[2-16]

P2P 유해정보방지를 위한 P2P 트래픽 식별 방안 연구

이호균*, 남택용*, 장종수**

*한국전자통신연구원 개인정보보호연구팀, **한국전자통신연구원 정보보호연구단

{hglee,tynam,jsjang}@etri.re.kr

The Method of P2P Traffic Detecting for P2P Harmful Contents Prevention

Ho-Gyun Lee*, Taek-Yong Nam*, Jong-Soo Jang**

*Privacy Protection Research Team, ETRI,

**Information Security Research Division, ETRI

{hglee,tynam,jsjang}@etri.re.kr

요 약

인터넷 저변 인구 확대에 따라 전자 상거래, 원격 교육, 전자 선거와 같이 실세계에서 이루어지던 많은 활동들이 사이버 세계에서 이루어지고 있다. 그 결과 인터넷의 순기능뿐만 아니라 역기능 또한 매우 다양하게 나타나고 있다. 각종 바이러스와 DDoS 공격과 같은 컴퓨터 시스템에 대한 피해뿐만 아니라 스팸이나 성인물, 자살, 테러 조장 등과 같이 인간의 정신에 악영향을 끼치는 컨텐츠에 대한 방지 방안이 논의될 때이다. 본 논문에서는 최근 유해 정보 유통에 가장 많이 사용되는 P2P 망에 대해서 내용 기반 방식으로 유해 정보를 탐지, 차단하는 시스템을 구축할 때 필수 요소 중의 하나인 P2P 트래픽 식별 기술의 개발 과정을 보이고 있다.

I. 서론

2001년과 2003년에 발표된 2건의 미 의회 보고서는 P2P 네트워크를 통한 음란물 배포의 심각성을 잘 말해 주고 있다[1]. P2P 서비스는 기존의 네트워크 서비스가 클라이언트/서버 방식으로 구현됨으로써 서버단에서의 가능했던 제어를 더 이상 불가능하게 만들었다. 중앙에 집중되었던 헤게모니가 각 클라이언트 단으로 흩어져버린 것이다. 중앙에서의 제어가 불가능하고 모든 개체가 완전 자유도를 가진 상황에서는 각 개체들의 이상적인 행동을 통해서만 최적의 네트워크 상황을 기대할 수 있을 것이다. 하지만 불행히도 각 개체들은 망 전체의 상황을 고려하지 않고 자신의 요구에 따라서 행동할 뿐이다. 그 결과가 망 전체의 폭주, 불법 S/W, 불법 mp3, 불법 영화, 포르노물들이 범람하고 있는 현재의 상황이다. 브루스 스나이어가 Secrets and Lies 에서 언급한 바와 같이 유무선망에서의 트래픽 감시 기술 개발과 활용은 이제 공공연한 비밀이 되었다[2]. 대부분의 기업에서는 자사의 기업 비밀이 외부 망으로 유출되는 것을 방지하기 위해서 인트라넷 내부의 모든 트래픽을 감시하고 있다[3][4]. 이와 같이 제한된 망을 대상으로 허용 가능한 서비스를 지정하는 상황에서는 트래픽의 감시가 비교적 쉬운 주제가 될 수 있지만, 제한되지 않은 공용망에서 P2P 트래픽에 대해서 감시와 차단 작업을 수행하는 것은 간단하지 않는 과제이다. 본 논문에서는 현재 문제가 되고 있는 P2P 망에서의 불법 컨텐츠에 대한 식별, 차단 기술의 일부분으로 P2P 트래픽을 탐지하고 차단하는 기술