HYBRID BACKUP MODEL WITH GENETIC BRANCH POINT OPTIMIZATION FOR SINGLE ELEMENT FAILURE IN MPLS NETWORKS

Ruttikorn Varakulsiripunth[1]

[1]Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
e-mail: kvruttik@kmitl.ac.th

Received Date: May 27, 2011

Abstract

In this paper, we present an approach for enhancing current MPLS resilience, called Hybrid Backup model (HB), in order to restore a QoS protection path from both node or link failures. At present, there are three main MPLS fault management methods, i.e., global, reverse and local backup models. Firstly, the global backup model is the cheapest model but it suffers from high packet losses and long restoration time. Secondly, the reverse backup model improves the packet loss problem; however, the delay problem still remains. Thirdly, the local backup method is seemed to be the best choice in case of the minimum restoration time and packet losses, nevertheless, it has high cost in term of number of path switch label switching router (PSL), path merge label switching router (PML), label usage, and bandwidth reserved. Therefore, we proposed a new approach based on hybrid of four switching types which are global, global reverse, local and local reverse switching types. To evaluate number and location of branch point, branch point optimization based on Genetic Algorithm is then proposed. The proposed model can be reduce the cost of the local backup model, while it still maintains fast restoration and low packet losses. Furthermore, it can improve some significant network performances such as bandwidth reserved, rejection probability, and total throughput. According to performance comparison between all backup models, numerical and simulation results are presented to support the proposed backup model.

Keywords: Diff-Serv awareness, Failure recovery, Genetic algorithm, Guaranteed LSP, MPLS network, QoS protection, Resiliency, Routing optimization

Introduction

Conceived and developed in the late '90s by the Internet Engineering Task Force, MPLS, or Multi-Protocol Label Switching is a network management protocol originally intended to integrate layer 2 information about network links (bandwidth, latency, utilization) into layer 3 (IP) elements within a particular system. The MPLS framework is a solution of supporting Quality of Service (QoS) over IP network. Although, applications relying on the class such as FTP are not time-critical. However, the convergence of time-critical application such as video conference is concerned with QoS requirements such as bandwidth, delay, and delay jitter. MPLS relies on an approach that employs ATM-like "label swapping" technique to speed up the packet forwarding without any changes to the existing IP routing protocol. MPLS forwarding is based on connection-oriented mechanism to transmit data throughout the network. The MPLS path called Label Switched Path (LSP) is established along routers called Label Switching Router (LSR) using MPLS routing protocol [1]. Furthermore, the MPLS technology is extended and modified to be Generalized MPLS (GMPLS) which can support more general switching types other than ATM switching such as Packet Switch Capable (PSC), Layer-2 Switch Capable (L2SC), Time-Division Multiplex Capable (TDM), Lambda (λ) Switch Capable (LSC), and Fiber-Switch Capable (FSC) interfaces [2].

Resiliency is defined as the ability of the network to recover from failures and provide the services running despite the occurrence of failures: link or element (either node or link) failures [3]. Especially for time-critical or real-time applications, impact of link or nodes failure such as a fiber cut will cause severe data loss. Further, the impact will increased noticeably in high speed optical switching, since, just a few milliseconds duration of failure will cause retransmission of gigabit packet losses. Hence, MPLS resiliency issue is getting more interesting and much works are currently done by the Internet Engineering Task Force (IETF) to develop a standard framework for MPLS-based recovery [4].

This paper presents an approach called Hybrid Backup model (HB) integrated with Genetic Algorithm (GA) Optimization, in order to enhancing current MPLS-based recovery related to Differentiated Services-aware MPLS traffic engineering [5]. Major goals are to decrease implementation cost and complexity of existing backup models, to improve guarantee level of Quality of Service and to get better overall network performances in terms of bandwidth reserved, rejection probability, and total throughput.

The remainder of the paper is organized as follows. Section 2 presents framework of MPLS recovery mechanisms. Section 3 shows related works of MPLS-based recovery model. Section 4 describes detail descriptions of the proposed backup model. Section 5 illustrates network metrics used for performance comparison. Numerical results and discussions are shown in Section 6. Finally, Section 7 concludes the paper and points out further research topics.

MPLS Resiliency Framework

In this section, details of framework for MPLS-based recovery standardized by MPLS working group of IETF [4] are explained.

Failure Detection Mechanism

As mention in the introduction section, types of failure can be classified into link or element (node/link) failure. The basic recovery operation must be able to repair both types of failure. To detect such failures, Liveness Message is required to periodically exchange between two adjacent LSRs that serves as a link probing mechanism. It provides an integrity check of the forward and the backward directions of the link between the two LSRs as well as a check of neighbor aliveness.

Path Establishment and Resource Allocation

Backup path establishment can be divided into 2 classes which are *rerouting* and *protection switching* (see Figure 1). With rerouting, path establishment will be processed after the occurrence of a fault. On the other hand, in protection switching, backup paths are pre-established based on the chosen routing policies before the occurrence of a failure. In addition, the protection switching mechanism may sometimes be called "*fast rerouting*", because it provides fast recovery time.

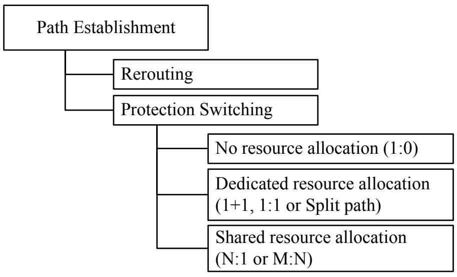

Path Establishment
Rerouting
Protection Switching
No resource allocation (1:0)
Dedicated resource allocation (1+1, 1:1 or Split path)
Shared resource allocation (N:1 or M:N)

Figure 1. Path establishment and resource allocation

With protection switching, there are three resource allocation models which are no, dedicated and shared resource allocations (see Figure 1). In *no resource allocation,* a backup path with zero resource allocation is setup. This may be called 1:0 protection (1 working path per 0 recovery path) or no protection. In *dedicated resource allocation*, there are some dedicated paths reserved. The examples for this allocation type are 1+1, 1:1 and split path protections. In the case of 1+1 protection, traffic is sent concurrently on both the working and the backup paths. This protection type brings fast restoration time and no packet losses, although it consumes double amounts of traffic. In 1:1 protection, a working LSP is protected (or restored) by one disjoints backup LSP. In split path protection, one working LSP is protected by multiple split backup LSPs. Both 1:1 and split path schemes utilize less bandwidth than 1+1 protection; however, they have slower restoration time and higher packet losses. In *shared resource allocation*, 1 backup LSP can be shared by multiple working LSPs such as N:1 and M:N protection. With N:1 protection, N working paths are protected by one backup path. In M:N protection, M working paths are protected by N backup paths. Besides, the share resource allocation carries more efficient bandwidth usage than the dedicated resource allocation.

Recovery Cycle Model

The MPLS recovery cycle model is illustrated in Figure 2. It can be divided into five durations. Firstly, *fault detection time* (T_{FD}) is time between the occurrence of network impairment and the moment the fault is detected by the Liveness Message process. Secondly, *fault hold-off time* (T_{FH}) is time between the detection of a fault and taking recovery action, to allow time for lower layer protection to take effect. The T_{FH} may be zero. Thirdly, fault notification time (T_{FN}) is time between initiation of a *Fault Indication Signal* (FIS) by the LSR detecting the fault and the time at which the Path Switch LSR (PSL) begins the recovery operation.

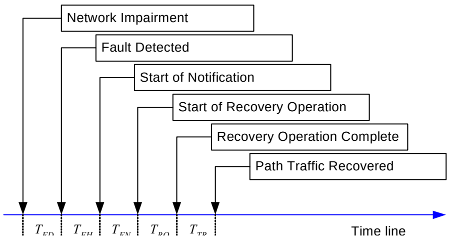


Figure 2. MPLS recovery cycle model

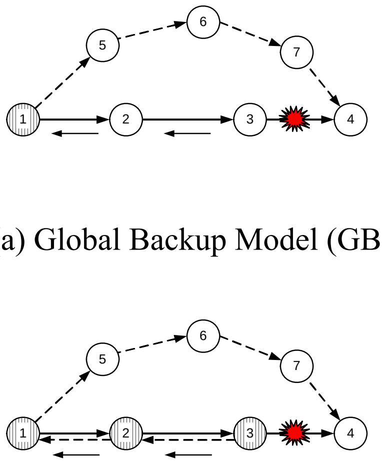
This is zero if the PSL detects the fault itself or infers a fault from such events as an adjacency failure. Fourthly, recovery operation time (T_{RO}) is time between the first and last recovery actions. This may include message exchanges between *Path Switch LSR* (PSL) and *Path Merge LSR* (PML) node. The PSL is the node responsible for the switchover function from the working path to the corresponding backup path, once the failure is identified. The PML is the node where the working and backup paths merge into a single outgoing LSP. Then, the large number of PSL and PML nodes will be effect on the more recovery delay. Fifthly, traffic recovery time (T_{TR}) is time between the last recovery action and the time that the traffic is fully repaired. Finally, the restoration time is defined as total time spent to complete the recovery cycle.

Related MPLS Backup Models

Many works for MPLS resiliency issues have been previously proposed [6]-[15]. However, those works could be concluded into three types of backup model [11], [12]: global, reverse and local backup model. The main ideas of each methods and their pros and cons are described as follows.

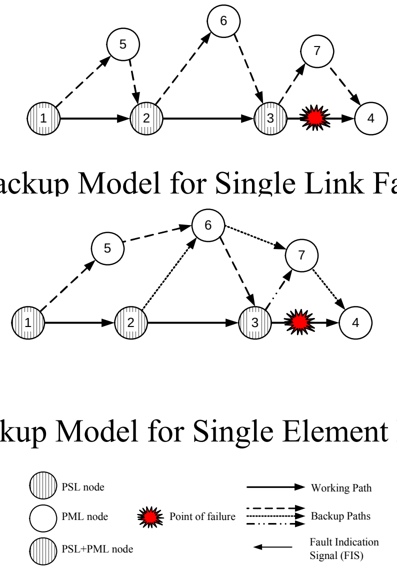
Global Backup (GB) Model

With this model (see Figure 3 (a)), an ingress LSR is responsible for path recovery when the FIS arrives. It requires an alternative, end-to-end, unconnected path to be a backup path for each working path. Since the protection process is initiated by the ingress LSR, hence it is centralized protection. This method requires setting up only one backup path per one working path and only two LSP have to be provided with PSL/PML functions. However, the method has high packet losses during the switchover period. Further, it also requires an additional LSP to reverse the FIS back to the ingress node.



(a) Global Backup Model (GB)

(b) Reverse Backup Model (RB)



(c) Local Backup Model for Single Link Failure (LLB)

(d) Local Backup Model for Single Element Failure (ELB)

Figure 3. Related MPLS-based recovery models

Reverse Backup (RB) Model

This model improves the global backup model in case of packet losses during the switchover time. It reverses traffic closed to the point of failure, back to the ingress LSR (See Figure 3 (b)). This model is especially good for the traffic which is very sensitive to packet losses. However, there are three main disadvantage of the reverse backup. Firstly, it could be poor resource utilization, because two backups (reverse path and back up path) per protected domain are needed. Secondly, it wastes time taken to reverse FIS to the ingress node. Thirdly, it requires packet reordering capability at the ingress node.

Local Backup (LB) Model

In local backup model, traffic restoration begins at LSR much closer to the failure point (See Figure 3 (c) and (d)). Therefore, it offers a faster restoration time than both previous models. This brings a reduction of amount of packet losses. In local backup model, the switchover process is transparent to the ingress node, thus, no FIS is required to reverse to the ingress node. On the other hand, every protected LSR has to be provided with a switchover and merge function. Moreover, the model requires multiple backup paths. Higher setting up of protected path, brings higher complexity and can lead to low resource utilization. To support both failure types (link and element failure), the LB model is separated into single link (LLB) and single element protection (ELB) as shown in Figure 3 (c) and (d), respectively. The ELB model uses longer backup paths than the LLB model.

Hybrid Backup Model

Although, the LB model achieves fastest restoration time, it utilizes high amount of bandwidth reserved, number of backup paths, labels used and number of PSL/PML nodes. Then, our first solution for a single point of failure protection, called "*Local Reverse Backup*," was proposed in [15]. From the proposed results, they obviously show that the proposed algorithm can reduce numbers of PSL/PML and backup paths of the LB model, where as Quality of Service protection is still on acceptable level. However, some issues about effects of network scalability to overall network performances are still unanswered.

Therefore, in this paper, we propose “*Hybrid Backup (HB) model*,” as an extension to the previous solution.

Main Objectives

There are two main objectives listed as following items.

1) Minimizing number of backup paths, in order to reduce numbers of backup path which leads to low number of label used and low amounts of bandwidth reserved. The less number of label used brings the less memory space required at the node. Also, the less amount of bandwidth reserved increases the more probability of successful traffic request and more network throughput.

2) Providing fast restoration with low packet losses from a single element failure, in order to maintain QoS guaranteed level required by the traffic based on Differentiated Services (or other similar QoS system).

According to the first objective, branch point approach is proposed (see Section 4.2). Therefore, HB model utilizes lower number of backup paths than those of LB model. And numbers of PSL/PML nodes are also reduced comparing to the LB model. This leads to lower hardware cost and implementation complexity, where as the fast restoration and low packet loss are still maintained.

According to the second objective, the HB model is designed based on the protection switching model. As a result, the backup (or recovery) paths are completely pre-established before an occurrence of failure. We propose local reverse switching (see Section 4.3) in order to attain faster restoration than those of GB and RB model.

Backup Path Establishment Based on Genetic Algorithm Optimization

With HB model, there are three types of backup path to be pre-established: global, reverse, and branch (or local) backup paths. First of all working and global backup paths should be established based on existing MPLS routing algorithm. We choose the Widest Shortest Path (WSP) [16] for main routing algorithm.

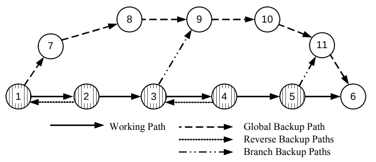


Figure 4.Example for backup path establishment

Figure 4. shows example network with 11 nodes. Path {1-2-3-4-5-6} and {1-7-8-9-10-11-6} are working and global backup paths, respectively. After working and global backup paths are chosen, one or more branch point nodes in part of working path members are then selected based proposed GA optimization. The optimized function for GA can be shown in Equation (1). Where QoSP refers to Quality of Service Protection level which related to total packet lost, restoration time and bandwidth consumption. Details of QoSP calculation can be found in sub section 5.2. From Equation (1), n_{BP} denotes to total numbers branch points selected where $n_{BP} \leq n_{MBP}$. Where n_{MBP} denotes to maximum numbers (or upper bound) of branch points, which can be used by network administrator to reduce the optimization time. Calculation process of the optimization function is illustrated in Figure 5.

$$Maximise \frac{QoSP}{n_{BP}} \qquad (1)$$

In sub section 5.2, higher value of QoSP influences lower chance of total packet lost, faster restoration time and lower bandwidth consumption. Further, overall network performance is higher. However, the larger numbers of branch point brings the higher restoration time. Also, the larger number of branch point affects the higher bandwidth consumption and larger number of PSL and PML nodes. Therefore, the fitness function tries to minimize number of branch point while tries to maximize the QoSP value.

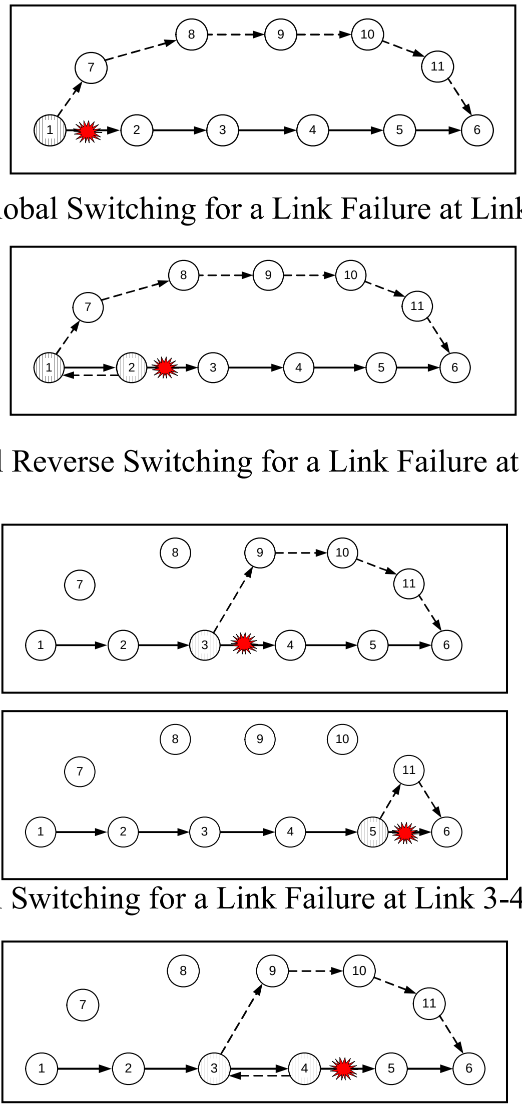
From the example network shown in Figure 4, we assume that node 3 and 5 are selected to be branch points by the GA optimization with $n_{MBP} = 2$. Branch paths {3-9}and {5-11} are then routed from the selected branch points to the nearest node along the global backup path. Further, reverse paths {2-1} and {4-3} are established from downstream nodes to the PSL nodes those are able to switch over to the global backup path. Note that, no reverse path is required at an upstream link to the branch point such link 3-2 and 5-4. The ingress (node 1) and branch point nodes (node 3 and 5) must be able to switchover and merge traffic, then, they must be both PSL and PML node. The egress node (node 6) requires only merging capability. Finally, the other nodes (node 2 and 5) are set to PSL node. Note that, for more efficiency, bandwidth of the backup paths can be utilized by lower priority traffics such as best effort service. For further research, higher order of GA optimization such as [17] can be employed in the study.

```
Procedure GA_Branch_Point_Optimization
  Inputs: A network graph $G(N,L,B)$, an ingress $N_I$ and an egress $N_E$ nodes, QoS routing
  algorithm $A_{RT}$, request bandwidth $B_R$, maximum numbers of branch points $n_{MBP}$ and Input
  Gene (branch_point$_1$, .., branch_point$_n$, number_of_branch_point)
  Outputs: result and Output Gene (branch_point$_1$, .., branch_point$_n$,
  number_of_branch_point)
  Procedures: {
  1. Remove links that bandwidth $B$ less than bandwidth request $B_R$
  2. If number_of_branch_point > $n_{MBP}$ then result = Infinite and exit procedure
  3. For generated branch_point = 1 to number_of_branch_point
      3.1 Establish branch_path from generated branch_point to a nearest node
          corresponding to the backup path
      3.2 Establish reverse path from generated branch_point upstream to $N_{PSL}$
     Next
  4. Let packet_loss = 0, restoration_time = 0, and bandwidth_consumption = 0
  5. For failure_chance = 1 to total hop of working path
     5.1. packet_loss = packet_loss + total packet loss calculated by Equation(10) .
     5.2. restoration_time = restoration_time + total restoration_time calculated by
          Equation(11)
     5.3. bandwidth_consumption = bandwidth_consumption + total
          bandwidth_consumption calculated by Equation(17)
     Next
  6. QosP = 1 –(packet_loss + restoration_time + bandwidth_consumption)
  7. result = QoSP / number_of_branch_point
  }
```

Figure 5. Details of branch point optimization function.

Hybrid Switching

According to hybrid backup mechanism, the HB model has four switching types which are global, global reverse, local and local reverse switching (see Figure 6). If a failure is detected at adjacent downstream link/node to the ingress node, global switching is activated (see Figure 6 (a)). If a failure is identified at adjacent downstream link/node to the PSL node that is the most upstream to the first branch point, global reverse switching is started (see Figure 6 (b)). If a failure is discovered at adjacent downstream link/node to the branch point, local switching is operated (see Figure 6 (c)). Lastly, if a failure is occurred at adjacent downstream link/node to the downstream PSL node from branch point, local reverse switching is activated. (see Figure 6 (d)). Note that, PSL/PML nodes are activated according to different switching types.



(a) Global Switching for a Link Failure at Link 1-2

(b) Global Reverse Switching for a Link Failure at Link 2-3

(c) Local Switching for a Link Failure at Link 3-4 and 4-5

(d) Local Reverse Switching for a Link Failure at Link 5-6

Figure 6. Examples for four hybrid switching types of HB model

Routing and Recovering Procedures

Here, details of the HB procedures are shown. The procedures could be divided into two phases: *Routing* and *Recovering phase*. We define *G(N,L,B)* as an input network graph composed of sets of node *N,* link *L*, and residual bandwidth *B*. N_I and N_E are denoted to an ingress node and egress nodes, respectively. According to routing phase (see Figure 7), a working, global backup, branch backup and reverse backup paths are defined. Also, PSL and PML functions are activated at corresponding nodes. We assume that there is only single element failure occurred in the mean time. Then in recovering phase (see Figure 8), traffic is switched based on four switching types described in the previous sub section. Note that, for simplicity, the routing phase is based on 1:1 dedicated restoration allocation. Then, the routing performance can further be improved for the shared restoration allocation. This is one of our research topics.

Performance Metrics

Performance metrics we considered are cost effectiveness, level of QoS protection based on the Diff-Serv model, and network performances which are described in following sub-sections.

```
Procedure HB_Routing_Phase
  Inputs: A network graph $G(N,L,B)$, an ingress $N_I$ and an egress $N_E$ nodes, QoS routing
  algorithm $A_{RT}$ , request bandwidth $B_R$ , branch_point$_1$, …, branch_point$_n$ and
  number_of_branch_point
  Outputs: Sets of working $P_{WK}$, global backup $P_{GB}$, branch backup $P_{BP}$ and reverse
  backup $P_{RB}$ paths.
  Procedures: {
  1. Remove links that $B<B_R$
  2. Route for a $P_{WK}$ from $N_I$ to $N_E$ based on $A_{RT}$.
  3. Set PSL+PML functions at $N_I$. Set PML function at $N_E$.  Set PSL function at all
  $N \in P_{WK}$ except $N_I$ and $N_E$.
  4. Remove $P_{WK}$ from $G(N,L,B)$.
  5. Route for a disjoint $P_{GB}$ from $N_I$ to $N_E$ based on $A_{RT}$.
  6. Run GA_Branch_Point_Optimization
  7. Route for branch backup $P_{BP}$ and reverse backup $P_{RB}$ paths based on $A_{RT}$.
  8. Establish $P_{WK}$, $P_{GB}$, $P_{BP}$ and $P_{RB}$
  }
```

Figure 7. Routing phase of HB model

```
Procedure **HB_Recovering_Phase**
  Input: A failure of node $N_F$ or link $L_F$
  Output: Recovery operation
  Procedures: {
  1. If the failure is identified by an $N_I$
       Global switching: switch traffic over $P_{GB}$
  2. If the failure is identified by a $N_{PSL}$ downstream to $N_I$ and upstream to the first branch point ($N_{PML}$)
       Global reverse switching: switch traffic upstream to $N_I$ and then $P_{GB}$
  3. If the failure is identified by a $N_{PML}$
       Local switching: switch traffic over $P_{BP}$ and subset of $P_{GB}$
  4. If the failure is identified by a $N_{PSL}$ downstream to the branch point
       Local reverse switching: switch traffic over upstream $N_{PML}$ and then subset of $P_{GB}$
  }
```

Figure 8. Recovering phase of HB model

Cost Effectiveness

According to cost effectiveness, there are four performance metrics related to the working path *w*: number of PSL nodes (n^w_{PSL}), PML nodes (n^w_{PML}), backup paths (or flows) (n^w_{BKP}), and labels used (n^w_{LBU}). Firstly, the higher number of n^w_{PSL} and n^w_{PML} brings higher implementation costs and complexity and also affects longer recovery operation time (T_{RO}) according to switching over and merging processes. Secondly, the higher number of backup paths, n^w_{BKP}, directly increases size of routing table and label matching space of particular nodes belonging to the working path *w* and the backup path *b*. Thirdly, because of limitation of label space related to type of switching infrastructure, number of labels used for traffic swapping over backup paths must be taken into consideration. Then, the minimal number of label used is preferred. Therefore, establishment of backup paths must take into account those four metrics, in order to minimizing cost of the backup model. Finally, n^w_{PSL}, n^w_{PML}, n^w_{BKP} and n^w_{LBU} could be simply obtained by Equation (2) ~ (5), respectively.

$$n^w_{PSL} = \sum N_i, \qquad i \in \left\{ N^w_{PSL} \right\} \tag{2}$$

$$n^w_{PML} = \sum N_i, \qquad i \in \left\{ N^w_{PML} \right\} \tag{3}$$

$$n^w_{BKP} = \sum P_i, \qquad i \in \left\{ P^w_{BKP} \right\} \tag{4}$$

$$n^w_{LBU} = \sum L_i, \qquad i \in \left\{ P^w_{BKP} \right\} \tag{5}$$

Where $\left\{ N^w_{PSL} \right\}$ is denoted to set of PSL nodes used along the working path *w*. $\left\{ N^w_{PML} \right\}$ is referred to set of PML nodes along the working path *w*. $\left\{ P^w_{BKP} \right\}$is designated to set of backup paths reserved for the working path *w*. And R^w_{TX} is denoted to the requested transmission rate of the working path *w* (bps)

Quality of Service Protection (QoSP) Level

When a failure is detected over the working path *w*, the Quality of Service Protection metric of the path (*QoSP_w*) is evaluated to signify guarantee level of each backup models. In Equation (6), $QoSP_w$ is function of *Packet Loss* (E^w_{PK}), *Restoration Time* (T^w_{RS}) and *Bandwidth (or Resource) Consumption* (B^w_C) measured during recovery operation. The α,

β, and λ (see Table 1) are weighted values defined based on the *Differentiated Services* (Diff-Serv) traffic characteristics [12]. For example, in the expedited forwarding (EF) traffic class, guaranteed QoS traffic strictly requires very low packet loss and delay time. Then, weighted value of packet loss (α), restoration time (β) and bandwidth consumption (λ) are set to 50%, 45% and 5%, respectively. According to performance comparison between difference models, corresponding normalized values of E_{PK}^{w}, T_{RS}^{w} and B_{C}^{w} should be obtained by dividing with their reference values ($E_{PK}^{w,REF}$, $T_{RS}^{w,REF}$ and $B_{C}^{w,REF}$). These reference values are determined by the maximum worst-case performance among all considered backup models (see Equation (7) ~ (9)). H_w is denoted to number of hop along the working path *w*. From Equation (5), the higher value of *QoSP* demonstrates better QoS protection (or guaranteed) level of backup model. Hence, the *QoSP* ranges from 0 (worst *QoSP* case) to 1 (best *QoSP* case).

$$\begin{aligned} QoSP_w &= f\left(E_{PK}^{w}, T_{RS}^{w}, B_{C}^{w}\right) \\ &= 1 - \left\{ \alpha \times \left(\frac{E_{PK}^{w}}{E_{PK}^{w,REF}}\right)^{H_w} + \beta \times \left(\frac{T_{RS}^{w}}{T_{RS}^{w,REF}}\right)^{H_w} \right. \\ &\quad \left. + \lambda \times \left(\frac{B_{C}^{w}}{B_{C}^{w,REF}}\right)^{H_w} \right\} \end{aligned} \tag{6}$$

$$\begin{aligned} E_{PK}^{w,REF} &= \max\left(E_{PK}^{w,ALL}\right) \\ &= \max\left(E_{PK}^{w,GB}, E_{PK}^{w,RB}, E_{PK}^{w,LLB}, E_{PK}^{w,ELB}, E_{PK}^{w,BHB}\right) \end{aligned} \tag{7}$$

$$\begin{aligned} T_{RS}^{w,REF} &= \max\left(T_{RS}^{w,ALL}\right) \\ &= \max\left(T_{RS}^{w,GB}, T_{RS}^{w,RB}, T_{RS}^{w,LLB}, T_{RS}^{w,ELB}, T_{RS}^{w,BHB}\right) \end{aligned} \tag{8}$$

$$\begin{aligned} B_{C}^{w,REF} &= \max\left(B_{C}^{w,ALL}\right) \\ &= \max\left(B_{C}^{w,GB}, B_{C}^{w,RB}, B_{C}^{w,LLB}, B_{C}^{w,ELB}, B_{C}^{w,BHB}\right) \end{aligned} \tag{9}$$

Table 1: Diff-Serv QoS Protection Requirements and Assignments of α, β, and λ values.

Traffic Class	QoS Requirements	α	β	λ
Expedited Forwarding (EF)	Very Low Packet Loss and Restoration Time	0.5	0.45	0.05
Assured Forwarding 1 (AF1)	Very Low Packet Loss	0.5	0.3	0.2
Assured Forwarding 2 (AF2)	Low Packet Loss	0.33	0.33	0.33
Best Effort (BE)	No requirements	0.05	0.05	0.9

Generally, the packet loss can be defined by numbers of discarded packet during the time before recovery process starts (the time during fault detection (T_{FD}), fault hold-off (T_{FH}) and fault notification time (T_{FN})). It is a product of transmission rate (R_{TX}) multiply by the time ahead of recovery process starts (T_{FD}+T_{FH}+T_{FN}) and then divided by the packet size (S_{PK}) (see Equation (10)). Therefore, longer duration of fault detection and notification brings higher numbers of lost packets.

$$E_{PK} = \frac{R_{TX} \times (T_{FD} + T_{FH} + T_{FN})}{S_{PK}} \qquad (10)$$

$$T_{RS}^{w} = T_{FD}^{w} + T_{FH}^{w} + T_{FN}^{w} + T_{RO}^{w} + T_{TR}^{w} \qquad (11)$$

$$T_{FD}^{w} = [0, T_{LMI}] \qquad (12)$$

$$T_{FH}^{w} = T_{LLD} \qquad (13)$$

$$T_{FN}^{w} = \sum T_{D}^{p} \ , \quad p \in \{P_{FIS}\} \qquad (14)$$

$$T_{RO}^{w} = \left(T_{SWO} \times n_{PSL}^{w}\right) + \left(T_{MGO} \times n_{PML}^{w}\right) \qquad (15)$$

$$T_{TR}^{w} = \sum T_{D}^{p} \ , \quad p \in \{P_{RCO}\} \qquad (16)$$

$$B_{C}^{w} = R_{TX}^{w} \times T_{TR}^{w} \qquad (17)$$

The second term of Equation (6), restoration time, is defined as total delay during the MPLS recovery cycle. Therefore, from the section 2.3, restoration time is a total time between T_{FD}, T_{FH}, T_{FN}, T_{RO} and T_{TR} (see Equation (11)). The fault detection time, T_{FD}, ranges from 0 to Liveness Message (LM) interarrival time (T_{LMI}) which is at least 2 times of the propagation delay over detected adjacent node (see Equation (12)). The fault hold-off time, T_{HO}, could be set to delay of the lower layer protocol (T_{LLD}) before activation data transmission provided by the higher layer protocol, see Equation (13). This value can be neglected because of its small value comparing to other duration. The fault notification time (T_{FN}) depends on propagation time of an FIS to upstream PSL node (see Equation (14)). The recovery operation time, T_{RO}, is time during switchover and merging operation of PSL and PML nodes currently activated by the recovery operation (see Equation (15)). The traffic recovery time, T_{TR}, is duration of transmitting recovered traffic transmitted until it reaches the egress node once again (see Equation (16)). Other analysis of the restoration time could be obtained in [12], [13], and [14]. Finally, the bandwidth consumption (B_C) is evaluated by amount of bandwidth utilized over the activated recovery path (see Equation (17)).

Overall Network Performances

Here, three network performance metrics are evaluated which are bandwidth reserved (B_{RSV}), rejection probability (ρ_{REJ}), and total throughput (B_{TH}). Bandwidth reserved is evaluated by summation of transmission rate of backup path multiply by total number of links of the backup paths (see Equation (18)). In Equation (19), rejection probability is calculated by total number of call rejected divided by total number of call requested. Lastly, from Equation (20), total throughput is determined by summation of transmission rate of all successful established working paths.

$$B_{RSV} = \sum \left(R_{TX}^{b} \times \sum L_{b} \right) \quad , \; b \in \left\{ P_{BKP} \right\} \tag{18}$$

$$\rho_{REJ} = \frac{\sum Call_{REJ}}{\sum Call_{REQ}} \tag{19}$$

$$B_{TH} = \sum R_{TX}^{w} \qquad , \; w \in \left\{ P_{WK} \right\} \tag{20}$$

Numerical Models and Results

We have developed extensive MATLAB 7.0 simulator [18] in order to evaluating performance of the HB model. Moreover, for scalability issue, we also repeat performance evaluation over two experimental networks.

Numerical Models

Two experimental networks are chosen for performance evaluation described in previous sub-sections. The first network is shown in Figure 9. It composes of 15 nodes and 28 links. It has ten edge nodes which are node 1, 2, 4, 5, 8, 9, 12, 13, 14 and 15. The second network composes of 30 nodes and 56 links (see Figure 10). It also has ten edge nodes which are node 1, 2, 3, 4, 5, 6, 7, 8, 9 and 10. Although, both networks are different in size, but they have the same link characteristics and traffic parameters. According to link characteristics, all links are bi-directional. Capacity of links are 100 Mbps. Distance of all links is 100 km. Then, propagation delay of all links is 500 μs (100 km × 5 μs/km which is propagation velocity over single mode fiber). Average size of packets is set to 1024 bits. Fault detection or Liveness Message interarrival time is set to round-trip propagation time of link or 1000 μs (500 μs × 2). Lastly, fault hold-off time, switchover and merging delay are equally set to 1 μs. Size of traffic requests are 1-5 Mbps varied by uniformly distribution. For more accuracy, we use the same orders of traffic requests to test on different backup models including the HB model. Ingress and egress nodes (or source-destination node pairs) of each traffic request are also populated by uniformly distribution. QoS Routing algorithm A_{RT} is Widest Shortest Path (WSP) [16], which select a shortest path with the highest residual bandwidth. Note that, other exist QoS routing algorithms related to Diff-Serv model could be used to improve the routing performance. With GA parameters, we set GAOPTIMSET: ‘generations' = 100, 'PopulationSize' = 20 and 'StallGenLimit' = 50. And we left other parameters at default value. Finally, maximum number of branch point is set to 2.

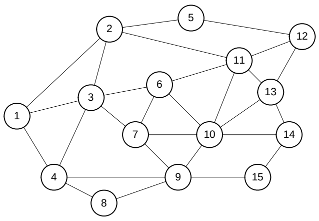


Figure 9. Example experimental network with 15 nodes

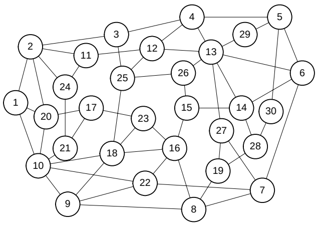


Figure 10. Example experimental network with 30 nodes

Table 2: **Comparison of Cost Effectiveness Parameters.**

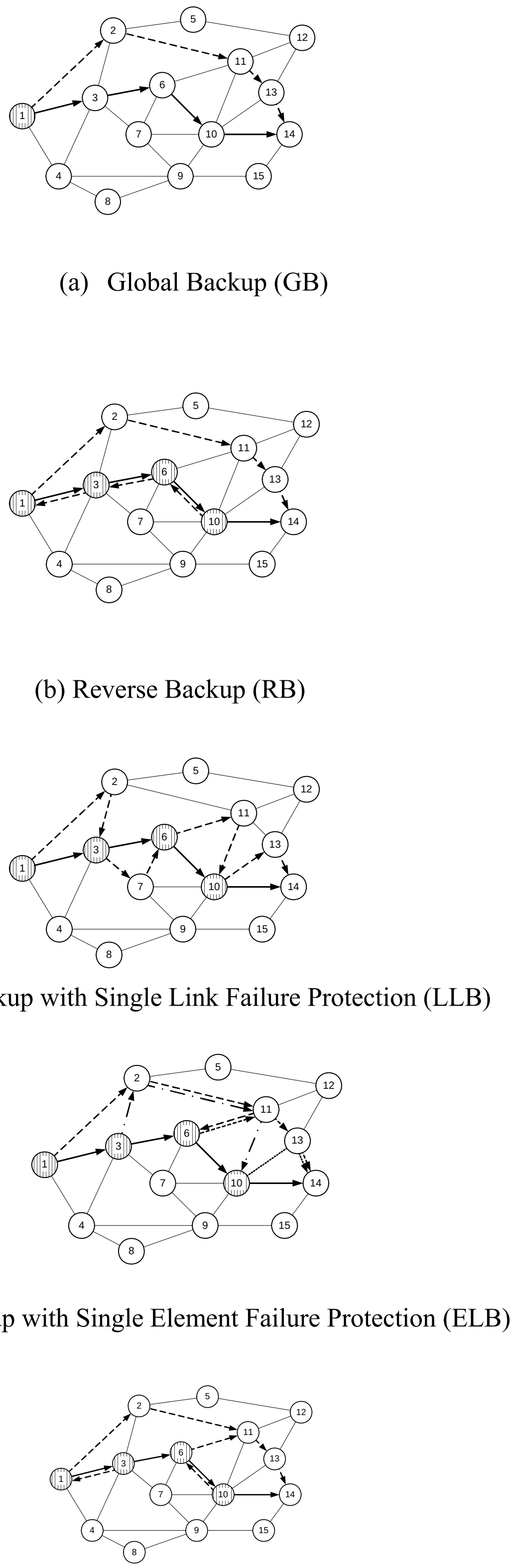
	n^{w}_{PSL}	n^{w}_{PML}	n^{w}_{BKP}	Backup Path List	n^{w}_{LBU}
GB	1	1	1	{1-2-11-13-14}	4
RB	4	2	2	{1-2-11-13-14}, {10-6-3-1}	7
LLB	4	4	4	{1-2-3}, {3-7-6}, {6-11-10}, {10-13-14}	8
ELB	4	3	4	{1-2-11-6}, {3-2-11-10}, {6-11-13-14}, {10-13-14}	11
HB	4	2	4	{1-2-11-13-14}, {3-1}, {6-11}, {10-6}	7

Numerical Results

CASE 1: Cost Effectiveness

Evaluating cost effectiveness, we choose node 1 and 14 to be ingress (source) and egress (destination) nodes, respectively.

Figure13 shows results of working and backup path based on five backup models: GB, RB, LLB, ELB and HB. According to the same routing algorithm, all backup models have a same working path {1-3-6-10-14}. However, backup paths of each backup model are different. Further, cost effective parameters are determined and shown in



(a) Global Backup (GB)

(b) Reverse Backup (RB)

(c) Local Backup with Single Link Failure Protection (LLB)

(d) Local Backup with Single Element Failure Protection (ELB)

(e) Hybrid Backup (HB)

Figure 11. Example for working and backup paths with N_I=1 and N_E =14

From the table, GB has the minimum cost of only one PSL, one PML, one backup path and four label used for backup path. Note that, label is determined by total hop of the backup path. Although, GB is the cheapest model, it suffers from high level of packet losses and restoration delay. This disadvantage will be discussed later in next experimental case. Further, both LB models have the highest cost. Because LLB has the highest number of PSL, PML and backup path, and ELB has the highest number of label used. In RB model, the cost effectiveness is considered in medium level.

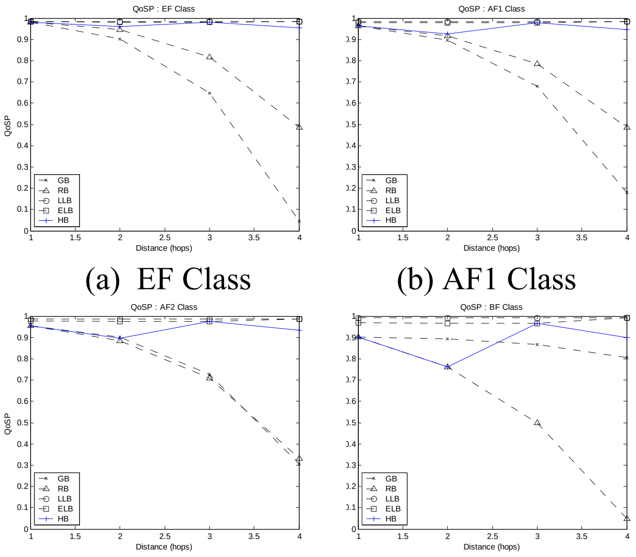
Comparing to both LB models, HB can reduce cost of number PML and label used. This implies that HB model can reduces implementation cost, while it still maintains level of QoS protection in case of fast restoration and low packet losses.

CASE 2: QoSP vs Point of Failure Detection

Based on CASE 1, QoSP value is determined by varying of point of failure detection from the 1st node (node 1) to the 4th node (node 10) of the working path. Transmission rate is set to 1 Mbps.

Figure12 illustrates QoSP of four Diff-Serv traffic classes related toα,β and λ values. As mention in the Section 5, high QoSP value is required. Because of FIS transmission delay, the longer point of failure detection highly increases restoration time and then degrades QOSP level of GB and RB (see Figure12 (a)-(c)).

While, point of failure detection rarely impacts on QoSP of both LLB and ELB, the result shows that with HB, QoSP is a little lower than LLB and ELB. This shows that the HB model has almost high QoS guaranteed level as equal as both LLB and ELB model. In Figure12 (d), because of best effort class, restoration time and packet losses are less important. Therefore, the RB model has the worst QoSP, because of high bandwidth consumption.



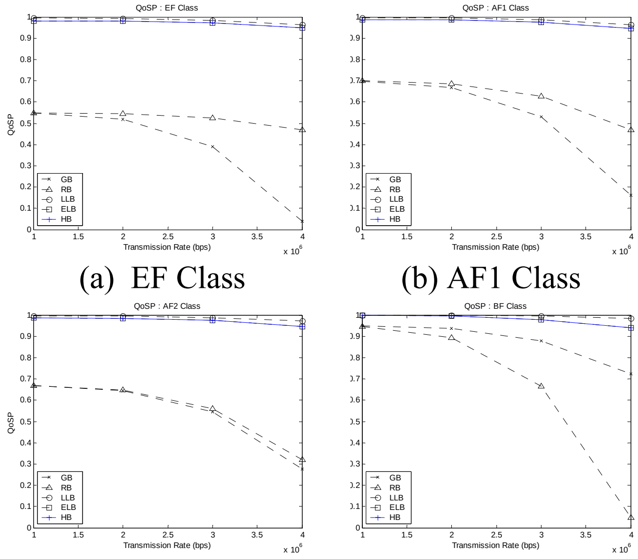
(a) EF Class (b) AF1 Class

(c) AF2 Class (d) BE Class

Figure 12. QoSP vs point of failure detection

CASE 3: QoSP vs Transmission Rate

Also, based on CASE 1, QoSP value is reevaluated by varying of input transmission rate from 1 to 4 Mbps. Point of Failure is fixed to the 3rd node (node 6) of the working path. Again, From Figure13, the HB model has high QoSP level and a little lower than LLB and ELB models. Further, because of high restoration delay of GB and RB models, QoSP level of GB and RB models are obviously lower than LLB, ELB and HB models (see Figure 13 (a)-(c)). Lastly, from Figure 13 (d), the RB model again has the lowest QoSP level because it consumes the maximum bandwidth due to the failure.



(a) EF Class (b) AF1 Class

(c) AF2 Class **(d) BE Class**

Figure 13. QoSP vs transmission rate

CASE 4: Network Performances of 15-Nodes Network

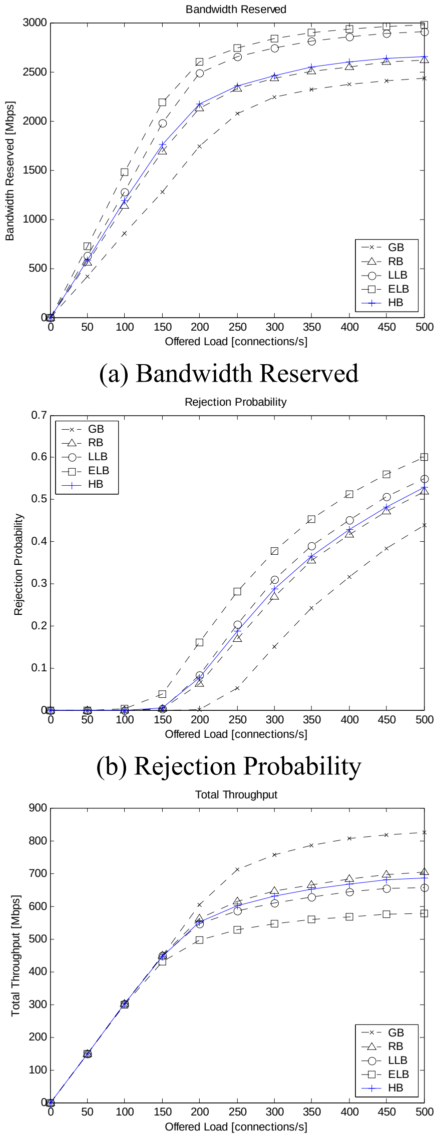
Here, overall network performances of the15-nodes network are evaluated by simulation. Input traffic is varied from 0 to 500 connections per second. As mention in sub-section 6.1, size of traffic requests are 1-5 Mbps varied by uniformly distribution. For more precise result, we repeat ten time simulation and show the averaged result. Figure 14(a) shows that the GB model reserves the minimum bandwidth. The RB and HB reserve the medium bandwidth, and the LLB and ELB reserve the highest bandwidth. The more bandwidth reserved brings the more chances for a future traffic to be rejected. Then, in Figure 14 (b), the GB model is the best model in case of rejection probability and the ELB model is the worst. Furthermore, the less rejection probability leads to high total throughput. Then, in Figure 14 (c), the GB model is again the best model in case of total throughput.

Although the GB model is the best backup model in case of the lowest bandwidth reserved, the lowest blocking chance, and the highest total throughput. It is still considered to be not suitable for QoS guaranteed traffic since this model has low QoSP level according to high packet losses and restoration time.

With RB model, all three network performances are in the medium level. However, because of its high restoration time, the RB model is only suite for the QoS traffic that guarantees only low packet losses such as AF1, AF2 and BE classes.

In LLB model, the model achieves high QoSP level and suites to apply to EF traffic. However, bandwidth reserved is high. This is resulted in high rejection probability and low total throughput. Moreover, it has high cost and can be used to protect only link failure type.

Also, the ELB model reaches high QoSP level as same as the LLB model. This model can be applied to both link and element failure protections. However, it has the highest cost and the lowest network performances.



(a) Bandwidth Reserved

(b) Rejection Probability

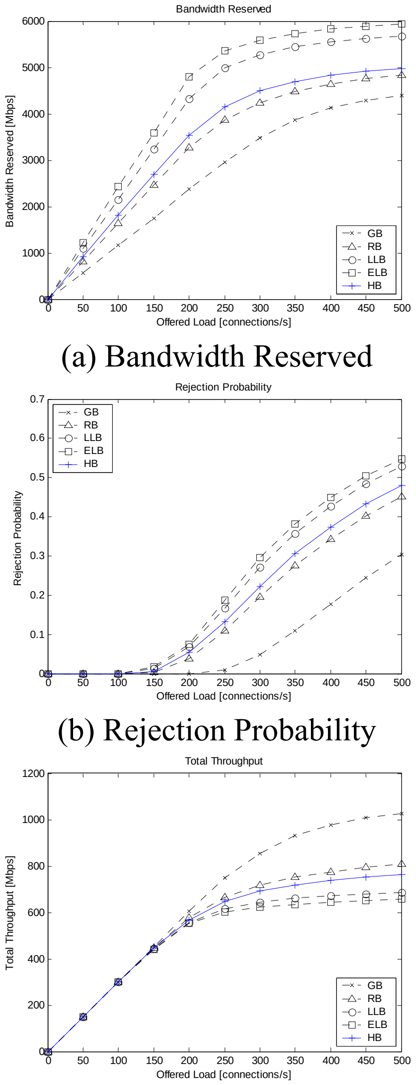
(c) Total Throughput

Figure 14. Network performances of 15-Nodes network

Clearly, HB model has high QoSP level as same as the LLB and ELB models. Then, it is suite for EF traffic. Besides, both link and element failures can be protected by the backup model. In case of cost and overall performance, the model is in the medium level. So, the HB model is the best choice for time-critical traffics.

CASE 5: Network Performances of 30-Nodes Network

According to scalability issue, overall network performances are retested by the 30-nodes network. From Figure 15., the HB can maintain the medium level. In addition, network performances of the LLB model become more a few worse than in the 15-nodes network.



(a) Bandwidth Reserved

(b) Rejection Probability

(c) Total Throughput

Figure 15. Network performances of 30-nodes network

Conclusions

In this paper, we present an approach for enhancing current MPLS resilience, called Hybrid Backup model (HB). Currently, there are three exist MPLS backup models: global, reverse and local backup models. Firstly, the global backup model is the cheapest model but it suffers from high packet losses and long restoration time. Secondly, the reverse backup improves the packet loss problem; however, the delay problem is still remaining. Thirdly, the local backup method is seemed to be the best choice in case of the minimum restoration time and packet losses, nevertheless, it has high cost in terms of number of path switch label switching router (PSL), path merge label switching router (PML), label usage, and bandwidth reserved. Therefore, we proposed a new approach based on hybrid of four switching types which are global, global reverse, local and local reverse switching types. Furthermore, branch point optimization based on Genetic algorithm is proposed. The proposed model can reduce the cost of the local backup model, while it still maintains fast restoration and low packet losses. Furthermore, it can improve some significant network performances such as bandwidth reserved, rejection probability, and total throughput. According to performance comparison between all backup models, numerical and simulation results are presented to support the proposed model.

Further research interests focus among other optimization model and improvement of routing algorithm for shared resource allocation model.

References

[1] E. Rosen, A. Viswanathan, and R. Callon, *Multiprotocol Label Switching Architecture,* RFC Multiprotocol Label Switching Architecture, 2001.

[2] E. Mannie, ed., *Generalized Multi-Protocol Label Switching (GMPLS) Architecture*, RFC 3945, 2004.

[3] M. Kodialam, and T.V. Lakshman, "Dynamic routing of locally restorable band-width guaranteed tunnels using aggregated link usage information," In: *Proceedings IEEE INFOCOM 2001: The Conference on Computers Communications-20th Annual Joint Conference of the IEEE Computer and Communications Society*, 2001.

[4] V. Shama, and F. Hellstrand, *Framework for Multiprotocol Label Switching (MPLS)-based Recovery*, RFC3469, 2003.

[5] F. Le Facheur, ed., *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*, RFC3564, 2003.

[6] O. Banimelhem, J. W. Atwood, and A. Agawal, "Resiliency issues in MPLS networks," In: *CCECE 2003-Canadian Conference on Electrical and Computer Engineering: Toward a Caring and Humane Technology*, Vol. 2, pp. 1039-1042, 2003.

[7] T.M. Chen, and T.H. Oh, "Reliable services in MPLS," *IEEE Communication Magazine*, Vol. 37, No. 12, 1999.

[8] J.L. Marzo, E. Calle, C. Scoglio, and T. Anjaili, "QoS online routing and MPLS multilevel protection: A survey," *IEEE Communication Magazines*, Vol. 41, 2003

[9] A. Agarwal, and R. Deshmukh, "Ingress failure recovery mechanisms in MPLS network," In: *MILCOM 2002 Proceddings*, Vol. 2, pp. 1039-1042, 2002.

[10] M. Yu, and B. Xie, "An analytical availability model for MPLS networks with end-to-end IP resilience," In: *2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM2003),* Vol. 2, pp. 820-823, 2003.

[11] E. Calle, T. Jove, P. Vila, and L. Marzo, "A dynamic multilevel MPLS protection domain," *Third International Workshop on Design of Reliable Communication Networks*, DRCN, Budapest, Hungary, 2001.

[12] J.L. Marzo, E. Calle, C. Scoglio, and T. Anjaili, "Adding QoS protection in order to enhancing MPLS QoS routing," In: *IEEE International Conference on Communications 2003* (*ICC'2003)*, Vol. 3, pp. 1973-1977, 2003.

[13] A. Autenrieth, "Recovery time analysis of differentated resilience in MPLS," *Fourth International Workshop on Design of Reliable Communication Networks'2003* (DRCN'2003), 2003.

[14] E. Calle, J. L. Marzo, A. Urra, and P. Vila, "Enhancing MPLS QoS routing algorithms by using the network protection degree paradigm," In: *Global Telecommunications Conference 2003*, Vol. 6, pp. 3053-3057, 2003.

[15] W. Sa-Ngiamsak, and R. Varakulsiripunth, "Local reverse backup and resiliency buffer approaches for MPLS-based recovery," *IEEE Region 10 Conference TENCON 2004*, Vol. 2, pp. 3053-3057, 2004.

[16] R. Guerin, D. Williams, and A. Orda,"QoS Routing Mechanisms and OSPF Extensions," In: *IEEE Global Telecommunications Conference-Globecom'97*, Vol. 3, pp. 1903-1908, 1997.

[17] P. Lacommea, C. Prinsb, and M. Sevauxc, "A genetic algorithm for a bi-objective capacitated arc routing problem," *Computers & Operations Research*, Vol. 33, No. 12, pp. 3473-3493, 2005.

[18] "*Mathtools.net: MATLAB/Genetic algorithms*" (n.d.) [Online]. Avaliable: http://www.mathtools.net/MATLAB/Genetic_algorithm [Accessed: January 2011]