[1-4]

플로우 기반 망 측정*

*이준복, **이성호, ***정광민, ****이영석, *****이재화, *전길남, **박용진,
******조일권
*한국과학기술원, **한양대학교, ***고려대학교, ****충남대학교
*{jblee, chon}@cosmos.kaist.ac.kr, **{shlee, park}@hyuee.hanyang.ac.kr
{ministream}@korea.ac.kr, *{yslee}@cs.cnu.ac.kr
*****{jhlee}@noc.koren21.net, ******ikcho@nca.or.kr

Flow-based Network Measurement

*Joonbok Lee, **Sung-Ho Lee, ***Kwang-Min Jeong,
****Young-Seok Lee, *****Jaehwa Lee, *Kilnam Chon, **Yong-Jin Park,
******Il-Kwon Cho
*KAIST, **Hanyang University
***Korea University, ****Chungnam National University,
*****KT Convergence Laboratory, ******National Computational Agency

요 약

본 논문에서는 망의 트래픽 엔지니어링을 위한 트래픽 측정 인프라를 제안한다. 제안한 측정 인프라는 플로우를 기반으로 한다. 플로우 기반의 측정은 같은 플로우의 패킷들의 정보를 합해서 플로우 정보를 만들기 때문에 각 패킷의 정보를 잃어버리는 단점이 있다. 하지만 패킷 기반에 비해 데이터의 양이 적어 트래픽의 저장과 분석에 용이하기 때문에 망의 전체 측정 인프라를 구축하는데 용이하다.

또, 이 논문에서는 선도망에 구축한 플로우 기반의 측정인프라를 이용하여 망 트래픽의 어플리케이션별 분석과 비정상적인 트래픽을 분석하였다. 분석 결과, 기존에 HTTP나 FTP 가 트래픽의 많은 부분을 차지했던데 비해 피어-투-피어 어플리케이션으로 보이는 트래픽들이 많이 늘어났으며, 잘 알려진 port 외에 많은 수의 port가 다양하게 사용되는 것으로 분석되었다. 또, 플로우 측정을 통해 DoS 어택 트래픽, 비대칭 경로 등을 찾는 방법을 소개하고 실제 분석 결과를 소개한다.

1. 서론

망 트래픽 엔지니어링은 망 자원을 효율적으로 사용함으로써 더 높은 품질의 서비스를 가능케 한다. 트래픽 엔지니어링은 단지 더 많은 양의 트래픽을 전송하기 위함이 아닌 보다 더 좋은 서비스(적은 딜레이, 지터, 패킷 손실 등)를 위해 점점 중요성이 높아지고 있다. 트래픽 엔지니어링을 위해서는 망의 트래픽 모델링, 트래픽 엔지니어링 알고리즘, 망의 라우팅 정보 등이 필요하다.

망의 트래픽 상황을 파악하기 위해서는 망의 한 곳에서의 트래픽 측정만으로 알 수 없다. 보다 정확한 상황 파악을 위해서는 망 전체의 트래픽의 측정과 원하는 데이터를 얻기 위한 분석이 필요하다. 이를 위해서는 트래픽 측정과 측정된 데이터의 효과적인 저장과 분석을 할 수 있는 인프라가 필요하다.

망의 대역폭이 증가하고, 트래픽의 양도 증가함에 따라 트래픽의 측정뿐 아니라 이를 저장 분석하기도 힘들어 지고 있다. 플로우 기반의 측정 시스템은 패킷 별로 저장, 분석하지 않고, 같은 플로우, 즉 일정 시간동안 Source IP, Destination IP, Source Port, Destination Port 가 같은 패킷들을 합하여 다루기 때문에 분석, 저장해야할 데이터의 양이 패킷 기반의 측정 시스템에 비해 적다. 따라서 플로우 기반의 트래픽 측정은 망 전체의 트래픽을 다루어야 하는 측정 인프라에 적합하다.

우리는 플로우 기반 트래픽 측정 인프라를 디자인하고, 실제 망에 구축하여 트래픽을 측정하였다. 측정 인프라는 구축된 망의 각 노드의 트래픽을 분석하고, 이들을 모아 전체 망의 트래픽 정보를 알도록 구축되었다. 또, 측정된 트래픽의 분석 결과 뿐 아니라, 일정 기간의 트래픽 데이터를 저장하여 후에 이를 이용한 자세한 트래픽 분석이

* 본 연구는 NCA지원에 의해 수행되었음.