P2P기반 VoIP 트래픽 분석 및 VoIP Detection System

김대진○ 권택근
충남대학교 컴퓨터공학과
eddykim@cnu.ac.kr, tgkwon@cnu.ac.kr

The traffic of VoIP based on Peer-to-Peer analysis and VoIP Detection System

D. Kim○ T. G.
Dept. of Computer Science and Engineering, Chungnam National University

최근 들어 컴퓨터 시스템의 비약적인 발달과 컴퓨터 시스템 네트워크간의 광 대역 통신망으로 연결됨에 따라 수화자간의 음성 및 화상통신을 하는 수단으로써 컴퓨터 네트워크에 의존하는 경우가 늘고 있다. 그 대표적인 이유는 컴퓨터 네트워크 시스템은 이미 광 대역 통신망으로 연결되어 있기 때문에 필요한 S/W 만 장착한다면 추가비용 없이 무료로 통화가 가능하기 때문이다.

사례로 Skype 와 같은 P2P 기반의 VoIP 메신저를 사용하는 것을 들 수 있다. 컴퓨터를 이용하여 수화자간의 통신이 가능할 뿐만 아니라 컴퓨터 대 전화 단말기 간의 통신도 가능하다. 심지어 컴퓨터 네트워크 시스템에 의존하여 전화 단말기 간의 통신을 사용하는 사례도 늘고 있다. 그러나 컴퓨터 네트워크 상에서 음성 및 화상통신을 하는데 있어서 P2P 기반의 VoIP Traffic 은 보안상의 이유로 암호화를 하기 때문에 네트워크상에서 어떤 Packet 이 P2P 기반의 VoIP Traffic 인지 분류하는데 어려움이 있다. 뿐만 아니라 P2P 기반의 VoIP Packet은 5-tuple 상에 나타나는 특징 또한 존재하지 않는다. 그렇기 때문에 기존의 IDS Tool을 사용하여 P2P기반의 VoIP Packet을 분류하기란 쉽지 않다. 기존의 IDS Tool은 특정 Packet의 Payload의 특정 Signature를 찾아내기 위해, Knuth-Morris-Pratt, Robin Karp, Boyer Moore 등의 Brute Algorithm 방식을 사용한다. 그러나 요즘과 같이 Gigabit 단위의 수많은 Traffic 을 처리해야 하는 상황에서 Brute Algorithm 을 사용하여 P2P 기반의 VoIP Packet을 찾는다는 것은 기존 네트워크 Traffic 처리에 심각한 병목 현상과 부하를 야기 할 수 있다. 그래서 본 논문에서는 P2P기반의 VoIP Traffic을 분석하는 방법과 네트워크 시스템 상에서 P2P기반의 VoIP Traffic을 Detection 하기 위한 새로운 IDS툴을 제시하고자 한다.

컴퓨터 네트워크 시스템 상에서 P2P 기반의 VoIP 트래픽을 분류하고 분석해 내기 위해서 대표적인 IDS 툴로 Snort를 사용한다. Snort는 Packet의 5-tuple을 검색하여 P2P기반의 VoIP 트래픽을 찾을 수 있는 기능을 제공하며, 뿐만 아니라 특정 Packet 의 Payload 의 Signature를 검색할 수 있는 기능 또한 제공한다. 그러나 기존의 Snort와 같은 IDS툴로 P2P기반의 VoIP 트래픽을 찾을 수는 있지만 컴퓨터 네트워크 시스템 상의 수많은 Traffic을 처리하는데 있어서 Snort등과 같은 IDS툴은 많은 문제를 야기할 수 있다. 가장 큰 문제점으로 Snort는 특정 Packet을 분석하기 위해 서론에서 언급한 Brute Algorithm방식을 사용한다. 이는 Gigabit 단위를 처리하는 네트워크 시스템에서 기존의 IDS툴과 같은 방식으로 Packet을 검색하는 것은 수 많은 문제점을 야기할 수 있다. 뿐만 아니라 P2P 기반의 VoIP 트래픽은 5-tuple상의 특징이 존재하지 않는다. 그리고 수화자간의 음성 및 화상통신 시 보안을 이유로 Packet Payload에 암호화 알고리즘을 사용 하므로 기존의 IDS툴을 이용하는 것은 바람직하지 않다. 그러므로 P2P기반의 VoIP 트래픽을 분류해 내기 위해서는 어떠한 특징이 있는지 살펴볼 필요가 있다.

컴퓨터 시스템 네트워크상에서 P2P기반의 VoIP 트래픽을 VoIP Detection System을 이용해 분류하기 위해서는 고유한 Signature가 필요하다. 이 Signature는 Rule Set 이라는 Structure 형태로 가공하여 메모리에 상주 시키며 Packet 검색 시 메모리상에 상주하는 Rule Set과 비교하여 VoIP Packet 과 그렇지 않은

일반 Packet으로 분류하여 Hash 알고리즘을 이용하여 저장한다.

P2P기반의 VoIP 트래픽은 실제 LAN상에서 뿐만 아니라 광 대역 네트워크상에서도 주요한 역할을 차지할 만큼, 하나의 통신수단으로 자리 잡고 있다. 그렇기 때문에 P2P기반의 VoIP 트래픽을 분석하는 것은 실제 네트워크상에서의 부가적인 것이 아니라 필수적인 요소가 되었다. 그렇기 때문에 P2P 기반의 VoIP 트래픽이 어떠한 특징이 있는지 주로 사용되고 있는 메신저를 통해 그 특징을 알아봄으로써 실제 네트워크상에 미치는 영향을 예측할 수 있었다. 그리고 VoIP Detection System이 기존의 IDS툴에 비해 P2P기반 VoIP 트래픽을 분석하는 데 더 효율적이라는 것과 실제 네트워크상에 큰 영향을 미치지는 않는 것도 알 수 있었다. 그러나 Rule Set을 통하여 모든 Packet을 감시하므로 Network 상의 성능을 저하시키는 요소로 인하여 Packet 처리 시간의 지연이 있다는 것을 알 수 있었다. 향후 연구 방향으로 Rule Set을 통해 Packet 검색 시 성능 향상을 위한 알고리즘을 구현하고 광 대역 Network상에서 P2P 기반의 VoIP 트래픽이 미치는 영향에 대해 연구하고자 한다.