Hybrid FRR/p-Cycle MPLS Link Protection Design

Chang Cao[†], George N. Rouskas[††]

[†]Key Laboratory of Information Photonics and Optical Communications, BUPT, Beijing 100876, China

[††]Department of Computer Science, North Carolina State University, Raleigh, NC 27695-8206 USA

***Abstract*—Survivable MPLS technologies are crucial in ensuring reliable communication services. The fast reroute (FRR) mechanism has been standardized to achieve fast local repair of label switched paths (LSPs). We present a hybrid survivability scheme for MPLS networks that combines the well-known p-cycle method with FRR technology. While with pure FRR backup paths are planned individually for each link, the hybrid scheme selects backup paths embedded within a set of p-cycles that may be selected by taking a holistic view of network performance. The hybrid FRR/p-cycle method is fully RFC 4090-compliant, yet allows network operators to leverage a large existing body of p-cycle design techniques.**

I. Introduction

Multi-protocol label switching (MPLS) [1], originally developed to enable fast packet forwarding, has also facilitated traffic engineering, quality-of-service (QoS) routing, and differentiated services support in IP-based metro and backbone networks [2]. MPLS technology is widely deployed and is crucial to the operation of the Internet and its ability to support critical communication services efficiently. Consequently, MPLS survivability mechanisms [3] are key to ensuring that the network may continue to provide reliable services even in the presence of failures. In particular, with today's multilayer network architectures, it may be more economical for IP/MPLS layer operators to restore traffic within their own IP/MPLS logical environment rather than relying on physical layer restorability [4]–[6].

The IETF has standardized the fast reroute (FRR) mechanism [7] for protecting label switched paths (LSPs) in MPLS networks. FRR calls for local repair actions in the event of a link failure. Specifically, the two nodes adjacent to the failure are responsible for re-directing traffic onto pre-configured backup tunnels. As a result, all affected LSPs are rerouted over the same backup path within a few tens of milliseconds.

The p-cycle scheme [8] also employs local repair actions to re-direct traffic from the failed link onto a backup path along a pre-configured cycle. This method provides ring-like protection speeds with mesh (span-restorable) capacity efficiency, hence it has been studied extensively (for a survey of related work, see [9]). Although originally designed for protection in the optical layer, p-cycle technology can be applied to the IP [10] or MPLS [11] layers. It was shown in [10] that p-cycle design in packet-switched networks can be as capacity-efficient as optimized span restoration. Another study [11] presented mixed integer program (MIP) formulations for p-cycle design in MPLS networks, and investigated the relationship between protection bandwidth requirements and traffic load distribution.

The motivation for our work is based on the observation that both FRR and p-cycle are link-based (local repair) protection schemes, hence we expect the network operation, delay, and overhead incurred for failure detection, notification, and triggering of restoration action to be similar for the two technologies. However, FRR backup tunnels are typically planned individually for each link that needs to be protected, whereas p-cycle design takes a more holistic view of the network in determining the protection cycles. Therefore, we propose a hybrid technique that is fully compliant with the FRR standard but uses backup tunnels embedded within a set of pre-selected p-cycles.

In Section II we briefly review the operation of MPLS link protection and describe how to combine the p-cycle method with FRR. In Section III we present three performance metrics to compare the pure FRR and hybrid schemes. We present numerical results in Section IV, and we conclude the paper in Section V.

II. MPLS Link Protection

Consider a (directed) link in an MPLS network, e.g., the link $A \rightarrow B$ in the 5-node network shown in Figure 1. In FRR parlance, the upstream router A is referred to as the "point of local repair" (PLR) with respect to protecting traffic in the event that the link fail. The downstream router B is the next hop (NHop) router, also referred to as the "merge point" (MP). Link protection in MPLS consists of three steps [7]:

1) **Planning.** The key idea in FRR is to find, for each protected link and before any failure takes place, a backup path from the PLR node to the MP node. Referring to Fig. 1, the path $A \rightarrow E \rightarrow B$ is selected to protect link $A \rightarrow B$. Upon a link failure, all traffic on the failed link (regardless of the origin or destination of the corresponding working LSPs) is re-directed to this backup path.
2) **Backup LSP signaling.** Backup LSPs are established along the backup paths using the same signaling mechanisms (e.g., RSVP-TE) as for setting up working LSPs. Hence, the backup LSPs are *pre-configured*, i.e., exist as entries in the forwarding tables of the routers along the corresponding backup paths. Although backup LSPs do not carry traffic under normal conditions, they are ready to accept traffic re-directed from failed working LSPs.

Chang Cao was supported by 973 Program (2010CB328204), 863 program (2009AA01Z255), NSFC project (60932004), RFDP Project (20090005110013) and 111 Project (B07005) of China.

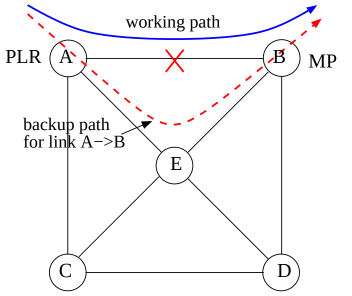


Fig. 1. Link protection with pure FRR

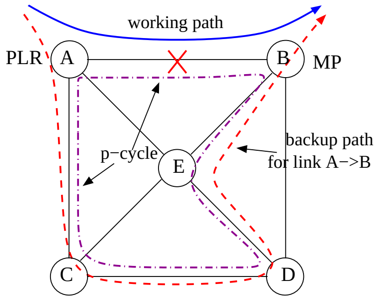


Fig. 2. Hybrid FRR/p-cycle link protection

3) **Local repair.** When a link (e.g., link $A \rightarrow B$ in Fig. 1) fails, the MP node B detects that it cannot receive any packets from its interface that connects to the PLR A. The MP node B then sends a failure message to A through another route, and both routers mark the ports that terminate the failed link as dead. From that instant, and until a global routing update takes effect, any packets that would have been forwarded along the failed link, are instead re-directed by PLR A onto the backup path, shown as the dotted line in Fig. 1, using a pre-configured backup LSP. Once the packets arrive at the MP node B over the backup LSP, they are forwarded towards their destination as if they had arrived over the working LSP.

Note that the second (signaling) and third (local repair) steps of this process must conform to the relevant MPLS standards, especially RFC 4090 [7]. However, the first step (planning) is outside the purview of standards, and network operators are free to employ customized algorithms to select a backup path for each protected link. It is in this step that we believe p-cycle design may provide benefits, as we discuss shortly.

A. Pure FRR

In pure FRR, the backup path for each protected link is selected by the PLR of that link, typically using a constraint-based shortest path first (CSPF) algorithm [7, Section 6.2]. For instance, in Fig. 1, PLR A selects the shortest (2-hop) path $A \rightarrow E \rightarrow B$ to protect link $A \rightarrow B$. Since the PLR of a protected link executes the CSPF algorithm independently of other routers, it makes a locally optimal decision. However, these locally optimal backup paths may not constitute a globally optimal solution, i.e., one that optimizes a network-wide objective such as backup resource cost and/or utilization. Since the planning step may take place *offline*, it is possible to employ a more sophisticated design methodology that takes a more holistic view of network performance and cost in selecting backup paths. Although such an approach would be more computationally intensive than the execution of a CSPF algorithm at each PLR, the fact that it can be performed offline means that the operation of the MPLS network need not be affected. In the next subsection we describe how to apply such a backup capacity design based on the p-cycle concept.

B. Hybrid FRR/p-Cycle Design

With the p-cycle scheme, a set of cycles are defined over the whole network such that each link is either an on-cycle link or a straddling link (i.e., a link that connects two nodes on the same cycle but is not itself part of the cycle). Fig. 2 shows a single, Hamiltonian p-cycle, $A-C-D-E-B-A$, that can be used to protect all links of the network. Note that, in the context of MPLS networks, a p-cycle is a *logical* entity, and its purpose is simply to define the backup path for each link that it protects. Consider again the link $A \rightarrow B$ in the above figure, which happens to be an on-cycle link for this p-cycle. The backup path for this link is the path from A to B along the counter-clockwise direction on the p-cycle, as illustrated in the figure. Similarly, all on-cycle links are backed up by the (unique) reverse path to their MP node. On the other hand, there are two potential backup paths for each straddling link (e.g., link $A \rightarrow E$), one along each direction around the p-cycle. Operators may use one of these two paths (e.g., the shortest one), or both.

We emphasize that the p-cycle design is simply an alternative way of carrying out the planning step of the link protection process. Once the set of p-cycles has been selected, the other two steps (signaling of backup LSPs and local repair) take place exactly as the standard [7] specifies. Hence, by adopting such an approach, network operators may capitalize on a large body of p-cycle design techniques (e.g., refer to [9] and references therein) to optimize the selection of p-cycles (and, hence, backup paths) for a wide range of performance objectives.

III. Performance Metrics and Analysis

We now discuss three performance metrics to evaluate the relative merits of the pure FRR and hybrid FRR/p-cycle schemes. Our objective is to protect all the links in the network considering a single-link failure scenario. For the pure FRR scheme, we assume that the backup path of each link is given; while for the hybrid scheme we assume that the p-cycle set is given and that each straddling link is protected by sending its traffic along the two backup paths around the p-cycle. Unless we explicitly specify otherwise, whenever we refer to a link l we assume that the link is directed.

A. B/W Ratio

By setting up bandwidth-guaranteed backup LSPs, it is possible for the MPLS network to provide fast restoration with bandwidth guarantees to all working LSPs. The B/W ratio, i.e., the ratio of the total backup capacity B required to protect all working capacity W, clearly depends on the design and planning of the backup paths. This ratio is an important metric we will use to compare the pure FRR and hybrid FRR/p-cycle designs.

Given the routing and amount of traffic carried by each working LSP, it is straightforward to compute the total working traffic W_l carried by any link l (note that the routing of working LSPs is independent of how backup LSPs are selected). Therefore, the total working capacity in the network is $W = \sum_l W_l$.

1) Backup Capacity for Pure FRR: In pure FRR, an amount of backup capacity equal to W_l must be provisioned along each link of the backup path for link l. Note, however, that under the single-link failure scenario we consider, if an amount of backup bandwidth $B_{l'} \geq W_l$ has already been provisioned on a link l' along the backup path for l, then no additional bandwidth needs to be allocated on l' for protecting link l. Based on this observation, we assign backup capacity using the following steps:

1) Label the L (directed) links in the network in decreasing order of the working traffic they carry, i.e., such that $W_1 \geq W_2 \geq \ldots \geq W_L$. Initialize the backup capacity of all links to zero: $B_l \leftarrow 0,\ \forall\ l$. Set $l \leftarrow 1$.
2) Let p_l be the backup path for link l. Assign backup capacity of each link l' of p_l: $B_{l'} \leftarrow \max\{B_{l'}, W_l\}$.
3) Set $l \leftarrow l + 1$. If $l \leq L$, repeat from Step 2; otherwise, stop.

Finally, the total backup capacity for FRR is:

$$B_{frr} = \sum_{l=1}^{L} B_l. \tag{1}$$

2) Backup Capacity for Hybrid FRR/p-Cycle: Let us assume that $C, C \geq 1$, p-cycles have been configured for protecting the network links. Note that, if a link l is a straddling link in some p-cycle c, then an amount of backup capacity equal to $W_l/2$ on the on-cycle links (in both directions) is sufficient to protect this link. On the other hand, if a link l is an on-cycle link, then W_l units of backup capacity need to be provisioned on all other links of the p-cycle *in the opposite direction*. However, if a link is an on-cycle link of k different p-cycles, each p-cycle needs to provision only W_l/k units of backup capacity. Let k_l denote the number of cycles for which link l is an on-cycle link. Also, let $\mathcal{L}_c^{cw}$ (respectively, $\mathcal{L}_c^{ccw}$) denote the set of clockwise (respectively, counter-clockwise) links of p-cycle c, and $\mathcal{L}_c^{str}$ denote the set of straddling links of p-cycle c. Based on these observations, the backup capacity for the clockwise on-cycle links of p-cycle c is given by:

$$B_l = \max\left\{ \max_{l' \in \mathcal{L}_c^{ccw}} \left\{ \frac{W_{l'}}{k_{l'}} \right\}, \max_{l' \in \mathcal{L}_c^{str}} \left\{ \frac{W_{l'}}{2} \right\} \right\},\ l \in \mathcal{L}_c^{cw}. \tag{2}$$

A similar expression can be written for the backup capacity of counter-clockwise links, while straddling links need no backup capacity. Consequently, the total backup capacity for hybrid FRR/p-cycle can be computed as:

$$B_{hfrr} = \sum_{c=1}^{C} \left(\sum_{l \in \mathcal{L}_c^{cw} \cup \mathcal{L}_c^{ccw}} B_l \right). \tag{3}$$

B. Traffic Weighted Backup Hop Cost

When a link fails, all traffic on the link is re-directed along the backup path for the link, incurring additional delay that depends on the length of the backup path. Let d_l denote the length (in hops) of path p_l that serves as the backup path of link l. If link l, carrying an amount W_l of working traffic, fails, the traffic weighted backup hop cost incurred by link l LSPs is given by: $H_l = W_l \times d_l$.

Assuming that all L links are equally likely to fail, the average traffic weighted backup hop cost for pure FRR can be written as:

$$\overline{H}_{frr} = \frac{\sum_{l=1}^{L} H_l}{L} \tag{4}$$

For the hybrid scheme, again assume that C p-cycles have been configured, and let $d_c \geq 3$ denote the length (i.e., number of directed on-cycle links) of p-cycle $c, c = 1, \ldots, C$. If link l is an on-cycle link for k_l p-cycles, the traffic weighted backup hop cost for this link is:

$$H_l = \sum_{j=1}^{k_l} \frac{W_l}{k_l} \times (d_j - 1). \tag{5}$$

For a link l that is a straddling link on p-cycle c, let d_c^s and d_c^l denote the length of the short and long backup paths, respectively, for the link along the p-cycle, i.e., such that $d_c^s \leq d_c^l$ and $d_c^s + d_c^l = d_c$. We send as much working traffic W_l^s as possible on the short backup path, i.e., $W_l^s = \min\{W_l, B_c\}$, where B_c is the spare capacity on the on-cycle links of the p-cycle, and the remaining traffic, $W_l^l = W_l - W_l^s$, if any, on the long backup path. Hence, the weighted cost is:

$$H_l = W_l^s \times d_c^s + W_l^l \times d_c^l. \tag{6}$$

Finally, the average traffic weighted backup hop cost for the hybrid scheme can also be obtained using expression (4).

C. Label Entry Overhead

The number of labels required to establish backup paths is an important metric for MPLS networks, as it determines the size of the forwarding tables at the LSRs. We assume that the *facility backup* method [7] is used to implement the local repair technique. This method takes advantage of the MPLS label stack and minimizes the use of labels for protection. For pure FRR, a link l is protected by creating a bypass tunnel from the PLR node to the MP node along the selected backup path. If link l fails, all traffic on the link is sent along the bypass tunnel by having the PLR node *push* the appropriate label on each affected packet and having the MP node *pop* that label and continue to forward the packet based on the original label. Therefore, the number of additional labels required to protect a link l is equal to the number of hops along its backup path.

For the hybrid FRR/p-cycle scheme, we use the same method. Specifically, the PLR pushes a new label and forwards traffic affected by the failure along the appropriate p-cycle, while the MP node (the only other node that is aware of the failure) pops this label and continues with regular forwarding. Therefore, for each p-cycle in the p-cycle set used to protect the network links, the number of labels required is twice the number of links in the p-cycle; i.e., one set of labels for each direction along the p-cycle. This arrangement is possible because each node on the p-cycle may *reuse* the same set of labels to accommodate *any* (on-cycle or straddling) link failure without ambiguity: under any failure, only the MP node of the failed link is aware of the failure and is the one to remove traffic redirected due to the failure on the bypass tunnel from the p-cycle.

IV. Numerical Results

We compare the pure FRR and hybrid FRR/p-cycle schemes on a simulation testbed implemented using the OPNET modeler. For this performance study, we consider the three network topologies shown in Fig. 3 that have been widely used in survivability research [12], [13]. The Cost-239 ($N = 11$ nodes, $L = 52$ directed links) topology is relatively dense, with an average node in-/out-degree $\overline{D} = 4.73$, while the Havana network ($N = 17$, $L = 52$) is relatively sparse, with $\overline{D} = 3.06$); the Bellcore topology ($N = 15$, $L = 58$) lies between the other two in terms of connectivity, with $\overline{D} = 3.87$.

We set up traffic demands between every pair of nodes in each network, and we used Dijkstra's algorithm to compute shortest-hop paths for working traffic. Let t_{sd} denote the amount of working traffic carried by the LSP from s to d. To investigate the sensitivity of the relative performance of the two schemes, we generated working traffic demands that follow four different patterns:

- *Equal (EQ):* $t_{sd} = t =$ constant, $\forall(s, d)$.
- *Uniform (UF):* t_{sd} is uniformly distributed in the interval $[0, 20], \forall(s, d)$.
- *Locality (LC):* t_{sd} is uniformly distributed in the interval $[4(h - h_{sd}), 4(h - h_{sd} + 1) - 1]$, where h_{sd} is the length (in hops) of the shortest path between s and d and h is the length of the longest shortest path in the network; in this pattern, the traffic demand between each node pair decreases with the distance between the two nodes, and models the traffic locality observed in some networks.
- *Reverse locality (RL):* t_{sd} is uniformly distributed in the interval $[4(h_{sd} - 1), 4h_{sd} - 1]$, where h_{sd} is the length (in hops) of the shortest path between s and d, hence, it increases with the length of the shortest path h_{sd}.

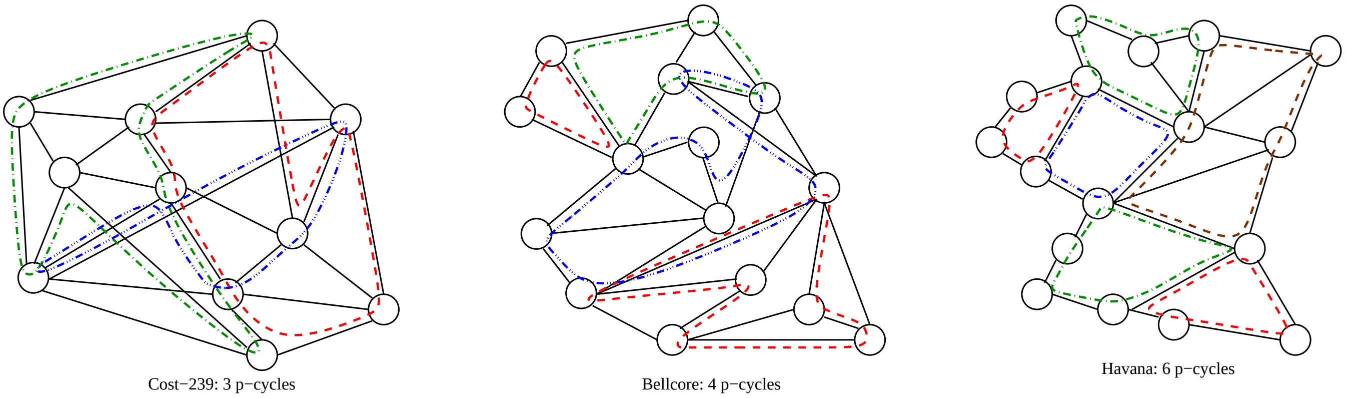
For pure FRR, we also used Dijkstra's algorithm to find the shortest backup path for each link l. For the hybrid FRR/p-cycle scheme, we selected the set of p-cycles as follows. First, for each topology we selected a Hamiltonian cycle. While a single Hamiltonian cycle provides protection to all the links in the network, it generally results in long backup paths. Therefore, for each topology we also selected one set of smaller p-cycles to protect its links. There has been extensive research in developing optimization techniques for selecting optimal sets of p-cycles [9]. Since our focus is not on such optimization, we used a faster technique to obtain a "good" p-cycle set. Specifically, we divided each topology into smaller, overlapping sub-networks, and selected a Hamiltonian cycle for each smaller network. The set of these Hamiltonian cycles for each sub-network formed the p-cycle set for the original topology, and is shown in Fig. 3.

A. B/W Ratio

Fig. 4 compares the B/W ratio of the pure FRR and hybrid FRR/p-cycle schemes in terms of the B/W ratio. There are three sub-figures, one for each of the three network topologies of Fig. 3. Each sub-figure plots the B/W ratio as a function of the traffic patterns we discussed above, and contains three curves: one for the pure FRR scheme, one for the hybrid scheme when a single Hamiltonian cycle is used to protect all links in the network, and one for the hybrid scheme where a set of smaller p-cycles, obtained as described earlier in this section, is used to protect the network links. In order to make meaningful comparisons, although working traffic demands were generated according to the four traffic patterns, the total (working) traffic in each case was set to 1000 units.

The figure shows that for the Cost-239 and Bellcore topologies, the hybrid FRR/p-cycle scheme requires less protection bandwidth than pure FRR across all traffic patterns (with one exception), while the opposite is true for the sparse Havana topology. This behavior can be explained by the observation that, in denser networks, there are more opportunities for links to be straddling spans on some p-cycle, hence increasing the protection efficiency (since straddling spans do not need to have any spare capacity). The results of Fig. 4 are also consistent with the findings of [8] which proved that the p-cycle scheme achieves the same lower bound on the ratio of spare to working capacity as a span-restorable mesh network, and also showed that larger p-cycles tend to provide higher capacity efficiency. Given that current and future networks are likely to be highly connected [14] (i.e., as dense or denser than the Cost-239 topology), it is clear that the hybrid scheme may provide significant benefits in backup capacity efficiency. We further note that the p-cycle sets we consider here were not optimized for any specific objective. Hence, the results of Fig. 4 are only an upper bound on what can be achieved using p-cycle design; using sophisticated optimization techniques to select the p-cycle set, additional improvements in capacity efficiency would be possible.

We also note that the traffic pattern does affect the B/W ratio, but the relative performance among the various schemes is similar. Specifically, the locality (LC) pattern results in the lowest amount of protection capacity: since the majority of traffic is between nodes close to each other in distance, the corresponding backup paths are relatively short, resulting in low overall spare capacity. Similar arguments can be used



Cost−239: 3 p−cycles

Bellcore: 4 p−cycles

Havana: 6 p−cycles

Fig. 3. Network topologies used in the performance study

to explain why the reverse locality (RL) pattern requires the highest amount of backup capacity among the four patterns considered here, while the equal (EQ) and uniform (UF) patterns fall between the other two in terms of this metric.

B. *Traffic Weighted Backup Hop Cost*

Fig. 5 is similar to Fig. 4 but compares the pure FRR and hybrid FRR/p-cycle schemes in terms of weighted backup hop cost. We can see that using a single Hamiltonian path incurs high cost, due to the long backup paths involved. On the other hand, using a set of smaller p-cycles reduces this cost significantly, which now becomes only slightly larger (or slightly smaller, in the case of the Havana topology) than the cost of pure FRR. We also observe the effect of the traffic pattern on the results, but the relative performance of the schemes is similar.

C. *Label Entry Overhead*

Table I compares the protection schemes in terms of the number of additional labels needed for protecting all links in the network. For pure FRR, the number of labels is high as each link is protected independently of others by establishing a separate bypass tunnel. Hence, the number of labels is proportional to the total length of all backup paths in the network. Since backup paths are longer in sparser topologies, we also observe that the label overhead for pure FRR increases from the Cost-239 topology to the Bellcore topology and then to the Havana topology.

For the hybrid scheme, when a single Hamiltonian p-cycle is used, the total number of protection labels is simply twice the length of the Hamiltonian cycle (an equal number of labels for each direction along the cycle), i.e., twice the number N of nodes in the network. Similarly, when a set of p-cycles is used, the total number of labels is twice the total length of all p-cycles. As a result, the label overhead is significantly lower in the hybrid scheme, about one-fifth of the overhead under pure FRR. This is further demonstration of the fact that, by taking a global design approach in protecting the network links, the p-cycle scheme is more efficient in its use of network resources.

TABLE I
LABEL ENTRY OVERHEAD COMPARISON

Topology	FRR	Hybrid FRR/p-cycle	
		Hamiltonian	p-cycle set
Cost-239	160	22	42
Bellcore	180	30	44
Havana	198	34	56

V. CONCLUSIONS

We have introduced a hybrid FRR/p-cycle scheme for MPLS networks. The scheme uses backup paths along a set of pre-configured p-cycles that may be selected using design methodologies that consider the overall network performance, but otherwise is RFC 4090-compliant. Numerical results indicate that using a set of relatively short p-cycles outperforms pure FRR in terms of backup capacity and label overhead, and is comparable to pure FRR in terms of backup hop cost. The benefits of the hybrid scheme increase with the density of the network, hence adopting a p-cycle design is an attractive alternative for MPLS network operators.

REFERENCES

[1] E. Rosen, A. Viswanathan, and R. Callon, “Multiprotocol label switching architecture,” RFC 3031, January 2001.

[2] A. Viswanathan, N. Feldman, Z. Wang, and R. Callon, “Evolution of multiprotocol label switching,” *IEEE Communications Magazine*, vol. 36, no. 5, pp. 165–173, May 1999.

[3] R. Nagarajan, Y. Wang, and M. Qureshi, “Reliable packet transport technologies for MPLS networks,” in *Proceedings of NETWORKS 2004*, June 2004, pp. 351–357.

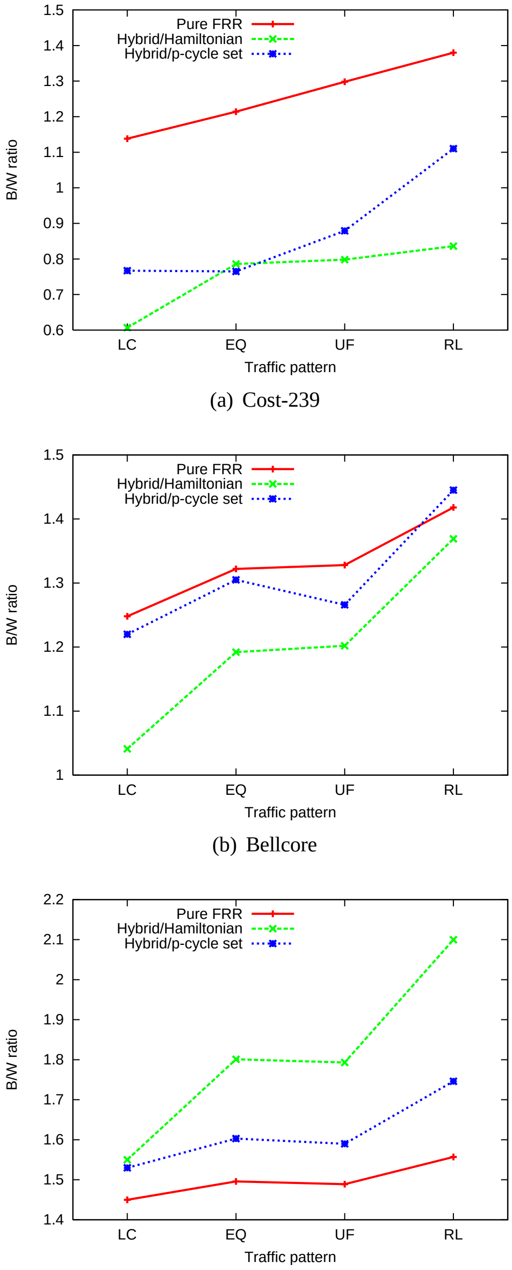
[4] W. B. *et al.*, “Survivable MPLS over optical transport networks: Cost and resource usage analysis,” *IEEE Selected Areas in Communications*, vol. 25, no. 6, pp. 949–962, June 2007.

[5] R. Aubin and H. Nasrallah, “MPLS fast reroute and optical mesh protection: A comparative analysis of the capacity required for packet link protection,” in *Proceedings of DRCN 2003*, October 2003, pp. 349–355.

[6] Q. Zheng and G. Mohan, “An efficient dynamic protection scheme in integrated IP/WDM networks,” in *Proceedings of ICC 2003*, May 2003, pp. 1494–1498.

[7] P. Pan, G. Swallow, and A. Atlas, “Fast reroute extensions to RSVP-TE for LSP tunnels,” RFC 4090, May 2005.

[8] D. Stamatelakis and W. Grover, “Theoretical underpinnings for the efficiency of restorable networks using preconfigured cycles p-cycles),” *IEEE Transactions on Communications*, vol. 48, no. 8, pp. 1262–1265, August 2000.

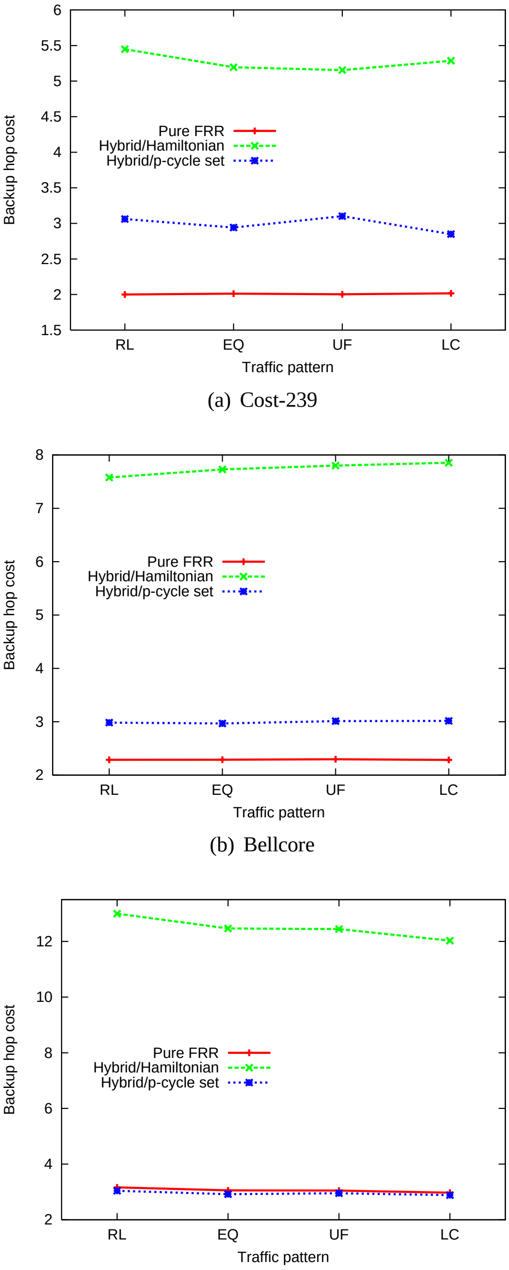


(a) Cost-239

(b) Bellcore

(c) Havana

Fig. 4. B/W ratio comparison



(a) Cost-239

(b) Bellcore

(c) Havana

Fig. 5. Weighted backup hop cost comparison

[9] M. Kiaei, C. Assi, and B. Jaumard, “A survey of the p-cycle protection method),” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 3, pp. 53–70, 3rd Quarter 2009.

[10] D. Stamatelakis and W. Grover, “IP layer restoration and network planning based on virtual protection cycles,” *IEEE Selected Areas in Communications*, vol. 18, no. 10, pp. 1938–1949, October 2000.

[11] J. Keng and M. Reed, “Bandwidth protection in MPLS networks using p-cycle structure.” in *Proceedings of DRCN 2003*, October 2003, pp. 356–362.

[12] W. Grover and D. Onguetou, “A new approach to node-failure protection with span-protecting p-cycles.” in *Proceedings of ICTON 2009*, June 2009.

[13] S. Gangxiang and W. Grover, “Extending the p-cycle concept to path segment protection for span and node failure recovery,” *IEEE Selected Areas in Communications*, vol. 21, no. 8, pp. 1306–1319, October 2003.

[14] C. LiYing, S. Kumara, and R. Albert, “Complex networks: An engineering view,” *IEEE Circuits and Systems Magazine*, vol. 10, no. 3, pp. 10–25, August 2010.