Common Protection Path: Novel MPLS-based Recovery using Path Failure Probability and Service Criticality

Seema Anand Ladhe* and Vijay T. Raisinghani
School of Engineering, NMIMS University, Mumbai - 400056, Maharashtra, India; seema.ladhe@ieee.org, rvijay@ieee.org

Abstract

Background/Objectives: Existing one-to-one, dedicated path-based and link-based MPLS-based recovery schemes are not resource efficient. We propose Common Protection Path, a novel protection scheme which ensures efficient utilization of resources. Methods/Statistical Analysis: Common Protection Path (CPP) selects a common protection path for traffic demands having the same ingress and egress routers. CPP factors in path failure probability and restoration priority levels of the traffic demands, unlike other schemes. We validated CPP algorithm using ns-2, over realistic network topology COST 239 with different link capacities. We compared CPP with one-to-one, dedicated path-based, link-based schemes and our modification of UNIFR (RFNS) i.e. UNIFR-similar. Findings: Our results show that using CPP scheme, more working bandwidth can be protected and more number of demands can be protected as compared to dedicated path-based, one-to-one, link-based and UNIFR-similar schemes. Our experimental results show that depending on the link capacity and the scheme taken for comparison, CPP provides up to 7.72% to 93.63% higher protection for COST 239 topology. Also with respect to restoration overbuild per Gbps protected bandwidth, CPP scheme is better as compared to other schemes. Applications/Improvements: Our results show that the CPP scheme results in efficient utilization of resources.

Keywords: Dedicated Path-Based, Link-Based, MPLS-Based Recovery, Protection Path

1. Introduction

Internet Service Provider (ISP) must ensure fast recovery in case of failure of link or node to achieve the required Quality of Service (QoS) guarantees. Traffic Engineering (TE) plays an important role in the service providers’ community. The principal objective of TE is to achieve network resiliency with proficient resource utilization while ensuring traffic performance. Traffic engineering objectives can be segregated as either traffic oriented or resource oriented. The traffic oriented objectives are to achieve reduction in packet dropping, reduction in delay and increase in throughput. Resource oriented TE objectives mainly focus on the efficient resource (bandwidth, buffers) utilization to allow maximum traffic demands to be routed and protected. MPLS Traffic Engineering (MPLS TE) offers combined approach to traffic engineering. The key feature of MPLS TE is fast recovery in case of failure of link/node because of its explicit path setup capability. Various MPLS recovery mechanisms have been published by IETF to provide network resiliency.

Depending on the time when the recovery paths are computed, MPLS-based recovery model can be segregated as rerouting recovery model or protection switching recovery model. In the protection switching recovery model, recovery time is less than that of rerouting since in case of protection switching recovery model, recovery paths are pre-computed before any fault occurs while in case of rerouting recovery model, recovery paths are computed on demand only after the fault occurs. MPLS...
protection schemes can be classified as either path-based protection or one-to-one protection or link-based protection schemes. One of the well-known path-based schemes is the dedicated path-based scheme. Dedicated path-based scheme requires one precomputed end-to-end recovery path which is link and/or node disjoint with the working path. The strength of dedicated path-based scheme is that resources of recovery path are fully reserved and cannot be preempted by any other traffic and hence provide guarantee for protection. One-to-one and link-based protection schemes require multiple precomputed recovery paths, protecting each link and/or node on the working path. Dedicated path-based scheme requires fewer resources than that of one-to-one and link-based schemes. Since the decision about switching of the traffic on to the recovery path is the responsibility of the immediate upstream node at the point of fault/failure, one-to-one and link-based protection schemes have a faster response than the path-based protection schemes in which ingress router is responsible for switching of the traffic on to the recovery path.

Guaranteed protection can be achieved using dedicated path-based protection. This scheme results in reservation of double bandwidth since resources are fully reserved and hence less bandwidth is available for actual traffic demand. Dedicated protection technique is mostly used where frequency of failure of link or node is more. By design core network is less susceptible for link or node failures. Hence in this situation dedicated path-based scheme would result in inefficient utilization of resources. Also path-based schemes using load balancing may result in increase in delay because of packet reordering issue.

To address the above challenges, we propose a Common Protection Path (CPP), a novel path-based protection scheme, which aims to reduce the resources required for protection. The CPP scheme selects a common protection path for all traffic demands having the same ingress and egress router. Existing MPLS-based recovery schemes (path-based, link-based and one-to-one) do not consider service criticality and path reliability for protection. The key input parameters of our proposed scheme are service criticality and path reliability. CPP aims reliable protection for the traffic demands having higher restoration priority. Our proposed scheme aims to provide the congestion free network. By congestion free network we mean that reservations for traffic demands and protection should not exceed the link capacity. The key objective of CPP is to achieve efficient utilization of resources while providing the required protection level. The proposed scheme aims to protect more bandwidth using lesser protection bandwidth and also reduce memory requirement at a node for storing the protection path information. In our prior work we had defined the preliminary version of CPP.

Next we describe existing work in MPLS protection and rerouting recovery schemes.

### 1.1 MPLS-based Recovery Schemes

MPLS TE ensures fast restoration in case of link and node failures. Below we discuss various MPLS-based recovery schemes proposed by several authors.

Ruan and Liu have proposed the Upstream Node Initiated Fast Restoration (UNIFR) scheme for fast recovery. The authors introduced the semi-global backup paths (the backup paths from the node which detects the failure of link/node to the destination/egress node). As a result of semi-global paths, UNIFR provides fast restoration as good as link-based scheme and capacity efficiency close to that of path-based schemes. Suchara M. et al. have provided a mechanism that combines path protection and traffic engineering using load balancing to provide reliable data delivery in case of link failures. R. Udayakumar et al. study the performance of resilient FTTH architecture with route protection mechanism, based on a hybrid WDM Passive Optical Network (PON) and TDM PON. Iannaccone G. et al. have presented the investigation on occurrence of failures in Sprint’s IP backbone and its effect on multimedia services. Ali and Habib have proposed a hybrid scheme for MPLS-based recovery. Their proposed scheme combines the pre-computed protection switching mechanism and the on-demand backup path computation. By simulation results the authors prove that their proposed scheme guarantees low packet loss as compared to protection switching (the standard framework of failure recovery proposed by the IETF). Wang and Li have provided an efficient distributed bandwidth management solution, a solution for inter sharing (sharing of bandwidth among backup paths of same and different service LSPs). Wang Y et al. introduced Resilient Routing Reconfiguration (R3), a novel link-based protection scheme which ensures congestion free network while handling multiple failures. Nelakuditi S. et al. have proposed an approach for fast local rerouting for handling transient link failures. Using their approach, a packet can be forwarded along a loop-free path when no more
than one link failure occurs. ITU-T Recommendation Y.2172\textsuperscript{13} has proposed various levels of restoration priority in next generation network. Traffics with restoration priority level 1, receives the highest assurance of restoration/protection than the traffics with restoration priority level 2 and level 3. Ho P. H. et al. have proposed a scheme based on shared backup path protection (SBPP)\textsuperscript{14}. Their scheme guarantees the End-to-End (E2E) availability of each Label Switched Path (LSP) and can handle up to two simultaneous failures. Izmailov R. and Niculescu D.\textsuperscript{15} have proposed path protection using load balancing to reduce the amount of spare bandwidth required for protecting LSPs. Xu M.\textsuperscript{16} et al. have presented a novel critical protection scheme for single link failure situation and multi-link failure situation based on link failure characteristics. Their scheme results in minimization of the backup cost since the problem is formulated as an optimization problem. Menth M.\textsuperscript{17} et al. introduced a new E2E protection switching mechanism, Self Protecting Multipath (SPM) that may be implemented in MPLS. By simulation results the authors proved that using their scheme, the required backup capacity can be reduced using load balancing of traffic across the disjoint paths. Ahn G.\textsuperscript{18} et al. introduced the rerouting mechanism which establishes a LSP along the least cost recovery path of all possible alternative paths. The strength of their proposed scheme is it can handle all possible failure types like link failures, node failures and faults on both a working path as well as its recovery path. Chen J.\textsuperscript{19} et al. introduced a mechanism which establishes working and backup path concurrently and results in shorter path recovery time than the End-to-End recovery mechanism. The Recommendation ITU-T G.808.3\textsuperscript{20} provides an overview of generic aspects of a Shared Mesh Protection (SMP) mechanism for connection-oriented layer networks. The mechanism in ITU-T G.808.3 is targeted for mesh network architectures. It uses protection switching recovery model to maximize speed of recovery. Hablinger G. et al. describe the Inherent Network Management (INM)\textsuperscript{21} design which focuses on fast failure response and improves traffic engineering by appropriate utilization of bandwidth.

As can be seen above, several authors have discussed the issues of restoration/rerouting and protection paths. All the schemes present either dedicated path-based or link-based or one-to-one protection. To the best of our knowledge, the existing protection schemes do not consider the following parameters for determination of protection path: link failure probability, path failure probability and restoration priority level. In our prior work we had presented preliminary version of CPP\textsuperscript{6}. We have extended our prior work\textsuperscript{6} by updating the CPP algorithm to handle partial disjoint protection path. Also, in this paper we provide detailed evaluation of CPP with realistic topology and more schemes. Also performance metrics are revised in this paper for appropriate comparison of the schemes. CPP handles partial disjoint protection path by computing extra protection path(s) to protect the nodes overlapping between protection path and working path(s). We compute these extra protection path(s) using the concept similar to UNIFR\textsuperscript{4} (protection path from the upstream node adjacent to the failure to the egress node) but in our approach we compute protection path which is totally node and link disjoint with the working path which is not the case in UNIFR. In the next section, we present our Common Protection Path scheme which selects a common protection path for all traffic demands between the same ingress-egress pair. Our scheme is unique since it considers multiple parameters to determine the backup paths, which ensures efficient utilization of resources while providing adequate protection.

The rest of the paper is organized as follows: Our CPP scheme is detailed in Section 2. We evaluate our proposed scheme (CPP) by implementing it in ns-2 and present the results in Section 3. In Section 4 we analyze the simulation results and finally Section 5 concludes the paper.

## 2. Common Protection Path (CPP): Design and Algorithm

In the previous section we discussed various MPLS-based recovery schemes. Our scheme Common Protection Path (CPP) uses Link Failure Probability (LFP), Path Failure Probability (PFP) and Restoration Priority Level (RPL) for determining the protection paths with efficient utilization of bandwidth. RPL reflects the criticality of services/traffic demands\textsuperscript{13}. This means the traffic demand with RPL = 1 receives the highest assurance of restoration. By efficient bandwidth utilization we mean how a scheme ensures that the minimum bandwidth is reserved for protection, while providing the required protection levels. Our scheme – Common Protection Path (CPP) – attempts to address the above issues.

We assume that our Common Protection Path (CPP) scheme will be run by the Network Management System (NMS). NMS has knowledge of the entire network.
Common Protection Path: Novel MPLS-based Recovery using Path Failure Probability and Service Criticality

paths for the working paths (with same ingress-egress router). CPP Computes Multiple Path Failure Probability (MPFP) to determine adequate number of protection paths. Since path failure probabilities of working paths are independent, CPP computes MPFP using binomial distribution as follows:

Let, \( S \) be the set of working paths (which are arranged in ascending order of their PFPs) with same ingress-egress router; \( N \) be the number of working paths in \( S \); \( r_w \) be the path failure probability of a working path in \( S \); \( R_S \) be the maximum of path failure probability of the working paths within \( S \) such that:

\[
R_S = \max \{ r_w \} \tag{1}
\]

Let \( Q_S \) be the MPFP of the working paths within \( S \) such that at least two or more paths in \( S \) will fail. CPP computes \( Q_S \) as follows:

\[
Q_S = \sum_{k=2}^{N} \binom{N}{k} R_S^k (1 - R_S)^{N-k} \tag{2}
\]

CPP uses a threshold \( \alpha \) as an upper bound for \( MPFP \).

If \( Q_S \leq \alpha \) then CPP allows the working paths within \( S \) to share a single common protection path. If \( Q_S > \alpha \) then more than one protection path will be required for \( S \). This ensures that adequate protection is provided to a set of working paths and avoids competition on failure of multiple working paths within \( S \). The NMS informs the ingress router of each traffic demand about the working path and also informs the ingress router of each set within a group about its protection path. The details of the CPP algorithm are as given below:

### 2.1 Common Protection Path Algorithm

**Algorithm**

1. **Categorize into groups**: Categorize the traffic demand-working path pairs into two groups based on RPL of traffic demand and determines the protection paths accordingly. The logic is that critical traffic (with RPL = 1) should be protected using highly reliable paths, while less critical traffic may be protected using less reliable paths. This segregation helps in efficient planning of the protection paths and thus provides a means for efficient utilization of the bandwidth along the protection paths. The groups are sub-divided into subgroups containing working paths with common ingress-egress routers. Within each of these subgroups, two or more working paths may fail simultaneously. Hence for each subgroup, CPP determines adequate number of common protection paths for the working paths (with same ingress-egress router).

   a. \( G1 \) contains sets of working paths of traffic demands having RPL = 1.

   b. \( G2 \) contains sets of working paths of traffic demands having RPL = 2 or 3

2. Within each group \( Gi \) determined in step 1, for each set \( Gi-Kg-s \) do the following:
A. Sub-grouping based on MPFP: Compute set $M$ such that $M = \{S | S \notin K_{z_b} \text{ and } Q_b = \alpha \}$ where $Q_b$ is the multiple-PPF (MPFP) of the working paths, computed by CPP scheme. Further, $S = \{w_n \mid PFP(w_n) \leq PFP(w_{n+1}) \text{ and } 1 \leq n \leq |S| \}$, where $w_n$ is a working path in $S$. $S = G(V_S, E_S)$ - graph of nodes $V_S$ and edges $E_S$.

Note: Since $S$ contains working paths which are arranged in ascending order of their PFPs, to compute $Q_b$ we start from first working path (which is having lowest PFP in $S$) till $Q_b = \alpha$.

B. Determination of protection path: Within $M$ determined in step 2.A, for each $S$ do the following:

I. Compute a set $H_S$, where $H_S = \{b_n \mid b_n = \text{required protection bandwidth} (w_n), w_n \notin S \}$ i.e. $H_S$ contains required protection bandwidth of all working paths of set $S$. From $H_S$, select $h_S$, where $h_S = \text{max} (H_S)$.

II. Compute a set $T_S$, where $T_S = \{v \mid v \notin V_S, v \notin S \}$, contains intermediate nodes of all working paths of set $S$.

III. Let $G(V,E)$ be the entire network under consideration. Let $G' = \{e \mid e \notin E \text{ and available bandwidth} (e) < h_S \}$. Let $J = G \setminus G'$. That means, from the network topology prune the links having bandwidth $< h_S$ is computed as stated in step 2.B.1).

IV. Compute a set $Y | J$ where $Y = \{z_b \mid z_b = \text{possible protection paths for working paths within } S, T_S \cap T_{z_b} = \text{Null} \text{ where } T_{z_b} \text{ is the set of intermediate nodes of } z_b \text{ and } b = 1, 2, 3, \ldots \}$

Note: $T_S \cap T_{z_b} = \text{Null}$ ensures that the possible protection path is node as well as link disjoint with its respective set of working paths $S$.

V. If $Y \neq \text{Null}$ then select the protection path $z_b$ from $Y$ having minimum PFP and go to step 2.B.VII.

VI. If $Y = \text{Null}$ then do the following steps:

a. Compute a set $Y' | J$ containing all possible protection paths, $z_b$ where $b = 1, 2, 3, \ldots$

b. From $Y'$ select the protection path with minimum value of $|T_S \cap T_{z_b}|$ where $T_{z_b}$ is the set of intermediate nodes of a possible protection path $z_b$. The logic is that since $|T_S \cap T_{z_b}|$ is minimum it ensures minimum overlapping between protection path $z_b$ and its respective set of working paths $S$.

c. Let selected protection path $z_b$ contain $k$ nodes overlapping with its set of working path $T_S$. For each working path $w_i$ of $S$ (where $i = 1 \text{ to } |S|$) do the following:

i. Compute set $X = T_{w_i} \cap T_{z_b}$, where $T_{w_i}$ is the set of intermediate nodes of $w_i$ excluding ingress and egress nodes. That means, set $X$ contains the nodes of $z_b$ overlapping with working path $w_i$.

   If $X = \text{Null}$ then go to next step, 2.B.VI.c.ii, else if $X = \text{Null}$ then go to step 2.B.VI.c (take the next working path $w_{i+1}$).

ii. Let $bw_i$ represent the bandwidth reserved for working path $w_i$. Let $node_u$ be the upstream node relative to all other nodes in $X$, on working path $w_i$. Let $node_m$ be the immediate upstream node of $node_u$ within $w_i$. Compute a set $Z | J$ of all possible protection paths from $node_u$ to $s$ (where $s$ is the egress node of $w_i$) such that each protection path is disjoint with $X$. From $Z$ select the protection path $z_{\text{minPPF}}$ with minimum PFP.

iii. For the protection path $z_{\text{minPPF}}$, mark the bandwidth of value $bw_i$ as reserved.

Low priority traffic demands can be routed over the path $z_{\text{minPPF}}$. By low priority traffic demand we mean that the traffic demand whose RPL is greater than the RPL of traffic demand having working path $w_i$. However, for the traffic demand having working path $w_i$ if RPL=2 then traffic demand with RPL=2 or 3 is permitted.

iv. In case of failure of any node in $X$ allow the low priority traffic demand to be pre-empted by the high priority traffic demand having working path $w_i$.

v. Go to step 2.B.VII.

VII. For the protection path $z_b$ computed above (in step 2.B.V if $Y \neq \text{Null}$ or in step 2.B.VI.b if $Y = \text{Null}$) reserve the bandwidth of value $h_S$. The logic is that since $h_S$ is the maximum value of $H_S$ (computed in step 2.B.I), so any
working path of set $S$ would be fully restorable using the protection path in case of failure of its link/node.

In worst case CPP algorithm may not compute the protection path for a set of working paths due to unavailability of resources, indicating that the set cannot be protected.

### 2.2 Evolution of CPP

We had presented the preliminary version of CPP, CPP version 1. Our prior work does not consider partial disjoint protection path and detailed evaluation of CPP with realistic topology and more schemes. In CPP version 1, we created three groups G1, G2 and G3 based on RPL and thresholds of PFP. Groups G1 and G2 contain working paths of traffic demands having RPL = 1 and G3 contains working paths of traffic demands having RPL = 2 or 3. For working paths with RPL = 1, our logic of creating two groups G1 and G2 was as follows: Typically, if the PFP increases with the path length. To protect more number of traffic demands having RPL = 1, the working paths of shorter length should get higher priority for protection than the working paths of longer length. We used a threshold $\tau_1$ for this purpose. CPPv1 computes protection paths for the working paths in order of groups G1, G2 and G3. CPPv1 used threshold $\tau_1$ as an upper bound for the working paths to be in group G1. The working paths with RPL = 1 and having PFP $\leq \tau_1$ get higher priority for protection than the working paths with RPL = 1 and having PFP $> \tau_1$. We used threshold $\tau_2$ as an upper bound for the working paths to be routed. Paths having PFP $> \tau_2$ are considered more susceptible to failure and hence not selected to route the traffic demands.

After our detailed experimental evaluations on realistic network, we concluded that $\tau_1$ and $\tau_2$ do not help to reduce the resources utilized for protection of paths and can lead to poor grouping and waste of resources. Only the threshold on MPFP, $\alpha$ is sufficient to create groups for resource sharing. The final version of CPP is CPPv2 (presented here) without using thresholds $\tau_1$ and $\tau_2$.

### 2.2.1 Implementation and Simulation Results

The CPP algorithm has been implemented in ns-2 and tested for realistic network topology, European COST 239. We use the term topology or test network interchangeably. We use the terms working bandwidth, protection bandwidth, protected bandwidth, fully protected demands to compare the results of various schemes. Working bandwidth means the summation of the total bandwidth used by working paths on each link and protection bandwidth means the summation of the total bandwidth reserved by protection paths on each link. Protected bandwidth means the summation of the total bandwidth used by working paths of fully protected demands on each link. A traffic demand is said to be fully protected if all links of its working path are protected otherwise it is partially protected. We compare CPP scheme with MPLS one-to-one protection scheme, dedicated path-based scheme and link-based scheme.

Further, for comparison we have simulated a scheme similar to UNIFR for our comparisons as we could not simulate exactly the same characteristics of the scheme. We call this scheme as UNIFR-similar. The key difference between UNIFR and UNIFR-similar is that in the UNIFR scheme, traffic demand is admitted only when 100% restoration is possible. However, UNIFR-similar scheme first computes the working paths of all traffic demands and then computes the protection paths. So in UNIFR-similar scheme, if sufficient resources are not available, then the traffic demand cannot be protected, even though it is admitted. For comparing with CPP, to ensure that the sequence of computation of working and protection paths does not affect the results, for all schemes we first compute the working paths for all traffic demands and then compute the protection paths. In case of CPP scheme, the working path and PFP of each traffic demand is computed by NMS as described in Section 2. For all other simulated schemes, we select the working paths using CSPF algorithm with available bandwidth of each link as a constraint. We simulate all the schemes over realistic network topology COST 239. The details of the traffic demand matrix for COST 239 are given in Section 3.1.

In case of CPP, for COST 239 network topology, we configure all the duplex links with random LFP ranging from 0.001 to 0.03. For CPP, we assume certain RPLs for each of the traffic demands. For all of our simulations we assume $\alpha$ as an upper bound for Multiple Path Failure Probability (MPFP). Threshold on MPFP, $\alpha$ would have an effect on the efficiency of CPP, since it controls the number of working paths that can share a Common Protection Path. For our simulation setups, our initial experimentation showed that for $\alpha = 0.003$, two working paths can share a Common Protection Path. Higher value of $\alpha$ will give higher number of working paths sharing a
Common Protection Path. That is more number of working paths will compete for a protection path in case of concurrent failure of their link/node. Hence, we decided to keep $\alpha = 0.003$ for all our simulations. Network administrators can determine a suitable $\alpha$ for their networks based on the efficiency that they want to achieve. Further, we also assume that the required protection bandwidth for a working path is same as the bandwidth reserved for it. As we had mentioned earlier, the other schemes simulated do not consider separately or a combination of Link Failure Probability (LFP), Path Failure Probability (PFP) and Restoration Priority Level (RPL) for determining the protection paths. In the next section, we describe our simulation of CPP scheme and other existing protection schemes using the European COST 239 network topology.

2.2.2 Simulation using COST 239 Network Topology

COST 239\textsuperscript{23,24} network topology has 11 nodes and 26 links as shown in Figure 1. The traffic demand matrix given in Table 1 is adopted from ref.\textsuperscript{23} and used in the simulation.

Each entry of the traffic demands in Table 1 represents the aggregate traffic between two nodes. We assume that each demand is a summation of sub-demands. Hence we split each demand, which is greater than 2.5, randomly into 2 to 5 sub-demands, for our simulations. Thus we have generated 225 sub-demands using the data in Table 1. The working path and PFP of each traffic demand is computed by NMS as described in Section 2. Our aim was to determine the performance of CPP and other schemes for various link capacities. We created three scenarios for testing the schemes. We created the first scenario where all demands could be routed. Using this case we could evaluate how a scheme performs in case all demands are routed. In the next two scenarios we kept the link capacities lower so that some demands could not be routed. These scenarios could mimic scenarios in actual networks. Through iterations we determined the close to minimum link capacity which could permit all the demands to be routed. We determined the link capacity as 100 Gbps for this case. For the other two scenarios we determined the link capacities as follows. In the second scenario, we kept link capacity as 30% higher than the maximum two-way traffic i.e. 130% of $27.5^2 = 71.5$ Gbps. In the third scenario, we kept the link capacity ranging from 50-100 Gbps.

We compute working bandwidth, protection bandwidth, protected bandwidth, number of fully protected demands as discussed above.

Table 1. Traffic demands (in Gbps) between nodes in the COST 239 network

|   | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 |
|---|----|----|----|----|----|----|----|----|----|----|----|
| 1 | X  | 12.5| 15 | 2.5| 5  | 27.5| 12.5| 2.5| 17.5| 25 | 2.5 |
| 2 | 12.5| X  | 15 | 2.5| 7.5| 22.5| 5  | 2.5| 5   | 7.5| 2.5 |
| 3 | 15 | 15 | X  | 2.5| 7.5| 27.5| 7.5| 2.5| 7.5 | 7.5| 2.5 |
| 4 | 2.5| 2.5| 2.5| X  | 2.5| 5   | 2.5| 2.5| 2.5 | 2.5| 2.5 |
| 5 | 5  | 7.5| 7.5| 2.5| X  | 22.5| 2.5| 2.5| 2.5 | 5  | 2.5 |
| 6 | 27.5| 22.5| 27.5| 5 | 22.5| X  | 20 | 5  | 15 | 20 | 7.5 |
| 7 | 12.5| 5  | 7.5| 2.5| 2.5| 2.5 | 20 | X  | 2.5| 10 | 12.5| 2.5 |
| 8 | 2.5| 2.5| 2.5| 2.5| 2.5| 5   | 2.5| X  | 2.5| 2.5| 2.5 | 2.5 |
| 9 | 15 | 5  | 15 | 2.5| 2.5| 15  | 10 | 2.5| X  | 10 | 2.5 |
| 10| 25 | 7.5| 2.5| 2.5| 5  | 20  | 12.5| 2.5| 10 | X  | 2.5 |
| 11| 2.5| 2.5| 2.5| 2.5| 2.5| 7.5 | 2.5| 2.5| 2.5| 2.5| X  |

Figure 1. COST 239 Network (11 nodes, 26 links).
From Table 2, at link capacity 100 Gbps, total number of routed demands is 225 (i.e. all simulated demands are routed) and working bandwidth is 1341 Gbps. When the link capacity is 71.5 Gbps then the total number of routed demands is 200 (25 demands cannot be routed) and working bandwidth is 1204 Gbps. For the scenario when the link capacity is between 50 Gbps to 100 Gbps, the total number of routed demands is 196 (29 demands cannot be routed) and working bandwidth is 1152.5 Gbps.

Table 3 represents the protected bandwidth (Gbps), protection bandwidth (Gbps), number of fully protected demands and number of reserved protection paths for three scenarios having different link capacity as discussed above and all schemes (said above) using network topology COST 239 (as shown in Figure 1). From Table 3, for all link capacity scenarios, using CPP scheme, protected bandwidth is more and also more demands are protected as compared to other schemes taken for comparison.

### 3. Result Analysis

In this section we presented the simulation set-up and the observations for COST 239 network topology and compared it with other multiple existing protection schemes. In the next section, we carry out the result analysis.

**Table 2.** Working bandwidth and number of routed demands for Cost 239 network

| Parameter                              | Link-capacity (Gbps) |
|----------------------------------------|----------------------|
|                                        | 100                  |
| Working Bandwidth (Gbps)               | 1341                 |
| Number of routed demands               | 225                  |
| Total Simulated demands: 225           |                      |

| Parameter                              | Link-capacity (Gbps) |
|----------------------------------------|----------------------|
|                                        | 71.5                 |
| Working Bandwidth (Gbps)               | 1204                 |
| Number of routed demands               | 200                  |
| Total Simulated demands: 200           |                      |

| Parameter                              | Link-capacity (Gbps) |
|----------------------------------------|----------------------|
|                                        | 50-100               |
| Working Bandwidth (Gbps)               | 1152.5               |
| Number of routed demands               | 196                  |
| Total Simulated demands: 196           |                      |

**Table 3.** Protected bandwidth, protection bandwidth, number of fully protected demands and number of reserved protection paths for Cost 239 network

| Parameter                              | Scheme                      |
|----------------------------------------|-----------------------------|
|                                        | CPP | Dedicated path-based | One-to-one | Link-based | UNIFR-similar |
| Protected bandwidth (Gbps)             | 100 | 730                   | 617        | 405.5      | 385.5         | 377          |
|                                        | 71.5| 390.5                 | 357        | 206        | 202.5        | 206          |
|                                        | 50-100| 446.5                 | 414.5      | 278.5      | 259.5        | 276.5        |
| Protection bandwidth (Gbps)            | 100 | 1035.5                | 982        | 1035       | 1078.5       | 1030.5       |
|                                        | 71.5| 574                   | 560.5      | 589        | 580          | 596.5        |
|                                        | 50-100| 644                   | 622.5      | 736        | 750          | 740          |
| Number of fully protected demands      | 100 | 126                   | 118        | 90         | 86           | 87           |
|                                        | 71.5| 78                    | 77         | 51         | 49           | 51           |
|                                        | 50-100| 89                    | 86         | 66         | 64           | 67           |
| Number of reserved protection paths    | 100 | 115                   | 118        | 154        | 155          | 150          |
|                                        | 71.5| 73                    | 77         | 94         | 89           | 94           |
|                                        | 50-100| 86                    | 86         | 119        | 113          | 121          |
node. ANCPB reflects the average memory requirement at a node for storing the protection path information per Gbps Protected Bandwidth.

We use the results from Table 2 and Table 3 to compute and plot the performance metrics discussed above for each of the simulated schemes. We represent protected bandwidth in Figure 2, ROB in Figure 3, PEB in Figure 4, RP in Figure 5 and ANCPB in Figure 6.

The efficiency of CPP is evident by higher protected bandwidth, lower ROB, lower RP, higher PEB and lower ANCPB than that of other schemes. CPP computes the protection paths for the groups of working paths and reserves less protection capacity relative to the summation of bandwidth allocated to the working paths. Other schemes taken for comparison do not use RPL and PFP to compute the protection paths (described in section 3). So using CPP, amount of spare bandwidth needed per unit protected bandwidth is less as compared to that of other schemes (shown in Table 3).

CPP performs better because the paths are grouped based on RPL as explained in CPP algorithm in Section 2. For every group, CPP computes sets of working paths (having same ingress-egress pair) based on MPFP. Then for each set, CPP computes a protection path. This results in substantial reduction in protection bandwidth per Gbps protected bandwidth and the number of protection paths per Gbps protected bandwidth, which ultimately results in decrease in redundancy, increase in protection efficiency and decrease in average node complexity.

In the next section, we present our conclusion and future work.

4. Conclusion

The major challenge for the service providers is to provide network resiliency in case of link and/or node failure. We
proposed the Common Protection Path (CPP) scheme using which we can minimize the number of protection paths per unit protected bandwidth, which ultimately results in decrease in redundancy and average node complexity. We have also proved that using CPP scheme, protected bandwidth is higher as compared to other schemes taken for comparison. We created various link capacity scenarios and validated CPP scheme using ns-2, over realistic network topology COST 239. From Figure 2, CPP provides higher protection than other schemes taken for comparison. By detailed validation we conclude that the resource efficiency of CPP scheme is better than the other schemes taken for comparison since in general CPP results in lower ROB, as shown in Figure 3. Higher protection (depending on the scheme and link capacity taken for comparison higher protection up to 7.72% to 93.63%), lower ROB (up to 7.69% to 50%), lower RP (up to 3% to 49%), lower ANCPB (up to 5% to 62%) and higher PEB (up to 2.7% to 34.75%) of CPP scheme leads to higher utilization of resources as compared to other protection schemes which are taken for comparison with CPP. Our experimental results show that with respect to efficient utilization of resources (amount of spare bandwidth needed per unit protected bandwidth, number of protection paths per unit protected bandwidth), CPP would perform better than most schemes which are similar to the schemes considered for comparison with CPP above.

5. References

1. Awduche D, Malcolm J, Agogbua J, O’Dell M, McManus J. Requirements for traffic engineering over MPLS. RFC 2702; 1999. pp. 1–29.
2. Bhatia RS, Kodialam M, Lakshman TV, Sengupta S. Bandwidth guaranteed routing with fast restoration against link and node failures. Journal IEEE/ACM Transactions on Networking. 2008 Dec; 16(6):1321–30.
3. Sharma V, Hellstrand F. Framework for Multi-Protocol Label Switching (MPLS)-based Recovery [Internet]. IETF RFC. 2003 Feb. p. 7–14.
4. Ruan L, Liu Z. Upstream node initiated fast restoration in MPLS networks. IEEE International Conference Communications; ICC. 2005 May 16–20. p. 959–64.
5. Suchara M, Xu D, Doersspike R, Johnson D, Rexford J. Network architecture for joint failure recovery and traffic engineering. ACM Sigmetrics Performance Evaluation Review - Performance evaluation review; 2011. p. 97–108.
6. Ladhe SA, Raisinghani VT. A resource efficient common protection path approach for MPLS-based recovery. 2013 5th International Conference on Communication Systems and Networks, COMSNETS 2013; Bangalore. 2013 Jan 7–10. p. 1–9.
7. Udayakumar R, Khanna V, Kaliyamurthie KP. Performance analysis of resilient FTTH architecture with protection mechanism. Indian Journal of Science and Technology, 2013 Jun; 6(56):4737–41.
8. Iannaccone G, Chun CN, Mortier R, Bhattacharyya S. Analysis of link failures in an IP backbone. IMW ’02 Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement; 2002. p. 237–42.
9. Ali EK, Habib Y. An efficient hybrid recovery mechanism for MPLS-based networks. Proceedings - IEEE Symposium on Computers and Communications. ISCC’09; Sousse. 2009 Jul 5–8. p. 474–80.
10. Wang D, Li G. Efficient distributed bandwidth management for MPLS fast reroute. IEEE/ACM Transactions on Networks. 2008 Apr; 16(2):486–95.
11. Wang Y, Wang H, Mahimkar A, Alimi R. R3: Resilient Routing Reconfiguration. Proceedings of the ACM SIGCOMM 2010 Conference SIGCOMM [Internet]; 2010. p. 291–302.
12. Nelakuditi S, Lee S, Yu Y, Zhang ZL, Chun CN, Member S. Fast local rerouting for handling transient link failures. IEEE/ACM Transactions on Networking. 2007 Apr; 15(2):359–72.
13. ITU-T Recommendation Y. 2172. Service restoration priority levels in Next Generation Networks, ITU-T Recommendation. 2007. p. 3.
14. Ho PH, Tapolcai J, Haque A. Spare capacity reprovisioning for shared backup path protection in dynamic generalized multi-protocol label switched networks. Transactions on Reliability. 2008 Dec; 57(4):551–63.
15. Izmailov R, Niculescu D. Flow splitting approach for path provisioning and path protection problems. Workshop on High Performance Switching and Routing, Merging Optical and IP Technologies; 2002. p. 93–8.
16. Xu M, Hou M, Wang D, Yang J. An efficient critical protection scheme for intra-domain routing using link characteristics. Computer Networks. 2013 Jan; 57(1):117–33.
17. Menth M, Reifert A, Milbrandt J. Self-Protecting Multipaths – A simple and resource-efficient protection switching mechanism for MPLS Networks NETWORKING 2004 Networking Technologies, Services and Protocols, Performance of Computer and Communication Networks; Mobile and Wireless Communications; 2004. p. 526–37.
18. Ahn G, Jang J, Chun W. An efficient rerouting scheme for MPLS-based recovery and its performance evaluation. Telecommunication Systems. 2002 Mar; 19(3-4):481–95.
19. Chen J, Chiou CC, Wu SL. A fast path recovery mechanism for MPLS Networks. Networking - ICN 2005. Berlin Heidelberg, Springer: 2005. p. 58–65.
20. G.808.3 I-T. Generic protection switching – Shared mesh protection. 2012. p. 1–10.
21. Hablinger G, Nunzi G, Meirosu C, Fan C, Andersen FU. Traffic engineering supported by Inherent Network Management: Analysis of resource efficiency and cost saving potential. International Journal of Network Management. 2011 Jan-Feb; 21(1):45–64.
22. Deepankar M, Karthikeyan R. Network Routing: Algorithms, Protocols and Architectures. San Francisco, CA, USA. Morgan Kaufmann Publishers Inc; 2007. p. 250–1.
23. P709 EP. Planning of full optical network. Deliverable 2 Basic factors influencing optical networks. 1999. p. 30.
24. Avci SN, Hu X, Ayanoglu E. Hitless recovery from link failures in networks with arbitrary topology. Conference Proceedings of 2011 Information Theory and Applications Workshop, ITA 2011; La Jolla, CA. 2011 Feb 6-11. p.1–6.
25. Li G, Wang D, Kalmanek C, Doverspike R. Efficient distributed path selection for shared restoration connections. Proceedings - IEEE Twenty First Annual Joint Conference of the IEEE Computer and Communications Societies. INFOCOM; 2002. p. 140–9.