국가수리과학연구소 NIMS-FI-2011-01

현재 인터넷의 문제점 조사

진보람 김도형 정유철

융복합수리과학연구부
미래인터넷연구팀

2011 년 2 월 7 일

국가수리과학연구소 기술문서

요 약

현재 인터넷에 어떠한 문제들이 있는지를 알아야 미래인터넷을 왜 만들어야 하고 어떠한 식으로 연구 개발되어야 하는지를 알 수가 있다. 본 문서에서는 현재 인터넷이 어떠한 면들에서 부족한지 알아보고 이 때문에 어떠한 구체적인 문제들이 발생했는지를 조사한다. 이를 토대로 미래인터넷 연구에서 실제로 무엇이 중요한지 알 수 있는 자료가 본문서에서 제공된다.

차 례

그림 차례

제 1 장

서론

1969 년 소련의 우주선 Sputnik 호 발사 성공은 미국에 있어 충격적인 일이었다. 미국은 이에 자극을 받아 과학 기술분야에서 소련을 앞서기 위해 과학교육을 강화하는 등 다방면으로 노력을 하였다. 그 중의 하나가 군사기술 분야를 발전시키기 위해 만든 현재 인터넷의 원형인 ARPANET 이다 (신명기, 2007).

이 통신망에는 미 국방성의 고등 연구 계획 기관에서 위치적으로 멀리 떨어져 있는 유타대학, 산타 바바라의 캘리포니아 대학, 로스엔젤리스의 캘리포니아 대학, 스탠포드 대학이 참여하였다. 소련과의 갑작스러운 전쟁이 발발하여 일부 통신이 두절되더라도 다른 곳을 경유하여 국방관련 자료, 각종 연구자료나 연구원들의 개발 정보를 나눌 수 있도록 하였다. 또한 ARPANET 은 소규모 네트워크로 이루어진 수많은 컴퓨터들의 분산 자율형 구조로 만들어 졌다. 이러한 구조로 미국방성은 전쟁에 대비하여 전쟁 수행에 필요한 컴퓨터와 정보를 보호하고 자원을 분산시켜 피해를 최소화하고자 하였다.

1972 년 세상에 공개된 ARPANET 은 국방 기술 프로젝트를 수행하는 대학과 연구소들의 참여로 규모가 점점 커졌고, 기존의 네트워크 관리에 어려움이 생겼다. 결국 1981 년 IETF 표준 RFC 를 통해 동일한 TCP/IP, UDP 를 기반으로 현재의 인터넷 구조를 정립하였고 1983 년 1 월 1 일에 ARPANET 의 NCP protocol 을 TCP/IP 로 일제히 전환하였다 (Leiner et al., 2011).

1986 년에는 미국과학재단(NSF) 이 ARPANET 을 흡수하여 미국의 전체 통신망을 대표하는 기관으로 자리잡게 되었다. 이후, NSF 는 자신들이 가지고 있는 수퍼 컴퓨터를 대학과 연구 기관이 이용할 수 있도록 NSFNET 을 구축하고, 비교적 빠른 통신 속도를 제공하였다. 결국 ARPANET 외의 중소 네트워크까지 NSFNET 에 참여하며 네트워크의 활용도가 점점 높아지게 된다.

인터넷은 일종의 연구망으로 만들어졌지만, 1991 년 World Wide Web 의 개발과 상용 인터넷 협회 설립으로 기업과 개인이 비지니스에서 인터넷을 이용하게 되는 것이 가능하게 되었다. 이제는 통신과 신문, 방송까지 수용하고 전

자상거래, 인터넷 뱅킹, 전자정부 등으로까지 활용될 정도로 인터넷이 일반 대중에게 급속도록 전파되어 우리 생활의 필수 불가결한 요소가 되었다 (변성혁, 2009).

그러나 2000 년 들어 통신환경의 급격한 변화 및 다양한 사용자 요구사항의 증대로 인해 현재 인터넷 상의 많은 문제점들이 제기되었는데 (Fisher, 2007; Gavras et al., 2007), 이에 대해서는 2 장에서 간단히 소개되어 있다. 이러한 인터넷의 문제를 해결하고자 지금까지도 국내외로 활발히 논의가 진행되고 있다 (김성수 et al., 2008). 3 장에서는 현재 인터넷의 문제들이 어떠한 것인지를 대표적인 연구 기관들에서 보는 관점이 소개되어 있고, 4 장에서는 문제점들이 구체적으로 어떤 것들이 있는지 조사한다. 5 장에서는 이들 문제들을 넣고 어떻 서로 연관이 되어있으며 이들을 해결하기 위해 미래인터넷을 만들어나가는 방법에 대해 토의를 하며, 6 장에서 결론을 맺는다.

제 2 장

현재 인터넷의 문제점 소개

여태까지 인터넷을 개발하고 쓰게 되면서 현재 인터넷에서 여러 가지 부족한 부분들이 드러나고 있다. 현재 인터넷에서 부족한 부분들을 여기서 간략하게 소개한다.

제 1 절 확장성

강문식 (2009)에 따르면 1969년 미국방성의 주도 하에 이루어진 대규모 시험 네트워크 ARPANET은 단지 4개의 컴퓨터를 연결한 것이었으나 현재는 세계 180여개 국에서 2억 6천만 대 이상의 호스트 컴퓨터가 연결되어 있으며 그 사용자의 수가 14억 5천만명을 넘고 하루 평균 100만 명 이상이 인터넷에 접속을 하고 있는 것으로 추산될 정도로 급속도로 확산되고 있다고 한다. 이로 인해 멀티호밍, 트래픽 엔지니어링 등으로 라우팅 테이블의 크기가 기하급수적으로 증가하고 있다. 신명기 (2007)은 앞으로도 인터넷 대역폭은 50배 내지 100배 이상 증가하고 센서와 같은 유비쿼터스나 멀티홈 등의 이유로 네트워크 자체의 복잡도가 커질 것으로 예상되고 있기에 확장성 부족은 현재 인터넷이 갖고 있는 가장 큰 문제점으로 대두되고 있다.

제 2 절 이동성

몇 대의 컴퓨터를 케이블로 서로 연결하여 사용하기 시작한 인터넷은 점점 그 활용이 확대되면서 수많은 컴퓨터들이 다양한 케이블들로 서로 연결되어 복잡한 구조를 띄게 되었다. 이와 같은 환경에서는 통신 중 단말이 이동하거나 하는 일이 발생하지 않았기 때문에 단말의 위치를 반영하는 주소 체계를 통해 효율적인 메시지 전달을 구현할 수 있었다. 그런데 노트북, 스마트폰 등 이동성을 지닌 휴대기기들이 등장하고 이들을 통한 인터넷 서비스가 시작되면서 단말들

은 메시지를 받고 있는 중에도 위치를 변경하는 경우가 빈번히 발생하게 되었다. 현재 주소 체계에서는 이와 같이 단말이 통신중에 새로운 위치로 이동을 할 경우, 인터넷은 단말의 이동을 인식할 수 없기 때문에 더 이상 통신이 불가능해진다. 이와 같이 단말의 이동으로 인해 발생하는 메시지 전달의 불연속성을 해결하고자 인터넷의 이동성에 대한 연구가 시작되었다. 이와 같은 인터넷에서의 이동성은 이동단말의 위치 관리 및 위치변경 중에도 서비스의 연속성 보장을 위한 메커니즘 전부를 포함한다.

제 3 절 다양성

인터넷은 지난 수십년간 유선망을 기반으로 하여 데이터를 효율적으로 전달할 수 있도록 개발되어 왔다. 목적지까지의 최적의 경로를 찾는 방법, 신뢰성 있는 통신을 위한 전달 메커니즘, 링크 사용의 효율성을 위한 알고리즘 등의 모든 인터넷 기술들이 유선망의 특징을 바탕으로 설계되고 개발되어 사용되고 있다. 그런데 최근들어 다양한 무선 기기들 및 무선망 기술들을 인터넷으로 통합시키는 노력이 진행되면서 기존의 인터넷 기술들에 대한 고찰이 필요하게 되었다. 인터넷을 구성하던 단말들이 PC, 서버 및 라우터 등에서 배터리 및 컴퓨팅 능력에 제한이 있는 휴대용 기기들로 확장되고, 고속으로 데이터를 전송할 수 있으며 전송 중 데이터 손실이 작은 유선망에서 상대적으로 저속으로 데이터를 전송하고 전송시 데이터 손실율이 높으며 전송거리가 제한적인 여러 무선망들로 확장되면서, 인터넷 기술들 역시 이와 같은 이종 기기 및 망들의 특성을 다양하게 고려할 수 있도록 하는 연구가 필요하게 되었다.

제 4 절 관리성

컴퓨터와 통신 기술의 발달은 인터넷의 전세계적인 대중화와 실시간 멀티미디어를 이용한 다양한 응용 서비스의 출연을 가지고 왔다. 이러한 네트워크 자원을 효과적으로 관리하는 것이 필요하다. 현재의 인터넷은 네트워크 관리를 염두에 두지 않고 설계된 것으로 네트워크 장비와 네트워크 내의 오류 등이 단순히 모니터링 되고 있을 뿐이다. 관리자의 직접적인 설정을 통해 네트워크 분리, 라우팅 설정, 보안설정, BGP 정책 설정 등의 관리가 이루어지고 있다. 네트워크 서비스 중단 등의 사고가 관리자의 사소하게 잘못된 네트워크 설정으로 인해 야기될 정도로 관리자의 능력에 의존적인 상황인 만큼 네트워크 설정 및 관리에 대한 요구가 높다.

제 5 절 보안성

보안성은 모든 종류의 통신에 있어서 중요시되고 있는 문제이다. 인터넷 역시 개발된 이래로 많은 보안 공격을 경험하였고, 이에 대한 해결책을 제시하여 왔다. 다른 사용자들의 통신을 엿듣기도 하고 단말들에 불법적인 접근을 하여 정보를 조작하기도 하며, 특히 특정 단말이나 망이 제대로 동작하지 못하도록 만드는 등의 공격들이 인터넷 기술상의 헛점을 이용하여 이루어져 왔다. 이와 같은 공격이 있을 때마다 인터넷은 보안을 고려한 새로운 기본 기술을 제시하기 보단 기본 기술은 그대로 두고 보안을 위한 메커니즘을 추가하는 쪽으로 보안 문제를 해결하여 왔다. 이와 같은 방법은 보안성을 얻는 대신 전송 효율성 측면을 희생시켰고, 이는 개발된 보안 기술들의 적용에 걸림돌이 되어 왔다. 전송 효율성 문제는 제한적인 자원의 무선 기기 및 망들이 인터넷에 통합되면서부터 더욱 부각되고 있다. 또한 무선 기기 및 망의 제한된 특성은 보안 공격을 더욱 쉽게 만든 반면 유선망에서 사용해왔던 보안 대책들을 적용시키기 어렵도록 하였다. 따라서 무선으로의 인터넷 영역의 확장은 인터넷의 보안성 측면에서 더욱 근본적인 접근을 요구하고 있다.

제 3 장

주요 과제에서 보는 관점

1974 년 처음 제안된 인터넷은 TCP/IP 단일 프로토콜을 설계 및 표준화로써 30 여년 넘게 글로벌 네트워크로 사용되어 왔다. 인터넷은 그동안 급격한 통신환경의 변화와 증대된 사용자의 요구사항에 민감하게 반응하며 끊임없이 변화를 거듭하고 있다. 현재 인터넷은 단순한 사회 커뮤니케이션 시스템을 넘어 사회 공공 인프라로서 중추적인 역할까지 하고 있다 (변성혁, 2009). 이렇게 중요한 인터넷에서의 주도권을 확보하고 유지하기 위해서 대표적으로 미국 FIND, EU FP7 하의 FIRE, 일본 AKARI 프로젝트에서는 현 인터넷의 상황을 분석하고 문제점을 파악 및 해결하고자 연구를 진행하고 있다 (Chen et al., 2010).

일본의 AKARI 에서는 전화를 이용한 단순한 네트워크가 컴퓨터를 연결한 정보 네트워크로 변화하면서 네트워크가 단순 사회 연결 그 이상의 의미를 갖고 세계적으로 필수요소가 된 상황에 관심을 두고 있다 (AKARI Architecture Design Project, 2010). 앞으로도 인간사회의 복잡성과 다양성이 점점 증가할수록 사람과 정보 사이의 상호연결은 점점 더 단단하게 될 것이고, 그것이 다시 네트워크에 반영 되어 결국은 새로운 문화와 과학이 생성될 것으로 예상하고 있다. 일예로 21 세기 들어 개발된 기술과 장치만 해도 너무나 다양하다. 어플리케이션과 서비스들도 끊임없이 사용자의 요구사항을 반영하며 출시되고 있다. 이러한 성공적인 인터넷의 상용화에도 불구하고 인터넷의 관리성이나 확장성에 대한 우려는 점점 더 커지고 있다.

유럽의 FIRE 에서도 현재 인터넷은 단순한 커뮤니케이션 시스템이라기 보다는 현대 사회의 중추적인 역할을 하고 있다고 하였다 (European Commission, 2010). 인터넷은 예상했던 것보다 더 대단하며 지금은 인터넷으로 연결되지 않은 삶 자체를 상상할 수 없는 시대가 되었다고 언급한다. 미래의 요구사항이 반영되고 새롭고 예상할 수 없는 어플리케이션과 서비스들이 만들어지고 있으며 환경과 문화의 발전과 더불어 현재 인터넷은 끊임없이 변화하고 있다. 이러한 급속한 변화와 그 추이를 모두 예측할 수 없어 예상치 못한 결과가 발

생하는 상황에 문제를 제기하고 있다.

미국의 FIND도 이러한 문제점에 대한 지적을 하고 있다. 현재 인터넷의 성공에도 불구하고 관리성이나 확장성, 보안성 등에 대한 걱정은 날로 커지고 있으며, 인터넷이 인류가 만든 시스템 중에서 규모가 가장 큰 것 인만큼 이것을 이해하고 관리할 수 있는 능력의 필요성을 강조하고 있다 (Fisher, 2007). 더불어 인터넷 보안 관련 문제의 해결은 물론 앞으로 인터넷이 지속적으로 수많은 새로운 무선 네트워크와 연결성을 유지할지, 인터넷이 지속적으로 개방적인 사회를 위해 기여를 할지 등도 고려해야 한다고 언급하고 있다.

제 4 장

기존 연구에서 보는 문제점

이장에서는 기존 연구들에서 구체적으로 인터넷에서 어떤 문제들이 있다고 보는지를 조사한다.

제 1 절 라우팅 테이블 크기 폭발

1990 년 대 웹서비스의 폭발적인 인기와 2000 년 대 인터넷 서비스 제공업자 (Internet Service Provider ; ISP) 와 무관한 주소의 할당, 멀티호밍, 트래픽 엔지니어링 등으로 라우팅시 그룹화되지 않은 주소들이 인터넷 전산망 근간의 연결된 부분에 대량으로 유입되었다.

각 ISP 가 패킷을 전송하기 위해서는 라우터를 사용하고, 이들 라우터들이 동작하기 위해서는 라우팅 테이블에 패킷을 어디로 보내야 하는지의 정보가 있어야 한다. 하지만 그림 4.1 에서도 확인할 수 있듯이, 1998 년에서 2002 년 사이에 라우팅 테이블 사이즈는 2 배로 증가하였고, 이로 인해 패킷이 전송되기 위한 부하가 늘어나고 있고 더 큰 용량의 라우터 메모리가 요구되고 있다. 이러한 추세는 인터넷의 효율적인 작동에 위협이 되고 있다. 여기서는 현 인터넷 문제 중 가장 많이 언급되는 라우팅 테이블의 증가추세와 확장의 원인에 대해 살펴보고자 한다.

1.1 라우팅 테이블의 증가 추세

제 1 장에서 언급하였듯 4 개의 컴퓨터를 연결하면서 시작된 네트워크는 1980 년대 들어 TCP/IP 를 기반으로 현재의 인터넷 구조가 정립되면서 네트워크의 크기가 확장되었다 (Massey et al., 2007). 1990 년대와 2000 년대로 나누어 라우팅 테이블 증가의 원인을 살펴보도록 하겠다.

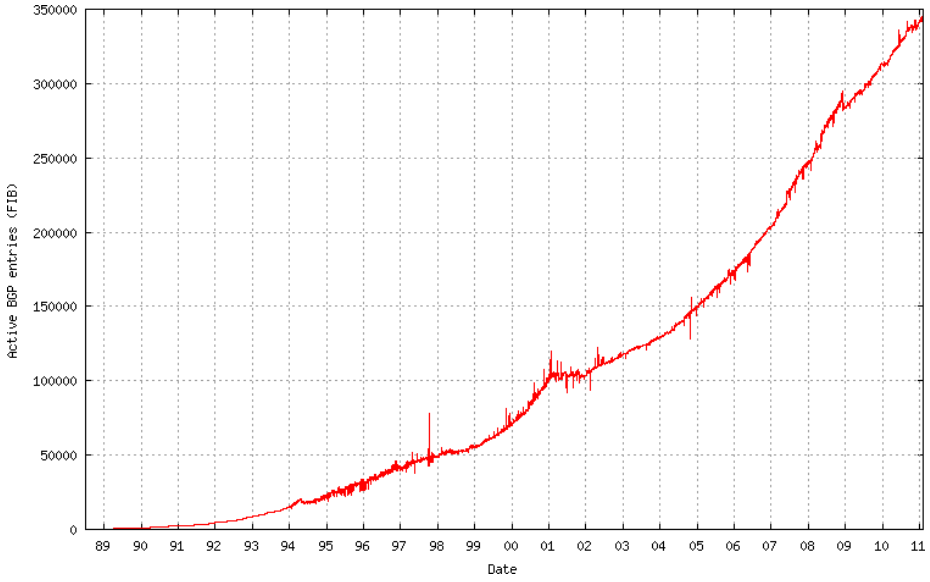

그림 4.1: Growth of the BGP Forwarding Table (BGP Reports, 2011).

1.2 1990 년대의 라우팅 테이블 증가

4 개의 컴퓨터를 연결하면서 시작된 네트워크는 1980 년대 들어 갑자기 네트워크에 연결된 노드의 수가 증가하였다. 호스트들의 이름들을 분산 시켜 관리할 수 있는 DNS 과 link state 방식의 라우팅 프로토콜이 개발되었고, 이와 동시에 도메인의 확장을 통한 inter-domain 프로토콜인 EGP 가 개발되었다. 특히 DNS 의 경우 호스트의 이름을 유일한 IP address 로 매칭 시키는 시스템으로 여러 다른 기관들의 노드들의 이름과 IP 주소를 매칭시키고 그 정보를 분산시킴으로 인터넷이 확장할 수 있도록 큰 영향을 줄 수 있었다. 이처럼 1990 년대 초까지만 해도 인터넷에서 발생하는 문제들은 즉각적인 해결책 제시 및 적용으로 지속적으로 확장되어 왔다.

1990 년대에는 비로소 World Wide Web 가 개발되어 급격한 인터넷의 확장이 이루어졌다. 이러한 인터넷의 확장과 더불어 인터넷의 호스트의 수 역시 증가하게 되었고, 기존 IP address 의 A, B, C 클래스로 나뉜 주소 중 B 클래스의 주소 블록들이 급격히 감소하게 되었다. 인터넷의 확장과 더불어 부족한 B 클래스 대신 A 와 C 클래스 주소들이 할당되어 호스트 대비 네트워크 프리픽스가 늘어나는 현상을 보이게 됐다. 이러한 인터넷의 확장성 문제는 인터넷의 미래에 대한 고찰로 이어졌고 Clark et al. (1991) 를 통해 인터넷의 미래에 대한 논의를 하게 되었다. 특히 이 문서는 routing 과 addressing 관점에서 계속해서 확장되는 인터넷의 상황을 고려하여 새로운 기능 또는 아키텍쳐의 필요성을 역설하였다. 이후 새로운 IP addressing scheme 의 개발이 시작 되었고, 드디어 1995 년 새로운 IP 주소체계인 IPv6 가 완성되었다 (Deering and Hinden, 1995,

1998).

Clark et al. (1991)에서 언급된 routing과 addressing 확장성 문제는 class B 네트워크의 고갈과 routing table의 폭발적 증가 및 IP 주소 영역의 고갈이었다.

1.3 2000년대의 라우팅 테이블 증가

인터넷 라우팅 시스템은 인터넷의 근본적인 요소이다. 인터넷의 규모가 점점 더 커질수록 인터넷 라우팅 시스템은 다양한 확장성 문제에 직면할 수밖에 없다. Meyer et al. (2007b)은 그 원인을 멀티호밍, 트래픽 엔지니어링, IP 주소의 의미 중복 등으로부터 찾고 있다 (Wang et al., 2010a; Guo et al., 2009; Massey et al., 2007; Menth et al., 2009; 유태완 and 이승윤, 2007; 유태완 et al., 2010; Bu et al., 2004; Wang et al., 2010b). 다음은 확장성 문제의 원인으로 일컬어지는 이슈들이다.

- *Provider Independent* 주소의 활용
  인터넷 IP주소소 영역은 ISP 별로 부분공간이 할당되어 있고, 그 부분마다 특징을 갖고 있다. 이로서 어떤 데이터가 IP주소와 함께 목적지로 이동할때, IP주소의 특징만을 고려하여 routing aggregation 되므로 좀 더 경로를 단축할 수 있다. 즉, 라우팅 테이블의 사이즈를 축소할 수 있다. 그러나 ISP의 주소 공간이 변경되는 경우 그 안에 해당된 컴퓨터와 기기들의 주소도 모두 새로운 ISP에 포함된 것으로 재설정된다.

  이 과정은 엄청난 시간과 비용을 필요로 하기 때문에 사용자들은 제공자와 독립적인 주소를 선호한다. 사용자들이 독립적인 주소를 갖게 되면, 네트워크 내에서 어떤 특징을 갖는 그룹에 속하지 않는다. 결국 라우팅 테이블에 독립적으로 명시될 수 밖에 없고 결국 라우팅 테이블의 증가를 초래한다 (Guo et al., 2009; Menth et al., 2009; 유태완 and 이승윤, 2007; 유태완 et al., 2010; Bu et al., 2004).

- 멀티호밍 *(multihoming)*
  사용자들은 기본적으로 자신의 기기가 네트워크 상황에 영향을 받지 않고 인터넷에 완벽하게 연결되기를 원한다. 연속적인 연결을 위해 하나의 단말기를 두 개 이상의 ISP와 연결하기도 하는데 이것도 일종의 멀티호밍이다. 한 라우팅 테이블에 공표되어 있는 부분이 따로 라우팅 테이블로 만들어지기 때문에 결국 테이블의 크기를 증가시킨다 (Wang et al., 2010a; Massey et al., 2007; Menth et al., 2009; 유태완 and 이승윤, 2007; 유태완 et al., 2010; Bu et al., 2004).

- 트래픽 엔지니어링 *(traffic engineering)*

트래픽 엔지니어링은 부하분산 등의 목적으로 인터넷 경로를 우회시키거나 반대로 특정경로로 가지 못하도록 하는 것을 의미한다. 제공자 무관 주소를 이용하는 사용자들은 각각의 서비스마다 서로 다른 ISP가 존재하기를 원한다. 그래서 사용자들은 IP 주소공간을 작게 나누어 각각 다른 목적으로 사용하고 작은 부분마다 다른 ISP와 연결한다. 결국 경로를 우회시키기 위해서는 그 주소가 포함된 부분의 라우팅 테이블을 별도로 알리게 되고, 멀티호밍과 같이 테이블이 중복적으로 공표되어 라우팅 테이블의 사이즈가 커지는 것이다 (Wang et al., 2010a; Menth et al., 2009; 유태완 and 이승윤, 2007; 유태완 et al., 2010; Bu et al., 2004).

- *IP* 주소의 의미 중복 문제
  현재 인터넷에서 사용하는 IP 주소는 개개인이 통신에 사용하는 기기 등의 대상물과 그 대상물의 위치를 모두 포함한다. Rekhter and Li (1995)는 확장성 있는 라우팅 시스템의 설계 기본조건을 "Addressing can follow topology or topology can follow addressing. Choose one." 이라 말한 바 있다. 그러나 수십년전 설계된 인터넷 아키텍처는 IP 주소의 의미 중복이라는 성질을 갖고 있기 때문에 이 조건을 만족하기는 어렵고 최근의 인터넷에서 요구되는 멀티호밍, 이동성 등을 근본적으로 지원하기에도 역부족이다 (유태완 et al., 2010; Bu et al., 2004).

2000년대 중반 직면한 인터넷 확장성 문제를 해결하고자 Meyer et al. (2007a)에서는 identifier와 locator가 분리되는 아키텍처를 해결책으로 제시하였다.

제 2 절 이동시 연결성 유지 문제

현재 인터넷은 TCP/IP 기반에서 동작한다. 현재 IP주소는 인터넷 상에서의 단말의 위치정보를 담고 있기 때문에, 단말이 네트워크를 이동하게 되면 패킷 전달을 위해서 반드시 IP주소도 변경되어야 한다. 현재 인터넷 하에서 IP주소의 변경은 단말의 위치 관리 및 이동시 통신의 연속성 보장에 있어서 문제를 야기시킨다. 본 섹션에서는 현재 인터넷에서 이동성을 지원하기 위한 기술들과 관련하여 Le et al. (2006)의 내용을 살펴보고 현재 기술들의 한계점 등을 고찰해보고자 한다.

2.1 Mobile IP

앞서 언급한 바와 같이 패킷에 적힌 주소를 통해서 라우터들은 수신 단말이 이동하기 전의 위치로 패킷을 전달한다. 하지만 수신 단말이 이미 새로운 위치로 이동한 뒤이므로 변경 전 위치로 전달된 메시지들은 목적지를 찾을 수 없어 버려지게 된다. Mobile IP는 이와 같이 버려지는 패킷들에 대해서 이동성을 지

원하는 서버를 두어 단말이 새롭게 이동한 곳으로 전송해주는 방법을 구현하기 위한 프로토콜이다.

Mobile IP의 기본적인 동작방법은 다음과 같다. 단말이 새로운 위치로 이동하게 되면, foreign agent를 통해서 현 위치에서의 care-of address로 불리는 새로운 주소를 할당받는다. 단말이 새롭게 할당받은 care-of address를 변경 전 위치에 있는 home agent에 등록시키게 되면, 기존 주소를 이용해 단말로 향하던 패킷이 home agent에 도착된 뒤 care-of address를 통해 단말의 이동된 위치로 전달될 수 있게 된다. 이렇게 도착한 패킷이 단말에 도착하게 되면 원래대로 기존 패킷을 복원하게 되고 이를 통해서 세션을 깨뜨리지 않고 통신의 연속성을 보장하게 된다. Mobile IP는 IPv4에서 동작하는 MIPv4 (Perkins, 2002)와 IPv6에서 동작하는 MIPv6 (Johnson et al., 2004)가 표준화되었으며 IP 단계에서의 이동성을 지원하기 위한 가장 대표적인 기술로 인식되고 있다.

그러나 Mobile IP는 다음과 같은 한계들을 가진다. 첫째, 패킷들이 home agent를 거쳐서 foreign agent로 전달되면서 패킷의 이동경로가 길어지게 된다. 응답 패킷 역시 보안 상의 문제로 foreign agent에서 home agent를 거쳐서 이동하게 되는데, 이와 같이 이동경로가 길어지면서 발생하는 전달 지연의 증가는 네트워크 효율성 측면에서 문제를 발생시킨다 (Yap et al., 2000). 둘째, 새로운 네트워크로 이동하면서 foreign agent로부터 care-of address를 할당받고 이를 home agent에까지 등록하는 데 걸리는 시간으로 인해 서비스의 연속성 지원에 한계가 있다 (Hsieh et al., 2003). 특히 단말이 이동한 네트워크가 home agent가 존재하는 홈네트워크로부터 거리가 길 경우, 등록에 필요한 시간은 더욱 늘어나게 된다. 셋째, Mobile IP에서는 agent의 역할이 절대적이다. 모든 단말들이 agent의 도움을 받아 이동성을 지원받게 된다. 이와 같은 방법은 agent에서 관리하는 단말의 수가 많아질 경우, agent에 걸리는 프로세싱 오버헤드 및 인접링크에서의 congestion등과 같은 확장성 문제를 야기시킬 수 있다 (Chiussi et al., 2002).

2.2 Session Initiation Protocol

단말이 새롭게 이동한 위치에서 인터넷을 통해 통신을 하기 위해서는 그 위치에서 사용가능한 새로운 주소를 할당받아야 한다. 이렇게 새로운 주소를 할당 받더라도 누군가에게로부터 단말에게 전달되어지는 데이터는 단말이 위치를 변경하기 전의 위치로 전송되게 된다. 이와 같은 문제를 해결하기 위해서는 이동 단말로 데이터를 전송하기전 이동단말의 현재 위치를 알수 있어야 하는데 Session Initiation Protocol (SIP)가 이런 목적으로 확용될 수 있다.

SIP는 멀티미디어 시그널링 프로토콜로 개발되었으나 이동성 지원에 응용되고 있는 기술이다 (Johnston, 2009). 이동단말은 네트워크를 변경할 때마다 홈네트워크에 있는 SIP 서버에 현재 위치에서 새롭게 할당받은 IP주소를 등록

한다. 따라서 이동단말에게 데이터를 전송하기 전에 단말들은 SIP 서버를 통해 이동단말이 현재 위치에서 사용하고 있는 IP 주소를 획득하고 그 주소를 가지고 통신을 시도한다. 통신 중 이동단말이 네트워크를 변경할 경우에는 이동단말이 직접 상대 단말에게 변경된 IP 주소를 알려주는 방법으로 핸드오프를 지원한다.

SIP 는 개발 자체가 이동성 지원을 목적으로 개발된 것이 아니기 때문에 이동성 지원에 있어서 한계가 있다. SIP 시그널링 메시지 자체의 오버헤드가 커서 빈번히 발생할 수 있는 이동성 지원에 적합하지 않다 (Banerjee et al., 2003). 그리고 단말이 핸드오프를 수행할 경우 SIP 에서 이동성 지원을 처리하기 위한 시간 지연이 상당히 커서 리얼타임 서비스를 위한 이동성 지원 방안으로 적합하지 않다.

2.3 Location Independent Network Architecture for IPv6

앞서 언급한 바와 같이 IP 주소 자체는 수신 단말이 누구인지 뿐만 아니라 그 수신 단말이 어디에 있는지를 같이 나타내고 있기 때문에, 현재 인터넷 시스템 하에서는 수신 단말이 위치를 변경하게 되면 변경된 위치를 찾아갈 수 있는 방법이 없다. 또한 변경된 위치로 패킷을 전달시키기 위해서 새로운 IP 주소를 사용하게 되면 세션이 깨지는 문제가 발생한다. 이와 같은 이동성의 한계를 근본적으로 해결하고자 IP 주소에서 단말 식별자와 위치 지시자 역할을 분리시키고자 하는 아이디어로 Location Independent Network Architecture for IPv6 (LIN6) 가 제안되었다 (Teraoka et al., 2003).

LIN6 주소 체계하에서 단말은 단말의 식별을 위한 LIN6 ID 및 위치 식별을 위한 LIN6 주소의 두개 네트워크 주소를 가진다. 통신을 시작하면서 LIN6 는 기존 IP 주소 대신에 LIN6 ID 를 사용하여 세션을 생성한다. LIN6 ID 는 단말이 누구인지만을 나타내고 있기 때문에 단말의 위치변화에 따라 새롭게 바뀔 필요가 없는 주소이다. 따라서 단말의 이동중에도 생성된 세션을 그대로 유지할 수 있도록 한다.

위치를 알려주기 위한 LIN6 주소는 network prefix 에 LIN6 ID 를 연결한 형태를 취한다. 여기서 network prefix 는 기존 IP 주소에서 위치를 나타내는 부분으로 라우터들이 이 정보를 통해 패킷의 전달 경로를 결정하게 된다. 수신 단말이 위치를 변경하게 될 경우 LIN6 는 다음과 같이 동작한다. 수신단말은 변경된 위치에서의 network prefix 을 가지고 새로운 LIN6 주소를 생성한다. 물론 이때도 LIN6 ID 값은 변하지 않는다. 수신 단말은 새로 생성한 LIN6 주소를 송신 단말에게 직접 알려주어 변경된 LIN6 주소로 통신을 계속할 수 있다. 또다른 방법으로 변경된 LIN6 주소를 mapping agent 에 등록, 통신을 원하는 단말이 mapping agent 에서 LIN6 주소를 알아낼 수 있도록 하는 방법으로 송신측에 위치를 알게 할 수 있다. 이와 같은 mapping agent 를 이용하는 방법에 있어서는 송신하고자 하는 단말들이 mapping agent 의 위치를 알 수 있어야 하

는데, 이는 DNS를 이용하도록 한다.

LIN6 기술은 2.1 절의 Mobile IP 에서 가지는 확장헤더나 터널링 기법이 필요하지 않기 때문에 agent를 도입하면서 생기는 부하 및 라우팅 경로가 길어지면서 생기는 지연 등을 피할 수 있는 이점을 가진다.

2.4 Dynamic Updates in the Domain Name System

현재 도메인 이름은 단말의 IP주소에 따라 정적으로 할당되어있다. 따라서 단말이 이동함으로써 IP주소가 바뀔 경우 현재의 DNS는 제대로 동작할 수 없다. 이와 같은 한계에서 인터넷의 이동성을 지원하고자 DDNS가 제안되었다 (Vixie et al., 1997). 이동단말은 네트워크간 이동이 있을 때마다, DNS 서버의 name-to-address 항목을 새롭게 갱신할 수 있도록 하여 위치관리를 수행한다.

DDNS 기술은 기존의 DNS 시스템을 사용함으로써 별도의 서버를 둘 필요가 없는 장점이 있지만, DNS 항목 갱신 지연이 길어서 문제가 될 수 있다. 뿐만 아니라 핸드오프시 연속적인 서비스 지원은 실제적으로 불가능하다 (Le et al., 2006).

2.5 Host Identity Protocol

Host Identity Protocol (HIP)은 2.3 절의 LIN6와 유사하게 단말이 누구인지를 나타내는 것과 단말이 어디에 위치하는지 나타내는 것의 IP주소가 가지는 두 가지 역할을 분리시키려는 아이디어를 기반으로 제안되었다 (Nikander et al., 2003). HIP에서도 IP주소를 대신하여 host identifier라는 새로운 식별자를 통해 세션을 생성한다. LIN6에서의 LIN6 ID와 유사하게 host identifier는 위치 변경에도 변하지 않는 주소이다. 따라서 단말의 위치 변경에도 생성된 세션이 깨지는 일을 방지할 수 있다. 뿐만 아니라 host identifier는 복수개의 IP주소와의 매핑이 이루어질 수 있으므로, multihoming을 지원하는 데도 용이하다.

HIP에서는 RVS서버 통해 위치관리가 이루어지는데 RVS서버는 이동단말의 host identifier와 IP주소간의 매핑 정보를 유지한다. 패킷을 송신하는 단말은 DNS를 통해서 해당 host identifier정보를 가지고 있는 RVS서버 주소를 얻어내고, RVS서버와의 통신을 통해 host identifier에 해당하는 IP주소를 받아 이동단말과 통신을 하게 된다. 통신 중에 수신 단말이 위치를 변경하여 IP주소를 새롭게 할당 받게 되면, 송신하는 단말에게 직접 바뀐 IP를 알려주게 되고, 송신단말은 바뀐 IP주소로 통신을 계속할 수 있도록 한다. 이때 IP주소는 변경되지만 IP주소 대신 변하지 않는 host identifier를 사용하여 세션을 생성하였기 때문에 세션의 연속성을 구현할 수 있다.

2.6 Multiple Address Service for Transport

인터넷에서 이동성 및 multihoming을 지원하기 위해 고안된 Multiple Address Service for Transport (MAST)는 별도의 ID등을 두는 대신 기존의 IP만을 사용하여 동작한다 (Crocker, 2003). 처음 세션을 생성할 때의 IP주소가 단말의 식별자로서의 역할을 수행하는데, 단말의 이동으로 위치가 바뀌어도 이 IP주소를 삭제되지 않고 세션을 유지하는데 사용된다. 단말의 현재 위치에서의 IP주소는 단말의 위치 지시자의 역할을 수행하게 된다. 즉 MAST하에서 단말은 복수개의 IP주소를 허용할 수 있다.

통신하고자 하는 단말은 이동 단말의 식별자 IP주소 및 DNS를 통해서 이동단말의 현재 위치의 IP주소를 얻게 된다. 단말이 위치 변경에 따른 새로운 IP주소를 얻게 될 때마다 DNS에 등록하여 통신을 원하는 단말들이 자신의 현재 위치를 알수 있도록 한다. 단말이 패킷을 받는 도중에 위치변경이 이루어지면 새롭게 할당받은 IP주소를 통신하던 단말에게 직접 알려주어 서비스의 연속성을 지원한다. 이렇게 하는 이유는 변경된 위치에서 새로 할당받은 IP주소를 DNS에 등록하는 과정에서 긴 시간지연이 발생할 수 있기 때문에 이로 인한 서비스 연속성 측면의 문제가 발생하는 것을 막기 위해서이다.

제 3 절 다양한 망환경의 미비한 수용

다양한 특성을 가진 무선 단말들 및 기술들을 인터넷으로 통합시키는 노력이 진행되면서 통합된 환경에서 기존 인터넷 기술들이 가지는 문제점이 하나둘 등장하기 시작하였다. 본 섹션에서는 이와 같이 현재 인터넷 상에서 존재하는 이종성으로 인해 야기되는 문제점들, 특히 현재 인터넷의 핵심 기술인 TCP/IP에서 야기시킬 수 있는 문제점들에 대해서 좀 더 자세히 살펴보고자 한다.

3.1 이종성의 종류

망의 이종성 각각의 독립된 망 기술들은 목적에 따라 다음과 같은 항목에서 차이를 보인다. 인터넷으로 통합하기 위해서는 이와 같은 망의 특징들을 모두 고려한 네트워크 기반 기술이 설계되어야 할 것이다 (Barakat et al., 1999; Lakshman and Madhow, 1997; Balakrishnan et al., 1997b; Allman et al., 2000; Balakrishnan et al., 1997a; Gurtov and Ludwig, 2003; Huang and Cai, 2005).

- Bit error rate
- Bandwidth, delay
- End-to-end connectivity
- Transmission power (coverage)

- Addressing and naming

단말의 이종성 디바이스의 종류에 따라서, 특히 무선 디바이스일 경우 아래와 같은 특성에 있어서 다양한 차이를 보일 수 있다 (Akkaya and Younis, 2005).

- Battery power
- Mobility (pattern, speed, location)

3.2 이종성이 Transport Layer에 미치는 영향

대표적인 transport layer 프로토콜인 TCP는 신뢰성있는 통신뿐만 아니라 네트워크의 혼잡성 및 사용률 제어의 기능을 제공하고 있다. 그러나 변화된 인터넷 환경에서는 TCP 의 성능이 크게 저하될 수 있음이 Barakat et al. (1999)를 통해서 제시되었다.

3.2.1 Long round trip time

전송 단말은 정상적으로 전송되는 패킷마다 ACK를 수신하게 된다. 전송측 단말은 수신되는 ACK마다 congestion window를 늘려가면서 전송률을 증가시키는데, 네트워크의 효율적인 사용을 위해서 congestion window가 어느 수위에 이르기 전까지는 기하급수적으로 증가시킨다. 만약 패킷을 전송하고 ACK을 수신하기까지의 왕복시간이 길어진다면 congestion window를 증가시키는데 시간이 오래 소모되고, 이로 인하여 네트워크를 비효율적으로 사용하게 될 수 있다. 이 경우 특히 웹 트래픽과 같은 작은 크기의 플로우들의 성능이 급격히 저하될 수 있게 된다. 그리고 왕복시간이 긴 플로우들이 왕복시간이 짧은 플로우들에 비해서 상대적으로 전송률을 높이는 데 오랜시간이 걸리게 되므로 병목구간에서 작은 대역폭을 차지할 수 밖에 없고, 이는 TCP에서의 대표적인 공평성 문제로 인식되고 있다 (Lakshman and Madhow, 1997).

3.2.2 TCP congestion control mechanism

유선 네트워크에서의 패킷 손실은 대부분 병목에 의한 라우터 큐에서의 패킷 소거에서 발생한다. 이와 같은 사실을 이용하여 TCP는 패킷이 손실될 때마다 congestion window를 줄이는 방법으로 혼잡 제어를 수행한다. 그러나 인터넷 상에서 무선구간이 확장되면서 채널상태의 악화, 충돌 및 간섭현상 등과 같은 병 이외의 이유들로 패킷 손실이 발생하게 되었고, 패킷 손실을 병목의 지표로 삼는 기존의 TCP 혼잡 제어는 대역폭의 효율적인 사용에 있어서 문제를 야기시킨다. 즉 병목이 아님에도 전송속도를 줄이게 되므로 사용 가능한 대역폭을 충분히 사용하지 못하는 일이 발생하기 때문이다.

이에 대한 해결책으로 연결을 유선구간과 무선구간으로 분리시켜 별도의 혼잡제어방식을 사용하는 방식이 제안되었다. 별도의 agent가 유선구간과 무선구간의 연결지점에 위치하여 연결을 분리시키는 방법 (Balakrishnan et al., 1997b)이 제안되었으나 이는 인터넷의 end-to-end semantic을 위반하는 문제점을 가지고 있다. Balakrishnan et al. (1997b)에서는 별도의 연결 생성 없이 혼잡제어하는 방식 또한 소개하고 있다. 무선 구간의 끝에서 단순히 TCP 패킷을 저장하고 있다가 채널 상태에 따른 패킷 손실이 발생하여 이를 알리는 ACK가 저장 지점에 도착할 경우, 무선구간내에서만 재전송이 이루어지도록 하는 방법을 소개하고 있다.

3.2.3 Bandwidth asymmetry

유선 네트워크에서는 패킷의 순반향 전송 및 그 역 방향 전송이 같은 경로를 따라 이루어지므로, 전송 방향 및 역방향이 같은 링크 대역폭을 가진다. 따라서 TCP 패킷에 대한 ACK의 경우는 보통의 경우 손실없이 전송되고, 이를 바탕으로 순방향 혼잡제어가 가능하게 된다. 그러나 무선 영역으로 인터넷이 확장되면서 패킷의 전송 경로와 그 역방향 전송 경로가 달라질 수 있으며, 이는 결국 대역폭 대칭에 대한 가정을 유효하지 않게 하였다. 만약 역방향에서의 작은 대역폭으로 인해 ACK가 손실될 경우, 순방향 대역폭이 충분함에도 불구하고 전송률을 낮추는일이 발생하게 되고 이는 곧 링크의 비효율적인 사용을 초래할 수 있게 된다.

이에 대한 해결책으로 ACK의 header를 압축하여 ACK 전송속도를 증가시키는 방법 (Allman et al., 2000) 및 cumulative ACK의 성질을 사용하여 ACK 수를 줄이는 방법 (Balakrishnan et al., 1997a) 등이 제안되었다.

3.2.4 Sudden bandwidth change during vertical handoff

서로 다른 대역폭을 가진 이종 망 사이에서 단말의 핸드오프가 발생할 경우 현재의 TCP하에서 다음과 같은 현상이 발생할 수 있다. 첫째, 단말이 전송지연이 긴 망으로 옮겨가는 경우, 갑작스레 늘어난 왕복시간으로 인하여 TCP timeout이 발생하게 될 수 있다 (Gurtov and Ludwig, 2003). 이 경우 패킷이 정상적으로 전송되고 있음에도 불구하고 TCP timeout으로 인하여 단말은 패킷을 재전송하게 되고, 또 병목 제어을 수행하게 된다. 둘째, 단말이 대역폭이 작은 망으로 옮겨가는 경우 새로운 망의 작은 대역폭이 현재의 congestion window에 해당하는 만큼의 패킷을 감당할 수 없어 돌발적인 패킷소거가 발생하게 된다 (Huang and Cai, 2005). 이 두가지 현상은 단말의 이종망 간의 이동시 현재의 TCP를 통해서는 매끄러운 전환을 지원할 수 없음을 보여주는 대표적인 예이다.

3.3 이종성이 Network Layer에 미치는 영향

현재 인터넷은 IP 기반의 라우팅을 통하여 통신이 이루어진다. 그러나 다양한 디바이스들의 등장으로 인한 다음과 같은 특징들은 미래인터넷에서 기존 IP 기반의 라우팅 기술의 적용을 어렵게 한다 (Akkaya and Younis, 2005).

첫째, 미래인터넷 환경에서는 휴대용 디바이스 및 센서등과 같이 배터리 사용에 있어서 제약이 있는 기기들이 함께 네트워크를 구성하게 된다. 만약 배터리에 제약이 있는 센서 및 휴대용 단말들에 현 IP 기반의 global addressing scheme을 그대로 적용할 경우 단말의 작동되는 시간이 급격히 줄어드는 심각한 문제가 발생하게 될 것이다.

둘째, 미래인터넷의 다양한 단말들은 전송 파워 및 프로세싱 능력, 대역폭 및 저장공간에 큰 차이를 보인다. 만약 이런 단말의 특성이 고려되지 않고 현 IP 기술에서와 같이 모든 단말들을 동일하게 간주하여 라우팅 경로를 정하거나 채널자원등을 할당하게 되면, 비효율적인 전송으로 인한 전체 네트워크 성능저하를 야기시킬 수 있다.

셋째, 미래인터넷에서는 단말의 이동 특성에 따라 네트워크의 위상적인 구조가 결정 되어진다. 따라서 단말의 이동패턴을 고려하지 않고 네트워크를 형성하게 되면 단말의 움직임에 따라 위상적 구조가 자주 바뀌게 되며, 이와 같은 위상적 구조의 불안정성은 네트워크 구성에 많은 부하를 야기시킬 수 있다. 움직임 패턴에 따라 야기될 수 있는 이동성과 관련한 기타 문제들은 2 절에서 살펴보았다.

제 4 절 인터넷 관리의 어려움

신명기 (2007); 변성혁 (2009)에 따르면 초기 인터넷을 설계할 당시에는 관리성을 핵심적인 사항으로 고려하지 않았다. 더욱이 인터넷 초기에는 단순히 패킷을 최종 목적지까지 보내는 것에 중점을 두고 있었다 (Caesar and Rexford, 2005). 그러나 인터넷의 크기가 점점 더 커지고 ISP가 경제적, 정치적인 이유로 트래픽의 흐름을 제어하려 하면서 다양한 프로토콜이 필요하게 되었다. 이처럼 초기와는 다른 상황에서 인터넷 관리에 있어 문제가 발생하고 어려움을 느끼는 것은 불가피한 일이다 (Clark, 1988).

4.1 SNMP의 문제점

현재는 단순한 망 관리 프로토콜 SNMP를 통해 장비와 네트워크의 오류 등을 감시하는 수준으로 국한되어 인터넷 관리 기능이 제공되고 있다 (Wijnen et al., 2002). 그러나 이 프로토콜은 대규모 망 관리와 라우팅 테이블과 같은 대용량 데이터를 가져오는 데 부적합하다는 단점을 갖고 있는데, SNMP는 net-

work management station이 중심이 되어 각각의 서버로부터 원하는 정보를 가져와 처리하는 중앙집중형 네트워크 관리이기 때문이다 (신명기, 2007; Kim et al., 2010; Baldi and Picco, 1998; Carzaniga et al., 1997). Network management station에 관리 작업이 집중화될 수밖에 없고 처리부하와 함께 네트워크의 트래픽이 증가하게 되는 것이다 (Baldi and Picco, 1998).

더욱이 네트워크의 크기가 증가할 수록 네트워크의 혼잡도와 연결성을 잃는 노드의 수도 증가하여, SNMP를 직접 이용하여 수집할 수 없는 정보도 생겨나고 있다. 네트워크 정보의 수집은 매우 중요하기 때문에 연결성에 영향을 받지 않도록 전체 데이터를 네트워크에 보내어 유지할 수도 있다. 그러나 전체 데이터를 네트워크에 보내면 네트워크 부하의 증가를 초래하고, 네트워크 관리도 더욱 어려워진다 (Liu et al., 2008; Ballani and Francis, 2006).

4.2 BGP의 문제점

BGP는 서로 다른 AS에서 작동하는 라우터가 라우팅 정보를 교환할 수 있도록 해주는 외부 라우팅 프로토콜이다. 초기에는 매우 간단한 거리벡터 프로토콜로 소개되었다. 그러나 시간이 지날 수록 ISP가 라우팅을 제어할 수 있도록 하기 위해 기능이 추가되었고, 예측불가능한 많은 상황들이 있었고 많은 매커니즘이 겹치는 경우가 일어나 프로토콜의 복잡도가 증가하였다. 복잡도의 증가는 서로 다른 ISP간 정책에서의 혼란 발생 등 많은 문제들을 야기시켰다. 이러한 BGP 상의 문제점은 Clark et al. (2007)도 지적하고 있다.

ISP 간에 협상할 수 있는 경제적인 관계에 있어 BGP는 제한을 두었다. BGP의 문제점들은 아주 천천히 개선되기도 했지만, 충분히 보안성이 보장된 것이 아니었고 몇몇 상황 속에서 다시 불안정한 상태가 되며 라우팅에 있어서 일관되지 않는 상태가 발생하였다 (Varadhan et al., 2000). BGP의 문제점들은 그 원인까지 충분히 규명되지 않았지만, 여전히 규모가 큰 인터넷 상에서 쓰이고 있다. BGP를 대신할 수 있는 좀 더 나은 수렴성을 보장하는 프로토콜의 개발이 필요하다.

4.3 관리자의 실수로 인한 네트워크 사고

지금의 인터넷은 변성혁 (2009)에 따르면 네트워크 분리, 라우팅 설정, 보안설정, 트래픽 엔지니어링, BGP 정책 설정, VPN관리 등의 설정을 숙련된 관리자가 직접 한다고 알려져 있다. 이때, 네트워크 설정에 있어 관리자의 실수는 곧 네트워크 사고로 이어진다.

Kerravala (2004)의 그림 4.2은 전체 네트워크 사고의 62퍼센트는 관리자의 실수에 의한 것으로 그 사고중의 일부는 예방할 수도 있었던 일이었음을 보여준다. 네트워크 문제가 발생했을 때에도 그 발생 원인을 쉽게 찾아낼 방법이

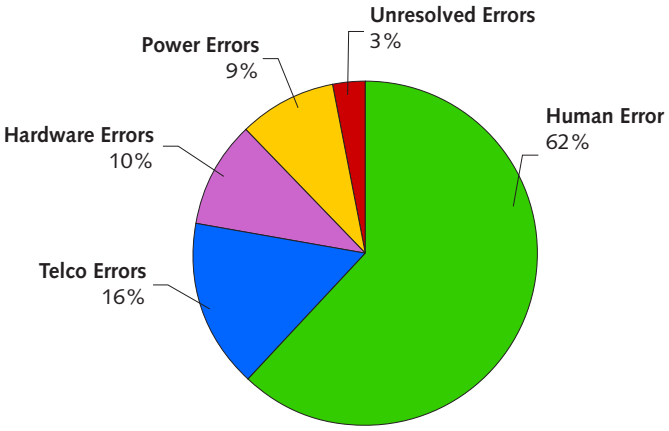

그림 4.2: Network downtime survey by the Yankee Group (Kerravala, 2004)

부족하고 제한적인 망 상황 데이터를 바탕으로 관리자의 능력에 의존하여 원인을 분석하는 실정이다. 다음은 관리자의 실수에 의해 네트워크가 마비되었던 사고들이다. 본 섹션에서는 관리자의 실수로 네트워크 설정 사고가 일어났던 몇몇 예들을 살펴보겠다.

- *2010*년 *4*월 *8*일 중국, 잘못된 라우팅 정보의 전송
  McMillan (2010)에 의하면 2010년 4월 8일 중국 IDC China Telecommunication에서 잘못된 라우팅 데이터가 전송되어 Deutsche Telecom, Qwest Communications와 같은 인터넷 서비스 제공업체에 영향을 미쳤다. 문제가 해결될 때까지 CNN, Starbucks, Apple에서 전송되어야 할 32000 내지 37000개 정도의 라우팅 정보들이 중국 ISP에서 잘못 전송되었다.

- *2008*년 *2*월 *24*일 미국 및 아태지역, 유튜브가 *40*분간 중단
  Svensson (2008)에 의하면 유튜브에 이슬람교에서 신성시 하는 마호메트를 풍자한 만화와 이슬람을 부정적으로 묘사한 네덜란드 영화의 예고편이 유통되었다. 파키스탄 통신당국은 자국민의 유튜브 접근을 차단하였다. ISP에 유튜브 이용 중단을 지시하면서 웹서버 주소를 탈취하여 이 사이트로 접속할 경우 자동으로 다른 사이트에 옮겨지도록 하였다. 이 과정에서 홍콩 통신업체인 PCCW에도 웹서버 주소가 전해져 태평양권 국가들의 ISP에서 유튜브 접근이 차단되는 사고가 일어났다.

- *1997*년 *4*월 *25*일 플로리다, *2006*년 *1*월 *22*일 *Con Edison* 사
  1997년 4월 25일 플로리다에서 일어난 사건 (Barrett et al., 1997)과 2006년 1월 22일 Con Edison 사 (Underwood, 2006)에서 일어난 사건의 원인은 모두 BGP의 잘못된 설정으로 인한 라우터의 환경설정 상의 실수에

있다. 이로 인해 인터넷 상에 잘못된 라우팅 정보가 송신되었고, 대부분의 인터넷 트래픽은 이 작은 ISP로 보내져 인터넷이 제 기능을 못하였다.

- *2009*년 *2*월 *16*일 체코
  2009년 2월 16일 체코에서도 BGP의 잘못된 설정으로 인해 다른 회사들의 네트워크가 작동되지 않는 일이 발생했다 (Miller, 2009). 체코의 ISP가 잘못된 명령을 브로드캐스팅하면서 iWeb이나 Media Temple등의 웹 호스팅 회사들이 피해를 입었다.

이와 같은 네트워크 상에서 발생한 문제를 단순히 관리자의 능력에 의존하여 원인을 분석하고 해결하기보다는 좀 더 체계적이고 시스템적 망관리를 통해 문제의 원인을 찾아낼 수 있도록 해야 한다는 요구가 높다 (Clark et al., 2007).

제 5 절 Spoofing

Spoofing은 일반적으로 데이터를 조작하여 위장함으로써 사용자들 및 시스템들을 속이는 형태의 보안 공격을 의미한다. 현재까지의 보고된 spoofing 공격은 인터넷 시스템의 각 layer에 걸쳐 다양한 형태를 띄고 있으며 심각한 보안 문제들을 야기시켜 왔다. 여기서는 spoofing 공격의 종류와 각각의 공격에 대한 발생 원인에 대해서 알아보고자 한다.

5.1 ARP spoofing

ARP는 사용자들로 하여금 최신의 경로 정보를 유지하게 하기 위해서 자신의 요청에 대한 ARP reply가 아니더라도 수신되는 모든 ARP reply를 바탕으로 ARP 테이블을 업데이트 하도록 한다. 또한 이렇게 전송되는 ARP reply 패킷에 대해서 어떠한 인증절차도 제공하지 않는다. ARP spoofing 공격은 이와 같은 로컬 네트워크에서 사용하는 ARP의 취약점을 악용하여 자신의 MAC 주소를 다른 사용자의 MAC 주소인 것처럼 속이는 공격이다 (Ramachandran and Nandi, 2005). 악의적인 사용자는 ARP 패킷을 조작하여 자신이 게이트웨이인 것처럼 MAC 주소를 위장하고는 로컬 네트워크에 있는 사용자들에게 전송한다. 따라서 사용자들은 진짜 게이트웨이 대신에 악의적인 사용자쪽으로 패킷을 전송하게 되고, 이를 통해 악의적인 사용자들은 통신을 엿듣거나 패킷을 조작할 수 있다.

5.2 IP spoofing

IP spoofing은 자신의 IP주소를 해당 노드가 신뢰하는 노드의 주소로 바꾸어 인증받지 못하는 컴퓨터에 접근하는 공격이다 (Harris and Hunt, 1999). 이는

IP layer에서 별도의 인증절차 없이 단순히 패킷의 송신측 주소 항목만을 보고 전송측 노드를 확인하기 때문에 발생하게 된다. 기타 상위 계층 및 애플리케이션에서 역시 이와 같이 패킷에 적혀있는 송신측 주소 항목만으로 노드를 인식하는 경우가 많은데 이로 인하여 송신측 주소값만 수정하게 되면, 비정상적인 접근이 얼마든지 가능하게 된다.

5.3 Web spoofing

Web spoofing은 phishing의 본래 이름이다. Web spoofing은 신뢰할 만한 사이트와 비슷한 모양의 위장 사이트를 만들어 놓고 사용자들로 이 위장 사이트에 접속하게 한 뒤 사용자 정보를 빼내는 형태의 보안 공격이다 (Felten et al., 1997). 공격자는 DNS cache에 정보를 조작하여 사용자들이 위장싸이트로 접근하도록 하며, 웹 브라우저에는 현재 방문하고 있는 위장 사이트 주소가 아닌 원래 접속하려던 신뢰할만한 사이트 주소를 보여주도록 하는 URL spoofing을 수행하기도 한다. 위장 사이트에 접속된 사용자들은 로그인을 위해서 계정과 패스워드를 입력하게 되고 이 정보들은 고스란히 공격자의 서버에 기록되게 됨으로써 개인 신상에 대한 보안 위협을 가하게 된다.

5.4 E-mail spoofing

E-mail spoofing은 e-mail의 보내는 사람 주소 및 기타 정보를 수정하여 마치 다른 사람이 보내는 것처럼 위장하는 형태의 보안 공격 방법으로 스팸이나 phishing e-mail등에서 주로 사용된다 (Lawton, 2005). 일반적으로 메일 서버인 SMTP 서버에서 특별한 인증 절차를 제공하고 있지 않기 때문에 보내는 사람이 쉽게 자신을 숨길 수 있다. 특히 e-mail spoofing의 경우, 제 삼자에게 피해를 끼칠 수도 있는데 악의적인 사용자가 제 삼자의 주소로 스팸을 전송했을 경우, 스팸의 수신측 서버에서 제 삼자의 주소를 차다시키는 경우가 발생할 수 있기 때문이다.

5.5 Caller ID spoofing

Caller ID spoofing은 Voice over IP (VoIP) 서비스가 인터넷을 통해 제공되면서부터 그 심각성을 더하게 된 공격 방법이다 (Butcher et al., 2007). VoIP 기술에서는 기존 전화망에서와 비교하여 전화를 건 사용자의 정보 수정이 보다 용이하다. 따라서 공격자들이 위장된 번호로 전화를 걸어 수신한 사용자로 하여금 신뢰할만한 사람으로 오인하게 만들 수 있다. VoIP가 인터넷을 통해 기존의 전화망까지 연결되어 서비스되는 것을 생각해보면 그 적용범위가 매우 큰 공격 방법 중 하나이다.

제 6 절 DDoS 공격

Denial of service (DoS) 공격은 악의적인 사용자가 컴퓨터나 네트워크 시스템의 자원들을 고갈시킴으로써 정상적인 서비스가 불가능하도록 만드는 형태의 공격을 의미한다. DoS 공격은 일반적으로 피해 시스템을 직접적으로 파괴시키기보다는 시스템으로의 정상적인 접근을 차단시키거나 시스템 성능을 저하시키는 특징을 가진다. 최근 들어서는 분산적인 형태의 공격인 distributed denial of service (DDoS) 로 진화하면서 인터넷에 더욱 큰 피해를 야기시키고 있다. DDoS 공격은 다수의 컴퓨터들이 동시에 피해 노드에 DoS 공격을 행하는 형태이기 때문에 공격을 사전에 예방하거나 혹은 발생시 피해를 줄이는 데 있어서 훨씬 큰 어려움이 있다. 여기서는 DDoS 공격에 대한 발생 원인 및 공격 방법, 그리고 현재까지 보고된 공격 형태들에 대해서 기술한 Douligeris and Mitrokotsa (2004) 의 내용을 정리해보았다.

6.1 DDoS 공격을 가능하게 하는 요인

현재 인터넷 시스템은 효율성 측면을 고려하여 end-to-end paradigm 에 기반하여 설계되어 있다. 네트워크는 단지 best-effort 형태로 최소한의 패킷 포워딩 서비스만을 수행하며, 기타의 QoS, 신뢰성, 보안성 등의 측면은 송수신 노드쪽에서 구현하도록 하고 있다. 이와 같은 설계는 패킷 전달이라는 측면에서 효율성을 극대화 할 수 있지만, 통신하는 두 노드 중 한쪽이 악의적인 노드일 경우 쉽게 다른 한쪽에 피해를 줄 수 있기 때문에 보안상의 문제를 야기시키게 된다. 인터넷의 보안상 취약점과 더불어 Mirkovic and Reiher (2004) 에서 설명하는 다음과 같은 DDoS 공격의 특징은 DDoS 공격이 쉽게 수행될 수 있도록 하는 이유이다.

- Internet security is highly interdependent
  DDoS 공격은 인터넷상의 보안이 취약한 노드들을 이용하기 때문에 피해 시스템의 보안 상태와는 직접적으로 연관이 없다.

- Limited Internet resource and many against a few
  인터넷 상에서의 노드들은 제한적인 자원을 가진다. DDoS 공격은 이런 자원의 제한성을 이용하여 공격 대상에 비해 훨씬 큰 자원을 이용하여 공격을 수행하기 때문에 대부분 성공할 수밖에 없다.

- Intelligence and resources are not allocated
  앞에서 언급한 바와 같이 네트워크는 패킷 전달에만 최적화되어 있으며, 기타 서비스의 필요에 대해서는 송수신 노드 쪽에서 구현하도록 하고 있다. 또한 패킷 전달의 최적화로 중간 네트워크의 대역폭이 훨씬 크게 설

계되어 있다. 따라서 대용량의 메시지 flooding이 가능하며, 이를 네트워크 단에서 차단할 수 없다.

- Accountability is not enforced
  5.2 절에서 설명된 IP spoofing을 통해 패킷의 송신자를 얼마든지 위장할 수 있기 때문에 공격자들은 이점을 이용하여 다양한 공격을 수행할 수 있다.

- Control is distributed
  인터넷의 관리는 분산적으로 이루어지며, 각각의 네트워크들은 각기 다른 정책을 바탕으로 관리된다. 이와 같은 분산적인 관리체계로 인해 보안정책 및 보안관련 기술 적용등이 쉽지 않다.

6.2 DDoS 공격 방법

DDoS 공격은 수많은 컴퓨터들이 피해 시스템에 연결되어 이루어진다. 이들 컴퓨터들은 대부분 취약한 보안 상태로 유지되어 공격자의 제어하에 빠지게 된다. 이런 컴퓨터들은 자체적으로도 보안 문제가 생기는 것이지만 이들은 독립된 피해 시스템에 DDoS 공격을 가하게 되는 것으로 악용되게 된다. 공격자가 이들 수많은 컴퓨터들을 하나의 피해 시스템과 연결하여 DDoS 공격을 수행하게 되는 것이다. 수많은 컴퓨터들을 모두 상대하기 위해 피해 시스템은 자원을 과도하게 필요하게 되고, 이 때문에 공격과 상관없는 실질적인 작업들을 수행할 수 없고 정당한 사용자들도 피해 시스템을 이용할 수 없도록 한다.

6.3 DDos 종류

6.3.1 Flood attack

Flood attack은 agent들이 피해 노드쪽으로 많은 양의 패킷을 전송하여 피해 노드의 대역폭을 점령하는 형태의 공격이다. 이때 전송되는 패킷의 양이 피해 노드에서의 패킷 처리 속도를 넘어서게 되는 경우는 시스템을 다운시킬 수도 있다. 대표적인 예로 UDP flood attack과 ICMP flood attack이 있다 (Criscuolo, 2000). UDP flood attack은 agent들이 피해 노드의 임의의 포트로 처리능력 이상의 대량의 UDP 패킷을 전송하면서 이루어진다. 이때 공격에 사용되는 패킷에 송신측 주소를 조작함으로써 공격자는 자신을 숨길 수 있다. ICMP flood attack에서는 원격에 있는 노드가 살아 있는지를 확인하기 위해 사용되는 ICMP echo request 패킷이 사용된다. 이런 패킷을 수신하게 되면 피해 노드는 이에 대한 응답 패킷을 생성하게 되기 때문에 대량의 응답 패킷들로 인해 피해 노드의 네트워크 연결를 마비시킬 수도 있다.

6.3.2 Amplification attack

Amplification attack은 broadcast IP 주소의 특성을 이용하는 공격 방법이다. 패킷의 수신주소가 broadcast IP 주소일 경우는 broadcast 주소 범위 안에 있는 모든 노드들에게 패킷이 전송되게 되어있다. 이와 같은 주소 특성을 이용하여 공격자는 agent들로 하여금 broadcast 주소로 패킷을 전송하게 하여 공격 트래픽의 양을 늘려 대역폭을 소모하게 만들 수 있다. 또한 공격자가 broadcast 패킷을 직접 전송하여 다수의 수신 노드들로 하여금 공격을 위한 agent들로 사용하는 방법이 있다. 이렇게 사용되는 agent를 reflector라 이름한다. Smurf와 fraggle attack이 대표적인 amplification attack이다. Smurf 공격은 attacker가 ICMP echo request 패킷을 broadcast address로 전송을 하면서 이루어진다 (Huegen, 2000). 이때 공격 대상 노드의 주소를 송신측 주소로 세팅하면 패킷을 수신한 많은 reflector들로부터 엄청난 양의 답장이 피해 노드쪽으로 전송되면서 피해 노드를 마비시키게 된다. Fraggle attack은 ICMP echo 패킷 대신에 UDP echo 패킷을 사용하는 공격으로 그 형태는 smurf와 비슷하지만 더 많은 양의 traffic을 생성시킬 수 있기 때문에 smurf보다 더 큰 피해를 야기시킬 수 있다.

6.3.3 Protocol exploit attack

Protocol exploit attack은 인터넷 프로토콜 상의 특징이나 구현상의 버그를 이용하여 공격하는 방법으로 TCP SYN attack이 대표적인 예이다. TCP SYN attack은 TCP 연결을 처음 맺을 때 수행되는 three-way handshake의 구현상의 문제를 이용한 공격방법이다. TCP는 신뢰성 있는 데이터 전송을 위해서 sequence number를 사용하는데 TCP 연결을 맺을 때 sequence number의 시작값을 서로 통일시키기 위해서 three-way handshaking과정을 수행한다. 먼저 전송측 노드가 SYN request 패킷을 수신측 노드로 전송하면 이를 수신한 노드는 SYN/ACK 패킷을 전송측 노드로 보내고 마지막으로 전송측 노드가 수신측 노드에게 ACK패킷을 전송함으로써 서로간의 sequence number를 통일시키게 된다. 이때 SYN request를 수신하기 위해서 수신측 노드는 SYN request를 위한 listen queue를 마련하고 열려진 connection으로부터 패킷이 오기를 75초간 기다리도록 구현되어 있다. 공격자들은 listen queue의 크기가 작다는 점을 이용하여 SYN requests를 flooding 시키고는 돌아오는 SYN&ACK에 대한 응답하지 않는다. 이럴 경우, 공격자들이 flooding한 패킷으로 수신 측 노드의 listen queue를 채울 수 있기 때문에 다른 정상적인 노드로부터의 연결요청을 차단시킬 수 있다 (Schuba et al., 1997).

6.3.4 Malformed packet attacks

Malformed packet attack은 정해진 프로토콜 규격에 맞지 않는 IP 패킷들을 전송함으로써 피해 시스템을 마비시키는 형태의 공격방법이다. 대표적인 예로 IP address attack과 IP packet option attack이 있다. IP address attack은 패킷의 source address 및 destination address field를 모두 피 시스템의 주소로 세팅하여 피해 시스템의 운영체제를 공격하는 방법이다. IP packet option attack은 IP 패킷의 option field들을 다 1로 세팅함으로써 타켓 시스템의 프로세싱 시간을 증가시키는 공격방법이다. 많은 agent들이 동원되어 IP packet option attack이 이루어질 경우 피해 시스템을 마비시킬 수도 있다.

6.4 DDoS 대비 현황

DDoS 공격은 그 형태가 다양한 만큼 DDos 트래픽의 특성도 다양하기 때문에 감지를 하는 것이 쉽지 않다. 또한 분산된 형태로 공격이 진행되기 때문에 공격에 대처하거나 공격자를 찾아내는 것 또한 상당히 어렵다. 필터를 이용하여 DDoS 공격 패킷들을 사전에 걸러내거나 보안패치를 통해 시스템 버그를 줄임으로써 기존의 DDoS 공격에 대해 효과적으로 예방할 수 있도록 하였지만, 이와 같은 예방법들은 새로운 형태의 공격에 대해서는 보안상 취약할 수 밖에 없다. DDoS 탐지 역시 발생된 공격에 대해 트래픽의 통계를 수집하고 이를 분석하는 방법을 통해 이루어지게 되는데, 탐지 방법 역시 습득을 통한 데이터 베이스구축에 기반한 방법이기 때문에 새로운 타입의 보안 공격에 있어서는 한계를 드러낼 수 밖에 없다.

제 7 절 기타 보안 문제

본절에서는 spoofing과 DDoS 이외의 보안 공격들과 관련하여 현재 인터넷 시스템에서의 보안 취약점 및 이를 해결하기 위해 제시된 방안들에 대해 간략하게 살펴본다.

7.1 TCP/IP 기반의 보안 취약점을 이용한 보안 공격

7.1.1 Routing attack

이 방법은 Routing Information Protocol을 이용하는 방법이다. Routing Information Protocol은 네트워크 내에서 routing 정보를 퍼뜨리거나 하기 위해서 사용되는 프로토콜이다. TCP/IP과 같이 프로토콜 내에 별도의 인증 절차가 없기 때문에 단순히 Routing Information Protocol에서 제공되는 정보들이 확인없이 그대로 사용되는 경우가 많다. 따라서 악의적인 노드는 이 Routing

Information Protocol의 정보를 임의로 수정함으로써 라우팅 경로를 원하는쪽으로 바꿀 수 있다. 이로 인하여 원하는 패킷을 악의적인 노드를 지나가도록 함으로써 패킷을 모니터링하거나 수정할 수 있게 된다. 뿐만 아니라 특정 노드에게 가는 모든 패킷들을 다른 경로로 지나가게 설정함으로써 특정 노드를 네트워크에서도 배제시킬 수 있게 된다 (Baltatu et al., 2000).

7.1.2 ICMP attack

ICMP 역시 프로토콜 내 인증과 관련된 절차가 없기 때문에 이 패킷을 사용하여 여러가지 보안 공격이 가능하다. ICMP를 이용한 가장 대표적인 공격으로는 앞에서 언급한 바와 같이 ICMP Time exceeded 메시지나 Destination unreachable 메시지를 이용하는 DoS공격이 있다. 또한 ICMP redirect 메시지를 통해서 다른 노드에게 가는 패킷을 가로챌 수도 있다. ICMP redirect 메시지는 송신측 노드의 라우팅 정보를 업데이트 하게 하기 위해서 gateway router로부터 송신측 노드로 전송되는 메시지이다. 즉 송신측 노드의 라우팅 정보가 잘못되어 있을 경우 이를 바로잡기 위한 목적으로 사용되는 메시지이다. 만약 악의적인 노드가 이 ICMP redirect 메시지를 악용할 경우, 임의의 노드로 하여금 특정 connection으로 패킷들을 전송하게끔 할 수 있다 (Baltatu et al., 2000).

7.1.3 DNS attack

DNS는 인터넷 상에서 호스트 이름과 IP주소를 매핑시켜주기 위해 사용되는 프로토콜이다. 악의적인 노드가 이 매핑 정보를 이용하게 되면 name-based 인증절차에 문제를 일으킬 수 있다 (Bellovin, 1995).

7.1.4 IPsec

앞에서 살펴본 바와 같이 지난 수십년간 현재의 인터넷 시스템 버그 및 디자인 한계에 기반한 네트워크 보안 공격 등이 보고 되었고, 또 그에 대한 해결책들이 등장하였다. (Bellovin, 1989; Howard, 1997; Harris and Hunt, 1999). IETF에서는 현재 인터넷 구조 내에서 보안 시스템을을 제공하고자 IPsec 아키텍쳐를 제시하였다 (Oppliger, 1998). IPsec은 아래와 같은 취약점에 대한 해결책을 제시한다.

Password sniffing 악의적인 사용자가 연결을 도청하는 방법으로 암호화되지 않는 비밀번호를 알아내는 방식의 공격

IP spoofing 패킷의 IP 주소를 수정함으로써 악의적인 노드가 신뢰할 수 있는 노드인 것처럼 가장하여 시스템에 침입하는 방식의 공격

Session hijacking 다른 노드가 연결에 대한 인증을 받은 후에, 해당 연결을 넘겨받는 방식의 공격

7.2 무선 환경의 특성으로 인한 보안 취약점 및 보안 이슈

무선 환경에서의 인터넷 시스템은 유선 환경과는 구별된 다음과 같은 특징을 보인다.

- No fixed infrastructure
- Peer-to-peer architecture with multi-hop routing
- Mobile device physical vulnerability
- Strigent resource contraints
- Wireless medium
- Node mobility

무선 환경에서 보여지는 인터넷 특징들은 새로운 형태의 보안 공격들을 가능하게 하였으며, 또 기존의 보안 대책들을 적용시키는데 문제를 야기시키고 있다. 여기서 Djenouri et al. (2005); Hu and Perrig (2004); Yang et al. (2004)의 내용을 정리하여 무선 환경의 특성들을 이용한 보안 공격들에 대해 알아보고자 한다.

No expert maintenance 무선 네트워크에서 각각의 단말들의 역할이 커짐에 따라서 단말이 네트워크 시스템을 유지하는데 역할도 크다. 커진 역할 만큼 강화된 보안을 유지하는 것이 필수적이 되었다. 그러나 단말들에 대한 관리는 개개인을 통해서 이루어지기 때문에 단말 자체의 보안성 유지에 한계가 있다. 악의적인 노드는 이런 취약한 노드를 쉽게 공격할 수 있으며, 이런 공격을 통해 유선과는 달리 그 나쁜 영향력을 보다 쉽고 빠르게 네트워크에 전파시킬 수 있다.

Routing and packet forwarding attack 멀티홉 무선환경에서는 각각의 노드들이 목적지까지 패킷을 전해주는 라우터 역할을 담당한다. 노드들간 라우팅 메시지를 교환하면서 경로를 설정하고 해당 경로로 패킷을 전달하게 되어 있다. 이와 같은 라우팅 및 패킷 포워딩에 각각의 단말들이 참여하게 되면서 악의적인 노드가 쉽게 이를 악용할 수 있다. 원래 설정된 경로를 임의로 바꾸거나, 악의적인 노드쪽으로 패킷을 전송하게 함으로써 패킷을 도청할 수 있다. 고의로 라우팅 loop을 만들 수도 있으며, 네트워크를 고의로 혼잡하게 만들거나 특정 노드를 네트워크에서 배제시키거나 네트워크를 분리시킬 수도 있다. 뿐만 아니라 임의로 쓰레기 패킷들을 전송함으로써 특정 단말 및 네트워크를 공격할 수 있다.

Impossiblity of complex computation 미래 인터넷환경에서는 PDA 및 센서 등과 같이 에너지나 대역폭등이 제한적인 기기들도 네트워크를 구성하게 된다. 이와 같은 기기들에 있어서는 현재의 복잡하고 많은 자원을 필요로하는 암호화나 보안 대책들을 적용시키는 데는 한계가 있다.

No fixed security infrastructure 암호화를 통한 보안은 현재 네트워크에서 널리 사용되는 보안 방법이다. 그러나 이동성 단말들이 참여하는 미래의 인터넷환경에서는 고정된 인프라를 가정하는 것이 쉽지 않다. 단말이 네트워크간을 이동하거나 새롭게 로컬 네트워크를 구성하는 경우에도 계속적으로 보안을 유지하도록 하기 위해서는 보안 인증센터 등과 같은 고정된 인프라에 의지하지 않는 방법이 강구되어야 한다.

Link layer의 보안 취약점 가장 널리 쓰이는 무선 인터페이스인 802.11의 경우 경쟁을 통해 채널을 할당받는다. 악의적인 노드는 이 경쟁의 규칙을 따르지 않고 경쟁에 참여함으로써 채널을 독점적으로 소유, 다른 노드들의 채널 접근을 차단시킬 수 있다. 뿐만 아니라 잘못된 이벤트를 고의적으로 발생시킴으로써 denial of service attack도 가능하다.

제 5 장

현재 인터넷의 문제점 분석

인터넷의 모태인 ARPANET 이 처음 만들어졌을 때 연구의 중점은 단지 멀리 떨어져 있는 여러 컴퓨터들을 어떻게 연결할 수 있는가에 집중되었다. 당시에 컴퓨터들은 상당히 고가의 장비였기 때문에 이는 다른 조직을 직접 방문하지 않고도 그 조직의 컴퓨터를 쓸 수 있도록 하는 획기적인 발전이었다. 수백대 정도의 컴퓨터들을 연결시키기 위한 작업에 노력이 집중되었고, 컴퓨터들을 들고다니면서 연결 도중에도 수시로 움직이는 것은 상상도 못하였다. 그리고 ARPANET 에 연결된 컴퓨터들을 악의적으로 사용하는 경우에 대한 고려를 많이 하지 못했다.

ARPANET 이 NSFNET 으로 바뀌고 지금의 인터넷으로 발전하면서 상황은 많이 바뀌었다. 이제 인터넷은 전세계적으로 많은 사람들이 일상적인 통신 수단 및 정보 수집 수단으로 사용하게 되었다. 이중에서 악의적으로 인터넷에 접촉하는 사람들도 많으며, 아예 상업적으로 인터넷의 보안 허점을 악의적으로 이용하여 범죄행위를 저지르는 경우가 많아졌다. 컴퓨터들도 매우 가격이 떨어지고 크기가 작아져 지금은 주머니 안에 ARPANET 당시의 컴퓨터들보다도 강력한 소형 기기를 인터넷에 연결해 들고 다니면서 생활하고 있다. 이렇게 상황이 바뀌면서 인터넷의 한계가 여러 가지 드러나고 있다.

우선은 인터넷의 규모가 급격하게 커지면서 인터넷의 설계에서 확장성이 모자라는 부분이 많이 드러나고 있다. 인터넷에서 가장 중요한 기능인 정보 전송은 인터넷의 핵심이 되는 라우터들에 의존하는데, 이들이 사용하는 라우팅 테이블들의 크기가 매년 급격하게 증가하고 있다. 이를 수용하기 위해 라우터들의 비용도 따라서 급격하게 증가해야 할 뿐만 아니라, 이들 라우팅 테이블들을 유지하기 위한 통신 부하도 급격하게 증가하고 있다. 라우팅 테이블의 크기가 이처럼 문제가 될만큼 커지게 된 것에는 인터넷 라우팅의 설계가 이론적으로 확장성이 있도록 되어있지 못했기 때문이다.

인터넷의 확장성 부족이 관리성 부족으로도 이어졌다. 인터넷의 관리를 상

당 부분 수동적으로 이루어지도록 설계되었는데, 이는 인터넷의 규모가 아직 작았을 때에는 문제가 생기지 않도록 관리하는 것이 상대적으로 쉬었고 문제가 생겨도 이에 영향을 받는 사람이 적었기 때문에 상대적으로 큰 문제는 아니었다. 하지만 현재 인터넷의 규모가 엄청 커지면서 조그마한 설정 실수가 전 세계적으로 문제를 일으키는 경우들이 빈번하게 생기고 있고, 하물며 현재 인터넷 전체의 모습을 정확하게 아는 것조차도 가능하지 않다. 이를 고려하면 미래인터넷은 관리가 최대한 자동적으로 되어 문제가 없도록 해야 하고, 수동으로 관리하는 부분이 있어도 문제가 생기지 않도록 설정 실수를 막을 수 있어야 한다.

인터넷의 규모 확장으로 distributed denial of service 공격들도 가능하게 되었다. 소프트웨어나 네트워크 프로토콜의 설계 및 구현에 문제가 있어 denial of service에 취약하게 되는 경우도 많았지만, distributed denial of service는 근본적으로 과부하가 생길 수 있을만큼 한 곳으로 요청이 몰렸을 경우 이를 수용하지 못하기 때문에 가능하게 되는 것이다. 이러한 공격을 막기 위해 온갖 방법들이 개별 조직들에서 동원되고 있는 상태인데, 인터넷 자체는 여전히 이러한 문제를 막아주지는 못한다. 악의적이지 않은 정당성 있는 요청이 과하게 몰려도 과부하가 생기지 않도록 되면 distributed denial of service 공격도 무력화되므로, 근본적으로 이는 인터넷의 확장성을 개선하여 해결이 되야 할 문제이다.

Distributed denial of service 공격 외에도 인터넷에는 수많은 보안 문제들이 생겼다. 많은 부분들이 소프트웨어 버그에서 생긴 경우들도 많지만, 네트워크 프로토콜들의 설계에서 근본적인 보안 문제들이 존재하는 경우들도 많다. 이를 고려하면 소프트웨어나 네트워크의 설계에 있어서 이론적으로 치밀한 바탕 위에서 버그 등을 근본적으로 막아주는 도구들이 필요가 있다. 반면에 여러 보안 문제들이 생각하지도 못한 부분에서 허점을 찾아 생기는 경우들도 많다. 다른 문제들과 달리 사람이 어떻게든 허점을 찾아 악용하려고 하기 때문에 보안 문제들을 완전히 근절할 수 있다고 기대하기는 어렵다. 따라서 보안 문제가 생겼을 때 이에서 회복할 수 있는 것도 중요하다.

인터넷에서 또하나 매우 부족한 부분은 이동성에 관한 고려이다. 가지고 다니면서 인터넷에 연결하여 이용하는 소형 기기들의 수가 크게 증가하고 있고 근미래에 이동기기가 오히려 고정된 컴퓨터가 많아질 전망이지만, 인터넷 자체에서 이동성을 위한 지원이 거의 없는 상태이다. IPv4나 IPv6를 확장하여 이동성을 지원하기 위한 시도들은 여러번 있었지만 아직까지는 널리 쓰이는 경우가 거의 없다. 미래인터넷이 현재 인터넷의 확장이 아니라 새로운 구조를 이용하게 된다면, 이는 이동성이 미래인터넷 구조에서 덧붙여서 지원되는 것이 아니라 근본적으로 지원되어야 함을 시사한다.

현재 인터넷에 이러한 문제들이 있는 것을 고려하였을 때, 미래인터넷을 만

들기 위한 연구는 어떻게 이루어져야 할 것인가? 이런 문제들이 생기게 된 원인을 생각해보면 필요한 네트워크 기술들이 서로 체계적으로 개발되지 않고 이론적으로 치밀한 고려가 부족한 상태에서 그때그때 만들어져 적용된 면이 많았기 때문이라고 생각할 수 있다. 또한 많은 문제들이 독립적으로 발생되는 것이 아니라 연관이 되어 있는 것도 볼 수 있다. 이를 고려하면 미래인터넷을 만들어나가기 위해서 현재까지 인터넷에서 얻은 교훈들을 바탕으로 이론적으로 탄탄한 기반 위에서 연구 개발이 이루어야 되지 않을까 생각을 한다.

제 6 장

결론

1972 년 ARPANET 으로 태동된 인터넷은 TCP/IP 기반 네트워크로서 그 형태를 갖추기 시작하여 지난 40 년간 전 세계를 연결하는 네트워크로서 중요한 역할을 담당해왔다. 최근 통신 기술들의 발달과 더불어 새로운 형태의 기기 및 사용자들의 다양한 요구사항은 인터넷으로 하여금 새로운 변화의 필요성을 느끼게 하였다. 통신 기기들의 폭발적인 증가와 더불어 통신 영역의 확대로 인해 인터넷은 급속도로 규모의 성장을 거듭하게 되었고, 인터넷의 확장성을 지원하기 위한 보다 근본적인 기술들을 필요로 하게 되었다. 뿐만 아니라 거대해진 인터넷에 대한 효율적인 관리 시스템의 부재로 인해 전세계적인 통신 장애가 발생하여 큰 문제로 인식되기 시작하였으며, 다양한 무선 기기 및 네트워크를 통합시키기 위한 이동성 지원 및 이종성 지원 관련 문제, 그리고 더욱 커지고 다양해진 인터넷 환경에서의 보안 문제 등이 집중적으로 거론되기 시작하였다.

본 기술문서에서는 확장성, 관리성, 이동성, 이종성, 그리고 보안성 측면에서 현재 인터넷이 직면하고 있는 대표적인 문제 사례들을 살펴보았다. 라우팅 테이블의 폭발적인 증가 및 BGP 프로토콜의 복잡도의 증가로 인한 문제들은 인터넷 기반 기술들이 가지는 확장성 측면의 한계를 보여주고 있다. 유선 망을 기반으로 개발되어 발전해온 인터넷에서의 이동성 지원 부재 역시 현재의 보편화된 무선 환경에 적합하지 않은 인터넷 디자인의 한계를 나타낸다. 다양한 통신 기술 및 기기들을 인터넷으로 통합시키는 데 있어서 제기된 기반 기술들의 비효율성 및 부적합성은 현재의 인터넷 모델이 미래의 다양한 특성들을 수용하는데 있어서의 어려움이 있음을 지적하고 있다. SNMP 로 대표되는 중앙 집중형 형태의 인터넷 모니터링 시스템은 더 이상 거대해진 인터넷을 관리하는데 부적합하다는 것이 보고되고 있고, 특히 관리자가 직접적으로 관여하는 현재의 관리 체제하에서 보고된 인적 사건 사고들을 통해 효율적인 관리성 측면의 강화에 대한 필요성을 제시하고 있다. 그리고 대표적인 보안 공격인 Spoofing 및 DDoS 공격과 더불어 새로운 무선 인터넷 환경에서 야기될 수 있는 여러가지

형태의 보안 공격들을 살펴봄으로 현재 인터넷이 가지는 보안 관련 취약점등을 살펴보았다.

현재의 인터넷은 개발 당시부터 확장성, 관리성, 이동성, 다양성, 보안성 등에 대한 고려가 상당히 부족한 상태에서 설계되었다. 또한 이들 부족한 부분들을 보완하기 위해 기술을 개발하여도 기존에 있던 인터넷에 덧붙이는 식으로 되어 널리 쓰이게 되는 경우가 적었고, 널리 쓰이게 되어도 또다른 문제들을 일으키는 경우도 많았다. 이런 부족한 부분들을 극복한 안정된 미래인터넷을 만들기 위해서는 한쪽 측면만으로 기술들을 개발하지 않고 모든 측면을 같이 고려하여 이론적으로 탄탄한 기반 위에서 연구 개발이 이루어져야 한다.

참고 문헌

AKARI Architecture Design Project. *New Generation Network Architecture AKARI Conceptual Design*. NICT, May 2010. Version 2.0 (preliminary).

Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3:325–349, May 2005. doi:10.1016/j.adhoc.2003.09.010.

Mark Allman, Spencer Dawkins, Dan Glover, Jim Griner, Diepchi Tran, Tom Henderson, John Heidemann, Joe Touch, Hans Kruse, Shawn Ostermann, Keith Scott, and Jeffrey Semke. Ongoing TCP research related to satellites. IETF RFC 2760, February 2000.

Hari Balakrishnan, Venkata N. Padmanabhan, and Randy H. Katz. The effects of asymmetry on TCP performance. In *Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking*. ACM, September 1997a. ISBN 0-89791-988-2. doi:10.1145/262116.262134.

Hari Balakrishnan, Venkata N. Padmanabhan, Srinivasan Seshan, and Randy H. Katz. A comparison of mechanisms for improving TCP performance over wireless links. *IEEE/ACM Transactions on Networking*, 5(6): 756–769, December 1997b. doi:10.1109/90.650137.

Mario Baldi and Gian Pietro Picco. Evaluating the tradeoffs of mobile code design paradigms in network management applications. In *Proceedings of the 20th International Conference on Software Engineering*, pages 146–155. IEEE, April 1998. ISBN 0-8186-8368-6. doi:10.1109/ICSE.1998.671111.

Hitesh Ballani and Paul Francis. CONMan: Taking the complexity out of network management. In *Proceedings of the 2006 SIGCOMM workshop on Internetd network management*, pages 41–46. ACM, September 2006. ISBN 1-59593-570-3. doi:10.1145/1162638.1162645.

Madalina Baltatu, Antonio Lioy, Fabio Maino, and Daniele Mazzocchi. Security issues in control, management and routing protocols. *Computer Networks*, 34:881–894, December 2000. doi:10.1016/S1389-1286(00)00159-6.

Nilanjan Banerjee, Wei Wu, Sajal K. Das, Spencer Dawkins, and Jogen Pathak. Mobility support in wireless Internet. *IEEE Wireless Communications*, 10:54–61, October 2003. doi:10.1109/MWC.2003.1241101.

Chadi Barakat, Eitan Altman, and Walid Dabbous. On TCP performance in a heterogeneous network: A survey. *IEEE Communications Magazine*, 38 (1):40–46, January 1999. doi:10.1109/35.815451.

R. Barrett, S.Haar, and R.Whitestone. Routing snafu causes Internet outage. *Interactive Week*, April 1997.

S. M. Bellovin. Security problems in the TCP/IP protocol suite. *ACM SIGCOMM Computer Communication Review*, 19:32–48, April 1989. doi:10.1145/378444.378449.

Steven M. Bellovin. Using the Domain Name System for system break-ins. In *Proceedings of the Fifth USENIX UNIX Security Symposium*, page 199–208, June 1995.

BGP Reports. AS65000 BGP routing table analysis report, February 2011. URL `http://bgp.potaroo.net/as2.0/`.

Tian Bu, Lixin Gao, and Don Towsley. On characterizing BGP routing table growth. *Computer Networks*, 45(1):45–54, May 2004. doi:10.1016/j.comnet.2004.02.003.

David Butcher, Xiangyang Li, and Jinhua Guo. Security challenge and defense in VoIP infrastructures. *IEEE Transactions on Systems, Man, and Cybernetics — Part C: Applications and Reviews*, 37:1152–1162, November 2007. doi:10.1109/TSMCC.2007.905853.

Matthew Caesar and Jennifer Rexford. BGP routing policies in ISP networks. *IEEE Network*, 19(6):5–11, 2005. doi:10.1109/MNET.2005.1541715.

Antonio Carzaniga, Gian Pietro Picco, and Giovanni Vigna. Designing distributed applications with mobile code paradigms. In *Proceedings of the 19th International Conference on Software Engineering*, pages 22–32, May 1997. ISBN 0-89791-914-9. doi:10.1145/253228.253236.

Jinzhou Chen, Chunming Wu, Ming Jiang, and Dong Zhang. A review of future Internet research programs and possible trends. In *Proceedings of the 6th International Conference on Wireless Communications, Networking and Mobile Computing*, September 2010. ISBN 978-1-4244-3709-2. doi:10.1109/WICOM.2010.5601269.

Fabio M. Chiussi, Denis A. Khotimsky, and Santosh Krishnan. Mobility management in third-generation All-IP networks. *IEEE Communications Magazine*, 40:124–135, September 2002. doi:10.1109/MCOM.2002.1031839.

David Clark, Scott Shenker, and Aaron Falk. *GENI research plan*. GENI Research Coordination Working Group and GENI Planning Group, April 2007. Interim status (Version 4.5).

David D. Clark. The design philosophy of the DARPA Internet protocols. In *SIGCOMM '88 Symposium Proceedings on Communications Architectures and Protocols*, pages 106–114. ACM, August 1988. ISBN 0-89791-279-9. doi:10.1145/52324.52336.

David D. Clark, Vinton G. Cerf, Lyman A. Chapin, Robert Braden, and Russell Hobby. Towards the future Internet architecture. IETF RFC 1287, December 1991.

Paul J. Criscuolo. Distributed denial of service. Tribe Flood Network, February 2000. URL `http://ftp.se.kde.org/pub/security/csir/ciac/ciacdocs/ciac2319.txt`.

Dave Crocker. Multiple address service for transport (MAST): An extended proposal. IETF Internet-Draft, September 2003.

Stephen E. Deering and Robert M. Hinden. Internet Protocol, version 6 (IPv6) specification. IETF RFC 1883, December 1995.

Stephen E. Deering and Robert M. Hinden. Internet Protocol, version 6 (IPv6) specification. IETF RFC 2460, December 1998.

Djamel Djenouri, Lyes Khelladi, and Nadjib Badache. A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications Surveys & Tutorials*, 7:2–28, 2005. doi:10.1109/COMST.2005.1593277.

Christos Douligeris and Aikaterini Mitrokotsa. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 44:643–666, April 2004. doi:10.1016/j.comnet.2003.10.003.

European Commission. *Future Internet Research and Experimentation: An Overview of the European FIRE Initiative and its projects*. Publications Office of the European Union, September 2010. ISBN 978-92-79-15714-1. doi:10.2759/31445.

Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Web spoofing: An Internet con game. In *Proceedings of the 20th National Information Systems Security Conference*, pages 95–103, October 1997.

Darleen Fisher. Us national science foundation and the future internet design. *ACM SIGCOMM Computer Communication Review*, 37(3):85–87, July 2007. doi:10.1145/1273445.1273459.

Anastasius Gavras, Arto Karila, Serge Fdida, Martin May, and Martin Potts. Future Internet Research and Experimentation: The FIRE initiative. *ACM SIGCOMM Computer Communication Review*, 37(3):89–92, 2007. doi:10.1145/1273445.1273460.

Huaming Guo, Shuai Gao, and Hongke Zhang. Towards a scalable routing architecture for future Internet. In *Proceedings of the 2009 IEEE International Conference on Network Infrastructure and Digital Content*, pages 261–265. IEEE, November 2009. ISBN 978-1-4244-4898-2. doi:10.1109/ICNIDC.2009.5360878.

Andrei Gurtov and Reiner Ludwig. Responding to spurious timeouts in TCP. In *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, pages 2312–2322. IEEE, March 2003. ISBN 0-7803-7752-4. doi:10.1109/INFCOM.2003.1209251.

B. Harris and R. Hunt. TCP/IP security threats and attack methods. *Computer Communications*, 22:885–897, June 1999. doi:10.1016/S0140-3664(99)00064-X.

John Douglas Howard. *An Analysis of Security Incidents on the Internet 1989–1995*. PhD thesis, Carnegie Mellon University, 1997.

Robert Hsieh, Zhe Guang Zhou, and Aruna Seneviratne. S-MIP: A seamless handoff architecture for Mobile IP. In *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, pages 1774–1784. IEEE, March 2003. ISBN 0-7803-7752-4. doi:10.1109/INFCOM.2003.1209200.

Yih-Chun Hu and Adrian Perrig. A survey of secure wireless ad hoc routing. *IEEE Security and Privacy*, 2:28–39, May 2004. doi:10.1109/MSP.2004.1.

H. Huang and J. Cai. Improving TCP performance during soft vertical handoff. In *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, pages 329–332, March 2005. ISBN 0-7695-2249-1. doi:10.1109/AINA.2005.216.

Craig A. Huegen. The latest in denial of service attacks: Smurfing description and information to minimize effects. Personal publication, February 2000. URL `http://www.pentics.net/denial-of-service/white-papers/smurf.html`.

David B. Johnson, Charles E. Perkins, and Jari Arkko. Mobility support in IPv6. IETF RFC 3775, June 2004.

Alan B. Johnston. *SIP: Understanding the Session Initiation Protocol*. Artech House, Canton Street Norwood, MA 02062, 3rd edition, 2009. ISBN 978-1-607-83995-8.

Zeus Kerravala. As the value of enterprise networks escalates, so does the need for configuration management. Technical report, The Yankee Group, January 2004.

Sung-Su Kim, Young J. Won, John Strassner, and James Won-Ki Hong. Manageability of the Internet: Management with new functionality. In *Proceedings of the 2010 IEEE Network Operations and Management Symposium*, pages 837–840. IEEE, April 2010. ISBN 978-1-4244-5366-5. doi:10.1109/NOMS.2010.5488361.

T. V. Lakshman and Upamanyu Madhow. The performance of TCP/IP for networks with high bandwidth-delay products and random loss. *IEEE/ACM Transactions on Networking*, 35(5):336–350, June 1997. doi:10.1109/90.611099.

George Lawton. E-mail authentication is here, but has it arrived yet? *Computer*, 38:17–19, November 2005. doi:10.1109/MC.2005.377.

Deguang Le, Xiaoming Fu, and Dieter Hogrefe. A review of mobility support paradigms for the Internet. *IEEE Communications Surveys & Tutorials*, 8: 38–51, 2006. doi:10.1109/COMST.2006.323441.

Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. A brief history of the Internet. Web page continuously maintained by the Internet Society, 2011. URL `http://www.isoc.org/internet/history/brief.shtml`.

Shufen Liu, Liang Chen, Tie Bao, Lu Han, Xiaojuan Xu, and Ming Qu. Study on LEAPS-based method for network data collection. In *Proceedings of the 2008 IEEE International Symposium on IT in Medicine and Education*, pages 207–211. IEEE, December 2008. ISBN 978-1-4244-3616-3. doi:10.1109/ITME.2008.4743854.

Daniel Massey, Lan Wang, Beichuan Zhang, and Lixia Zhang. A scalable routing system design for future Internet. In *Proceedings of the ACM SIGCOMM Workshop on IPv6 and the Future of the Internet*. ACM, August 2007. ISBN 978-1-59593-790-2.

Robert McMillan. A Chinese ISP momentarily hijacks the Internet (again). Computerworld, April 2010. URL `http://www.computerworld.com/s/article/9175081/A_Chinese_ISP_momentarily_hijacks_the_Internet_again_`.

Michael Menth, Matthias Hartmann, Phuoc Tran-Gia, and Dominik Klein. Future Internet routing: Motivation and design issues. *IT Information Technology*, 50(6):358–366, April 2009. ISSN 1611-2776. doi:10.1524/itit.2008.0507.

David Meyer, Lixia Zhang, and Kevin Fall. Report from the IAB Workshop on Routing and Addressing. IETF RFC 4984, September 2007a.

David Meyer, Lixia Zhang, and Kevin Fall. Report from the IAB workshop on routing and addressing. IETF RFC 4984, September 2007b.

Rich Miller. Routing snafu causes downtime for web hosts. On the Data Center Knowledge web site, February 2009. URL `http://www.datacenterknowledge.com/archives/2009/02/16/routing-snafu-causes-downtime-for-web-hosts/`.

Jelena Mirkovic and Peter Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34:39–54, April 2004. doi:10.1145/997150.997156.

Pekka Nikander, Jukka Ylitalo, and Jorma Wall. Integrating security, mobility and multi-homing in a HIP way. In *Proceedings of 10th Annual Network and Distributed System Security Symposium*. Internet Society, February 2003. ISBN 1-891562-16-9.

Rolf Oppliger. Security at the Internet layer. *Computer*, 31:43–47, September 1998. doi:10.1109/2.708449.

Charles E. Perkins. IP mobility support for IPv4. IETF RFC 3344, August 2002.

Vivek Ramachandran and Sukumar Nandi. Detecting ARP spoofing: An active technique. In *Proceedings of the First International Conference on Information Systems Security*, volume 3803 of *Lecture Notes in Computer Science*, pages 239–250. Springer, 2005. ISBN 978-3-540-30706-8. doi:10.1007/11593980_18.

Yakov Rekhter and Tony Li. An architecture for IPv6 unicast address allocation. IETF RFC 1887, dec 1995.

Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, and Diego Zamboni. Analysis of a denial of service attack on TCP. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pages 208–223. IEEE, May 1997. ISBN 0-8186-7828-3. doi:10.1109/SECPRI.1997.601338.

Peter Svensson. Pakistan causes worldwide youtube outage. Associated Press, February 2008. URL `http://www.msnbc.msn.com/id/23339712/`.

Fumio Teraoka, Masahiro Ishiyama, and Mitsunobu Kunishi. LIN6: A solution to multihoming and mobility in IPv6. IETF Internet-Draft, December 2003.

Todd Underwood. Con-ed steals the 'net. On the Renesys Blog, January 2006. URL `http://www.renesys.com/blog/2006/01/coned_steals_the_net.shtml`.

Kannan Varadhan, Ramesh Govindan, and Deborah Estrin. Persistent route oscillations in inter-domain routing. *Computer Networks*, 32(1):1–16, January 2000. doi:10.1016/S1389-1286(99)00108-5.

Paul Vixie, Susan Thomson, Yakov Rekhter, and Jim Bound. Dynamic updates in the Domain Name System (DNS UPDATE). IETF RFC 2136, April 1997.

Yangyang Wang, Jun Bi, and Jianping Wu. NOL: Name overlay service for improving Internet routing scalability. In *Proceedings of the Second International Conference on Advances in Future Internet*, pages 17–21. IEEE, July 2010a. ISBN 978-1-4244-7528-5. doi:10.1109/AFIN.2010.11.

Yangyang Wang, Jun Bi, and Jianping Wu. Empirical evaluation for the impact of core-edge separation on Internet routing scalability. In *Proceedings of the 2010 IEEE Conference on Computer Communications Workshops*, pages 1–2. IEEE, March 2010b. ISBN 978-1-4244-6739-6. doi:10.1109/INFCOMW.2010.5466631.

Bert Wijnen, David Harrington, and Randy Presuhn. An architecture for describing Simple Network Management Protocol (SNMP) management frameworks. IETF RFC 3411, December 2002.

Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wireless Communications*, 11:38–47, February 2004. doi:10.1109/MWC.2004.1269716.

C. N. Yap, M. Kraner, N. A. Fikouras, and S. R. Cvetkovic. Novel and enhanced mobile Internet protocol for third generation cellular environments compared to MIP and MIP-LR. In *Proceedings of the First International Conference on 3G Mobile Communication Technologies*, pages 143–147. Institution of Electrical Engineers, March 2000. ISBN 0-85296-726-8. doi:10.1049/cp:20000031.

강문식. 데이터 통신과 컴퓨터 네트워킹*:* 기초 이론과 최신 응용, chapter 7, pages 172–175. 한빛미디어, September 2009. ISBN 978-8-979-14656-1.

김성수, 최미정, and 홍원기. 미래 인터넷 연구 동향과 관리기능 정의. In *Proceedings of the 2008 Korean Network Operations and Management Conference*, April 2008.

변성혁. 미래인터넷 아키텍처 연구동향. 전자통신동향분석, 24(3):1–12, June 2009.

신명기. 미래인터넷 기술 및 표준화 동향. 전자통신동향분석, 22(6):116–128, December 2007.

유태완, 권태경, and 최양희. 미래인터넷을 위한 addressing 및 routing 아키텍처 연구 동향. 정보과학회지, 28(1):52–60, January 2010.

유태완 and 이승윤. Internet 확장성 문제에 관한 연구. In 한국해양정보통신학회 *2007*년도 춘계종합학술대회 논문집, pages 852–855, June 2007.