[1-1]

IPFIX 기반 캠퍼스망 트래픽 측정 및 분석

이병준, 이영석*
전자통신연구원
bjlee@etri.re.kr
*충남대학교 전기정보통신공학부 컴퓨터전공
*yslee@cs.cnu.ac.kr

IPFIX-based Campus Network Traffic Measurement and Analysis

Byoung-Joon Lee, Youngseok Lee*
Electronics and Telecommunications Research Institue
*Dept. of Computer Science and Engineering, Chungnam National University

요 약

본 논문에서는 IPFIX(IP Flow Information eXport) 기반으로 캠퍼스망 트래픽을 측정하는 환경을 구축하고 측정한 결과를 제시하도록 한다. IPFIX는 Cisco NetFlow기반의 IETF표준으로 라우터가 인터넷 패킷 흐름을 플로우 정보로 가공하여 제공하여 다양한 트래픽을 분석하게 한다. 본 논문에서는 오픈 소스 기반의 도구를 이용하여 라우터에서 IPFIX를 지원하지 않는 환경에서 광케이블의 분배기 또는 스위치의 포트 미러링을 이용하여 패킷을 IPFIX 형태의 플로우로 생성하여 충남대학교 캠퍼스 백본 링크의 트래픽을 측정하고 분석한 결과를 제시한다. 특히, 서브넷별의 통계를 통해 위해 트래픽의 공격 패턴에 대한 결과를 제시한다.

1. 서론*

다양한 인터넷 응용들과 사용자 수의 증가와 함께 인터넷 트래픽은 폭증하고 있다. 기존의 파일 전송, 이메일, 웹 및 스트리밍 등의 응용 뿐만 아니라 p2p, 바이러스 등의 트래픽이 급증하고 있다. 따라서, 캠퍼스망과 같은 소규모 접속망에서는 지속적으로 증가하는 트래픽을 효과적으로 지원하기 위하여, 고속의 링크와 라우터를 기반으로 하는 기가급의 네트워크 형태로 발전하고 있다. 특히, 캠퍼스망일 경우에는 보안이 취약하기 때문에 이상 트래픽이 많이 발생하고 있다. 트래픽 측정 및 분석은 네트워크의 성능 모니터링 및 이상 트래픽 관찰 또는 과금을 위하여 필수적인 기능이고, 많은 인터넷 서비스 제공업체에서는 다양한 방법을 이용하여 트래픽 측정 및 분석을 시도하고 있다.

기가급의 네트워크에서의 트래픽 측정 방법에는 고속의 링크를 광케이블 분배기 또는 스위치의 포트 미러링 기능을 이용하여 전용 트래픽 측정 서버를 이용하는 방법과 라우터에서 직접 트래픽 측정 기능을 수행하는 방법이 있다. 링크-분배기를 이용한 트래픽 측정 방법은 전용 측정 서버를 두는 방법으로 정확한 패킷 단위의 측정이 가능하지만, 모든 링크에 대용량의 측정 서버를 설치해야하는 단점이 있다. 하지만, 라우터 또는 스위치에서의 측정 모듈을 이용하는 방법은 이미 설치된 라우터 또는 추가 트래픽 측정 모듈을 이용하여 쉽게 측정 환경을 구축할 수 있다. 하지만, 라우터 성능의 제한으로 인하여 트래픽 측정이 부정확할 수 있다.

Cisco사는 이미 NetFlow [1]기능을 이용하여 플로우 기반의 트래픽 측정을 거의 모든 Cisco 스위치/라우터에 제공하고 있다. 최근 IETF에서는 Cisco NetFlow를 기반으로 하는 표준을 IPFIX (IP Flow Information eXport) [2] 그룹에서 확정짓고 마무리하고 있다. 따라서, 향후 라우터/스위치에서는 IPFIX 기능을 트래픽 모니터링 기능으로 제공할 수 있어야 한다.

IPFIX에서 사용하는 플로우는, 예를 들어 (src IP addr, src port, dst IP addr, dst port, proto) 다섯 개의 TCP/IP 헤더 필드에 의해 일정시간 내에 지속적으로 도착하는 연속적인 패킷들로 정의된다. 즉, TCP 연결 또는 UDP 스트림 등이 하나의 플로우로 정의되고 탐지될 수 있다. Cisco NetFlow에서는 라우터의 입/출력 인터페이스 번호를 덧붙여 플로우 규격을 정의했으며, 일정 시간 내에 패킷이 도착하지 않으면 플로우의 종료를 선언하고, 플로우 데이터를 외부 측정 서버로 전송하도록 한다. 이 때 사용되는 플로우 종료 조건은 TCP 세그먼트들(FIN, RST)도 사용가능하다.

IPFIX에서의 플로우 정의는 Cisco NetFlow version 9을 기반으로 정의되고 있는데, IPv6, MPLS, Multicast 등의 다양한 플로우 포맷들을 동일 플로우에 실어 보낼 수 있게 하고 있다. 또한 기존의 UDP 기반 플로우 전송을 TCP또는 SCTP 전송 계층을 이용하도록 하여 신뢰성을 강화시켰다.

본 논문에서는 플로우 단위의 측정을 위하여 라우터에서 지원되지 않는 환경에서 링크 단위의 패킷을 가공하여 플로우 정보로 변환하여 측정한 데이터를 충남대학교 백본 링크에서 측정한 결과를 제시하도록 한다. 본 측정환경은 라우터의 IPFIX 지원이 없더라도, 공개된 소스들을 이용하여 쉽게 구축할 수 있는 장점을 가진다. 캠퍼스망에서의 트래픽 측정결과는 일반 대규모 네트워크의 결과와는 상이하다고 알려져있다. 특히, 위해 트래픽의 중점 대상인 지역이기 때문에 본 논문에서도 위해 트래픽 패턴을 사용되지 않는 서브넷별로 구분하여 분석하였다.

2. 측정 환경

* 본 논문은 과학기술부 지정 지역협력연구센터(RRC)인 충남대학교 소프트웨어연구센터의 지원으로 수행된 과제의 결과입니다.