IPv6-over-IPv4 인터넷 트래픽 분석

박하늘, 박준상, 김명섭
고려대학 컴퓨터정보학과

{skzizix, junsang_park, tmskim}korea.ac.kr

Analysis of the IPv6-over-IPv4 Internet traffic

Ha-Neul Park, Jun-Sang Park, and Myung-Sup Kim
Korea Univ.

요 약

IPv4 주소자원이 고갈됨에 따라 IPv6 로 주소체계의 변환이 필요한 시점이지만 완전한 체계 변화까지는 많은 노력과 비용이 요구될 것으로 예상된다. 현재 IPv6 기반 네트워크 통신을 위해 IPv4 에 기반한 IPv6 트래픽이 증가하고 있는 추세이다. 하지만 현재의 트래픽 분석 시스템은 IPv4 트래픽에 중점을 두고 분석을 수행하고 있어 IPv4 상에서 발생하는 IPv6 트래픽에 대한 분석이 제대로 이루어지지 않고 있다. 본 논문에서는 IPv6-over-IPv4 트래픽을 IPv4 기반 분석시스템에 적용할 수 있도록 변환하는 방법을 제시하고, 이를 바탕으로 학내망에서 발생하는 IPv6-over-IPv4 트래픽에 대한 트랜드 및 특징을 분석한다.

1. 서 론

현행 IPv4 기반 인터넷 주소자원이 고갈됨에 따라 차세대 인터넷 주소(IPv6) 전환이 필요한 시점이다. 하지만 IPv4 주소체계를 IPv6 로 변환하기 위해서는 장기간의 노력과 많은 비용이 요구되기 때문에 IPv6 로의 완전한 체계 변화까지는 상당 시간이 필요할 것으로 예상된다. 이미 IPv6 의 트래픽은 발생 하고 있고, IPv4 트래픽과 공존하고 있는 시점에서 기존의 트래픽 분석 시스템은 IPv4 트래픽에 중점을 두고 분석을 수행하고 있다. 이러한 부분은 네트워크 안정적인 관리에 있어서 취약점으로 작용될 수 있다.

본 논문에서는 IPv6-over-IPv4 트래픽을 IPv4 기반 분석 시스템에 적용할 수 있도록 변환하는 방법을 제시하고, 이를 바탕으로 학내망에서 발생하는 IPv6-over-IPv4 트래픽에 대한 트랜드 및 특징을 분석한다. 본 논문에서 실험에 사용되는 트래픽을 수집하기 위한 환경으로 학내망에서 구축된 기존의 트래픽 수집 및 분석 시스템을 사용하였다. 이 시스템은 학내 망과 인터넷을 연결하는 링크의 모든 패킷을 수집하여 플로우와 패킷 형태로 구성하고, 수집된 플로우와 패킷은 트래픽 트레이스 저장소에 저장되고 분석된다 [1].

학내 망에서 발생하는 트래픽을 수집하여 하루 동안의 트래픽을 분석한 결과 TCP, UDP 를 제외한 나머지(Other)의 대부분은 IPv6-over-IPv4 트래픽이 차지했다. Total 트래픽에 대한 IPv6-over-IPv4 트래픽의 비율은 평균적으로 0.35%(flow), 3.77%(packet), 2.91%(byte)를 점유하였다. 또한 2012 년 일년 동안의 학내 망에서 발생하는 IPv6-over-IPv4 트래픽을 분석한 결과 IPv6-over-IPv4 트래픽의 변화 추이는 6 월달부터 증가 추세를 보였고, 9 월달은 급격히 증가하였다. 이러한 추세를 볼 때, 2013 년에는 더 높은 상승세를 보일 것으로 예상된다. 이러한 추세를 고려했을 때 IPv6-over-IPv4 트래픽에 대한 분석이 반드시 요구된다.

본 장에 이어서 2 장에서는 IPv6-over-IPv4 트래픽 특징 분석을 위한 IPv6-over-IPv4 패킷의 구조를 설명하고, IPv6-over-IPv4 트래픽의 Local host 의 특정 패턴에 따른 분석 결과를 기술한다. 마지막 3 장에서는 결론 및 향후 연구를 기술한다.

이 논문은 2012 년 정부(교육과학기술부)의 재원으로 한국연구재단 (2012R1A1A2007483) 및 2013 년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보.컴퓨팅기술개발사업(2010-0020728)의 지원을 받아 수행된 연구임.

2. IPv6-over-IPv4 트래픽 구조 및 특징 분석

본 장에서는 IPv6-over-IPv4 트래픽 특징을 분석하기 앞서 IPv6-over-IPv4 패킷을 변환하는 방법과 패킷의 구조를 기술한다. 또한 변화된 패킷 구조를 기반으로 수집한 트래픽에 대하여, IPv4 헤더의 Protocol 필드를 기준으로 분류된 트래픽의 양을 보여주고 Local host 에 대한 분석을 기술한다.

2.1. IPv6-over-IPv4 패킷 구조

IPv6 헤더는 고정된 40Bytes 크기를 가지며 IPv6 헤더와 전송 계층 헤더 사이에 확장 헤더들이 나타나도록 허용을 하고 있다[2]. 따라서 IPv6 의 Next 헤더는 IPv6 기본헤더 다음에 위치하는 확장 헤더의 종류를 명시하거나 상위계층인 전송 프로토콜을 사용하도록 지정한다.

IPv6-over-IPv4 패킷은 일반적인 IPv4 패킷과는 달리 상위계층 프로토콜 헤더로 IPv6 를 지정하는데 이때 IPv4 헤더의 Protocol number 41 을 사용한다. 또한 IPv4 패킷은 확장 헤더가 존재하지 않기 때문에 기존의 IPv4 기반 트래픽 분석 시스템은 IPv6-over-IPv4 패킷의 IPv6 헤더를 전송 프로토콜로 분석하는 오류를 범할 수 있다.

그림 1 은 기존의 트래픽 분석 시스템에서의 IPv6-over-IPv4 트래픽의 분석을 위해 패킷 변환방법을 나타낸다. IPv6-over-IPv4 패킷에 대해서는 확장 헤더의 유무를 판단하고, 상위 계층 프로토콜 헤더로 전송 프로토콜을 가리키는 Next 헤더를 IPv4 헤더의 Protocol 필드로 바꾸어 준다. 그 후에 고정된 IPv6 헤더 40Bytes 와 확장헤더의 유

무에 따라 확장 헤더의 Byte 를 제거하여 일반적인 IPv4 패킷 형태로 변환한다.

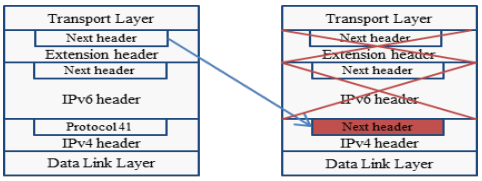

그림 1. IPv6-over-IPv4 패킷 구조 및 변환

2.2. IPv6-over-IPv4 트래픽 특징 분석

본 절에서는 변화된 패킷 구조를 기반으로 트래픽을 수집하고, IPv4 헤더의 Protocol 필드를 기준으로 분류하여 트래픽의 양을 보여준다. 또한 IPv6-over-IPv4 트래픽의 Local host 를 기준으로 분석하여 특징을 기술한다.

표 1. 트래픽 트레이스

구분	Flow(K)	PKT(K)	Bytes(M)
Total	2,354	28,456	22,474
No Next(59)	0.9	2	0.1
ICMP(58)	31	163	17
UDP(17)	2,260	21,242	16,385
TCP(6)	60	7,048	6,071

표 1 은 2013 년 07 월 11 일 하루 동안 학내 망에서 발생한 IPv6-over-IPv4 트래픽을 IPv4 헤더의 Protocol 필드를 기준으로 분류한 결과이다. Flow, Packet, Byte 의 대부분이 UDP 를 사용하였고 No Next 를 사용하는 프로토콜은 장비간 통신을 위한 프로토콜이다.

하루 동안 발생한 IPv6-over-IPv4 트래픽에 대해 Local host 의 개수를 일정한 분단위로 측정한 결과, 총 960 개의 host 에서 사용을 하였다. 이는 학내 망 전체 host 의 약 1/3 로 일시적인 목적의 특정 host 에서 발생한 것이 아님을 알 수 있다.

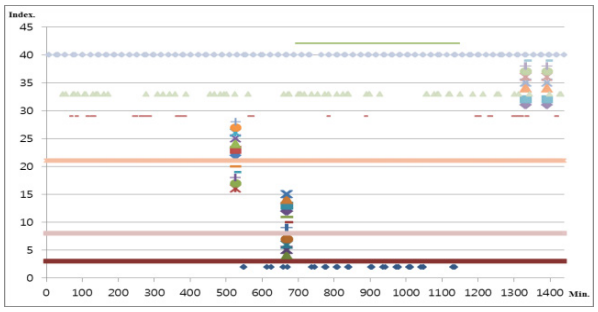

그림 2. IPv6-over-IPv4 트래픽의 Local host 발생 기간

Local host 960 개에 대하여 0 부터 각각의 index 를 부여하고, 하루 동안 매 분마다 Local host 의 발생 여부를 측정하였다. 그림 2 는 특정 패턴을 나타내는 host 들만을 대상으로 그래프화 한 것이다. x 축은 하루 동안의 시간을 나타내며 y 축은 각 host 에 대한 index 번호 이다. host 의 발생 패턴에 따라 크게 총 3 가지의 형태로 분류할 수 있다. 첫 번째는 특정한 시점에 한번만 발생한 host 이고 두 번째는 긴 시간 동안 반복적으로 발생한 host 이다. 세 번째 특징을 가지는 host 는 짧은 시간 주기적으로 발생한 host 이다.

그림 3 은 특징 1 을 가지는 host 들이 발생한 시점의 트래픽을 대상으로 Flow 단위로 분석한 결과를 도식화한 것이다.

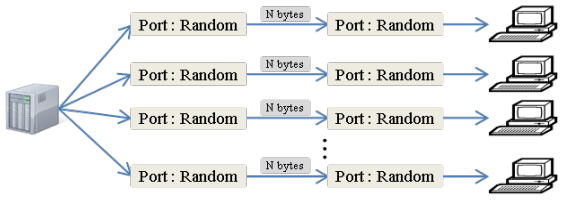

그림 3. Local host 특징1

발생한 Local host 의 개수는 144개 이었으며, 하나의 특정 목적지 host에서 128개의 Local host로 하나의 패킷과 고정된 크기인 N bytes를 보냈다. 첫 번째 특징을 가지는 트래픽은 특정한 하나의 목적지 host에서 다수의 Local host에게 하나의 패킷과 동일한 Byte를 가지는 패킷을 보냈다. 또한 단방향 통신이며 목적지 포트가 고정 되지 않았다. 따라서 첫 번째 특징을 가지는 트래픽은 비정상적인 트래픽일 확률이 높다.

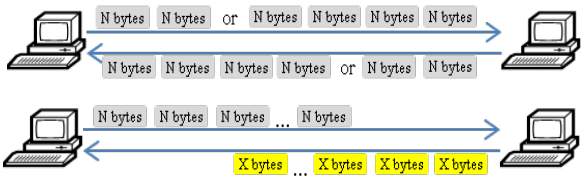

그림4. Local host 특징2, 3

그림 4 는 특징 2, 3 을 가지는 트래픽을 대상으로 Flow 단위로 분석한 결과이다. 두 번째 특징을 가지는 트래픽은 ICMP 프로토콜을 이용하여 일대일 통신이 이루어졌으며 고정된 크기인 N bytes 를 주고 받았다. 또한, 패킷의 개수가 2 개 혹은 4 개로 고정되었다. 세 번째 특징을 가지는 Flow 들은 특징 2 와 유사하지만 패킷의 개수가 고정적이지 않았고, 두 개의 고정된 N, X Bytes 를 사용하였다.

3. 결론 및 향후 연구

IPv6-over-IPv4 트래픽은 점점 증가하는 추세를 보이고 있고, IPv6-over-IPv4 트래픽 분석을 위해서 기존의 분석 시스템 혹은 패킷의 변환이 필요하다. 본 논문에서는 IPv6-over-IPv4 패킷을 변환하는 방법을 기술하고, 이를 바탕으로 트래픽 분석 결과를 보였다. IPv6-over-IPv4 트래픽은 UDP 프로토콜의 사용이 매우 높았으며, No Next 헤더라는 어플리케이션 관리를 위한 장비간 통신 프로토콜을 사용 한다는 차이점을 알 수 있다. 또한 Local Host 발생 기간에 따라 같은 패턴을 가지는 트래픽으로 분류하여 분석 하였을 때 첫 번째 특징으로 분류된 트래픽은 비정상적인 트래픽 일 확률이 높은 것으로 나타났다.

IPv6-over-IPv4 트래픽의 상세 분석을 통하여 응용 또는 비정상 트래픽 여부를 판단하고, 비정상 트래픽의 경우에는 이에 대한 대처 방안을 연구할 계획이다.

참 고 문 헌

[1] 박하늘, 박준상, 김명섭, "학내망에서 발생하는 IPv6-over-IPv4 트래픽 분석", 2013 년 통신망운용관리 학술대회 (KNOM 2013), 계명대학교, 대구, May. 09-10, 2013, pp.28-32.

[2] “Internet Protocol, Version 6(IPv6) Specification”, http://tools.ietf.org/html/rfc2460.

[3] 김용진, “IPv4/IPv6 변환기술”, TTA 저널, 79, 2002.