[9-17]

트래픽 분석 기반의 P2P 플로우 검출에 관한 연구

정재윤, 김영한, *이세현

숭실대학교 정보통신전자공학부, *(주)인티게이트

{imone, yhkim}@dcn.ssu.ac.kr, *shrhee@intigate.com

A P2P Flow Detection Algorithm Based on Traffic Analysis

Jaeyun Jeong, Younghan Kim, and *Sehyeon Rhee

School of Electronic Engineering, Soongsil University, Korea

*Integate, Inc.

요 약

현재 네트워크 트래픽의 대부분을 차지하고 있는 P2P 트래픽은 네트워크에 많은 영향을 주고 있다. 따라서 P2P 트래픽의 상태를 파악하고 플로우를 검출하여 적절한 정책을 수행하는 것은 매우 중요하다. 그러나 Well-known 포트를 기반으로 하여 플로우를 분석하는 기존 분석방법으로는 포트 홉핑 등 기존에 알려지지 않은 형태의 P2P 트래픽을 분석하기 어렵다. 본 논문에서는 P2P 트래픽의 특성을 이용한 플로우 단위의 검출방법을 제안하고 실험을 통해 적용 가능성을 확인하였다.

1. 서 론

최근 인터넷의 규모가 급격히 확장되고 인터넷 기반의 응용 프로그램들이 다양하게 개발되어 사용함에 따라 기존에 사용하던 WWW, FTP등의 전통적인 트래픽 외에도 스트리밍 트래픽, P2P 트래픽 등 이전에는 찾아볼 수 없었던 새로운 형태의 트래픽이 나타나고 있다.

특히 Napster, Gnutella로 대표되는 파일 공유를 목적으로 한 P2P 프로그램에서 발생시키는 트래픽의 양은 이미 HTTP, FTP의 양을 훨씬 넘어 네트워크에 많은 부하를 주고 망의 관리를 어렵게 한다. 따라서 네트워크의 상태를 파악하고 P2P 트래픽을 측정하고 분석하는 것은 매우 중요한 일이다.

회사나 학교같은 네트워크에서는 P2P의 과다한 이용으로 인해 네트워크가 마비되거나 느려지는 현상을 막기 위해 P2P 트래픽을 제한하기도 한다. 이러한 정책은 대부분 P2P 응용프로그램이 사용하는 포트에 대한 조사를 바탕으로 특정 포트를 제한하거나[1,2] 프로토콜이 공개된 경우 헤이로그의 특정 영역에 대한 패턴 매칭 기법을 사용한다. 그동안 P2P 프로그램은 이러한 트래픽 제한을 피하기 위해 다양한 형태로 발전하게 되었고 따라서 기존의 방법으로는 새로운 형태의 P2P Flow에 대한 검출이 어렵게 되었다.

본 논문에서는 well-known Port 기반이 아닌 P2P 트래픽의 특성을 이용한 Flow 단위의 검출 방법을 제안한다. 제안한 기법은 관리자의 감시를 피해 포트를 바꿔서 사용하거나 기존에 알려지지 새로운 P2P 프로토콜을 사용하는 P2P 트래픽을 플로우 단위로 효과적으로 검출할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 P2P 트래픽 검출에 관한 기존의 연구내용을 소개하고 3장에서는 본 논문에서 제안하는 플로우 기반의 P2P 트래픽 검출방법을 설명한다. 4장에서는 실험을 통해 제안한 검출방법의 성능을 분석한다. 끝으로 5장에서는 결론 및 향후 연구를 제시한다.

2. 관련 연구

본 장에서는 P2P 응용의 분류에 대해 간단히 살펴보고 P2P 트래픽 분석에 대한 관련 연구를 기술한다. 또한 기존의 응용레벨 트래픽의 분석방법을 P2P 트래픽에 적용할 때의 문제점에 대해 언급한다.

2.1 P2P 응용의 분류

SETI@HOME으로 대표되는 분산컴퓨팅과 Groove같은 소프트웨어 형태의 P2P 응용은 특수한 목적을 위해 사용된다. 이와 같은 특수 목적의 P2P를 제외하면, 현재 사용되고 있는 P2P 응용의 형태는 크게 메신저 형태와 파일 교환 형태로 구분할 수 있다. 표 1은 국내에서 주로 사용되고 있는 응용프로그램의 종류를 나타낸 것이다.