

# MPLS망의 보호 복구 기술의 비교\*

정회원 오 승 훈\*\*, 김 영 한\*\*

## A Comparison of Restoration Schemes in Multiprotocol Label Switching Networks\*

Seunghun Oh\*\*, Younghan Kim\*\* *Regular Members*

요 약

본 논문은 네트워크상에 발생된 오류를 MPLS(Multi-Protocol Label Switch)기반에서 복원할 수 있는 보호복구 기법을 분석하고, 이들 기술들을 조합하여 실제 적용이 가능한 세 가지 복원서비스 모델들 즉, 알람메시지기반 보호서비스와, 트래픽역류 보호서비스, 그리고 1+1 보호서비스를 정의하였다. 정의된 서비스들의 정성적 비교와, 시뮬레이션을 이용한 정량분석을 하였다.

분석된 결과로 1+1 보호서비스모델이 가장 신속하고 손실 적은 복원 서비스를 보장하였다. 그러나 망의 전체 자원 소비량과, 제어 트래픽의 비율이 높아 망 효율성면에서 저조하다. 이에 반해 알람메시지기반 보호서비스 모델은 망 자원을 가장 적게 소비하고 적은 제어 트래픽을 발생시켜 망의 효율성을 극대화 할 수 있었으나, 복원서비스 품질 차원에서는 가장 저조하였고, 트래픽역류 보호서비스모델은 알람메시지기반 보호서비스와 1+1 보호서비스의 중간 단계의 복원서비스와 망 효율성을 나타냈다.

### ABSTRACT

This paper investigates the restoration schemes which are applied to the MPLS domain upon a network failure. We define the following three restoration service models by combining the various restoration schemes: "FIS-based protection service" (FIS: failure indication signal), "inversion traffic protection service" and "1+1 protection service". After a qualitative analysis of the performance in them, we have analyzed it on quantitative basis by the simulation.

According to the simulation results, "1+1 protection service" guarantees the fastest and most lossless restoration service among them; however, it results in consuming considerable bandwidth and producing an amount of control traffic, which means poor network utilization. On the other hand, "FIS-based protection service" spends less bandwidth and generates less control traffic, which means better network utilization, but produces poor restoration service. "Inversion traffic protection service" provides the medium restoration service and utilization between "1+1 protection service" and "FIS-based protection service."

### I. 서론

MPLS기술은 트래픽 엔지니어링이 가능하고, 다양한 하위 네트워크 기반구조를 제어할 수 있다는 점들

때문에 인터넷세상에서 중요한 기술로 급속도로 발전하고 있다. 이와 함께 망의 오류 시에도 이를 복구하여 트래픽의 안전한 전달을 보장해주기 위한 다양한 보호복구 기술들이 IETF를 중심으로 연구되고 있다<sup>[1-4]</sup>. 본 논문은 이들이 논의하고 있는 개별 기술들을

\* 본 논문은 한국과학재단의 OIRC과제의 지원에 의해 수행된 결과입니다.

\*\* 숭실대학교 정보통신전자공학부

논문번호 : 020092-0226, 접수일자 : 2002년 2월 26일

비교분석하고 종합하여 실제 망에 적용할 수 있는 복합된 보호복구 서비스들을 정의하고 분석하였다.

조합된 방법으로 다수의 일반사용자들에게 복원서비스를 제공하기 위한 ‘알림메시지 기반 보호서비스’와 소수의 고급 사용자들의 요구를 만족시키기 위한 ‘1+1 보호서비스’, 마지막으로 두 보호서비스의 중간 성능을 갖는 ‘트래픽역류 보호서비스’를 정의하였다. 제시된 서비스모델들은 시뮬레이션을 통해 복원시간, 손실률, 망의 자원 사용률, 트래픽 분산정도 그리고 복원에 사용되는 제어 메시지의 비율 등의 항목들을 비교하여 각각의 관계를 고찰하였다<sup>5)</sup>.

서론에 이어 2 장에서는 MPLS망의 개별적인 보호 복구 기술과 이들을 응용한 세 가지 보호서비스 모델들을 정의한다. 이어서 3 장에서는 정의된 서비스 모델들에 대해서 비교 항목을 정의하고 이를 기반으로 정성적인 특성을 고찰하였다. 이어서 정량적인 해석을 위해 시뮬레이션을 이용하여 실험 하였고 마지막으로 결론을 맺는다.

## II. MPLS망의 보호 복구 기술

MPLS의 오류 보호복구기술은 오류를 복원하는 절차를 따라 크게 세 가지 방법으로 구성된다. 우선 네트워크 상에 발생한 오류를 감지하기 위한 오류검출 기술(Fault-Detection), 오류의 영향 받을 수 있는 동작경로 상의 노드들과 복원을 책임지는 노드에게 오류를 알리는 오류알림 (Fault-Indication)과 원래의 동작경로가 오류가 제거되었음을 알리는 회복알림 (Fault-Recovery)으로 이루어진 알림기술, 그리고 적절한 대체경로로 트래픽을 절체 시켜야 하는 복원스위칭과, 복원된 트래픽을 원 경로로 스위칭시키는 회복스위칭이 있다<sup>5)</sup>. 본 논문에서는 오류 발생 후 트래픽의 절체에 초점을 맞추고 회복알림과 회복스위칭에 대해선 고려하지 않았다.

그림 1은 MPLS망에서 동작경로를 보호하기 위한 망의 구성을 보여주고 있다. 하나의 동작경로와 상응하는 보호경로 그리고 두 경로가 분기되는 PSL(Path Switching LSR) 과 다시 두 경로가 합쳐지는 PML(Path Merging LSR)이 있다. 그림 1과 같이 동작경로와 대체경로 그리고 PML, PSL로 이루어진 구역을 보호 도메인이라고 한다. 또한 이 보호도메인 상에서 발생하는 오류를 알려주기 위한 메시지의 경로를 RNT(Reverse Notification Tree)라 하며, RNT는 동작경로와 물리적으로 같은 경로위에 설정되나 메시지가 전달되는 방향은 반대가 된다<sup>5)</sup>.

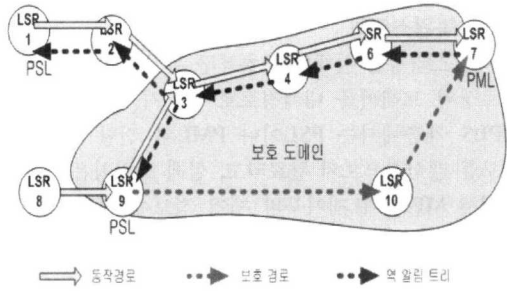


그림 1. MPLS의 보호도메인의 구성

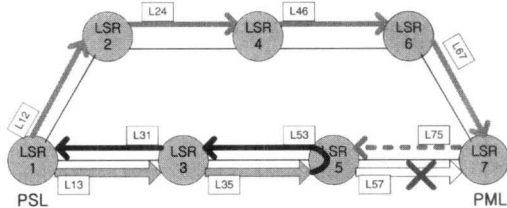


그림 2. 트래픽 역류 알림방법

### 1. 오류 검출(Fault Detection)

오류검출방법은 네트워크 각 계층별로 존재한다. IP(MPLS 계층)계층에서는 물리적인 검출<sup>6)</sup>대신 논리적인 검출이 이루어진다. 대표적인 논리적 검출방법은 주기적으로 확인 메시지(예: liveness Message)를 보내서 링크를 조사하는 방법으로서 오류가 발생한 패킷의 개수를 세어서 특정 임계값과 비교하거나 확인 메시지가 도달하지 않는 시간간격을 특정 임계시간과 비교하는 방법 등이 있다<sup>5)</sup>.

### 2. 알림기술(Indication)

알림기술이란 오류발생과 오류 회복됨을 이에 영향을 받는 모든 노드에게 알리는 기술로서 메시지를 이용하는 방법과 트래픽역류에 의한 방법이 있다<sup>2,5)</sup>.

메시지 이용방식에서는 오류알림 메시지(FIS: Fault Indication Signal)를 동작 링크 상에 오류를 검출한 노드들 중 업스트림 방향에 위치한 노드가 생성하여 이 오류의 영향을 받는 모든 LSR들로 전송한다. 이 메시지의 전달경로는 그림 1에서 설명한 RNT이다<sup>5)</sup>.

트래픽역류에 의한 오류 알림방법은 오류를 검출한 노드가 FIS 대신 오류에 영향을 받을 트래픽을 동작경로의 역 방향으로 PSL까지 역류시켜 오류 발생을 알린다<sup>2)</sup>.

이 때 트래픽을 역류시킨 노드부터 PSL까지 경로를 최초 복원 경로라 하고, 원래 복원경로는 최종 복원경로라 한다.

### 3. 복원스위칭

복원스위칭을 실제의 보호복구 동작 기술로서 동작 경로상의 트래픽을 대체경로로 대체시키는 것이다<sup>[5]</sup>. MPLS 계층에서는 PSL이나 PML의 전달 테이블의 정보를 갱신함으로써 완료되고, 실제 스위칭은 하부계층에서 MPLS의 제어부의 제어 정보에 따라 이루어진다<sup>[6]</sup>.

### 4. 보호 복구 기술의 분류

MPLS의 보호복구 기술들은 크게 동적-재-경로설정(dynamic rerouting)방식과 보호-스위치(Protection switch)방식이 있다. 본 논문에서는 보호도메인을 형성하기 위해 대체경로를 사전 설정한 보호 스위칭방식을 고찰하였다<sup>[5,8]</sup>.

또한 보호복구가 수행되는 범위에 따라 그림 3과 같이 지역 회복(local restoration)과 전역 회복(global restoration)방식으로 구분된다. 오류가 발생한 지점에 바로 근접한 두 노드사이에서 오류복원이 수행되는 방법을 지역 회복방식이라 하고, 동작경로와 물리적으로 겹치지 않는 경로로 복원이 수행되는 방법을 전역 회복방식이라고 한다. 지역 회복은 신속한 복원을 보장하며, 동작 노드상의 다른 노드들에게 영향 없이 복원을 수행할 수 있다.

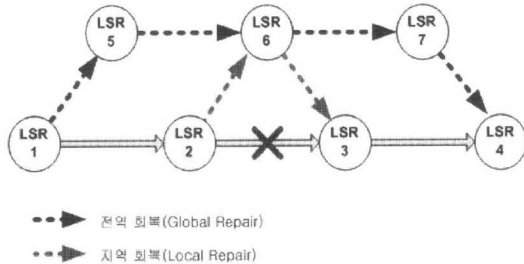


그림 3. 지역 회복과 전역 회복 방식

한편 동작경로와 대체경로 상에 트래픽을 전송하는 방법을 두 경로의 매핑이라고 정의하고, 크게 1+1 매핑과 1:1 매핑으로 나눈다. 한편, 1:M 과 N:M 매핑은 1:1과 같은 개념으로써 경로 상에 매핑 시킨 동작경로와 대체경로의 수가 차이가 있다. 1+1 매핑은 동작경로 및 대체경로에 동시에 동일 트래픽을 전송하게 하는 방식이다. 이 경우 수신되는 같은 두 트래픽을 두 경로가 서로 만나는 지점에 위치한 PML이 하나를 선택하게 된다. PML의 선택은 오류알림 메시지가 수신함에 따라 이루어지므로 오류알림 메시지(FIS)가 PML 쪽으로 전달되어야 한다. 1:(1:M, N:M)매핑은 동작

경로 상에 오류가 발생 후 알림메시지가 PSL에 도착하자마자 PSL에서 동작경로의 트래픽을 대체경로로 스위칭하는 복원 방식이다<sup>[5]</sup>.

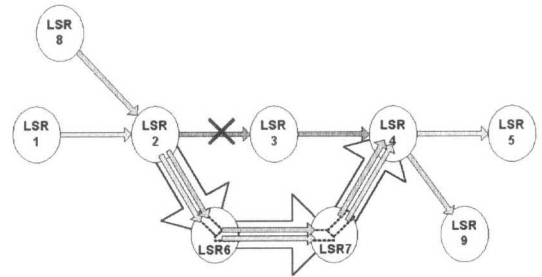


그림 4. 터널링을 이용한 다수의 동작경로 복원

1:M과 N:M의 방법에서 다수의 동작경로를 복원하기 위해서 MPLS 레이블 스택킹 (stacking)을 사용한 우회(bypass) 터널링을 이용한다<sup>[9]</sup>. 이 때에는 그림 4에서와 같이 터널링으로 보호될 다수의 동작경로의 LSP들을 머징 LSR (LSR4)에서 구별할 수 있어야 한다. 그러므로 터널링이 시작하는 노드 (LSR2)에서 레이블 정보를 푸시 (push)하여 머징 노드까지 전달하는 방법이 이용 된다<sup>[9]</sup>.

동작경로상의 LSP들 중 짧은 지연시간을 요구하는 서비스들이 있을 수 있다. 이런 특정 지연 경계치를 요구하는 서비스를 만족시키기 위해 오류의 지역화 (Fault localization)가 필수적이다. 여기서 오류의 지역화는 지역회복과 비슷하게 오류 발생지점에 가까운 노드에서 복원을 책임지는 것이다. 그림 5는 오류의 지역화를 위한 하나의 해결책을 보여 주고 있다. 동작 경로 상에의 특정 노드에서부터 PML에 이르는 단거리 LSP들을 사전에 설정한 후 높은 서비스 품질을 요구하는 FEC들의 정보를 유지관리 한다. 이 경로를 지름길 LSP라 하고, 오류가 발생하면 이 LSP를 통해 복구함으로써 요구되는 지연 경계치를 만족시킬 수 있다<sup>[2]</sup>.

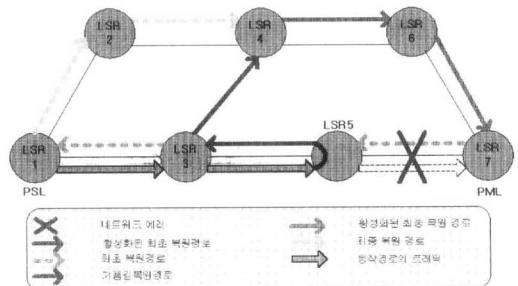


그림 5. 오류 발생 시 지름길을 이용한 지름길복원 방법



표 1. 복원 기술의 구분 방식

복원 모델	재-경로-설정(rerouting)	보호-스위칭
복원 범위	지역 복원	전역 복원
경로매핑	1:1( 1:N, M:N )	1+1
대체경로의 자원	고정 자원방식	타 트래픽 허용 방식
오류알림기술	메시지사용 방식	트래픽역류 방식

표 1 은 이상의 복원기술방법들을 정리한 것이다.

5. 통합 보호서비스들

표 1에 나열된 방법들을 조합해서 세 가지 보호서비스들을 정의했다. 재 경로 설정 방법의 성능은 복원 기법의 성능보다는 적용된 라우팅의 특성에 따라 성능이 좌우되고, 대체경로의 자원의 활용방법도 자원에 약 호처리의 기법에 따라 좌우된다. 그러므로 이 보호 서비스를 정의함에 있어 현실적으로 복원성능에 영향이 비교적 큰 경로매핑 방법과 오류 알림 기술들을 변형하여 고려하였다.

5.1. 알림메시지기반 보호서비스

알림메시지기반 보호서비스는 PSL과 PML사이의 동작경로의 대체경로를 사전에 설정해 놓고 동작경로 상에 오류발생시만 대체경로를 사용하는 방법이다. 오류알림 기술은 특정 제어 메시지(FIS: fault indication signal)를 이용하여 복원스위칭하는 노드(PSL)에게 전달하게 된다<sup>[5]</sup>.

5.2. 트래픽 역류 보호서비스

트래픽역류 보호서비스는 알림메시지기반 보호서비스와 같이 PSL과 PML사이의 전역경로를 보호하며 대체경로는 오류 발생시에만 사용하는 서비스이다. 그러나 오류알림 기술은 오류가 발생한 지점에 PSL방향으로 존재하는 이웃노드가 오류를 발견 후 바로 트래픽을 PSL까지 역류시키는 방법을 사용한다<sup>[2]</sup>.

5.3. 1+1 보호서비스

1+1 보호서비스는 알림메시지기반 보호서비스의 1:1 경로매핑방법 대신 1+1 경로매핑방법을 사용한 방식이다. 이 방식에서는 오류알림 메시지가 알림 메시지기반 보호서비스의 전달 방향과 반대인 PML로 전달된다<sup>[5]</sup>.

III. 정성적 비교

분류된 보호 복구 방법은 다음의 항목에 따라 비교

하였다<sup>[10]</sup>.

**복원 시간(Recovery time):** 오류 발생 후 복원 경로가 활성화되어서 복원된 트래픽의 첫 번째 패킷이 PML에 도착할 때까지 소요된 시간을 의미한다. 복원시간은 세부적으로 오류 검출하는데 걸리는 시간, 하위 계층에 신속한 복원의 기회를 제공하는 시간, 복원스위칭을 수행하는 LSR에게 오류를 알리는데 걸리는 시간, 복원스위칭이 수행되는 시간, 복원스위칭된 트래픽이 복원되어 PML에 도달하는 시간 등으로 구성된다

**패킷손실률 :** 네트워크에 발생한 오류를 복원하는 동안 발생하는 패킷 손실을 의미한다.

**자원 활용도(Resource Utility) :** 망의 오류를 복원하는데 소비되는 자원의 량을 측정하여 그 효율성을 가늠할 수 있다.

**제어 트래픽 비율 :** 망상의 총 트래픽 중 제어 용도로 사용된 트래픽의 량을 나타낸다.

**트래픽 분산 정도:** 복원과정 동안 네트워크상에 트래픽의 분산 정도를 나타낸다.

1. 복원시간

복원시간의 구성 요소 중 오류검출 시간과 오류를 알리는 시간 그리고 대체경로를 따라 트래픽을 PML까지 전달하는 데 걸리는 시간이 주된 영향을 주는 항목이다. 위에 정의된 세 가지 보호서비스들은 같은 오류 검출 방법을 택하였기 때문에 오류검출시간의 차이는 없다.

오류알림 시간은 세 가지 보호서비스를 마다 각각 다르다. 메시지기반 보호서비스와 트래픽역류 보호서비스의 오류알림 시간은 오류발생 지점에서부터 PSL까지 거리에 좌우되는 반면에, 1+1 보호서비스의 오류알림 시간은 PML까지의 거리에 좌우된다.

트래픽의 복원시간은 PSL에서 PML까지의 대체경로의 거리에 따라 다르다. 그러나 1+1 보호서비스에서는 트래픽이 두 경로로 동시에 전달되므로 PML이 오류알림 메시지를 수신하자마자 바로 대체경로의 트래픽을 선택함으로써 가장 빠른 트래픽의 복원시간을

갖게 된다.

### 2. 패킷 손실률

복원과정에 있어 손실되는 패킷은 크게 오류발견 시간동안과 오류알림 시간동안 발생하는 것으로 구분할 수 있다. 첫 번째 경우는 확인 메시지의 주기를 얼마로 설정하는가에 따르며 세 가지 보호서비스는 동일 방식을 사용하므로 차이가 없다. 이에 반해 두 번째 경우는 다른 방식을 사용하므로 영향을 미친다. 알림메시지기반 보호서비스에서는 알림 메시지가 PSL까지 전송되는 동안 동작경로에 존재하는 패킷들이 손실된다. 그러나 트래픽역류 보호서비스에서는 이미 도착한 패킷들을 반대방향으로 역류시킴으로써 패킷 손실을 막게 된다<sup>2)</sup>. 1+1 보호서비스의 경우는 PML까지 패킷들이 두 경로를 통해 전달됨으로 오류알림 과정이 끝나면 손실 없이 이어지는 대체경로의 트래픽 때문에 손실률이 최저가 된다.

### 3. 자원 활용도(Resource Utility)

알림메시지기반 보호서비스는 1:1 경로매핑을 채택하였기 때문에 실질 데이터 트래픽이 동작경로 또는 대체경로에만 존재한다. 또한 트래픽역류 보호서비스도 1:1 경로매핑을 채택했지만, 트래픽을 PSL까지 역류시키는 최초 보호경로와 최종 대체경로로 트래픽이 복원됨으로 알림메시지기반 보호서비스 보다 더 많은 자원을 소비하게 된다. 즉, 오류발생지점에서 PSL까지 거리에 따라 트래픽이 역류하는 구간인 최초 보호경로의 길이에 따라 좌우된다.

소비자자원량을 줄이기 위해서는 지역복원이 되어야 한다. 지역복원은 하부 계층에서 이웃 노드사이에 물리적인 대체 링크를 이용하여 가능케 할 수도 있고, 오류 발견노드에서 직접 복원할 수 있는 지름길 방법을 이용할 수도 있다<sup>2)</sup>.

### 4. 제어 트래픽 비율

복원을 위한 제어 트래픽의 종류는 먼저 네트워크의 오류 검출을 위한 확인 메시지와 오류알림 메시지, 및 확실한 복원을 위해 대체경로로 미리 전송되는 패킷들이 될 수 있다. 미리 전송되는 패킷들은 실질적인 데이터 이외에 복원의 목적으로 전송됨으로 제어 트래픽으로 분류하였다. 그러므로 별도의 트래픽을 가장 많이 발생하는 1+1 보호서비스가 가장 제어 트래픽 비율이 높다. 또한 트래픽역류 보호서비스의 경우 오류알림 기술로 제어 트래픽 대신 역류한 데이터 트래픽을 이용하기 때문에 알림메시지기반 보호서비스보다 제어트래픽 비율이 작다.

### 5. 트래픽 분산정도

이 항목은 대체경로를 계산하는 QoS 라우팅 알고리즘에 따라 달라질 수 있으며 동일 환경에 있어서는 같은 대체경로라 할지라도 1+1 보호서비스는 여분의 트래픽의 영향으로 분산정도가 나쁘게 나타난다. 또한 트래픽역류 보호서비스는 최초 복원 경로 상으로 복원된 트래픽의 영향으로 알림메시지기반 보호서비스보다는 분산정도가 뒤질 것이다.

## IV. 정량적 비교 분석

### 1. 시뮬레이션 모델

그림 6과 같은 모델 망을 통해 정성적으로 비교한 세 가지 복원서비스들의 성능을 정량적으로 비교하였다. 그림 6에서 노드 1과 7을 각각 PSL, PML로 하여 두 개의 보호 도메인을 형성하였다. 그리고 두 개의 동작경로(1-12-13-3-5-7, 1-15-14-9-10-7)의 보호를 위해 물리적으로 공통적인 대체경로(1-2-4-6-7)를 설정하였다.

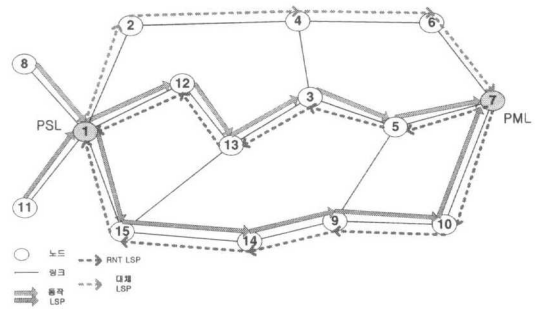


그림 6. 시뮬레이션 네트워크 모델

본 실험에 사용된 톨은 C-언어로 구현된 Event-driven방식의 시뮬레이터로서 전송속도와 노드의 처리속도 등의 모든 처리시간을 실제 데이터를 바탕으로 사전 설정 후, Event들의 가상시간에 따라 스케줄링 되어 처리된다. 네트워크의 복원 성능 측정을 위해 트래픽을 각각 2Mbps, 1Mbps의 CBR(constant bit rate)로 노드 8과 11에서 발생시켰다. 모델 네트워크 상의 모든 링크의 길이와 대역폭은 500km, 10Mbps로 같다고 가정하였고, 비교를 극대화 하기위해 당대적으로 큰 값을 선정하였다. 또한 각각의 노드에서 데이터 처리하는 데 걸리는 시간을 1msec로 단순화하였다. 본 실험에서 비교를 위한 기타 매개변수들은 확인 메시지 발생주기, 노드의 확인 메시지 검사주기, 그리고 오류를 발생하는 링크위치와 발생시간 등이

있다. 특히, 오류발생 링크위치와 발생시간은 복원성능에 영향이 미치므로 동작경로상의 모든 링크에 발생시간을 달리하면서 에러를 발생시켰을 때 얻은 값들의 평균값을 취하여 데이터로 사용하였다.

복원시간은 에러가 발생한 지점으로부터 PML이 처음으로 복원트래픽을 받은 시간을 뺀 값으로 데이터를 얻었고, 손실률은 PML이 데이터의 순차번호를 기록하여 얻었다. 자원활용도와 제어트래픽비율 그리고 트래픽의 분산정도는 각 링크의 트래픽량을 측정하여 얻은 데이터들이다. 특히 트래픽의 분산정도는 각 링크의 트래픽량의 평균값을 이용하여 분산을 계산하였다. 이런 방식을 타이머의 검사주기를 변경하면서 데이터를 얻었고, 이 값들을 Xgraph-툴을 이용하여 그래프를 만들었다.

## 2 결과 분석

### 2.1 복원시간

그림 7에 확인 메시지 검사주기에 따른 복원시간을 나타냈다. 정성 비교의 결과와 같이 1+1 보호서비스에서 사용한 1+1 경로매핑 방법이 가장 빠르게 오류를 복원함을 볼 수 있다. 메시지 확인주기를 120 msec로 하였을 때 메시지기반 보호서비스는 97 msec, 트래픽역류 보호서비스는 94 msec, 1+1 보호서비스는 92msec 가 각각 소요되었다. 모든 보호기법의 복원시간은 확인 메시지 검사주기에 크게 영향을 받으며 오류를 검출하는데 걸리는 시간에 큰 영향을 가지고 있음을 보여주고 있다.

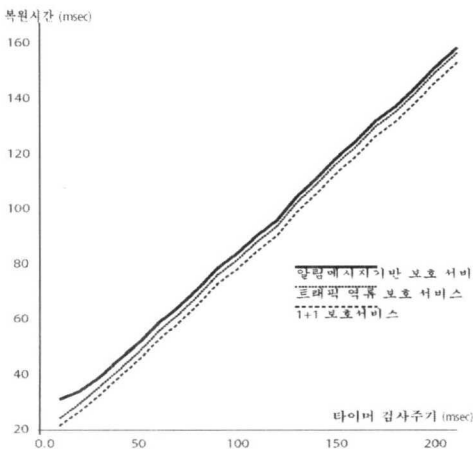
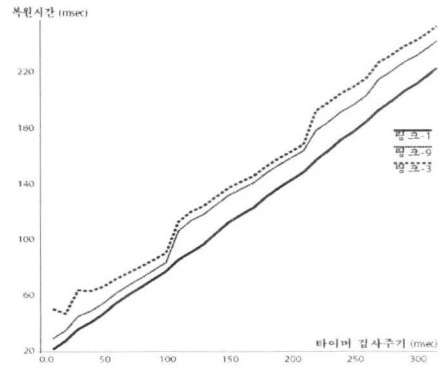


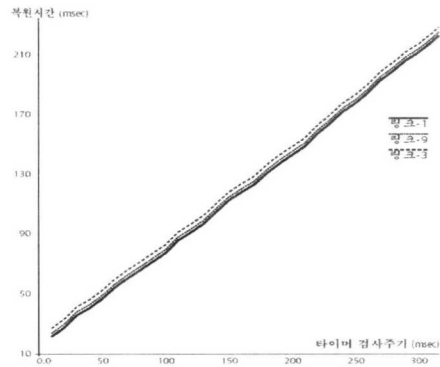
그림 7. 확인 메시지 검사주기에 따른 복원시간

그림 8은 PSL과 PML사이에서 오류 발생 링크의 위치에 따라서 복원시간의 변화를 나타낸 것이다. 링

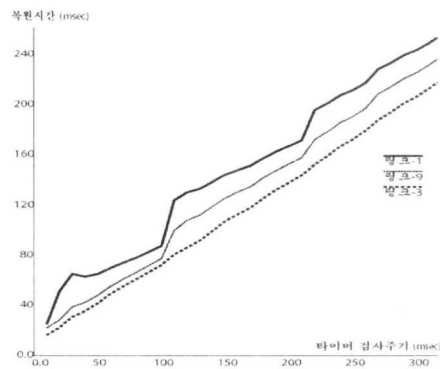
크1은 PSL에, 링크3은 PML에 가깝게 위치하고, 링크 9는 중간에 위치하고 있다. 그림에서 트래픽역류 보호서비스의 복원시간은 오류 발생 링크의 위치에 큰 영향을 받지 않음을 알 수 있다. 그러나 알림메시지기반 보호서비스는 오류링크가 PSL에 가까이 있을 때 복원시간이 짧고, 1+1 보호서비스는 PML에 가까울 때 복원시간이 짧아짐을 보여 주고 있다.



(a) 메시지기반 보호서비스



(b) 트래픽역류 보호서비스



(c) 1+1 보호서비스

그림 8. 복원 방법별 오류발생 위치에 따른 복원시간



2.2 패킷 손실률

패킷 손실률은 복원시간에 큰 영향을 받는다. 즉, 오류를 복원을 하는 동안 패킷이 손실되기 때문에 복원시간이 길수록 손실이 많아지기 때문이다. 그림 9은 보호서비스의 패킷 손실률을 나타내고 있다. 특이한 점은 1+1 보호서비스의 손실률이 트래픽역류 보호서비스의 것보다 높게 나타나고 있다. 그 원인은 PML에서 선택되어 있지 않은 인터페이스로 수신한 패킷들을 다른 상태정보 없이 무조건 제거하였기 때문이다. 무 손실 복원을 위해서는, PML에서 수신한 패킷들의 순차번호 등을 검사 확인하고 그 패킷의 중복된 패킷을 수신할 때까지 저장하고 있어야 한다.

손실률이 단순히 복원시간의 영향에 비례한다는 사실이 트래픽역류 보호서비스에 적용되지 않았다. 이 서비스의 복원시간 그래프는 알림메시지 기반 보호서비스의 그래프에 가깝게 나타난 반면 (그림 7), 패킷 손실률 그래프는 1+1 보호서비스에 더욱 근접해 있다 (그림 9). 이 현상의 원인은 트래픽역류 보호서비스를 사용하여 오류알림 시간동안 발생한 손실을 없앴기 때문이다.

그림 10은 그림 8과 같이 오류 링크의 위치에 손실률이 변화를 보여주고 있다. 오류링크의 위치에 따른 복원시간의 것 같은 결과를 보여주고 있다. 그러나 트래픽역류 보호서비스의 패킷 손실률은 오류링크의 위치에 전혀 영향을 받지 않는 것이 다른 점으로 보여지고 있다. 이는 트래픽역류 보호서비스에서는 오류알림 시간동안 발생하는 손실률을 제거했기 때문이다.

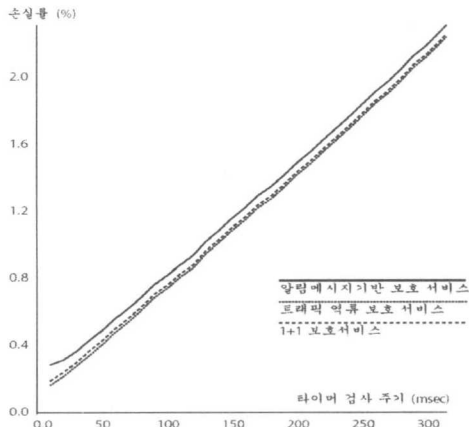
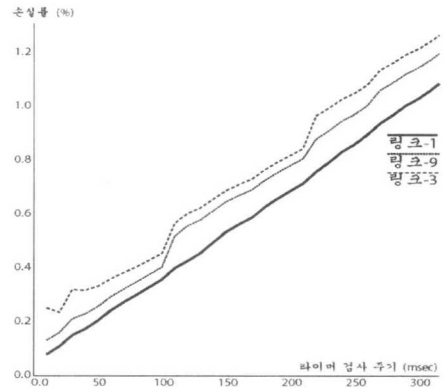


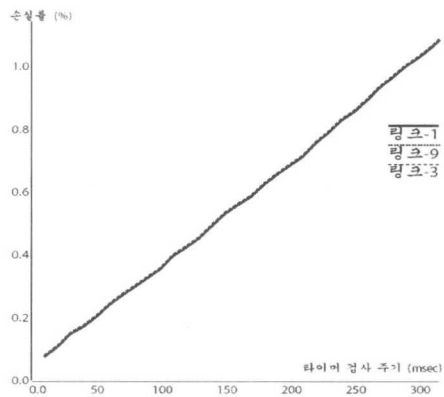
그림 9. 패킷 손실률

2.3 자원 활용도

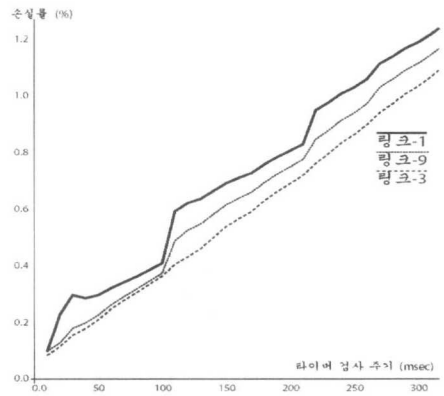
복원 과정을 포함한 일정 시간동안 발생된 모든 트



(a) 알림메시지기반 보호서비스



(b) 트래픽역류 보호서비스



(c) 1+1 보호서비스

그림 10. 복원 방법별 오류발생 위치에 따른 패킷 손실률

래픽으로 소비된 자원량을 측정된 결과를 그림 11에 나타냈다. 그림에서 보듯이, 1+1 보호서비스가 가장 많은 자원을 소비하고 있다. 트래픽역류 보호서비스가 다음으로 많이 소비하고 있다. 그럼으로 사업자 입장

에서는 자원활용도를 극대화하기 위해선 알림메시지 기반 보호서비스를 대중적으로, 1+1 보호서비스를 특수 사용자에게만 적용해야 한다.

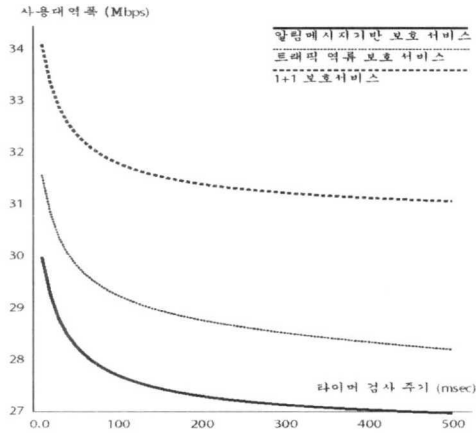


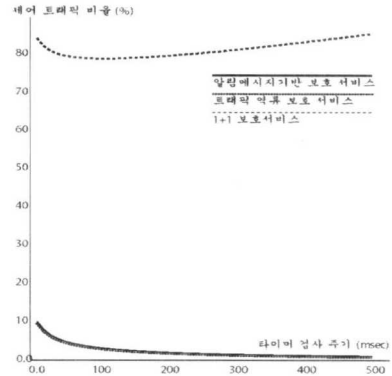
그림 11. 자원활용도

한편 본 실험에서는 확인 메시지 확인주기와 확인 메시지 생성주기를 변화시켜서 메시지 생성 주기를 확인주기의 특정 값보다 작게 했을 때 소비자원량이 급격하게 증가됨을 확인할 수 있다. 이를 통해 확인 메시지를 생성주기는 확인주기에 비해 적절한 값 이상으로 하는 것이 유용함을 알 수 있었다. 그러나 오류검출시간과는 trade off 관계가 있다.

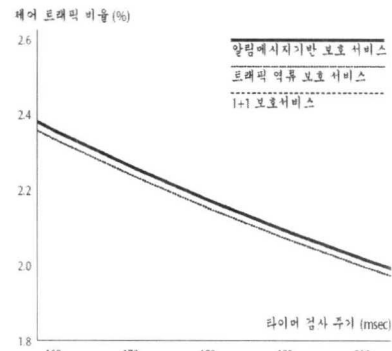
2.4 제어 트래픽의 비율

그림 11의 총 트래픽량은 실제 데이터 트래픽과, 제어 트래픽으로 분류된다. 여기서 실제 데이터 트래픽은 수신 측에서 순수하게 데이터로 인정되는 것이다. 그림 12에서 1+1 보호서비스의 제어 트래픽의 비율이 다른 보호서비스들에 비해 상당히 높은 것을 알 수 있다. 이것은 1+1 보호서비스에서 PML이 수신한 중복된 트래픽이 복원을 위한 제어 트래픽으로 간주되었기 때문이다.

그림 12-(b)는 알림메시지기반 보호서비스와 트래픽역류 보호서비스의 차이를 보이기 위해 확대한 것으로, 트래픽역류 보호서비스는 오류알림을 위한 제어



(a)



(b)

그림 12. 데이터와 제어 트래픽 비율

메시지를 생성하지 않으므로 알림기반 보호서비스보다 낮게 나타나고 있다.

2.5 트래픽 분산정도

각 링크별 트래픽을 측정된 결과를 이용하여, 트래픽 분산정도를 확인하였다. 트래픽 분산은 대체경로를 설정할 때 고려된 라우팅 알고리즘에 의해 결정된다. 그러나 논 실험에서는 정해진 환경에서 링크별 트래픽 분산 정도로만 이를 고찰하였다. 그림 13에서 1+1 보호서비스가 트래픽이 가장 불균형을 이루고 있음을 보여준다.

표 2. 보호서비스별 종합적인 비교

보호서비스	비교항목	복원시간	손실률	자원활용도	제어트래픽 비율	트래픽 분산정도
알림메시지기반 보호서비스		가장 길다	가장 크다	가장 좋다	작다	가장 좋다
트래픽역류 보호서비스		중간	가장 작다	중간	가장 작다	중간
1+1 보호서비스		가장 짧다	작다	가장 나쁘다	가장 크다	가장 나쁘다



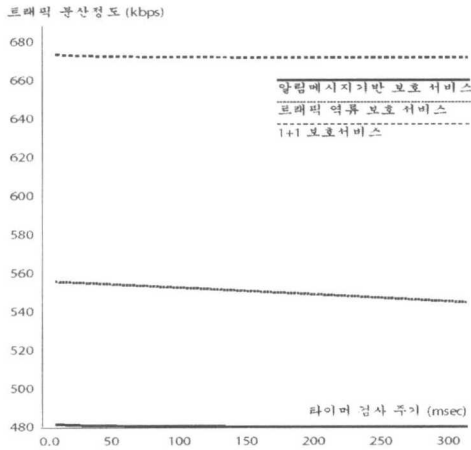


그림 13. 트래픽 분산정도

이상의 개별 시뮬레이션 결과를 표 2에 종합적으로 정리하였다. 첫 번째 두 번째 비교항목은 사용자 서비스 차원을 고려했다면, 나머지는 사업자차원을 고려한 사항이다. 1+1 보호서비스는 좋은 서비스를 제공할 수 있는 반면에 사업자 입장에서 망 전체적인 효율이 떨어진다. 트래픽역류 보호서비스는 상대적으로 중간 성능을 보여주고 있으나, 손실률 면에서는 1+1 보호 서비스를 능가하였다.

### V. 결론

본 논문은 네트워크상에 발생된 오류를 MPLS (Multi-Protocol Label Switch)기반에서 보호복구 기법을 분석하고, 이들 기술들을 조합하여 실제 적용이 가능한 세 가지 복원서비스 모델들 즉, 알림메시지 기반 보호서비스와, 트래픽역류 보호서비스, 그리고 1+1 보호서비스를 정의하였다. 정의된 서비스들의 정성적 비교와, 시뮬레이션을 이용한 정량적 분석을 하였다.

분석 결과, 사용자 차원에서 1+1 보호서비스 모델이 상대적으로 가장 좋은 성능을 보였다. 즉 오류가 발생했을 때 1+1 보호서비스를 적용하여 손실률을 줄이면서 빠르게 복원할 수 있다. 또한 손실률의 향상을 위해서는 PML에서 중복 패킷을 수신할 때까지 패킷들의 순차번호를 저장·유지해야함을 알 수 있었다. 그러나 이러한 번호 관리는 실제 망에 적용하기에는 어려운 부분일 것이다.

사업자 입장에서 메시지 기반 보호서비스 모델과 트래픽역류 보호서비스 모델은 자원 활용 면에서 우수하게 나타났다. 트래픽역류 보호서비스 모델은 제어 트래픽량이 알림메시지 기반 보호서비스 모델보다 적

었지만, 전체적인 자원 소비량은 더 많고, 트래픽 분산에서도 상대적으로 높아 알림메시지 기반 보호서비스 보단 활용도 면에서 뒤진다. 종합적으로 트래픽역류 보호서비스는 비교적 양호한 서비스를 제공할 뿐만 아니라, 중간단계 망 활용도를 나타냈다. 이와 같이 보호복구기법에 따른 사용자 품질의 차별화는 다른 형태의 사용자 차별화 서비스방법으로도 적용될 수 있을 것이다.

### 참고 문헌

- [1] Li Mo, "General Considerations for Bandwidth Reservation in Protection," IETF Draft, Jul. 2000. draft-mo-mpls-protection-00.txt.
- [2] Dimitry Haskin, et.al., "A Method for setting an Alternative Label Switched Paths to Handle Fast Reroute," IETF Draft, Nov. 2000. draft-haskin-mpls-fast-reroute-05.txt.
- [3] Ken Owens, Srinivas Makam. et. al., "A Path Protection/Restoration Mechanism for MPLS networks," IETF Draft, Nov. 2000. draft-chan-mpls-path-protection-02.txt.
- [4] Thomas M. Chen and Tae H. Oh, "Reliable Services in MPLS," IEEE Comm Magazine 11 1999, pp. 58-62.
- [5] Vishal Sharma, Ben-Mach Crane, et. al., "Framework for MPLS-based Recovery," IETF Draft, Jul. 2001. draft-ietf-mpls-recovery-firmwrk-03.txt.
- [6] Andrea Fumagalli and Luca Valcarengi, "IP Restoration vs. WDM Protection Is There an Optimal Choice?," IEEE Network Magazine, Nov 2000, pp. 34-41.
- [7] D. Awduche et al., "Multi-Protocol Lambda Switching: Combining MPLS Traffic Engineering Control With Optical Cross-connects," IETF Draft, Nov. 1999. draft-awduche-mpls-te-optical-03.txt.
- [8] Fiffi Hellstrand, et.al., "Extensions to CR-LDP and RSVP-TE for setup of pre-established recovery tunnels," IETF Draft, Nov. 2000. draft-hellstrand-mpls-recovery-merge-01.txt.
- [9] Robert Goguen, Geoge Swallow, et. al., "RSVP Label Allocation for Backup Tunnels," IETF Draft, Nov. 2000. draft-swallow-rsvp-bypass-

label-01.txt.

- [10] John Bicknel, C.Edward Chow, and Sami syed,  
"Performance Analysis of Fast Distributed  
Network Restoration Algorithms," Globecom  
'93 IEEE vol. 3, 1993 pp. 1596-1600.

오 승 훈(Seunghun Oh)   정회원  
2000년 2월 : 숭실대학교 전자공학과 졸업  
2002년 2월 : 숭실대학교 정보통신공학과 석사  
2002년 3월 ~ 현재 : 숭실대학교  
                  정보통신공학과 박사과정

<주관심 분야> 컴퓨터 네트워크, 인터넷 네트워킹,  
                  인터넷 QoS, 광인터넷 복원, 광버스  
                  트스위칭

김 영 한(Younghan Kim)   정회원  
1984년 2월 : 서울대학교 전자공학과 졸업  
1986년 2월 : 한국과학 기술원 전기 및 전자공학과  
                  석사  
1990년 8월 : 한국대학교 전기 및 전자공학과 박사  
1987년 1월~1994년 8월 : 디지콤정보통신연구소 데  
                  이터통신연구부장  
1994년 9월~현재 : 숭실대학교 보통신전자공학부 조  
                  교수  
<주관심 분야> 컴퓨터네트워크, 인터넷 네트워킹,  
                  ATM, 이동 데이터 통신망 등