네트워크 신뢰성

이향원
건국대학교

요 약

본고에서는 네트워크의 신뢰성에 영향을 미치는 요소들을 살펴보고, 네트워크 신뢰성을 보장하기 위한 여러 가지 회복기법들과 다계층 네트워크의 신뢰성을 최대화하기 위한 방법들을 소개한다. 이를 바탕으로 앞으로 네트워크 신뢰성 연구가 나아갈 방향에 대하여 고찰한다.

Ⅰ. 서 론

오늘날의 인터넷 백본망은 10Gbps가 넘는 초고속으로 데이터를 전달할 수 있도록 설계되었다 [13]. 이에 따라, 잠깐 동안의 링크실패(link failure)도 엄청난 양의 패킷 손실로 이어질 수 있기 때문에 네트워크 서비스의 신뢰성을 보장하는 것은 상당히 까다로운 일이다. 여기서 네트워크 신뢰성이라 함은 네트워크에서 링크실패 등이 일어났을 경우에도 사용자가 이것을 느끼지 못하도록 서비스를 계속할 수 있는 능력을 말한다. 즉, 네트워크 실패에 대한 강인성(Robustness)이라 할 수 있다. 본고에서는 네트워크 신뢰성에 관련된 여러 가지 기법들을 소개하고 향후 연구 방향을 토론한다.

네트워크 신뢰성 보장을 위해서는 그림1과 같이 다양한 기술이 필요하다. 먼저, Failure Monitoring 및 Localization 기법은 네트워크에 실패가 일어나는지 Lightpath 등을 이용하여 모니터링하고, 실패가 감지될 경우 네트워크의 어떤 위치에서 실패가 일어났는지 알아낸다. 본고에서는 실패 모니터링 및 위치 파악 기법은 자세하게 다루지 않는다 (이에 관한 자세한 내용은 논문 [14] 및 그 안의 참고문헌 참조).

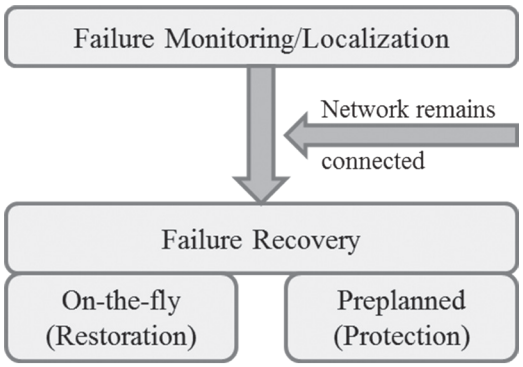

그림 1. 네트워크 신뢰도 보장을 위해 필요한 요소

네트워크의 어느 부분에서 실패가 일어났는지 알게 되면 이후에는 실패회복(Failure Recovery) 기법을 이용하여 실패가 일어난 곳을 지나가던 트래픽을 우회하는 방법으로 서비스를 계속 유지할 수 있도록 한다. 실패회복 기법은 크게 복원기법(이를 많은 논문들에서 Restoration 이라 칭한다)과 보호기법(이를 Protection[1]이라 칭한다)의 두 가지 방식으로 나눌 수 있다. 두 방식은 네트워크 실패로부터 회복하기 위한 자원을 할당하는 방식에 차이가 있다. 첫째, 회복기법은 실패가 일어났을 때 실패회복을 위한 네트워크 자원을 알아내고 그것을 이용하여 트래픽을 우회하는 방식이다. 따라서 미리 자원을 할당하지 않기 때문에 자원의 효율적 사용면에서는 좋으나 실패로부터 회복하는 데 걸리는 시간이 상대적으로 더 오래 걸릴 수 있다 [16]. 반면에, 보호기법은 실패가 일어났을 경우에 사용될 네트워크 자원을 미리 예약(Reservation) 해 놓고 실패 시에 이 자원을 이용하여 트래픽을 우회한다. 따라서, 실패로부터 회복하는 시간을 단축시킬 수 있고, 최근에는 더 빠른 회복을 위해 네트워크 계층이 아닌 MPLS([17])를 이용한 방법이 쓰이고 있다 [16]. 정리하자면, 복원기법은 수십 ms내에 실패로부터 회복해야 하는 여러 어플리케이션의 특성상 많이 쓰이지는 않는다. 이에 따라, 본고에서는 주로 보호기법에 대하여 서술할 것이다.

여기서 한 가지 중요한 점은 실패가 일어났을 경우에 네트워크가 끊어지면, 즉, 어느 한 노드로부터 다른 노드까지의 경로가 존재하지 않게 되면 복원기법이든 보호기법이든 무용지물이 된다는 것이다. 따라서, 네트워크의 연결성을 최대화하는 다르게 말하면 네트워크를 끊기 위해 필요한 실패의 개수를 최대화하는 네트워크 설계가 매우 중요하다. 특히, 네트워크 프로토

1 Restoration과 Protection은 종종 혼용해서 쓰기도 하지만 본문에서 언급한 바와 같이 엄밀하게는 서로 다른 방식의 회복기법을 칭한다. 용어에 관한 더 자세한 사항은 RFC 4427 [15] 참조.

콜처럼 네트워크 토폴로지 또한 계층구조로 되어있고 (예를 들어, IP-over-WDM) 상위계층의 링크들의 하위계층의 하나의 링크를 공유할 수 있어, 하위계층에서 링크 실패가 일어날 경우 여러 개의 상위계층 링크가 끊어질 수 있다. 이는 네트워크 연결성을 최대화 하기 위한 설계문제를 상당히 까다롭게 만드는데 이를 해결하기 위한 또한 본고에서 다룰 것이다.

본고는 다음의 순서로 진행될 것이다. Ⅱ장에서는 네트워크 신뢰성 보장을 위한 보호 문제를 정의하고 다양한 보호기법들을 최근 연구 중심으로 알아본다. Ⅲ장에서는 다계층 네트워크의 신뢰성 최대화 문제를 정의하고 이를 풀기 위한 디자인 기법을 소개한다. Ⅳ장에서는 네트워크 신뢰성 관련 향후 연구방향을 소개하고 마친다.

본고에서는 주로 링크실패를 가정하나, 많은 경우 노트실패 등 다양한 실패 시나리오로 확장할 수 있다.

Ⅱ. 네트워크 보호기법

서론에서 언급하였듯이 네트워크 보호(Protection)방식에서는 실패회복을 위한 자원을 미리 예약해 놓는다. 가장 전형적인 방법은 〈그림 2〉와 같이 경로보호(Path Protection)로서 주어진 송신단-수신단에 대해 주경로(Primary Path)와 백업경로(Backup Path)를 사전에 제공하는 것이다 [32]. 당연히 주경로와 백업경로는 똑 같은 링크를 사용하지 말아야 한다. 왜냐하면 그럴 경우 하나의 링크실패에 의해 두 경로가 모두 끊어질 수 있기 때문이다. 이때 링크를 공유하지 않는 두 경로를 Edge-Disjoint라 하고 이에 따라 경로보호 문제는 그래프 이론에서 고전적인 문제인 Edge-Disjoint 경로문제와 밀접한 관련이 있다.

〈그림 2〉에서처럼 주경로와 백업경로가 Edge-Disjoint 하기만 하면 어떤 하나의 링크실패가 일어나도 견뎌낼 수 있다. 하지만 서로 다른 두 링크가 동시에 끊어지면, 단순한 Edge-Disjoint로는 전송단과 수신단의 연결성을 보장하지 못한다. 이를 해결하려면 단순히 세 개의 경로를 찾으면 되지만 아래에 기술될 비용을 최소화하는 그러한 경로의 집합을 찾는 것을 쉽지 않다 (여러 개의 링크실패로부터 네트워크를 보호하는 문제를 다루는 논문은 많지 않은데 [20]이 하나의 예라 할 수 있다). 이러한 이유로 많은 논문에서는 한 번에 하나의 링크만 실패한다고 가정한다. 이는 문제의 용이성을 위해 단순히 가정하는 것으로 볼 수 있으나 실제로 유선 네트워크에서 링크실패율은 매우 낮기 때문에 충분히 정당화 될 수 있는 가정이라 할 수 있다 [21].

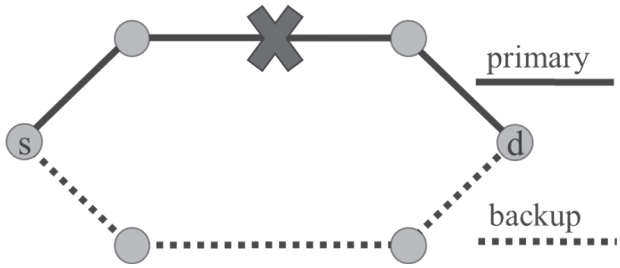

그림 2. 보호기법에서 Edge-Disjoint가 되도록 설정한 주경로와 백업경로 예

신뢰성 보장을 위해 주경로와 백업경로를 다양하게 활용할 수 있다. 예를 들어, 똑 같은 데이터를 주경로와 백업경로에 똑같이 보내게 되면 한쪽 경로에서 링크실패가 일어났다고 하더라도 다른 쪽 경로의 데이터가 수신단에 도달하므로 어떤 링크 하나가 실패하더라도 그것을 견뎌낼 수 있다. 이를 "1+1 보호"라 부른다. 다른 방법으로는 평상시에 주경로에만 데이터를 보내고 링크실패가 일어날 경우 백업경로에 데이터를 보내 서비스를 계속하는 것이 있다. 이를 "1:1 보호"라 부른다 (기타 다른 경로보호 방법은 [15] 참조). 이와 같은 경로보호 방식은 네트워크 자원을 효율적으로 사용한다는 장점이 있지만, 송신단에서 수신단까지의 전체경로를 재설정 해야 하기 때문에 회복까지 시간이 오래 걸린다는 단점이 있다.

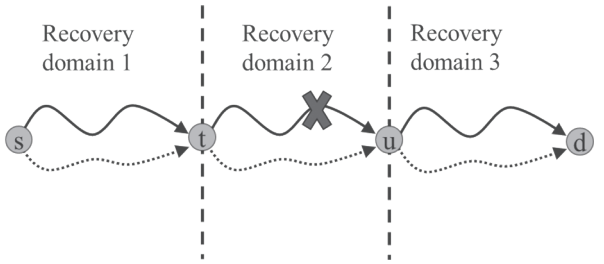

그림 3. Fast Reroute의 예: 하나의 회복 도메인에서 일어난 실패는 그 회복 도메인 안의 자원만을 이용해 회복한다.

이 단점을 극복하기 각각의 주링크(Primary Link) 또는 회복 도메인(Recovery Domain)[2]에 대해 백업경로를 따로 설정하는 Fast Reroute (FRR) 방법이 제안되었다 [18]. FRR은 그림 3에서와 같이 링크실패가 일어났을 경우 그 링크가 속한 회복 도메인의 백업경로로 트래픽을 우회시킨다. 따라서, 전송단까지 경로 재설정이 필요가 없게 되고, 링크실패로부터 회복하기까지 시간을 상대적으로 단축시킬 수 있다 [7].

위에서 언급한 두 네트워크 보호 방식은 모두 자원(예, 링크용량)을 미리 예약해 놓기 때문에 이에 따른 비용문제가 생긴다.

2 회복 도메인은 주경로 상에 있는 하나의 링크가 될 수도 있고, 또는 이웃한 여러 개의 링크들의 집합이 될 수도 있다.

이에 따라 대부분의 네트워크 보호 문제는 다음과 같은 High-Level 포뮬레이션으로 기술할 수 있다.

$$\min_{f} \quad c(f)$$
$$\text{subject to} \quad f \in F_S$$

여기서 f는 평상시의 트래픽 라우팅과 링크실패가 있을 경우의 라우팅을 모두 포함하는 변수이고 목적함수(Objective Function) $c(f)$는 해당 라우팅 f에 따른 비용(Cost)을 나타낸다. 예를 들어, $c(f)$는 라우팅 f를 사용했을 경우 평상시에 트래픽을 서비스하기 위해 필요한 링크용량과 네트워크 보호를 위해 필요한 잉여용량(Spare Capacity)을 사용하는 데 지불하는 비용이 될 수 있다. 위의 포뮬레이션에서 F_S는 네트워크 실패 시에도 전송단과 수신단의 연결성을 보장하는 라우팅의 모든 집합을 나타낸다. 예를 들어, 경로보호에서 F_S는 Edge-Disjoint경로 쌍을 모두 모아놓은 집합을 나타낸다. 따라서 위 문제의 최적해는 네트워크를 실패로부터 보호하면서 최소의 비용을 지불하는 라우팅이 된다.

예를 들어, 〈그림 4,5〉의 두 라우팅은 모두 링크실패 하나를 견뎌낼 수 있다. 즉, 임의의 링크 하나가 끊어지더라도 여전히 송신단-수신단(s-d)는 살아남게 되는 다른 하나의 경로로 데이터를 주고받을 수 있다. 하지만, 각 링크에 적혀있는 숫자가 링크를 사용하는 비용이라고 하면 〈그림 4〉에 있는 라우팅이 〈그림 5〉에 있는 라우팅보다 적은 비용이 들기 때문에 〈그림 4〉의 라우팅을 더 선호하게 된다. 이는 위에서도 언급하였듯이 Edge-Disjoint 경로 문제와 밀접한 관련이 있고 특히 여기서는 최단 Edge-Disjoint 경로문제가 된다. 이 문제는 대표적으로 Suurballe의 알고리듬을 이용해서 풀 수 있다 [33].

위에서는 하나의 송신단-수신단 쌍이 있는 경우만을 다뤘는데, 여러 개의 쌍이 존재하는 경우에도 비슷하게 확장할 수 있다. 다만, 이 때 중요한 문제는 여러 송신단-수신단 쌍들이 백업용량을 공유할 수 있어 어떤 쌍들이 어느 링크의 백업용량를 공유하도록 할 때 비용이 최소가 될 것이냐 이다. 즉, 백업 라우팅이 상당히 까다롭고 복잡해진다. 본고에서는 이에 대해 자세히 다루지는 않는다 (포뮬레이션 및 알고리듬은 [5], [22]-[31]에서 찾을 수 있다).

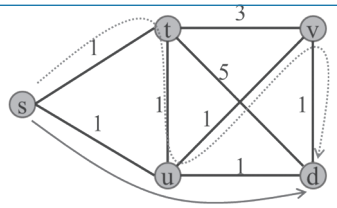

그림 4. 라우팅 1

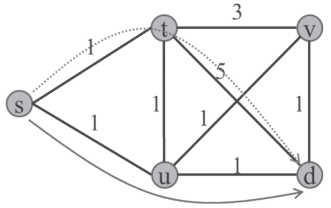

그림 5. 라우팅 2

지금까지는 링크실패가 일어났을 경우 그 링크를 지나가는 트래픽이 100% 다른 경로로 우회할 수 있도록 보장하는 Full Protection 방식에 대해 논하였다. 하지만, 비용 등의 이유로 인해 사용할 수 있는 링크용량이 제한되는 경우에 100%의 트래픽을 링크실패로부터 보호하는 것을 보장하지 못하는 상황이 발생할 수 있다. 이에 따라 최근에는 Partial Protection 즉, 링크실패에 영향을 받은 트래픽의 100%에 대해 회복을 보장하는 것이 아닌 일부분만을 보장하는 연구가 주목 받고 있다 [34]-[43]. 이는 플로우의 QoS 보장과 밀접한 관련이 있다. 즉, 비용을 더 지불하는 트래픽은 실패가 일어났을 때 높은 비율의 트래픽이 보호받을 수 있도록 하여 높은 QoS 보장을 만족시킬 수 있다. 반면에 낮은 QoS 트래픽은 상대적으로 낮은 비율의 트래픽이 링크실패로부터 보호받을 것이다.

〈그림 6-8〉은 Full Protection과 Partial Protection을 비교하고 있다. 먼저, 〈그림 6〉은 s에서 d까지 1만큼의 트래픽이 흐른다고 했을 때 1+1 Full Protection을 하기 위한 라우팅이다. 맨 위쪽의 경로에 1만큼의 주트래픽이 흐르고, 가운데는 1만큼의 용량이 백업으로 존재한다. 이 백업용량을 잉여용량(Spare Capacity)라고도 부른다. 따라서, 필요한 총 링크용량은 2이다. 반면에 〈그림 7〉에서는 1+q Partial Protection 즉, 주경로에서 링크실패가 일어날 경우 그 경로를 지나던 트래픽의 q만큼만을 회복시키는 보호방법이다. 〈그림 7〉에서 q는 2/3이고 따라서 5/3(=1+2/3)만큼의 링크용량이 필요하다. Partial Protection은 낮은 양의 트래픽을 보호하기 때문에 Full Protection에 비해서 낮은 용량이 필요하게 된다는 것을 볼 수 있다. 특히, 특정 라우팅 하에서는 잉여용량이 필요없는 경우도 있다. 예를 들어, 〈그림 6-7〉과 같은 시나리오에서 트래픽을 많은 경로로 나누어 보낼 수 있다고 하자 (이를 Traffic Splitting이라 부른다). 이 때, 〈그림 8〉과 같이 트래픽을 1/3씩 세 경로로 나누어 보내게 되면 잉여용량이 필요하지 않다는 것을 알 수 있다. 즉, 원래 트래픽을 서비스 하기 위해 최소로 필요한 용량인 1이 필요한 총 용량이 된다. Partial Protection문제의 Integer Linear Program 포뮬레이션과 보호받을 트래픽의 양인 q값에 따른 필요용량을 분석한 결과 및 그에 따른 라우팅 알고리듬은 [43]에 자세히 나와있다.

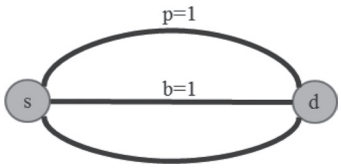

그림 6. 1+1 Full Protection: 필요용량=2

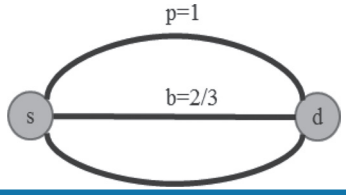

그림 7. 1+2/3 Partial Protection: 필요용량=5/3

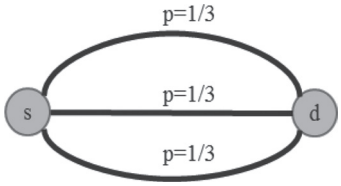

그림 8. 1+2/3 Partial Protection: 필요용량=1

이외에도 링크실패가 확률적으로 일어난다는 가정하에 주경로와 백업경로가 동시에 끊어질 확률이 최소가 되는 경로의 쌍을 찾는 연구는 [6], [8]-[12]에서 찾을 수 있다.

Ⅲ. 다계층 네트워크의 신뢰성

지금까지는 단일 계층 네트워크(Single-Layer Network)에서 네트워크 보호문제를 살펴보았다. 하지만, 실제 네트워크는 프로토콜 상에서 뿐만 아니라 토폴로지 상으로도 계층구조로 이루어져있다. 대표적인 예로는 물리적으로 존재하는 WDM (Wavelength Division Multiplexing) 광네트워크 위에 논리적으로만 존재하는 IP (Internet Protocol) 네트워크를 임베딩시킨 IP-over-WDM 네트워크가 있다. 이외에도 네트워크 가상화, VPN (Virtual Private Network) 등도 계층구조를 지닌다. 이 장에서는 다계층 네트워크에서 신뢰도를 보장하기 위한 여러 가지 방법들을 다룬다.

이를 위해 〈그림 9〉의 다계층 네트워크 모델을 가정한다. 먼저 논리적 토폴로지 GL은 논리적 노드 집합 VL과 이를 연결하는 논리적 링크 EL로 이루어져있다. 물리적 토폴로지 GP는 물리적 노드집합 VP와 물리적 링크집합 EP로 이루어져있다. 논리적 토폴로지는 물리적 토폴로지에 매핑이 된다. 즉, 각각의 논리적 링크 (s,t)가 물리적 토폴로지상의 s-t경로를 이용해 실제로 연결이 된다. 이 매핑을 임베딩(Embedding) 또는 광네트워크의 용어를 빌려 광경로 라우팅(Lightpath Routing)이라 부른다. 본고에서는 이 두 용어를 혼용하여 사용할 것이고, 논리적 링크를 Lightpath와 혼용하여 사용할 것이다.

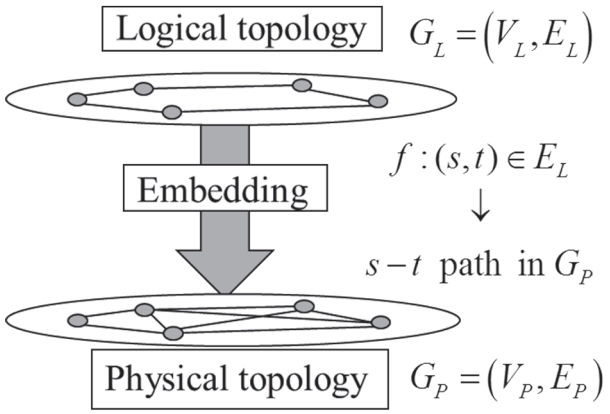

그림 9. 다계층 네트워크 모델: 논리적 토폴로지가 임베딩을 통해 물리적 토폴로지에 매핑이 된다.

위의 모델에서 볼 수 있듯이 임베딩 또는 토폴로지상의 한계에 따라 여러 개의 논리적 링크가 하나의 물리적 링크를 공유할 수 있다. 따라서 단일계층 네트워크와는 달리 다계층 네트워크에서는 하나의 링크실패가 상위계층에서 여러 개의 링크실패로 이어질 수 있다. 예를 들어, 〈그림 10〉과 같이 물리적 토폴로지와 논리적 토폴로지가 주어져있다고 했을 때, 임베딩 1은 어떤 물리계층 링크가 하나 끊어진다고 하더라도 여전히 논리적 토폴로지의 연결성을 유지한다. 반면에, 임베딩 2는 가운데에 있

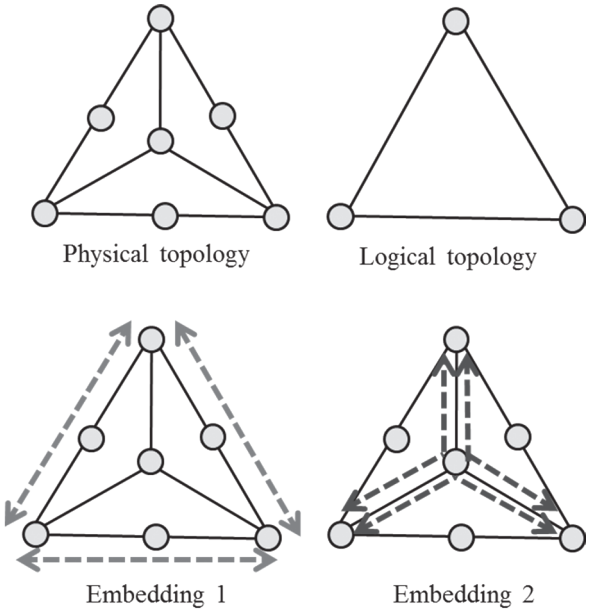

그림 10. 물리적 토폴로지, 논리적 토폴로지와 임베딩 예: 임베딩 1은 하나의 물리적 링크 실패를 견뎌낼 수 있지만, 임베딩 2는 견뎌내지 못한다.

는 물리적 링크 세 개 중에 하나가 끊어지면 두 개의 논리적 링크가 동시에 끊어지기 때문에 논리적 토폴로지의 연결성을 유지하지 못한다. 이와 같이 똑 같은 토폴로지에 대해 임베딩을 어떻게 하느냐에 따라 네트워크의 신뢰성이 결정된다고 볼 수 있다. 논문 [4]에서는 임베딩 1과 같이 하나의 물리적 링크실패를 견뎌낼 수 있는 것을 생존가능한 광경로 라우팅(Survivable Lightpath Routing)이라 정의하고, Survivable 임베딩을 찾는 알고리듬과 포뮬레이션을 개발하였다. 이 결과를 다중링크실패 등으로 발전시킨 연구는 [48]-[50]에서 찾을 수 있다.

위와 같이 다계층 네트워크의 연결성 또는 신뢰성은 임베딩에 의해 결정이 되는데, [1]에서는 [4]의 결과에서 더 나아가 다계층 네트워크의 연결성을 최대화 하는 임베딩을 연구하였다. 이를 위해 단일계층 네트워크에서의 MinCut 개념을 다계층 네트워크로 확장하여 Min-Cross-Layer Cut(MCLC)이라는 개념을 새로 정의하였다. MinCut은 네트워크를 단절시키기 위해 필요한 최소의 링크실패의 개수로 예를 들어 그림 10에서 물리적 토폴로지와 논리적 토폴로지 모두 MinCut이 2이다. 이를 다계층 네트워크로 확장하여 MCLC는 (물리적 토폴로지, 논리적 토폴로지와 임베딩이 모두 주어졌다고 했을 때) 논리적 토폴로지의 연결성을 끊기 위해 필요한 최소의 물리적 링크실패의 개수로 정의된다. 예를 들어, 그림 10에서 임베딩 1은 MCLC가 2이고, 임베딩 2는 MCLC가 1이다. 즉, 위에서도 설명하였듯이 임베딩 1은 물리계층의 링크실패 하나를 견뎌낼 수 있다. 따라서, MCLC는 네트워크의 신뢰성을 나타내는 좋은 척도라 할 수 있겠다.

하지만, 불행히도 다계층 네트워크에서는 단일계층 네트워크에서 성립하던 신뢰성 관련 성질들이 성립하지 않는다. 예를 들어, 단일계층 네트워크에서 링크용량이 모두 1일 때, MinCut과 Edge-Disjoint 경로의 수가 같다는 Menger의 정리[3]가 있다 [44]. 네트워크 신뢰성 입장에서 이는 매우 중요한 의미를 지닌다. 왜냐하면 Menger의 정리에 의하면 어떤 노드쌍 (s,t)에 Edge-Disjoint 경로 K개를 제공하면 K-1개의 링크실패가 있더라도 여전히 두 노드 사이의 경로가 존재하기 때문에 높은 신뢰성 보장을 위해서는 단순히 많은 Edge-Disjoint 경로를 제공하면 된다.

하지만 이 성질이 다계층 네트워크에서는 성립하지 않는다. 예를 들어, 〈그림 11〉에서 두 개의 노드 s와 d와 이를 연결하는 세 개의 평행링크로 이루어진 논리적 토폴로지를 생각하자. 이것이 만약 단일계층 네트워크 였다면 세 개의 에지 중에 두 개

3 Max-Flow Min-Cut 정리가 일반적인 링크용량을 가정한다면 Menger의 정리는 링크용량이 전부 1인 특이 케이스에서의 Max-Flow Min-Cut 정리라 할 수 있다.

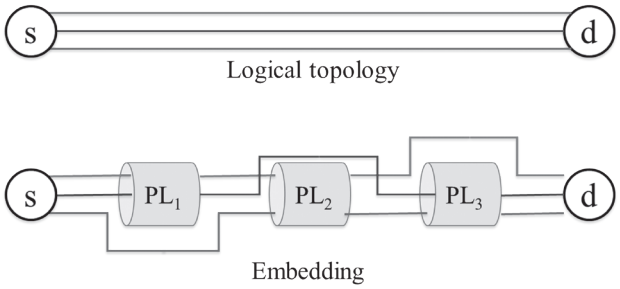

그림 11. 두 개의 노드와 둘을 연결하는 세 개의 에지로 구성된 논리적 토폴로지와 임베딩 예 (PL은 물리적 링크를 나타냄): 두 개의 논리적 경로는 하나의 물리적 링크실패를 견뎌낼 수 없고, 세 개의 논리적 경로를 모두 사용해야만 한다.

만 선택하여 제공하면 하나의 링크 실패를 견딜 수 있을 것이다. 하지만, 그 아래에 있는 임베딩을 생각해보자 (그림과 같은 임베딩이 가능한 물리적 토폴로지가 존재한다는 것을 수학적으로 증명할 수 있다 [1]). 이 상황에서는 어떤 하나의 물리적 링크가 끊어지면 두 개의 논리적 링크가 끊어지게 된다. 따라서, 논리계층에서 두 개의 경로 (즉, 여기서는 두 개의 에지) 만을 제공해서는 하나의 물리적 링크 실패를 두 노드가 견뎌낼 수 없다. 즉, s와 d는 단절된다. 따라서, 다계층 네트워크에서의 신뢰성 보장 문제는 단일계층에서의 문제와는 근본적으로 다르고 훨씬 복잡해진다. 일예로, MinCut은 Polynomial Time안에 계산할 수 있지만, MCLC를 계산하는 것은 NP-Hard문제가 된다. 또한 MCLC와 MaxFlow가 임의의 값으로 차이가 날 수 있다는 것도 증명할 수 있다 [1].

이러한 상황에서 [1]에서는 주어진 물리적 토폴로지와 논리적 토폴로지에 대해 MCLC를 최대화하는 임베딩 알고리듬을 Integer Linear Program 포뮬레이션과 Randomized Rounding 등의 테크닉을 이용하여 개발하였다.

[1]에서는 네트워크가 견뎌낼 수 있는 물리적 링크실패의 개수라는 신뢰도 지수를 최대화하는 임베딩을 연구하였다면 [2]와 [3]에서는 물리계층이 확률적인 링크실패를 겪는다고 가정하고 이 때 네트워크가 여전히 연결성을 유지할 확률을 신뢰도로 정의하고 이를 최대화 하는 임베딩을 연구하였다. 사실, 확률적 링크실패 모델 하에서 단일계층 네트워크의 신뢰성에 대한 연구는 상당히 많이 존재한다 ([45]와 그 안의 참고문헌 참조). 하지만, 다계층 네트워크의 신뢰성 연구는 [2],[3] 이전에는 없었고 [2]와 [3]이 최초의 연구라 할 수 있겠다.

먼저 각각의 물리적 링크가 p의 확률로 실패하고 독립이라 하자. 이해를 돕기 위해 〈그림 12〉는 〈그림 10〉에 있는 두 임베딩 방법의 신뢰성을 p에 따라 그린 그래프이다. 그림에서 볼 수 있듯이 링크실패확률 p가 낮은 영역에서는 임베딩 1이 높은 신뢰성을 지니고, p가 높은 영역에서는 임베딩 2가 더 높은 신뢰성

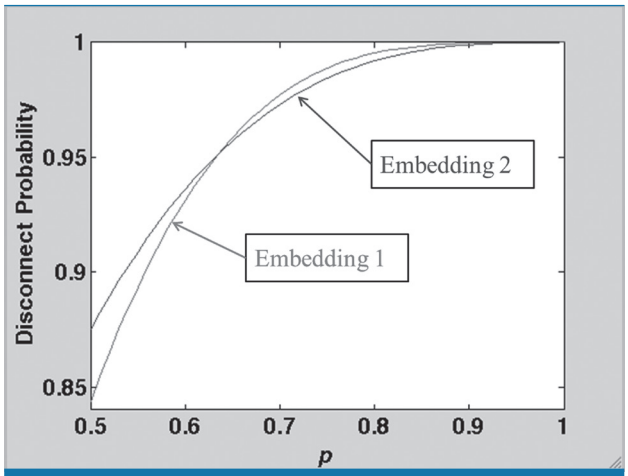

그림 12. 〈그림 10〉의 임베딩 1과 2의 신뢰성 그래프: 링크실패확률이 낮은 영역에서는 임베딩 1이 신뢰성이 높고 높은 영역에서는 2가 신뢰성이 더 높음을 알 수 있다.

을 지니는 것을 알 수 있다. 따라서 이 예는 링크실패확률에 따라 최적의 임베딩이 달라진다는 것을 보여준다. 즉, p에 대하여 최적인 임베딩이 존재하지 않을 수도 있다는 것을 보여준다.

이를 좀 더 체계적으로 연구하기 위하여 [2,3]에서는 MCLC 뿐만 아니라 Spanning Tree 또한 다계층 네트워크로 확장하여 Min Cross-Layer Spanning Tree (MCLST)라는 개념을 도입하였다. MCLST는 논리적 토폴로지의 연결성을 유지하기 위해 필요한 최소의 물리적 링크의 집합이다. 예를 들어, 그림 10에서 임베딩 1의 MCLST는 4이다. 왜냐하면 밖의 4개의 물리적 링크가 연결되어 있기만 하면 논리적 토폴로지의 연결성이 보장되기 때문이다. 반면에 임베딩 2의 MCLST는 3이라는 것을 알 수 있다.

[2,3]에서는 링크실패확률이 낮은 영역에서는 MCLC가 큰 임베딩이 가장 높은 신뢰성을 갖고 링크실패확률이 높은 영역에서는 MCLST가 작은 임베딩이 가장 높은 신뢰성을 갖는다는 것을 보여주었다. 이를 위해 단일계층 네트워크에서 정의되었던 신뢰성 다항식 (Reliability Polynomial) 또한 다계층 네트워크로 확장하였다. 이 연구결과들은 아직 초기단계로 앞으로 많은 후속 연구들이 기대되는 바이다.

Ⅳ. 결 론

본고에서는 네트워크의 신뢰성을 보장하기 위한 방법을 다루었다. 특히, 실패에서 회복하기 위해 필요한 링크용량 자원을 미리 예약해 놓는 네트워크 보호방식에 대해 이야기 하였고, 부분보호방식 또한 논하였다. 그리고, 다계층 네트워크 신뢰성을 최대화하기 위한 여러 가지 연구결과를 소개하였다.

네트워크가 발전을 거듭할수록 네트워크 용량이 커질 것이라는 점은 자명하다. 따라서, 네트워크의 신뢰도 보장 문제는 더욱 까다로워 질 것이다. 특히, 현재는 무선네트워크의 용량이 유선에 비해 그리 높지 않아 무선링크의 실패 (예를 들어, 재밍 공격(Jamming Attack)에 의한 링크실패)가 일어난다 하더라도 영향을 받는 트래픽의 양은 상대적으로 낮은 상황이다. 하지만, 앞으로 5G 에서는 데이터 속도가 Gbps단위가 될 수 있기 때문에 무선에서의 신뢰성 문제 또한 상당한 중요성을 지닐 것이다. 하지만, 무선네트워크의 신뢰성에 대한 연구는 아직 많이 이루어지지 않았고 이는 흥미로운 추후 연구주제가 될 수 있을 것이다 (하나의 예는 [46]이 될 수 있다).

뿐만 아니라, 위에서 언급한 다계층 네트워크 신뢰도 문제는 대부분 네트워크의 연결성에만 초점을 두고 링크용량에 대해서는 다루지 않았다. 즉, 링크용량은 충분하여 일단 연결성이 보장되면 트래픽을 모두 서비스 할 수 있다고 가정한다. 하지만, 이는 실제 네트워크에서 보장이 되지 않는 가정이다. 따라서 [47]과 같이 한정된 링크용량 하에서 다계층 네트워크의 신뢰성을 연구하는 것은 매우 중요한 추후 연구주제가 될 것이다.

참 고 문 헌

[1] K. Lee, E. Modiano and H.-W. Lee, "Cross-Layer Survivability in WDM-based Networks," IEEE/ACM Transactions on Networking, 2011.

[2] K. Lee, H.-W. Lee and E. Modiano, "Reliability in Layered Networks with Random Link Failures," IEEE/ACM Transactions on Networking, 2011

[3] H.-W. Lee, K. Lee and E. Modiano, "Maximizing Reliability in WDM Networks through Lightpath Routing," IEEE GLOBECOM, 2011.

[4] E. Modiano and A. Narula-Tam, "Survivable lightpath routing: a new approach to the design of wdm-based networks," IEEE JSAC, vol. 20, no. 4, pp. 800-809, 2002.

[5] R. Banner and A. Orda, "Designing Low-Capacity Backup Networks for Fast Restoration," IEEE INFOCOM'2010.

[6] Matthew Johnston, Hyang-Won Lee, Eytan Modiano, "A Robust Optimization Approach to Backup Network Design with Random Failures," IEEE Infocom, Shanghai, China, April 2011.

[7] G. Kuperman and E. Modiano, "Network protection with guaranteed recovery times using recovery domains," IEEE INFOCOM, 2013.

[8] H.-W. Lee, E. Modiano and K. Lee, "Diverse Routing in Networks with Probabilistic Failures," IEEE/ACM Transactions on Networking, 2010.

[9] J. Zhang, K. Zhu, H. Zang, and B. Mukherjee, "Service provisioning to provide per-connection-based availability guarantee in WDM mesh networks," OFC, Atlanta, GA, Mar. 2003.

[10] J. Zhang and B. Mukherjee, "A review of fault management in WDM mesh networks: Basic concepts and research challenges," IEEE Netwwork, vol. 18, no. 2, pp. 41-48, Mar. 2004.

[11] M. Tornatore, G. Maier, and A. Pattavina, "Availability design of optical transport networks," IEEE J. Sel. Areas Commun., vol. 23, no. 8, pp. 1520-1532, Aug. 2005.

[12] Mohammad Nurujjaman, Samir Sebbah, and Chadi M. Assi, "Design of Resilient Ethernet Ring Protection (ERP) Mesh Networks With Improved Service Availability," Journal of Lightwave Technology, Vol. 31, Issue 2, pp. 203-212, 2013.

[13] W. Grover, Mesh-based survivable networks: options and strategies for optical, MPLS, SONET, and ATM Networking. prentice hall, 2004.

[14] J. Tapolcai, Pin-Han Ho, L. Rónyai, Bin Wu, "Network-Wide Local Unambiguous Failure Localization (NWL-UFL) via Monitoring Trails," IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1762 - 1773, 2012.

[15] Deborah Brungard et al., "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)," IETF RFC 4427, 2006.

[16] V. Sharma and F. Hellstrand, "Framework for multi-protocol label switching (MPLS)-based recovery," IETF RFC 3469, 2003.

[17] K. Kompella et al., "The Use of Entropy Labels in MPLS Forwarding," IETF RFC 6790, 2012.

[18] P. Pan, G. Swallow, and A. Atlas, "Fast reroute extensions to RSVP-TE for LSP tunnels," IETF RFC 4090, 2005.

[19] N. Sprecher and A. Farrel, "MPLS-TP Survivability Framework," IETF RFC 6372, 2011.

[20] S. Ramasubramanian and A. Chandak, "Dual-Link Failure Resiliency Through Backup Link Mutual Exclusion," IEEE/ACM Transactions on Networking, Vol. 16, No. 1, 2008.

[21] M. To and P. Neusy, "Unavailability analysis of long-haul networks," IEEE JSAC, vol. 12, no. 1, pp. 100-109, 1994.

[22] R. Iraschko, M. MacGregor, and W. Grover, "Optimal Capacity Placement for Path Restoration in STM or ATM Mesh-Survivable Networks," IEEE/ACM Transactions on Networking, vol. 6, no. 3, pp. 325-336, 1998.

[23] W. Yao and B. Ramamurthy, "Survivable Tra_c Grooming with Path Protection at the Connection Level in WDM Mesh Networks," Journal of Lightwave Technology, vol. 23, no. 10, p. 2846, 2005.

[24] C. Ou, J. Zhang, H. Zang, L. Sahasrabuddhe, and B. Mukherjee, "New and Improved Approaches for Shared-Path Protection in WDM Mesh Networks,"Journal of Lightwave Technology, vol. 22, no. 5, 2004.

[25] G. Mohan, S. Murthy, and A. Somani, "Efficient algorithms for routing dependable connections in WDM optical networks," Networking, IEEE/ACM Transactions on, vol. 9, no. 5, pp. 553-566, 2002.

[26] A. Fumagalli, I. Cerutti, M. Tacca, F. Masetti, R. Jagannathan, and S. Alagar, "Survivable Networks Based on Optimal Routing and WDM Self-Healing Rings," IEEE INFOCOM'99.

[27] R. Bhandari, Survivable Networks: Algorithms for Diverse Routing. Kluwer Academic Pub, 1999.

[28] O. Gerstel and R. Ramaswami, "Optical layer survivability: A services perspective," Communications Magazine, IEEE, vol. 38, no. 3, pp. 104-113, 2000.

[29] O. Gerstel and R. Ramaswami, "Optical layer survivability-an implementation perspective," Selected Areas in Communications, IEEE Journal on, vol. 18, no. 10, pp. 1885-1899, 2000.

[30] G. Ellinas, A. G. Hailemariam, and T. E. Stern, "Protection cycles in mesh WDM networks," Selected Areas in Communications, IEEE Journal on, vol. 18, no. 10, pp. 1924-1937, 2000.

[31] A. Fumagalli and L. Valcarenghi, "IP restoration vs. WDM protection: Is there an optimal choice?" IEEE network, vol. 14, no. 6, pp. 34-41, 2000.

[32] A. Saleh and J. Simmons, "Evolution Toward the Next-Generation Core Optical Network," Journal of Lightwave Technology, vol. 24, no. 9, p. 3303, 2006.

[33] J. Suurballe, "Disjoint Paths in a Network," Networks, 1974.

[34] W. Grover and M. Clouqueur, "Span-Restorable Mesh Networks with Multiple Quality of Protection (QoP) Service Classes," Photonic Network Communications, vol. 9, no. 1, pp. 19-34, 2005.

[35] O. Gerstel and G. Sasaki, "Quality of Protection (QoP): a Quantitative Unifying Paradigm to Protection Service Grades," Optical Networks Magazine, vol. 3, no. 3, pp. 40-49, 2002.

[36] A. Das, C. Martel, and B. Mukherjee, "A Partial-Protection Approach Using Multipath Provisioning," in ICC '09.

[37] J. Fang and A. Somani, "On Partial Protection in Groomed Optical WDM Mesh Networks," International Conference on Dependable Systems and Networks, 2005.

[38] H. Wang, E. Modiano, and M. M_edard, "Partial path protection for WDM networks: End-to-end recovery using local failure information," in Computers and Communications, 2002.

[39] J. Zhang, K. Zhu, H. Zang, N. Matlo, and B. Mukherjee, "Availability-aware provisioning strategies for differentiated protection services in wavelength-convertible WDM mesh networks," IEEE/ACM Transactions on Networking, vol. 15, no. 5, pp. 1177-1190, 2007.

[40] C. Saradhi, M. Gurusamy, and L. Zhou, "Di_erentiated qos for survivable WDM optical networks," Communications Magazine, IEEE, vol. 42, no. 5, pp. S8-14, 2004.

[41] M. Tacca, A. Fumagalli, A. Paradisi, F. Unghv_ary, K. Gadhiraju, S. Lakshmanan, S. Rossi, A. Sachs, and D. Shah, "Differentiated reliability in optical networks: theoretical and practical results," Journal of lightwave technology, vol. 21, no. 11, p. 2576, 2003.

[42] Greg Kuperman, Eytan Modiano, and Aradhana Narula-Tam, "Partial Protection in Networks with Backup Capacity Sharing," Optical Fiber Communications Conference (OFC), Anaheim, CA, March, 2012.

[43] Kuperman, Greg, Eytan Modiano, and Aradhana Narula-Tam, "Analysis and algorithms for partial protection in mesh networks," IEEE INFOCOM, 2011.

[44] R. Ahuja, T. Magnanti, and J. Orlin, Network Flows: Theory, Algorithms, and Applications. Prentice-Hall, New Jersey, 1993.

[45] C. Tanguy, "Exact two-terminal reliability of directed networks," DRCN, La Rochelle, France, Oct. 2007.

[46] Kuperman, Greg, and Eytan Modiano. "Providing protection in multi-hop wireless networks." INFOCOM, 2013 Proceedings IEEE. IEEE, 2013.

[47] D. Kan, "Design of survivable IP-over-WDM networks: Providing protection and restoration at the electronic layer," Master's Thesis, Massachusetts Institute of Technology, 2003.

[48] Deng, Q., Sasaki, G., Su, C.F., "Survivable IP over WDM: a mathematical programming problem Formulation," 40th Allerton Conference on Communication, Control and Computing, Monticello, IL, 2002.

[49] Kurant, M., Thiran, P., "Survivable Routing in IP-over-WDM Networks in the Presence of Multiple Failures," EuroNGI Workshop on Traffic Engineering, Protection and Restoration for NGI, 2006.

[50] Kurant, M., Thiran, P., "Survivable Routing of Mesh Topologies in IP-over-WDM Networks by Recursive Graph Contraction," IEEE Journal on Selected Areas in Communications 25(5), 922 - 933, 2007.

약 력

이 향 원

2001년 한국과학기술원 공학사
2003년 한국과학기술원 공학석사
2007년 한국과학기술원 공학박사
2007년~2011년 메사추세츠공대 박사후과정 연구원
2011년~2012년 한국과학기술원 연구교수
2012년~현재 건국대학교 인터넷미디어공학부 조교수
관심분야: 무선네트워크 자원할당, 모바일 클라우드, 네트워크 신뢰도