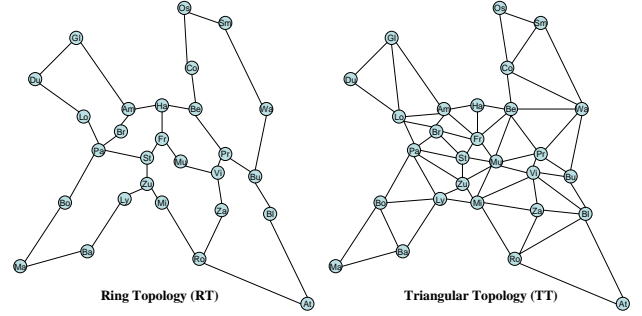


Figure 4. Network Topologies

In Table 2 some basic figures for the network topologies are summarized.

TABLE 2 BASIC FIGURES

	# nodes	# links	Mean Node degree	Mean Fiber Distance L (km)
RT	28	34	2.43	630
TT	28	61	4.36	638

Initially each span has 40 data channels vacant to be occupied and released by paths.

C. Events

Four types of events have been considered in the simulation here presented:

- *Set up Path*: Given a demand (source node, destination node, duration of the path, single/disjoint path), try to establish (determine the route and reserve the resources) a new path in the network taking into account the current spans occupation (and the failure state of the spans if the case). If successful, schedule the tear-down event of the path.
- *Tear-down Path*: Release the path resources.
- *Cable cut*: Set the span in the failure state and schedule the repair event of the cable.
- *Cable repair*: Set the span in the non failure state.

D. Stochastic processes

The simulation process is the sum of two stochastic families of independent processes [16]:

- *Connection Requests*: Connection requests arrive at each node in an independent way according to a Poisson process with a predefined mean interarrival time (iat). The connections holding time is exponentially distributed with a predefined mean (ht). The destination of each connection request is defined by the mix of traffic patterns described above. The average traffic intensity in Erlangs departing each node is therefore:

$$E = ht/iat \quad (6)$$

- *Cable cuts*: Cable cuts arrive at each span in the network in an independent way according to a Poisson process with a predefined mean time to

failure (MTTF) and depending on the span distance. The mean time to repair (MTTR) is also predefined.

E. Statistical counters

During the execution of the simulation at the end of each event, some statistical counters are compiled. The main counters are:

- *Number of Paths requests (RPn)*: This counter is incremented after the arrival of a set up path event.
- *Number of Paths created (Pn)*: This counter is incremented after the successful execution of a set up path event.
- *Number of span cuts (Cn)*: This counter is incremented after the execution of a cable cut event.
- *Number of span repairs*: This counter is incremented after the execution of a cut repair event.
- *Number of paths, $P(t_i)$* : The number of paths in the network at this moment.
- *Number of unavailable paths, $U(t_i)$* : The number of unavailable paths at this moment.

F. Statistical measures

After the execution of the simulation some statistical measures are calculated. The main measures are:

- Total Traffic (available + unavailable): Minutes of traffic.

$$Tt(n) = \int_0^{T(n)} P(t)dt \quad (7)$$

- Unavailable Traffic: Minutes of unavailable traffic.

$$Ut(n) = \int_0^{T(n)} U(t)dt \quad (8)$$

- Network availability:

$$A = 1 - \frac{Ut(n)}{Tt(n)} \quad (9)$$

- Blocking probability:

$$B = \frac{RPn - Pn}{RPn} \quad (10)$$

IV. PERFORMANCE EVALUATION

The results presented hereafter are the average of 10 simulation executions. Each execution ends when both more than 200,000 Set up Path events and more than 20,000 Cable cut events have been simulated.

Fig. 5 shows the network availability for the routing strategies over the Ring Topology (RT). The graph on the top represents the evolution with the holding time of the paths for a traffic intensity of 2 Erlangs. To illustrate the two opposite effects explained above, the graph is divided into three zones.

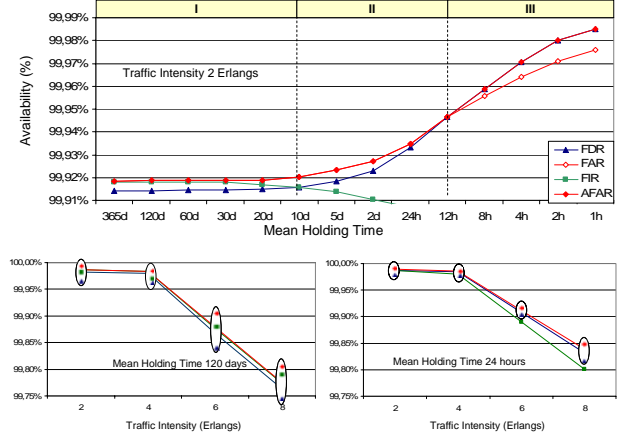


Figure 5. Availability in RT

For long holding times ($>20 \cdot \text{MTTR}$; Zone I) not taking into account failures in the network for routing (FIR strategy) results in better availability as the best disjoint path pair can be found by diverse routing algorithm. However, for short holding times ($20 \cdot \text{MTTR} \geq \text{mean holding time} \geq \text{MTTR}$; Zone II) eliminating failed resources for routing (FDR strategy) results in a much higher availability, as paths are guaranteed to be working when they are established. As we explained in advance, Failure Aware Routing (FAR), as it is a kind of mixture of both strategies, provides the best availability both for long and for short holding times.

Using this graph we choose the value of 24 hours (MTTR) for the holding time limit. For very short holding times ($< \text{MTTR}$; Zone III) the effect of simultaneous failures is higher than consecutive failures. So, looking for working and protecting routes with no failed spans make FDR as the best strategy. For very short holding times AFAR strategy performs as FDR.

Graphs on the bottom strengthen this conclusion. They represent the evolution with the traffic intensity for paths with a mean holding time of 120 days and 24 hours. To appreciate relative positions a zoom is performed.

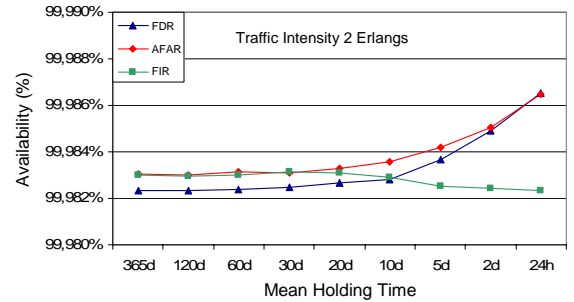


Figure 6. Availability in TT

Fig. 6 shows the network availability for the three routing strategies over the highly meshed Triangular Topology (TT). Here, the same effects can be appreciated.

Fig. 7 shows the evolution of the blocking probability for the three routing strategies over the sparse Ring Topology. The graph on the top represents the evolution with the holding time of the paths for a traffic intensity of 2 Erlangs. As shown, blocking probability remains at the same level for FDR and AFAR strategies and presents a slightly higher probability over FIR strategy. This is due to the fact that both strategies first search for a route without failures and both fail if it does not exist resulting in a higher blocking probability. FIR strategy presents a near 0% blocking probability as there are enough available resources in the network. Graphs on the bottom represent the evolution with the traffic intensity for paths with a mean holding time of 120 days and 24 hours. As expected, blocking probability increases when traffic intensity increases but the three strategies present equivalent figures.

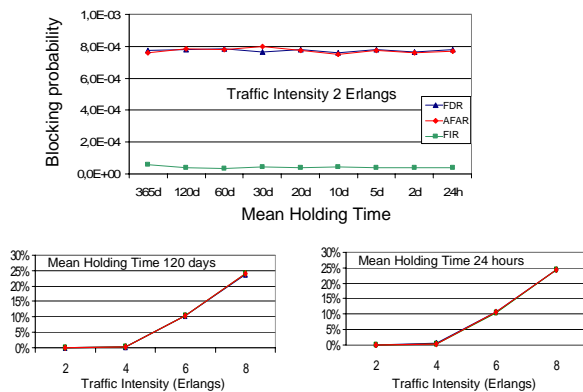


Figure 7. Blocking Probability

The three routing strategies present similar effects over the highly meshed Triangular Topology for network availability and blocking probability.

V. CONCLUSIONS

In this paper we have presented the influence of failure information over diverse routing. Moreover, we have introduced a holding-time-aware diverse routing algorithm to improve availability for on-demand path provisioning. Three strategies have been evaluated through simulation experiments.

For long holding times (e.g., order of days) the FIR strategy provides better availability as the best disjoint path pair can be found by diverse routing algorithm. On the other hand, for shorter holding times using FDR strategy results in a much higher availability, as paths are guaranteed to be working when they are established.

The new holding-time-aware strategy Adaptive Failure Aware Routing (AFAR) we propose provides the best availability in the whole range of holding times and over both topologies. We have found through simulation the value of 24 hours (MTTR) for the holding time limit. Briefly, AFAR strategy consists of:

- For long and short holding times working path is forced to use not in failure resources while allowing the protecting path to use in failure resources.
- For very short holding times FDR path is used preventing from simultaneous failures.

Regarding blocking probability, the three strategies present mainly the same figures with FDR and FAR strategies presenting a slightly higher probability over FIR strategy. This is due to the fact that both strategies first search for a route without failures and if it does not exist both fail.

According to these results we propose the general use of AFAR strategy for routing when path protection mechanism is used for on-demand path provisioning.

REFERENCES

- [1] ITU-T Rec. G.8080/Y.1304, "Architecture for the Automatically Switched Optical Networks," Nov. 2001, and Am. 1, Mar. 2003.
- [2] E. Mannie, "Generalized Multi-Protocol Label Switching (GMPLS) Architecture" RFC-3945, Oct. 2004.
- [3] Optical Internetworking Forum, "User Network Interface (UNI) 1.0 Signaling Specification, Release 2", Feb. 2004
- [4] Jajszczyk, "Automatically Switched Optical Networks: Benefits and Requirements", IEEE Optical Communications, Feb. 2005.
- [5] <http://www.fiberloops.com>
- [6] A. Iselt, A. Kirstdter and R. Chahine, "The role of ASON and GMPLS for the bandwidth trading market" in Proc. 1st International Conference on E-business and Telecommunications Networks (ICETE2004), Aug. 2004.
- [7] M. Tornatore, C. Ou, J. Zhang, A. Pattavina and B. Mukherjee, "PHOTO: an efficient shared-path protection strategy based on connection-holding-time awareness". In IEEE/OSA Journal on Lightwave Technology, Vol. 23, No. 10, pp 3138-3146, Oct 2005.
- [8] J-P. Vasseur, M. Pickavet, P. Demeester, "Network Recovery - Protection and Restoration of Optical, SONET-SDH, IP and MPLS", Elsevier, 2004.
- [9] K. Kompella, Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, Oct. 2005.
- [10] L. Velasco, S. Spadaro, J. Comellas, G. Junyent, "Diverse Routing Strategies for On-Demand Lightpath Provisioning in ASON/GMPLS Networks", Proc. of V Workshop in G/MPLS Networks, Mar. 2006, pp. 141-150.
- [11] L. Velasco, S. Spadaro, J. Comellas, G. Junyent, "Failure Aware Diverse Routing: a novel algorithm to improve availability in ASON/GMPLS networks", IEEE 8th International Conference on Transparent Optical Networks (ICTON), paper We.B3.3, Jun. 2006.
- [12] S. De Maesschalck, et. al, "Pan-European Optical Transport Networks: An Availability-based Comparison", Photonic Networks Communications, vol.3 no.5 May 2003, pp. 203-225.
- [13] W. D. Grover, "Mesh-Based Survivable Networks", Prentice Hall PTR, 2004
- [14] M. To, P. Neusy, "Unavailability Analysis of Long-Haul Networks", IEEE J. on Sel. Areas in Comm. Vol.12, no 1, Jan. 1994, pp. 100-109.
- [15] Dwivedi, R. Wagner, "Traffic Model for USA Long-Distance Optical Network", Proc. of Optical Fiber Communication Conference (OFC) 2000 Vol.1, TuK1-1, pp. 156-158.
- [16] Law, D. Kelton, "Simulation Modeling and Analysis" 3rd Ed, McGrawHill 2000