LSA Expansion for Fault Recovery in GMPLS Network

Changwoo Nam[1], Kwangsub Go[2], Minki Noh[2], Seunghae Kim[2]
Hyuncheol Kim[3], Jaeyong Lee[4], Jinwook Chung[1]

[1] Dept. of Electrical and Computer Engineering, Sungkyunkwan Univ., Suwon, Korea
[2] Korea Institute of Science and Technology Information, Daejeon, Korea
[3] Dept. of Computer Science, Namseoul Univ., Chonan, Korea
[4]Dept. of Internet Engineering, Hanseo Univ., Seosan, Korea

Summary
GMPLS-based optical network fault recovery does not consider an integration of connection when configuring a backup path. This can cause greater damages likely when a fault occurs to a link or path concentrated with many connections. Also, the concentration of such traffic results in a negative effect in terms of network survivability. This paper attempted to minimize the damage done by a network fault by selecting a more stable path and avoiding ones with lower survivability based on the number of connections to a node or link by expanding LSA of the link state algorithm.

Key words:
GMPLS, Optical Network, Fault Recovery

1. Introduction

The recently spotlighted ubiquitous and the IPv6 technology applied to PCs and other various devices causing the Internet traffic to soar forced ISPs to improve their network to the overlay structure using ATM (Asynchronous Transfer Mode) for traffic accommodation or to expand their network capacities beyond necessity in order to keep up with the increasing traffic. Nonetheless, the bandwidth supported by copper wire has already reached its threshold and the emergence of various high-speed convergence services such as IPTV, which is the trend in the broadcasting and telecom industry, require new forms of network.

This has induced the creation of NGN (Next Generation Network), which supports various types of telecom services as well as reduced network management and installation costs by IP-based integrating every type of telecom network with phone network, ATM, VPN, and wireless network, and Korea has introduced BCN (Broadband Convergence Network) in correlation with such.

The backbone of the next generation network consists of optical network that supports broadband and there are various ongoing researches that seek to develop a more efficient optical network using IP. However, the currently non-flexible and passive optical network faces realistic difficulties when it wants to support IPs with very passive traffic properties. This has caused the introduction of GMPLS (Generalized Multi-Protocol Label Switching)[4], initially named MPλS (Multi-Protocol λ(Lambda) Switching)[3], by applying MPLS (Multi-Protocol Label Switching)[2][3] to the optical network. Through this, the optical network is integrated as singular control surface thereby allowing a flexible control and management of the passive optical network with difficulties in allocating active broadband through reconfiguration and traffic of the network.

But fault such as termination of optical links are still an important issue to resolve. Massive traffic is transmitted to the optical network that takes most part of the backbone network and a fault in such backbone would result in a very critical and destructive network chaos. Problems with network fault recovery are more prioritized than building an economic network as there are many ongoing researches on this matter.

In this paper, in order for a prompt and stable path reconfiguration during fault in the GMPLS network, we propose a method that expands the routing protocol, which can promote the survival and stability of paths by expanding the LSA provided by OSPF-TE.

2. Network Survivability and Fault Recovery

WDM/ROADM/PXC Technologies have become core transfer technologies of BcN due to their ability to switch and integrate multiple high-speed transfer channels to one optical fiber. Optical fiber and WDM/ROADM/PXC technologies have not only significantly increased the capacity of the current transfer network but they also serve an important function of handling the rapidly growing traffic.

Although WDM/ROADM/PXC technologies significantly increased the ability of transfer networks, they also brought about a several issues. Since application

Manuscript received October 5, 2007
Manuscript revised October 20, 2007

of WDM/ROADM/PXC technologies concentrated various traffics through optical transfer network, the consequences of errors in the optical transfer network was also amplified. Due to such property, network survivability, protection, and restoration have become major issues in optical network hence the many researches.

2.1 Network Survivability

Network survivability indicates how much a service can persist in network faults and such indication has become the most important core idea that represents the recoverability of traffic affected by a defect during network faults in WDM/ROADM/PXC-based networks.
Such network survivability, as shown in Figure 1, can be categorized into three [5][6].

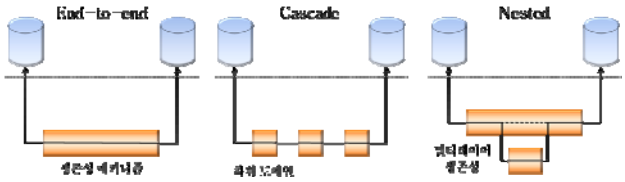

Fig. 1 Network Survivability Schemes

① End-to-end: uses only one survivability mechanism.

② Cascaded: uses many survivability mechanisms sequentially. Here, each survivability mechanism contains an object that handles faults in a particular sub-domain.

③ Nested: many survivability mechanisms operate under single sub-domain. Such mechanisms can operate in cascaded or end-to-end forms.

2.2 Recovery Schemes

The frequently occurring optical cable disconnection and the subsequent traffic loss have required network survivability to be considered when designing a network. Ring-type network connection structures have low expandability and they waste a great deal of resources. The mesh-type network organization is being explored in various ways to overcome such difficulties [7][8][9].
Network faults are classified as either a link fault or a node fault. When a fault occurs in the working path, recovery is done by configuring a backup path in order to restore the working path to the original. Fault recovery schemes are distinguished into protection and restoration [1][10].

2.2.1 Protection Mechanism

(1) 1+1 protection

1+1 protection configures a backup path that has a same resource as the working path and when traffic is sent to the working path, a same traffic is also sent through the backup path simultaneously. The destination of the two paths receives two same traffics and the decision is made at the destination. Therefore, configuring a working path requires twice as much network resources, depreciating resource efficiency but providing protection against traffic loss or having to recover from a fault.

(2) 1:1 protection
Similar to 1:1 protection, it configures same backup path with working path but traffic transfer is only done through the working path and not the backup path. When a fault occurs in the working path, a message is received from the node that detected the fault and the traffic is sent through the backup path, which can slightly reduce traffic loss.

(3) 1+N protection
Unlike the previously described 1+1 or 1:1 protection, in 1+N protection single path offers a backup path to many working paths. By supporting multiple working paths with single backup path, the resource efficiency can be enhanced but the constraint is that the transfer LSR and receiving LSR must be same and only one working path can be recovered when fault occurs to two or more working paths. To prevent this from happening, working paths must not be tricked by same SRLG[11].

(4) M:N protection
A scheme in which M number of backup paths and N number of working paths are configured as M number of backup paths may support any of the N number of working paths. Resource will be wasted since backup paths would not be used until a fault occurs and a more efficient version of this would be avoiding from setting up working paths within a same SRLG.

These protections use preconfigured backup paths and one or more dedicated protection lightpath is preconfigured for one or more working path and may be performed in various levels for network survivability.

2.2.2 Restoration Mechanism

A method in which optical network resource efficiency is improved by configuring a backup path in case of a network fault and a new path after a fault for recovery. While the restoration mechanism features efficient resource management by not pre-configuring a backup path, it entails a slower protection mechanism compared to the protection mechanism due to having to configure a backup path after the occurrence of a fault. However, its advantage is that the routing algorithm can optimize the

network by computing and configuring the backup path based on the current network state and policy [12][13].

2.3 Issues with the Restoration Mechanism

As mentioned earlier, the restoration mechanism uses the link state algorithm to select the optimal backup path. When configuring a backup path, the link state algorithm selects the path based on the bandwidth that the traffic requires and the cost. When the performance of a particular link is superior to other nearby links, the connection will be focused to that particular link and this is not exactly the preferred situation in terms of protecting network fault. A particular link having too many connections means that there is a large traffic that cuts through this link and a fault to this link is much more devastating than a fault to any other links with less of connections or traffic. More connection to a link means higher probability of fault occurrence and it induces frequent backup path configuration thereby depreciating the network's efficiency.

The following illustrates the problems with the existing fault recovery schemes.

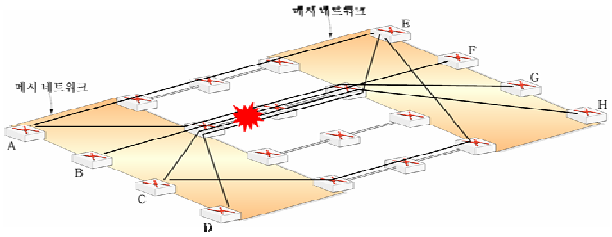

Fig. 2 Fault to a Path with Many Connections

Figure 2 shows a situation where more connections pass through a particular link than other links. More the number of connections to a link bring about deadlier consequences of a network fault.

The existing restoration schemes did not consider the survivability of a backup path when configuring a backup path. This could cause more network faults when selecting a link with many connections. Recurring faults can amplify the damage while dropping the network performance and efficiency. A link is prone to more fault risks when it accommodates more links.

This paper focuses on the method that prevents from additional network faults caused by the restoration mechanism's backup path configuration and a particular link from being concentrated with connections in order to minimize network damages and to evenly distribute the traffic to network resources.

3. OSPF-TE Expansion for Improvement of Network Survivability

The existing restoration mechanism did not consider the survivability of a backup path when configuring a backup path. This could cause more network faults when selecting a link with many connections. Recurring faults can amplify the damage while dropping the network performance and efficiency. A link is prone to more fault risks when it accommodates more links.

This paper focuses on the scheme that prevents from additional network faults caused by the restoration mechanism's backup path configuration and a particular link from being concentrated with connections in order to minimize network damages and to evenly distribute the traffic to network resources.

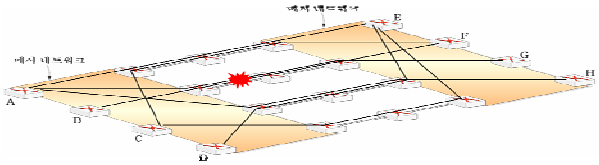

Fig. 3 Fault to a Scattered Working Path

Due to the nature of the link state algorithm that selects the optimal path, a few high-performing links are preferred as they attract connections more so than others. This is a situation to avoid because when a fault occurs to one of those links, it will result in a chaos incomparable to a fault in other links.

As a solution to this problem, we added sub-TLV, which stores the number of connections to a link in the link TLV of the existing LSA, and we minimized the damage done by a fault by distributing the connection concentrated to a particular link through path configuration and we finally designed it so that it configures more stable paths.

3.1 LSA Expansion for Addition of Sub-TLV

The newly added sub-TLV is defined as the path number and it has a total length of 8 octets including the header. The path number sub-TLV has a 4-octet-length field named Path_num to express the number of paths to a link.

The following illustrates the message format of the sub-TLV added in this paper.

Fig. 4 Path Number sub-TLV

① Type: A field for distinguishing Sub-TLV and has a fixed value of 10 and a length of 2 octets.

② Length: Shows the length of Path_num and has a length of 2 octets.

③ Path_num: Shows the number of connections to a link and has a length of 4 octets.

3.2 Constraint-based Algorithm

The constraint-based algorithm proposed in this paper configures a backup path by searching for the optimal path through the link state algorithm based on the number of connections to the newly added link and the existing TE constraint.

(1) Link Searching for TE

The following is a pseudocode that searches for the link that satisfies all constraints for TE.

```
L ← Set of Links (l)

Function Constraints_set (L)
1. FOR each link l in L
2.     IF l can not support TE
3.       L := L subtraction {l}
4.     ELSE IF l has not enough reservable bandwidth
5.       L := L subtraction {l}
                  :
           Other constraints
                  :
6.     END IF
7. END FOR
Return L
End
```

Fig. 5 Searching of Links that Satisfy Constraints

L shows the union of unit l that has the information about the number of connections for each link and L searches such link information filter the links according to the constraints. It discards the links that do not satisfy the constraints from the union L. Constraints may be modified based on the user's request.

(2) Modified Dijkstra's Algorithm

```
L <- The set of Links(l)
P <- The set of Paths
t <- Destination

Function Dijkstra(G, w, s, t)
1. FOR each vertax v in V[G]
2.         d[v] := infinity
3.         previous[v] := undefined
4.     d[s] := 0
5.     S := empty set
6.     Q := set of all vertices
7.     L := Constraint_set (Q)
8.     WHILE L is not an empty set
9.         u := Path_Num_Min(L)
10.        S := S union {u}
11.        FOR each edge (u,v) outgoing from u
12.            IF d[v] > d[u] + w(u,v)
13.                d[v] := d[u] + w(u,v)
14.                    previous[v] := u
15.        END IF
16.      END FOR
17.        IF u = t
18.          P := empty sequence
19.          n := t
20.              WHILE defined n in S
21.                  insert n to the beginning of P
22.                  n := previous[n]
23.           END WHILE
24.                Return P
25.      END IF
26.  END WHILE
27. END FOR
END
```

Fig. 6 Modified Dijkstra's Algorithm

The algorithm for configuring a backup path was designed to compute the path by receiving the L value returned by the Dijkstra's algorithm Figure 4. The algorithm searches and selects a link with the smallest number of connections within pool L. When the backup path computation from the transmitter to the destination is complete, it terminates the procedure and configures the backup path.

4. Conclusion

Increasing Internet user population and advancing Internet services technology have played a decisive role in the recent explosive soaring of the Internet traffic. The bursting Internet traffic now requires more bandwidth and ISPs (Internet Service Providers), in correlation to such demand, have made their transition to wider bandwidth optical network, in which IP packets are transferred.

Compared to the previously used copper cable, optical network supports a much wider bandwidth and therefore can accommodate more traffic. On the other hand, its hosting of more network traffic leads to deadlier damages done by network faults. Many researches are taking place

in order to mitigate such vulnerability against network faults.

Two prime fault recovery techniques are the protection scheme and the restoration scheme where the protection scheme causes inefficient resource management and the restoration scheme takes more time to recover a fault than the protection mechanism. Also, the restoration mechanism computes and configures a backup path after a fault has occurred. In the restoration scheme, searching and configuring a backup path is critical in terms of recurring a network fault. Also, optical network based post networks such as BcN or NGN allow a single optical link to take in many connections and this indicates how much optical network fault recovery and management is becoming critical. The previous restoration method's weakness is that it focuses traffic to high-performing links or to links that support larger bandwidth when it comes to selecting a backup path. Concentration of traffic means that a particular link is hosting many connections and a fault to such link will inevitably cause much harsher consequences than will a fault to other links.

This paper proposes a fault recovery scheme that identifies the number of paths each link has so that the ones with more links can be avoided when configuring a backup path.

In order to identify the number of paths a link has, we added sub-TLV, which stores the number of connections to a link in LSA of OSPF-TE, to apply it to the Dijkstra's algorithm when searching for a backup path so that it can prioritize links with less number of paths thereby ultimately distributing the traffic evenly throughout the links in the network.

The fault recovery scheme proposed in this paper can minimize the probability of fault and will evenly scatter the traffic to promote the network use efficiency.

For further research outlooks, there will need to be an investigation on a GMPLS-based management platform that can simplify the recovery and management of optical network faults along with further researches on the metrics required for recovering faults.

References

[1] Hyuncheol Kim, "A Study of Survivable Traffic Grooming in Broadband Convergence Networks", Thesis of Doctoral course, Sungkyunkwan Univ. 2005.

[2] Wayne D. Grover, "Mesh-Based Survivable Networks - Options and Strategies for Optical, MPLS, SONET, and ATM Networking," Prentice Hall, 2004.

[3] 김정윤, 이규명, "광인터넷", 표준기술동향, TTA Journal No. 87, 2003, pp. 149~ 156.

[4] K. Kompella, Ed., Y. Rekhter, Ed., "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4202, 2005.

[5] Sophie De Maesschalck, et al., "Intelligent Optical Networking for Multilayer Survivability," IEEE Communications Magazine, Jan. 2002, pp. 42~ 49.

[6] Ornan (Ori) Gerstel, Rajiv Ramaswami, ``Optical Layer Survivability - An Implementation Perspective," IEEE J. Sel. Areas in Communications, Vol. 18, No. 10, Oct. 2002, pp. 1885~ 1899.

[7] E. Mannie, Ed., D. Papadimitriou, Ed., "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4427, 2006.

[8] Ayan Banerjee, et al., "Generalized Multiprotocol Label Switching: An Overview of Signaling Enhancedments and Recovery Techniques," IEEE Communications Magazine, Jul. 2001, pp. 144~ 151.

[9] S. Makam et al., " A Path Protection/Restoration Mechanism for MPLS Netowrks", Internet Draft, draft-makam-mpls-protection-00.txt, Oct. 1999.

[10] Dimitri Papadimitriou, Eric Mannie, ``Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based Recovery Mechanisms (including Protection and Restoration)," draft-ietf-ccamp-gmpls-recovery-analysis-04.txt, IETF, 2004.

[11] Cisco co., "MPLS Traffic Engineering: Shared Risk Link Groups", http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s29/fs29srlg.pdf, 2007.

[12] Yang Qin, et al., "Study on a Joint Multiple Layer Restoration Scheme for IP over WDM Networks," IEEE Network, Mar. 2003, pp. 43~ 48.

[13] Gisli Hjalmtysson, Jennifer Yates and Sid Chaudhuri, "Restoration Services for the Optical Internet," Proceeding of SPIE, Terabit Optical Networking: Architecture, Control, and Management Issues, Vol. 4213, Oct. 2000.