Inter-Area Shared Segment Protection of MPLS Flows Over Agile All-Photonic Star Networks

Peng He and Gregor v. Bochmann
School of Information Technology and Engineering (SITE)
University of Ottawa, Ottawa, ON, K1N 6N5, Canada
{penghe, bochmann}@site.uottawa.ca

***Abstract*—We study the resilience of MPLS flows over an agile all-photonic star WDM network (AAPN). On the basis of our previous inter-area optimal routing architecture, we propose and develop a dynamic inter-area shared segment-based protection (SSP) framework. We consider the dynamic protection for optimal inter-area working paths and improve the recovery time by segment-based protection. We develop a distributed partial routing information management to increase the scalability in multi-area networks while maintaining good performance compared with the case of complete information. By simulation, we show that our framework outperforms existing scheme. Furthermore, our approach shows its good potential to be a protection solution for inter-AS protection.**

Keywords-inter-area routing; shared segment protection

I. INTRODUCTION

Currently, many network carriers that are still using a single IGP (Interior Gateway Protocol) area network may have to migrate to a multi-area environment as their network grows and approaches the single area scalability limits [1]. Hence, it would be meaningful to extend current MPLS traffic engineering (TE) capabilities across IGP areas to support inter-area resources optimization. That is why RFC4105 was published to define requirements for inter-area MPLS traffic engineering and asks for solutions.

A multi-area network running the OSPF/OSPE-TE [7] protocol consists of one backbone area (Area 0) surrounded by several non-backbone areas. Area border routers (ABRs) are located at the border between the backbone and the non-backbone areas. An inter-area connection normally starts in a non-backbone area, traverses a backbone area, and terminates in another non-backbone area.

Optimal routing and associated protection, which are the two key issues of traffic engineering, become much more difficult in multi-area networks than in single area networks. This is due to the fact that the MPLS TE mechanisms deployed today are limited to a single area and can not be expanded to multiple areas directly. The reason is that the OSPF/OSPF-TE hierarchy limits topology visibility of head-end LSRs (Label Switch Routers) to their area, and consequently head-end LSRs can no longer compute the optimal working path and associated backup path(s) to the tail-end, as this computation requires the whole topology information [1]. Current schemes for inter-area routing are either approaches based on per-area-path-computation [2] that can not guarantee global optimization, or PCE (Path Computing Element) based approaches [5] that can achieve global optimization but at the price of building up an independent overlay PCE network covering all the areas. In [3,4], by deploying an agile all-photonic network (AAPN) [6] as the backbone area, we developed a novel routing architecture that can implement globally-optimized inter-area routing with good compatibility to existing traditional IP/MPLS routers, but the protection issues were not considered yet. In this paper, we focus on inter-area shared link and node protection in multi-area networks with an agile all-photonic backbone.

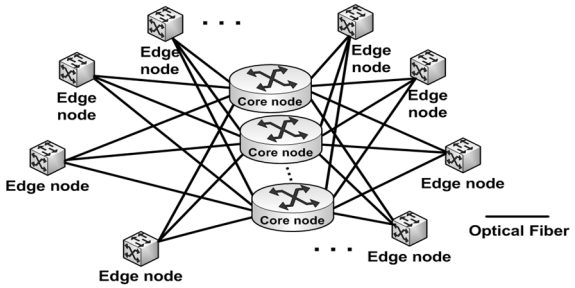

Figure 1. Agile All-Photonic Network (overlaid star topology).

A. Background: Overview of Agile All-Photonic Networks

As shown in Fig. 1, a centrally-controlled AAPN consists of a number of hybrid photonic/electronic edge nodes connected together via several load-balancing core nodes and optical fibers to form an overlaid star topology. Each core node contains a stack of bufferless transparent photonic space switches (one for each wavelength). A scheduler at each core node is used to dynamically allocate timeslots over the various wavelengths to each edge node. An edge node contains a separate buffer for the traffic destined to each of the other edge nodes. In these buffers, packets are collected together in fixed-size slots (e.g., 10μs) that are then transmitted as single units across the AAPN via optical links. The term "agility" in AAPN describes its ability to deploy bandwidth on demand at fine granularity, which radically increases network efficiency [6].

Note: due to the symmetric architecture of AAPN, we can adopt the "bundle" concept so that all the links from one edge node to the core nodes are exported as one single TE link. Similarly, the overlaid core nodes in AAPN are exported as one core node, named as "the core" (see Fig. 2).

B. Our Inter-Area MPLS Optimal Routing Framework

We adopted a novel way to deploy an AAPN as the backbone area within a multi-area OSPF network [3,4]. As shown in Fig. 2, we expand the OSPF non-backbone areas a little further so that there is an overlap between Area 0 and each expanded non-backbone area. Then the AAPN edge nodes located in the overlap, together with their TE links to the core,

and the associated part of the core, belong to both the Area 0 and a non-backbone area. In such a scenario, legacy routers in a non-backbone area see related AAPN edge nodes as normal internal IP/MPLS routers, see the AAPN TE links as normal internal links, and see the associated part of the core as the (only) ABR of their area, namely a virtual-ABR (v-ABR).

Hence an inter-area LSP (Label Switched Path) can be considered consisting of two half paths merging at the core: the 1st one in the head-end (expanded) area and the 2nd one in the tail-end (expanded) area (Fig. 2). As the direct result, independent local routing optimization on each of these two sub-LSPs can lead naturally to a globally-optimized inter-area LSP. As seen in Fig. 1&2, this is due to the star topology of the AAPN and the load-sharing core nodes that can be viewed as a single virtual router from the outside MPLS world. The local routing optimization can be performed by the source node (for 1st half path) and by any one of the edge nodes in the tail-end area (for 2nd half path).

C. Contributions of this Paper (problem statement)

In this paper, on the basis of our previous inter-area optimal routing architecture [3,4], we propose and develop a scalable inter-area shared segment-based protection (SSP) framework, which consists of three components, namely 1) the segment protection schemes (for the strict and a weakened single failure assumptions, Section II), 2) supporting routing information management (Section III) and 3) related signaling process (Section IV). Through sharing, we can utilize the network resource in an efficient way. Through segment-based protection, we can reduce the recovery time for inter-area connections.

In addition, segment-based protection can help us to develop a distributed routing information management to avoid the scalability issues related to multi-area networks. Meanwhile, for an inter-area connection, our SSP schemes provide not only link protection but also protection to failures of the "key" nodes along the working path. The key nodes include the edge and core nodes that act as ABR/v-ABR (Fig. 2). This follows the requirements of RFC4105.

D. Related Work

Few papers [2,8,9] have been published on inter-area resilience, although this topic has been studied extensively in single-area network scenarios. In [2], an inter-area SRLG-disjoint routing (ISDR) scheme was proposed where the routing is based on a non-optimal per-area mechanism. That is, the source node computes two disjoint sub-paths in its own area first, based on this, a far-end ABR computes the remaining sub-working-path and related backup-paths.

The scheme in [8] for inter-domain MPLS recovery is based on the establishment of static (manual setup) local repair paths at the domain boundaries. But this may not be suitable for multi-area non-linear network scenarios, where there might be many ABRs at area boundaries. No explicit backup bandwidth sharing was considered in the above schemes. A shared path protection (SPP) scheme in multi-domain optimal mesh networks was proposed in [9]. But besides the long recovery time due to the path-based protection, the complexity of the scheme is in the order of the square of the number of domain boundary nodes, which is also not suitable for our case.

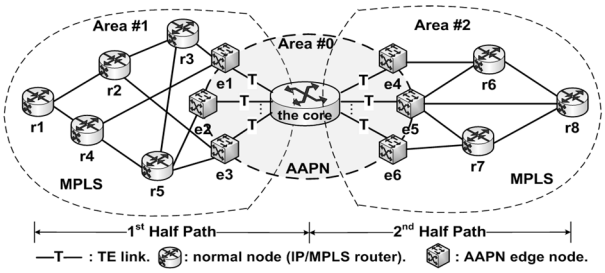

Figure 2. The Inter-Area MPLS optimal routing architecture through deploying AAPN as Area 0.

II. Proposed Schemes for Inter-Area Shared Segment-Based Protection

In this paper, we consider dynamic (e.g., on-line fashion) inter-area shared segment protection routing that aims to optimally identify an inter-area working path and associated backup paths for each arriving connection request.

A. Inter-Area Shared Segment Protection Scheme (IASSP)

Our scheme belongs to the active path first (APF) approach and we adopt the single-failure assumption. When an inter-area connection request (with protection requirement) comes in, the following steps are performed:

- An optimal inter-area working path for this connection request is determined (using our optimal routing framework in [3,4]).
- The working path is then divided into two overlapping (at AAPN) protected half-paths (see Figure 3 top).
- For each protected half-path, different protection techniques (link-, segment-, or path-based) can be applied independently.
- An extra optical cross-connection between the two AAPN edge nodes along the working path but through a different core node can be setup to provide further and instant protection against the failure of the core node or one of the two optical links along the working path. It is called "nested" protection.

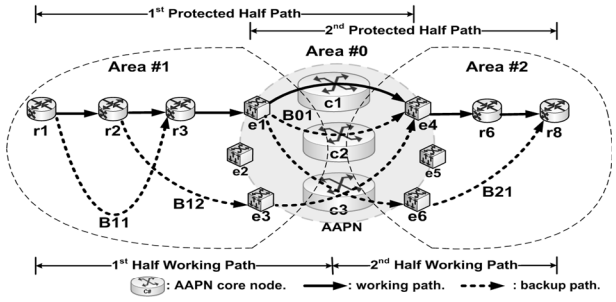

Figure 3. the Inter-Area shared segment-based protection

As shown in Fig. 3, for an inter-area connection request (*r1* to *r8*), suppose the optimal working path is *r1->r2->r3->e1->v-ABR->e4->r6->r8*. For the first protected half-path (*r1->r2->r3->e1->v-ABR->e4*), the source node, *r1*, is in charge of computing the associated optimal backup path(s). But according to our inter-area optimal routing framework [3,4], the farthest node *r1* can see is v-ABR not *e4*. Hence we need *e4* to "act" as v-ABR, which means to export the necessary routing information to *r1* so that the backup paths can be

computed optimally by *r1* without breaking our inter-area routing architecture. We call this as "*handoff-exporting*". Similarly, we need *e1* to "act" as v-ABR when computing the backup path(s) for the 2nd protected half-path.

Now suppose the 1st protected half path uses segment-based protection, as shown in Fig. 3, and then the associated backup paths are B11 and B12 with the branch nodes as *r1*, *r2* and the merge nodes as *r3*, *e4*, respectively. B11 and B12 protect the normal links along the working path from *r1* to *e1*. B12 also protects edge node *e1*.Suppose the 2nd protected half-path uses path-based protection, then the associated protection path is B21 protecting *e4* and the links from *e4* to *r8*. B01 is the nested protection path protecting optical links *e1->c1*, *c1->e4* and the core node *c1*. When a failure occurs, the first notified branch node will activate the shared backup path and then switch the traffic from the working path to the backup path.

B. Backup Bandwidth Sharing

Backup bandwidth sharing is an efficient way to reduce recovery resource utilization. The idea is to let backup paths share network resources when the working LSPs that they protect are physically disjoint (i.e., link, node, SRLG, etc.). There is nothing special in our framework for backup sharing in the MPLS part of a non-backbone area. Whereas for the AAPN part, as presented in the above example, for one inter-area connection request, there are in total four cross-connections involved in the AAPN domain: one for the working path, one for nested protection, and two for half-path protection. These backup optical cross-connections are setup within the AAPN to provide fast protection for inter-area connections; they all follow the time-slot constraint (since no time-slot interchanger at core nodes). Fig. 4 below illustrates the scenarios of backup cross-connections sharing in AAPN:

- Parallel case: 1 and 4 can share their backup cross-connections *e3->c2->e4* and/or *e1->c2->e6*.
- Same tail-end: 1 and 3 can share their backup cross-connections, e.g., *e3->c3->e4* or *e2->c3->e4*(nested).
- Same head-end: 1 and 2 can share their backup cross-connection, e.g., *e1->c3->e6* or *e1->c3->e4*(nested).
- Nested protection: 1 and 5 can share their nested backup cross-connection, e.g., *e1->c2->e4*.

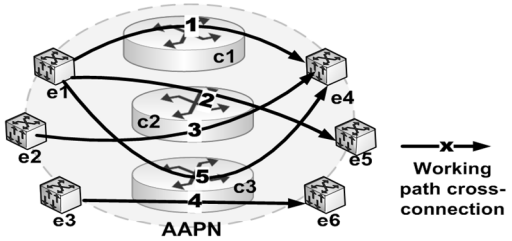

Figure 4. Backup Cross-connection sharing in AAPN

C. IASSP under a Weakened Single-Failure Assumption

Multi-area networks are normally large-scale networks, in which the commonly-used "single-failure" assumption becomes unrealistic. Hence we propose a weakened single-failure assumption for multi-area networks. As illustrated in Fig. 5, the modified single-failure assumption assumes:

- At any given time, there will be at most one failure occurred within one circle (one area).

Under this assumption, multiple failures could happen simultaneously. Our proposed protection scheme can still work, just with two minor modifications as follows:

- For the first protected half-path, there must be one backup path that ends at the edge node along it (see B11 ending at e1 in Fig. 6).
- For the second protected half path, there must be one backup path that starts at the edge node along it (see B22 starting from e4 in Fig. 6).

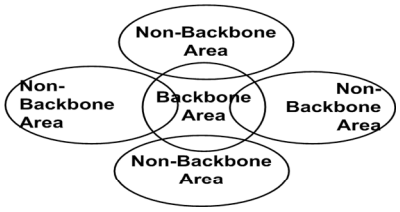

Figure 5. Weakened single-failure assumption

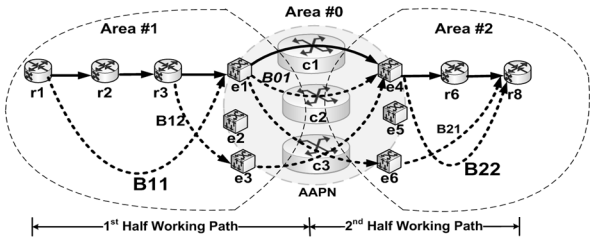

Figure 6. IASSP under the weakened single-failure assumption

It is worth mentioning that schemes in [2,8,9] do not consider the multi-failure scenario, hence they will not work under our modified single-failure assumption.

On the other hand, in order to make our proposed schemes work in the real world, we need to distribute and manage the routing information (see Section III) so that the nodes can compute the paths according to our schemes and we also need a related signaling process (see Section IV) so that the nodes can install the computed paths successfully.

III. ROUTING INFORMATION MANAGEMENT

We use the word "routing" to indicate both the working path selection and the backup path selection. Normally, routing information management can be classified according to whether it provides complete information (e.g., global per-flow or per-link information) or partial information (e.g., part of the complete information). In multi-area networks, the former may not be practical due to the scalability issue. Hence we adopt a partial routing information management scheme described in [10] and expand it to the case of the multi-area networks with node protection requirement, while treating the routing with complete information as the ideal case for comparison.

A. General Notations

We define the following notations:

- B_l, R_l: the total occupied backup bandwidth, and the residual free bandwidth on link l, respectively.
- d: the bandwidth requirement of an inter-area request.
- W_m^l: the total working bandwidth on/passing-through link/node(edge or core) m protected by link l ($l \neq m$).

- B_l^m : the total backup bandwidth occupied on link l used to protect m (link or edge/core node).
- Data set $WSet(m) = \{\langle W_m^l, l, m\rangle \mid l \neq m\}$.
- $\bar{W}_m = \max\{W_m^l \mid W_m^l \in WSet(m)\}$
- Data set $BSet(l) = \{\langle B_l^m, m, l\rangle \mid m \neq l\}$

Consider the overlap part between a non-backbone area and the AAPN (Fig. 2). We identify three kinds of links there, namely *physical link* (l^P), *TE link* (l^T), and *virtual link* (l^V). Physical links are individual AAPN optical links connecting edge nodes and core nodes. TE links are bundles of the AAPN physical links exported to the MPLS non-backbone area. A virtual link is like a "tunnel" from an edge node in one area through a core node to an edge node in another area. It includes all the bandwidths occupied by the existing working and backup paths traversing it. By adopting the virtual tunnel/link concept to manage the AAPN internal routing information, we can avoid maintaining the per-timeslot backup information which is due to the timeslot continuity constraint in AAPN.

B. Routing with Complete Information (ideal case)

We adopt the least cost routing for path selection, where the cost of a path is defined as the sum of the costs of all the links along the path.

1) *Finding first the least cost inter-area working path*. The link cost function for working path computing is:

- *For a normal link l*

$$\begin{cases} 1/R_l, & if\ d \le R_l \\ \infty, & otherwise \end{cases} \quad (1)$$

- *For an AAPN virtual link* l^V

$$\begin{cases} 1/R_{l^V} + 0.5\times d\times \bar{W}_{l^V}/M, & if\ d \le R_{l^V}; M = \max_{\forall l^V}(\bar{W}_{l^V}) \\ \infty, & otherwise \end{cases} \quad (2)$$

The $0.5\times d\times \bar{W}_{l^V}/M$ part in (2) was inspired from the concept of potential backup cost (PBC) proposed in [10] to make the performance of shared protection routing outperform even ILP model. By involving PBC, we can consider the potential impact of selecting a working path on the future backup paths. This is very necessary particularly in AAPN due to its symmetric topology.

2) *Based on the determined working path, computing the least cost backup paths*. We denote AB_l^{WPi} as the additional bandwidth required on link l to protect a working path segment (or half-path) WPi. Its exact value in backup bandwidth sharing scenario ($AB_l^{WPi} \le d$), is $AB_l^{WPi} = \max_{m\in WPi}\{0, W_m^l + d - B_l\}$. We then define the same link cost function of normal and virtual links for backup path computation as:

$$\begin{cases} 0, & if\ AB_l^{WPi} = 0 \\ 1/R_l, & if\ 0 < AB_l^{WPi} \le R_l \\ \infty, & if\ AB_l^{WPi} > R_l \end{cases} \quad (3)$$

C. Routing with Partial Information

In this scenario, the routing information is distributed among the nodes in the network and no one maintains global and complete view about the multi-area network.

1) *Routing procedures*: similar procedures are adopted with the following changes:

- *For selecting an inter-area working path*: following our optimal routing framework in [3,4] (see Fig. 2), use equation (1) to compute the 1st and 2nd half working paths and then use equation (2) to decide which core node to connect these two half paths.
- *For selecting a backup path*: same link cost function except AB_l^{WPi} is over-estimated [10] by

$$AB_l^{WPi} = \max_{m\in WPi}\{0, \bar{W}_m + d - B_l\} \quad (4)$$

2) *Link State* $\{R_m, \bar{W}_m, B_m\}$ *and data sets* $WSet(m)$, $BSet(l)$. Similar as [10], we define $\{R_m, \bar{W}_m, B_m\}$ as the link state but a general one, since in our case m could be a normal link, TE link, virtual link, AAPN edge node or core node depending on which node the link state is stored in. $WSet(m)$ is used to generate $\bar{W}_m$; while $BSet(l)$ is to adjust the actual amount of additional backup bandwidth after path determination as in [10]. In general, link state is updated through the OSPF-TE flooding mechanism within each area and the two data sets are updated by the RSVP-TE signaling process during call set-up.

3) *Routing information maintained at each normal node*. Similar as in [10]: link state for each link (normal links and TE links) in the non-backbone area, $WSet(l)$ and $BSet(l)$ only for each of its local outgoing link.

4) *Routing Information Maintained at each Edge Node*. On the non-AAPN side, same as above; whereas on the AAPN side, each edge node needs to maintain necessary AAPN internal routing information so as to export link state of its two TE links (to/from the core) to the normal nodes in the same non-backbone area. The necessary AAPN internal routing information at each edge node includes:

- $WSet(e_i)$, where e_i is the edge node itself;
- Link state, $WSet(l^V)$ and $BSet(l^V)$ for each local outgoing virtual link;
- Copy of links state of each local incoming virtual link.

5) *Exporting* $\{\boldsymbol{R}_{l^T}, \bar{\boldsymbol{W}}_{l^T}\}$ *through OSPF-TE Flooding*. Each edge node can derive the first two elements of the link state of its two TE links from its own AAPN internal routing information. We only show the results here to save space:

- let R_{l^T} be the maximal link residual bandwidth among the physical links represented by this TE link.
- let $\bar{W}_{l^T}$ be $\bar{W}_{e_i}$, where e_i is the edge node of this TE link. Since $\bar{W}_{l^T} \le \bar{W}_{e_i}$, we thus can avoid exporting $\bar{W}_{e_i}$.

6) *Edge node handoff exporting* $\{\boldsymbol{B}_{l^T}\}$ *through RSVP-TE*. Observing Fig. 3, suppose a working path traverses the virtual link *e1->c1->e4*. When computing the associated shared backup path(s) according to equations (3,4) in area 1, we notice that only the information about virtual links *e2->ck->e4*, *e3->ck->e4* ($k = 1,2,3$) are *useful*. That means the value of $\{B_{l^T}\}$ is actually working-path-dependent, and can be determined only after a working path is determined. Hence we have to use

the *handoff exporting* mentioned earlier to export $\{B_{l^T}\}$, and export only to the source node or edge node through the transmission of RSVP-TE message (instead of OSPF-TE flooding) to compute backup paths for the 1st or 2nd protected half paths. We approximate each B_{l^T} by the sum of B_{l^V} of all the related useful virtual links after a working is determined.

IV. Related Signaling Process

We use a simple two-phase signaling scheme, which is fully based on RSVP-TE protocol [11], to setup an inter-area LSP and its backup paths subsequently. Consider a request for inter-area connection with protection requirement from *r1* to *r8* in Fig. 3.

A. Signaling Phase I: Working Path Set-up

The signaling process in Phase I is almost the same as the one in our inter-area routing framework [3,4], which is a PATH↔RESV message "round-trip" for inter-area working path set-up. The only difference is when the RESV message arrives at *e4*, through the handoff exporting, *e4* attaches related $\{B_{l^T}\}$ (*to-e4 direction*) to the RESV message going back to *r1*.

B. Signaling Phase II: Backup Path build-up [12]

Signaling phase II is another PATH↔RESV "round-trip" process. After *r1* receives the RESV message (including $\{B_{l^T}\}$) from Signaling Phase I, it computes the optimal shared backup path(s) for the 1st protected half path and then starts Phase II by sending a PATH message that includes:

- One primary ERO (Explicit_Route Object) [12]: list of the explicit end-to-end inter-area working path.
- One or more SEROs (Secondary ERO [12]): list of the backup path(s) for the first protected half path.

1) *PATH message processing*. The PATH message propagates along the working path until a node finds itself a branch node by checking the SEROs in the PATH message. The node then uses the related SERO and other information in the received PATH message to create a new PATH message and send out: the original one traversing still along the working path while the new one along a backup LSP from this branch node to the related merge node (following the standard LSP setup procedures). When the original PATH message arrives at *e1*, *e1* exports necessary $\{B_{l^T}\}$ (*from-e1 direction*) through PATH message to *e4*. *e4* can thus compute the backup path(s) for the 2nd half protected path. After that, the same procedures as for the 1st protected half path are followed to set up the backup LSP(s) of the 2nd protected half path.

2) *RESV message processing*. There are two kinds of RESV messages now: one for the working path and others for various backup paths. During the transmission of these RESV messages, the local routing information ($WSet(m)$, $BSet(l)$ and hence link state) at each passed node is updated. When the RESV message of the working path arrives at a branch node, it will not be propagated upstream until the branch node receives the RESV message of the backup LSP starting from itself. Thus, when *r1* receives the RESV message of the working path, it means that all the related backup paths are set up.

C. Discussion

As we can see, the complexity of the information updates for our protection schemes after building up an inter-area connection is in the order of the number of (not the square of number of, as in [9]) edge nodes.

V. Simulations Results and Analysis

In this section, we study the performance of our segment-based shared protection framework through simulation. Simulation experiments are conducted on a 21-node 3-area ladder-like network (Fig. 7), which is the extended version of the topology adopted in [2]. In the simulations, the call requests arrive to the network following a Poisson process, and the call holding time is exponentially distributed. We assume that all the inter-area source-destination node pairs have the same traffic load, so do the intra-area node pairs. A call request is accepted only when both the working path and backup paths are available.

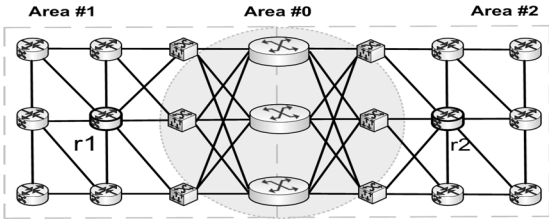

Figure 7. Network topology used for simulation (21 nodes and 96 directional links in total)

A. Blocking/Rejection Probability Analysis

There could be several IASSP schemes, namely IASSP-CS, IASSP-PS, and IASSP-PM, where C stands for complete information, P for partial information, S for single-failure assumption and M for weakened single failure assumption. We compare our IASSP schemes with the ISDR scheme proposed in [2].

As seen in Fig. 8, IASSP-CS has the best performance in term of blocking probability. This is reasonable since it has the complete information when doing the routing. ISDR has the worst performance, which is partially due to its non-optimal routing and partially due to its less backup bandwidth sharing for inter-area routing. The IASSP-PS scheme performs closely to IASSP-CS in general, which shows the routing information management we developed works quite well. IASSP-PS outperforms IASSP-PM but not so much. This is because IASSP-PS has more flexibility when selecting backup paths. It also shows that IASSP-PM achieves multi-failure protection without great performance degrading. Fig. 8 also shows the necessarility of involving PBC (see equation (2)) into the link cost function (see the curve of IASSP-PS without PBC).

IASSP-PM can be considered as a special case of IASSP-PS. But it has two distinguished features, namely isolation and security. By isolation, we mean that it isolates an inter-area working path into three "big" segments: two MPLS segments in the head- and tail-end areas and one AAPN segment in the middle (see Fig. 6). Each segment can use various protection techniques fully-independently. Thus the opportunity for backup bandwidth sharing in each segment is increased. By security, we mean that in IASSP-PM each normal node has no information about nodes outside its own area and each AAPN

edge node has no information about any normal node outside its area. These two features make IASSP-PM very attractive for inter-AS protection.

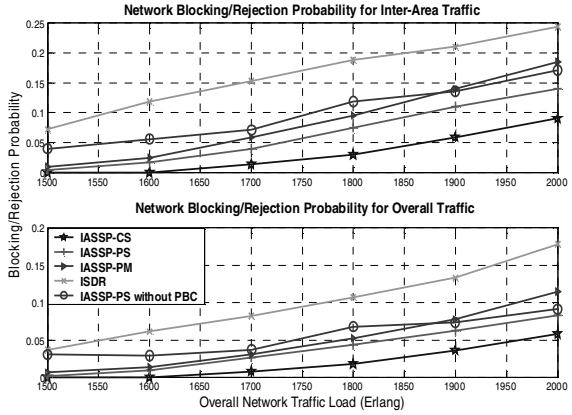

Figure 8. Blocking probabilities of various dynamic inter-area protection schemes with 95% confidence interval as +/ 0.1%. 60% of the overall network traffic is inter-area traffic.

B. Protection Bandwidth Cost Ratio

We define the protection bandwidth cost ratio as the percentage of the average overall backup bandwidth to the average overall working bandwidth at a fixed network blocking probability. On the basis of the results in Table I, we notice that the schemes we proposed have lower cost ratios (e.g., better backup bandwidth sharing efficiency) than ISDR scheme. In addition, the ratios of IASSP-PS and IASSP-PM are considerable similar to that of IASSP-CS.

TABLE I. PROTECTION BANDWIDTH COST RATIO OF SCHEMES

Blocking Prob.	IASSP-CS	IASSP-PS	IASSP-PM	ISDR
1%	59%	66%	78%	110%
10%	55%	62%	73%	105%

C. Backup Bandwidth Sharing within AAPN

To study the maximal efficiency of backup cross-connections sharing in AAPN (see Fig. 4), we remove all the normal nodes in the topology of Fig. 7 except *r1* in area 1 and *r2* in area 2. IASSP-CS is chosen for the evaluation. As seen in Table II, the protection cost ratio decreases (e.g., sharing efficiency increases) as the number of edge/core nodes increases. But the speed of the decreasing becomes slow when the number of edge and core node both reach 6.

TABLE II. PROTECTION BANDWIDTH COST RATIO IN AAPN

# of edge nodes in area 1 or 2	# of core nodes	Protection Bandwidth Cost Ratio
2	**2**	100%
3	**3**	67%
4	**5**	50%
6	**6**	40%
12	**12**	33%

VI. CONCLUSIONS

We studied the resilience issue of MPLS flows over an agile all-photonic star WDM network (AAPN). Based on our previous inter-area optimal routing architecture, we propose and develop a dynamic inter-area MPLS shared segment protection framework consisting of:

1. The IASSP schemes consider both single-failure and multi-failure (weakened single-failure) scenarios;

2. A distributed and partial routing information management greatly reduces the scalability issue in multi-area networks with link and key node protection;

3. A related signaling process consistent with RSVP-TE.

Meanwhile, our framework requires little change on existing traditional IP/MPLS routers to implement it. The simulation results show that our protection schemes have performance similar to the case with complete routing information and outperform greatly the inter-area protection scheme described in [2]. Indeed, together with our previous inter-area optimal routing architecture [3,4], we can now provide an attractive MPLS inter-area traffic engineering solution that satisfies the requirements defined in RFC4105. Furthermore, our protection scheme under the weakened single-failure assumption shows its great potential to be a solution for inter-AS protection, which is our future work.

ACKNOWLEDGMENT

This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada and industrial and government partners, through the Agile All Photonic Networks (AAPN) Research Network. This work is part of an AAPN Partnered Research Project sponsored by TELUS.

REFERENCES

[1] Le Roux, et al., “Requirements for Inter-Area MPLS Traffic Engineering”, IETF RFC 4105, June 2005.

[2] T. Miyamura, et al., “An Inter-Area SRLG-disjoint Routing Algorithm for Multi-segment Protection in GMPLS Networks,” Proc. ICBN 2004, 2004.

[3] P. He and G. v. Bochmann, “Routing of MPLS flows over an agile all-photonic network”, Proc. of IASTED Intern. Conf. on Communication Systems and Applications, July, 2006.

[4] P. He and G. v. Bochmann, “A Novel Framework for Inter-Area MPLS Optimal Routing”, Internet Draft, draft-he-ccamp-optimal-routing-00.txt, September, 2006.

[5] A. Farrel, J. P. Vasseur and J. Ash, “A Path Computation Element (PCE)-based architecture”, RFC 4655, Aug. 2006.

[6] Mason, L., A. Vinokurov, N. Zhao, and D. V. Plant, “Topological design and dimensioning of agile all-photonic networks," Computer Networks, Vol. 50, 268-287, 2006.

[7] Katz, D., Yeung, D., Kompella, K., "Traffic Engineering Extensions to OSPF Version 2", RFC 3630, Sept, 2003.

[8] C. Huang and D. Messier, "A Fast and Scalable Inter-Domain MPLS Protection Mechanism," Journal of Communications and Networks, Vol.6, No.1, March 2004.

[9] B. Thiongane, D.L. Truong , "Shared Path Protection in Multi-domain Optical Mesh Networks", in Proc. of IASTED Computer and Communication Network, Oct. 2005.

[10] C. Qiao and D. Xu, “Distributed Partial Information Management (DPIM) schemes for survivable networks - Part I, II”, Proc. of IEEE INFOCOM, Apr. 2001.

[11] Awduche, D., et al. "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December, 2001.

[12] Lou Berger, Igor Bryskin, Dimitri Papadimitriou, Adrian Farrel, “GMPLS Segment Recovery”, RFC 4873, May, 2007.