韓國 컴퓨터情報學會 論文誌
第12卷 第2號, 2007. 5.

2007-12-2-2-7

웹 트래픽 분석을 통한 유해 트래픽 탐지

신 현 준*, 최 일 준*, 추 병 균*, 오 창 석**

Harmful Traffic Detection by Web Traffic Analysis

Hyun-Jun Shin*, Il-Jun Choi*, Byoung-Gyun Chu*, Chang-Suk Oh**

요 약

웹 서비스 이외의 응용 서비스들이 웹 서비스 TCP/80 포트(Port)의 사용이 크게 증가하면서 이에 대한 보안이 시급한 실정이다. 이 포트를 통해 오가는 트래픽에 대해서는 기존의 트래픽 분석 방법으로는 서비스를 구별하기가 어려웠다. 기존의 프로토콜 및 포트 분석 기반 모니터링 기법으로는 페이로드(Payload)까지 구별 해 내기가 어려워 웹 포트를 사용하는 유해 트래픽에 대한 분석이 취약하다. 이에 본 논문에서는 웹 트래픽 분석을 위하여, 실시간으로 트래픽(Traffic)을 캡처(Capture)하여 웹 트래픽으로 분류하게 된다. 분류된 웹 트래픽을 각 응용 서비스별 세부 분류하여 가중치를 적용 후 유해 트래픽을 탐지 할 수 있도록 방법을 제안하고 구현한다. 기존 탐지에서는 분류하기 어려웠던 웹 트래픽을 정상 트래픽과 유해 트래픽으로 분류하고 탐지 성능을 향상시키는데 본 논문의 목적이 있다.

Abstract

Security of the port TCP/80 has been demanded by reason that the others besides web services have been rapidly increasing use of the port. Existing traffic analysis approaches can't distinguish web services traffic from application services when traffic passes though the port. monitoring method based on protocol and port analysis were weak in analyzing harmful traffic using the web port on account of being unable to distinguish payload. In this paper, we propose a method of detecting harmful traffic by web traffic analysis. To begin, traffic Capture by real time and classify by web traffic. Classed web traffic sorts each application service details and apply weight and detect harmful traffic. Finally, method propose and implement through coding. Therefore have a purpose of these paper to classify existing traffic analysis approaches was difficult web traffic classified normal traffic and harmful traffic and improved performance.

▸ Keyword : 유해 트래픽(Harmful Traffic), 트래픽 분석(Traffic Analysis), 웹 트래픽(Web Traffic)

• 제1저자 : 신현준, 교신저자 : 오창석(csoh@chungbuk.ac.kr)
• 접수일 : 2007.4.10, 심사일 : 2007.4.16, 심사완료일 : 2007. 5.15.
* 충북대학교 컴퓨터공학과, ** 충북대학교 전기전자컴퓨터공학부
※ 본 논문은 2006년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었습니다.

Ⅰ. 서 론

최근의 네트워크 트래픽은 웹, FTP, 전자우편 등과 같은 일부 애플리케이션 중심이었던 과거와는 달리 온라인 게임, 인터넷 뱅킹, VOD 등의 새로운 애플리케이션과 프로토콜의 출현으로 인해 매우 복잡해지고 세분화되어 웹 상에서 이용되고 있다[1]. 그런데, 파이어월(Firewall)의 검사를 받지 않도록 HTTP나 SSL, SMTP와 같이 잘 알려진 서비스를 이용한 공격이 증가하고 있다. 이와 같은 우회, 회피 공격이 증가하면서 이에 대한 네트워크 서비스 불안이 증가하고 있다[2]. 이외에도 P2P 트래픽과 같은 비 업무용 트래픽으로 인한 정상 서비스 보장의 실패도 점차 늘어나고 있는 상황이다. 하지만 이러한 포트를 사용하여 웹 서비스가 이뤄지는 80번 포트를 막을 수 없다는 것이 문제이다[1][2]. 이에 본 연구에서는 웹 트래픽의 포트와 페이로드를 분석하여, TCP 프로토콜에서 각 애플리케이션(HTTP, SMTP, POP3) 트래픽 분류, 전체 네트워크에서 P2P 애플리케이션을 분류하여 유해 트래픽을 탐지하는 방법을 연구하고자 한다. 분류된 트래픽을 HTTP 인식, HTML 인식(웹 페이지), 스트림의 구문 인식으로 단계적으로 구별하여, 유해 트래픽의 분석과 탐지 율을 향상 시킬 수 있는 알고리즘을 구현한다. 패킷의 포트와 페이로드를 분석하여, 응용 서비스별로 분류를 하게 되면, 기존의 전체 트래픽 분석, 프로토콜 분석, 포트 분석만으로 분류 할 수 없었던 유해 트래픽을 정상 트래픽과 분류 할 수 있다. 또한, 해킹 방법의 발달로 인해 정상 서비스 포트를 이용한 유해 트래픽 발생시 빠른 트래픽 분석이 요구된다. 실시간 데이터 수집 및 분석, 차단으로 기존의 대응 방법들보다 빠르고 정확하게 유해 트래픽을 분류해 낼 수 있다. 본 논문의 구성은 2장에서 프로토콜과 포트 분석을 통한 전체 트래픽 통계 방식이 NTop 모니터링 기법 및 문제점에 대해 기술하였으며, 3장에서는 본 논문에서 제안한 웹 트래픽 분석 방법에 대해 기술하였다. 4장에서는 본 논문에서 제안된 알고리즘을 실험을 통해 비교 분석 하였다. 마지막으로 5장에서는 결론 및 향후 연구과제에 대해 기술하였다.

Ⅱ. 연구 동향

최근 몇 년 동안 인터넷을 통한 각종 침해사고와 공격이 점점 증가하고 있으며 이로 인한 피해가 지속적으로 발생하고 있다. 유해 트래픽은 보다 다양화 되고 지능적이며 복합적인 형태로 발생하고 있으며 이에 맞춰 이를 차단하기 위한 솔루션도 보다 능동적이고 진보된 기술을 요구하고 있으며, 국내외 연구기관과 대학에서 트래픽을 분석하기 위한 많은 방법들이 현재 연구 중에 있다. 유해 트래픽은 정상적인 네트워크 운용이나 서비스 운영을 방해하는 악의적 공격성 패킷과 웜/바이러스, 그리고 최근 유행하고 있는 P2P 애플리케이션 등으로 분류할 수 있는데, 이 같은 트래픽의 급속한 확산은 네트워크에 직접적인 피해를 유발할 뿐 아니라, 최근에는 내부 정보 유출로까지 이어지고 있어 사회적으로 심각성이 계속 증가하고 있다[1][3].

표 1. 유해 트래픽 분류
Table 1. Harmful Traffic Classification

구분	유해 트래픽		
유해 트래픽 유형	바이러스, 스팸 메일	웜, 봇, 트로이목마 DoS/DDoS	P2P, 동영상 파일, 음악 파일
주요 증상	사용자 정보유출, 사용자 PC 자원 고갈	네트워크 및 보안 장비 장애, 각종 서비스 장애	트래픽 폭주로 인한 대역폭 고갈

표 1은 유해 트래픽 종류에 대해 정리한 것이다. 특히, 내부의 특정 시스템에서 발생하는 과도한 유해 트래픽으로 인한 패킷 로스(Packet Loss) 등으로 인해 전체 네트워크가 불안정하게 동작하거나 영향을 받는 사례가 최근 들어 자주 발생하고 있다. 현재까지는 유해 트래픽의 발생지와 원인 분석 작업에는 프로토콜 및 포트 분석을 기반으로 한 모니터링 기법이 많이 이용 되었다. 하지만 프로토콜과 포트 분석만으로는 TCP/80 한 포트에 집중되는 유해트래픽의 페이로드 분석은 어려운 현실이다. 그림 1은 패킷 전체의 구조를 나타내고 있다. 이더넷 헤더(Ethernet Header) 14 byte, IP 헤더 20byte, TCP 헤더 20byte, Data(페이로드) 0~1460byte, 이더넷 트레일러(Trailer) 4byte로 구

성 되어있다. 각 길이는 옵션 사항에 의해 가변될 수 도 있다[4].

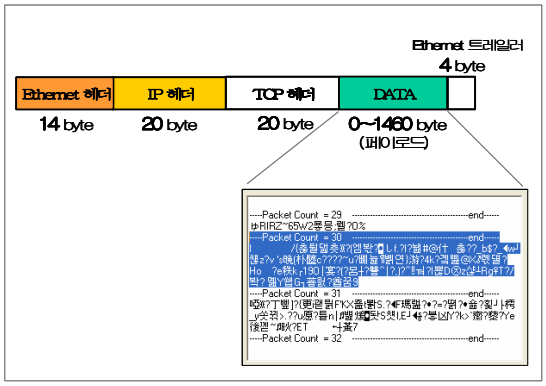

그림 1. 패킷의 구조
Fig. 1. Structure of Packet

페이로드에는 실제 패킷의 응용 데이터가 실리는 부분이다. TCP 연결의 경우 처음 연결(SYN) 패킷에는 공백이 대부분이다. 또한 실제로 연결 확립 후 데이터 전송 시에는 0~1460byte의 데이터가 실리게 된다[5][6][7]. 그림1의 페이로드는 P2P 데이터를 캡처 했을 때의 일부분이다.

2.1 기존의 프로토콜 및 포트분석 기법

NTop(Network Top)은 대표적인 오픈 소스 진영의 네트워크 트래픽 모니터링 도구로, 프로토콜과 포트 분석을 기반으로 전체 네트워크 상황에 대한 상세한 정보를 제공하므로 네트워크 관리자나 보안 관리자에게 매우 유용한 도구다[8]. NTop은 크게 네트워크에서 패킷을 수집하는 'Packet Sniffer', 수집된 패킷을 필터링하고 분석하는 'Packet Analyzer', 그리고 분석한 자료를 관리자가 읽을 수 있도록 보고서를 만드는 'Report Engine'으로 구성돼 있다[1][9]. 패킷 캡처와 패킷 필터링 기능은 Pcap(win32)를 활용하고 있다. 또한 'Packet Analyzer' 모드에서는 기존의 IP 레벨로 노드를 구분하고, 부가정보로 MAC 등을 제공하는 것이 아니라 MAC 기반으로 노드를 분석한다[9]. 따라서 TCP/IP 외에도 OSPF, IPX, Appletalk, UDP, STP 등 다양한 프로토콜에 대해 원활하게 지원할 수 있다. 그리고 'Report Engine'에서는 웹 기반 관리모드와 실시간 데이터가 갱신되는 셀에서의 기능을 제공해 'Packet Analyzer'에서 분석한 데이터를 가공해 보여준다. NTop은 터미널 방식과 웹 방식의 두 가지 환경을 지원하지만, 실제 트래픽 분석 작업에는 다양한 분석 정보와 리포팅 기능을 제공하는 웹 방식이 많이 사용된다[1][9]. 표 2는 NTop에서 분석 할 수 있는 정보들을 요약한 것이다.

표 2. 분석 정보
Table 2. Information of Analysis

분석 가능 정보	분석 가능 프로토콜
네트워크 트래픽 측정	TCP, UDP, ICMP
네트워크 프로토콜 통계정보	ARP, RARP
네트워크 트래픽 통계정보	IP : FTP, HTTP, DNS, TELNET, SMTP, POP, IMAP 등
네트워크 사용유형 정보	NetBIOS
현재 사용중인 세션(TCP) 정보 제공 각 호스트별 세션 정보	DLC, Decnet, AppleTalk 등

NTop을 이용해 모니터링하고 분석할 수 있는 정보는 네트워크 트래픽 측정, 프로토콜 및 트래픽 통계정보, 사용 유형 정보, 사용 중인 세션 정보 등을 분석할 수 있다.

2.2 기존 분석 기법의 문제점

기존의 유해 트래픽 분석에서는 전체 프로토콜과 포트 분석을 이용하였다. 유해 트래픽 가능성이 있는 프로토콜과 포트 번호를 가지고 비교를 하거나 추이를 분석하였다. TCP/80 트래픽 또한 단일 포트로 분류되어 TCP/80에 대한 전체 트래픽 추이만 확인 할 수 있었다[10]. 이는 현재 문제가 되고 있는 HTTP 이외의 유해 트래픽이 TCP/80 포트를 사용 할 경우 이 포트의 전체 트래픽 추이로는 분석이 어려운 문제가 있다. 그림 2는 Ntop에서 TCP/80 포트의 전체 트래픽 추이를 나타낸 것이다. 22:10분부터 22:30까지의 전체 트래픽 중 TCP/80 트래픽 이 보이고 있는데, 동 시간에 유해 트래픽이 TCP/80 포트를 사용했을 경우 전체 트래픽 추이에서는 유해 트래픽을 분류해 낼 수가 없다.

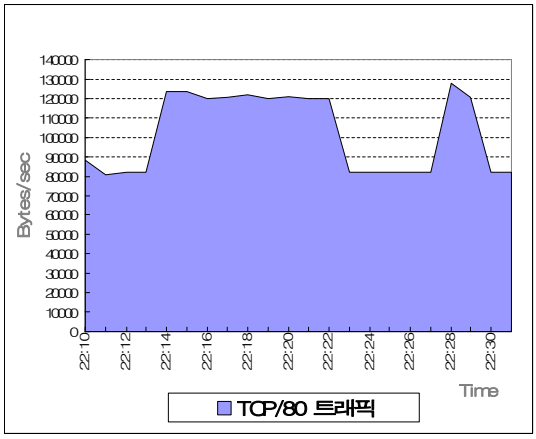

그림 2. TCP/80 포트의 트래픽
Fig. 2. Traffic of TCP/80 Port

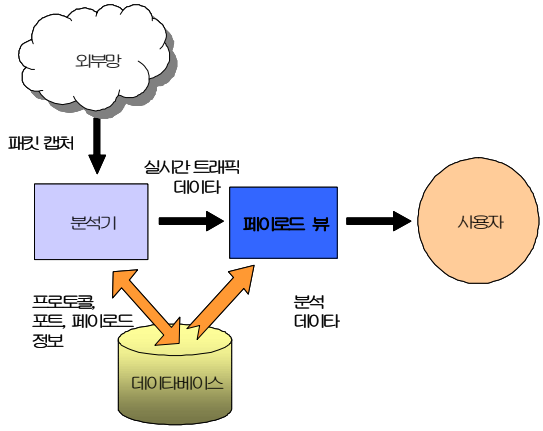

그림 3. 페이로드 분석의 동작 구조
Fig. 3. Model of Payload Analysis

현재 국내외에서 유해 트래픽을 분석하기 위하여 전체 트래픽 추이 방법[11], 프로토콜과 포트 분석 방법, 패턴 매칭 방법으로[4] 연구하고 있으나, 최근의 유해 트래픽이 과거의 방법으로는 탐지할 수 어려운 TCP/80 포트 사용하고 있으므로 대응이 미흡한 실정이다. 따라서 본 연구에서는 웹 트래픽 페이로드 분석을 기반으로 신뢰성과 정확도를 향상시킬 수 있는 유해 트래픽 탐지 방법에 대해서 연구한다.

III. 제안한 유해 트래픽 탐지 기법

본 논문에서는 페이로드 분석을 위하여, TCP/80 트래픽을 실시간으로 캡처하여 분석하는 방법을 사용한다. 각 분석 방법에 대한 내용은 다음과 같다.

▶ 페이로드 분석 모델

그림 3과 같이 트래픽을 분석하기 위해 패킷을 실시간 캡처하여 패킷 정보를 분석하는 분석기, 분석된 정보를 분류하여 보여주는 페이로드 뷰로 구성되어 있다. 네트워크 상의 패킷을 캡처한 다음 패킷 정보로부터 응용서비스 별로 분류하고 저장한다.

네트워크 상의 패킷을 캡처한 뒤 패킷 헤더 및 페이로드로부터 정보를 추출하여 분류하고 LogFormat에 저장한다. 이 데이터를 가지고 분석과 비교를 하게 된다. 그림 4는 LogFormat 정보를 추출하는 내용을 설명한다.

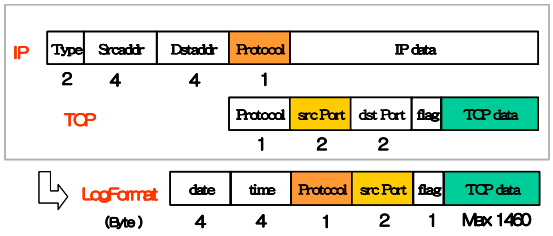

그림 4. LogFormat 구조
Fig. 4. Structure of LogFormat

Protocol 정보는 IP 프로토콜 헤더에서, src_Port정보와 TCP_data는 TCP 정보에서 가지고 온다. 페이로드 뷰는 실시간으로 캡처된 각 TCP/80 패킷의 데이터를 구문 인식을 통하여 분류하게 된다. 분류된 페이로드 부분을 Data에 저장한다.

▶ 응용 서비스별 트래픽 분류

실시간 패킷 캡처를 하기 위하여 IpWorks 라이브러리를 사용했으며, Promiscuous모드를 이용하였다. IpWorks 라이브러리는 윈도우즈 및 기타 운용체제에서 사용 할 수 있도록 독립적인 모듈을 제공한다.

표 3. 응용 서비스 별 분류
Table 3. Classification of Application Services

응용 서비스 구분	구문 인식 (예)
HTML 인식	모든 HTML TAG 포함
DDoS/DoS	패턴 매칭 ex) content : "login|3A|" , "betaalmostdone" , "gOrave" "killme" , "|FF F4 FF FD 06|" "|00|" , "|00 00|" , "GET" and "FTP|3A|//"
스팸 메일 인식	유해 단어 포함 ex) 대출,대%출, 대*출 등 유해 단어 포함 (단어 사이 특수문자 제거)
P2P 인식 (음악,동영상)	File download (mp3, avi 등)

캡처한 패킷 정보는 시간 정보와 함께 데이터베이스에 저장되며, 구문 인식에 따른 비교 분석을 통하여 각 서비스 별로 구별 하였다. 표 3은 페이로드의 응용서비스 별 분류 형식이다. TCP는 신뢰성 있는 통신을 제공하기 위하여, 커넥션 지향의 프로토콜이다. 통신을 시작할 때 커넥션을 연결하고 통신을 종료하면 커넥션을 끊는다. TCP 헤더에는 6비트의 제어 플래그가 있다. 순서대로 UGR, ACK, PSH, RST, SYN, FIN 이라고 하며, 삼중 핸드셰이크(Three-way Handshake)를 이용하여 연결을 설정한다. 페이로드 분석이 이를 이용하여, SYN 플래그 연결 확립 후 ACK 플래그 DATA 전송 완료된 다음 FIN 플래그 연결 종료 시까지의 페이로드를 같은 내용으로 보고 분류 및 분석을 한다. DDoS/DoS 패턴 매칭 룰은 www.snort.org에서 업데이트하여 사용하고, 스팸 메일 인식은 웹상에서 사용하는 웹 메일을 분석한다. 스팸 분류는 스팸 가능 문자를 포함하거나, 스팸 가능 문자 사이에 특수 문자를 삽입하였을 경우, 특수 문자를 제거하고 분석하도록 한다. 또한 시스템 성능을 높이기 위해 스팸 단어 검색 시 DFA검색을 이용한다.

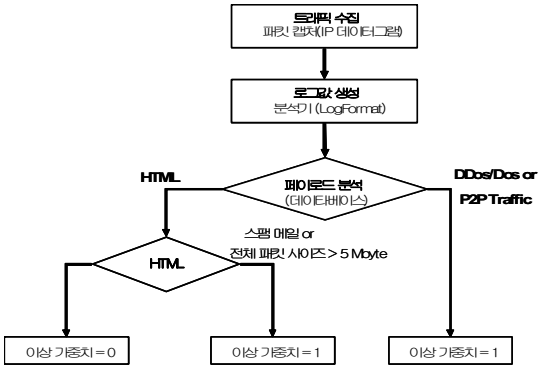

그림 5. 페이로드 분석 흐름도
Fig. 5. Flow Chart of Payload Analysis

그림 5는 페이로드 분석 흐름도에 관한 것이다. HTML 트래픽이 분석되었을 경우 스팸 단어 리스트를 확인하여 스팸 메일로 분류될 경우 이상 가중치를 1을 적용하고, 정상 HTML이 경우 이상 가중치를 0을 적용한다. 또한 분석 데이터에 DDoS/DoS 패턴이나, P2P 패턴이 분석 되었을 경우 그 출발지 주소지에서 오는 모든 패킷을 이상 가중치 1을 적용하여 유래 트래픽으로 분류한다. 그림 6에서는 각 서비스 별로 페이로드 분석 흐름도를 도시하였다. 이 분석 방법에서는 분석된 응용서비스를 정상 트래픽과 유해 트래픽으로 이상 가중치를 적용하여 분류하게 된다. 정상 트래픽은 이상 가중치 값을 0 으로 유해 트래픽은 이상 가중치 값을 1을 부여 한다.

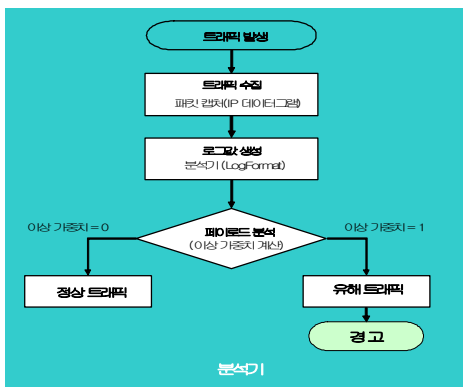

그림 6. 제안한 유해 트래픽 탐지 흐름도
Fig. 6. Flow Chart of Proposed Harmful Traffic Detection

IV. 실험 및 결과 고찰

본 논문에서 제안한 웹 트래픽 분석의 실험을 위해 사용된 환경은 일반 사용자들 그룹에서 유해 트래픽이 발생한다고 가정하고, 시뮬레이션 하였다. 관리 시스템에서는 발생되는 트래픽을 분석하도록 하였다. 실험 환경은 그림 7과 같다.

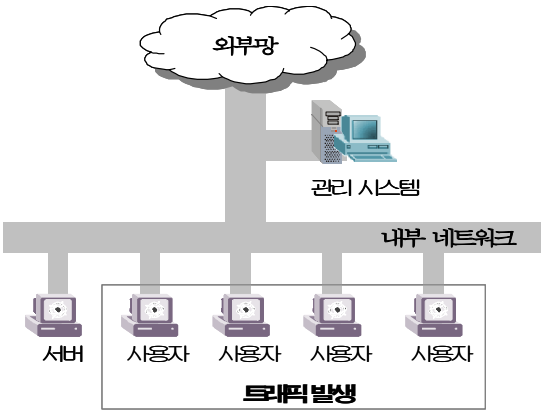

그림 7. 유해 트래픽 탐지 테스트 환경
Fig. 7. Test Environment of Harmful Traffic Detection

P2P 트래픽 탐지는 MSN 메신저, 네이트온 메신저를 사용하고, DDoS/DoS 트래픽 탐지는 TFN(Tribe Flood network) 공격 도구를 이용하였다[12]. 스팸 메일은 다음(www.daum..net), 네이버(www.naver.com) 메일을 이용하여 보낸 메일을 사용하여 분석하였고 정상 트래픽은 유해 트래픽을 제외한 서비스로 구별하였다.

4.1 기존 방법의 트래픽 분석 결과

기존 방법의 트래픽 분석 결과는 Ntop의 프로토콜 및 포트분석 기반 방법을 사용하였다. TCP/80 포트의 트래픽을 실험을 통하여 발생시키고 모니터링 하였다. 그림 8은 기존 방법인 Ntop을 이용한 TCP/80 포트의 트래픽 추이 분석 결과이다. PM 12:30분 ~ PM 12:51 분까지 TCP/80 포트를 이용하여 HTML, P2P, DDoS/DoS, 스팸 트래픽을 발생시켰을 때의 트래픽 분석 결과 TCP/80 포트에 대해서는 전체 트래픽 추이로 평균 81.8 KByte/sec로 모니터링 되었다. 그림 8과 같이 전체 트래픽으로 분석되기 때문에 응용 서비스 별로 분류할 수 없는 문제가 발생되었다.

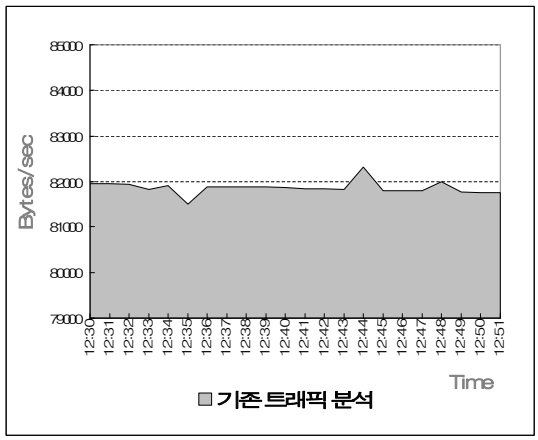

그림 8. TCP/80 포트의 Ntop 트래픽 탐지
Fig. 8. Ntop Traffic Detection of TCP/80 Port

4.1 HTML과 P2P 트래픽 분석 결과

본 논문에서 제안한 방법을 사용하여, 그림 8의 동일 트래픽을 같은 시간대에 분석하였을 경우, TCP/80 트래픽 중에서 웹 사용의 대부분을 차지하는 HTML 트래픽과 P2P 트래픽을 탐지 할 수 있었다.

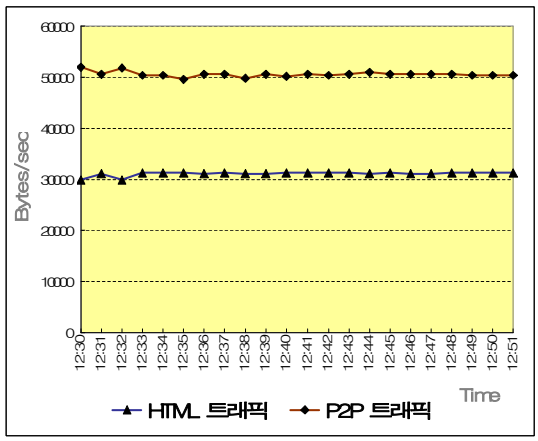

그림 9. HTML과 P2P 트래픽 탐지
Fig. 9. Detection of HTML AND P2P Traffic

기존의 트래픽 분석에서는 그림 8에서 보는 것과 같이

TCP/80 포트의 트래픽 평균 81.8 KByte/sec로 웹 트래픽 전체만 파악 할 수 있어서, 세부적인 HTML 트래픽을 분류할 수 없었는데, 그림 9에의 HTML 트래픽처럼 측정 시간대 평균 31.1 KByte/sec의 트래픽이 탐지가 가능해 졌다. 그림 9의 HTML 트래픽은 PM 12:30 ~ PM 12:51까지의 트래픽 추이 분석 결과이다. 또한 P2P 프로그램은 다양한 포트 번호들을 사용한다는 특성을 가지고 있고, 이 포트 번호들이 1024 이하의 well-known port가 아니라 시스템에서 자동으로 생성되는 랜덤 포트와 같은 범위였다. 그런데 공공기관, 기업체, 학교 등 정보보안과 관련하여 P2P 포트들을 차단하기 시작했다. 이에 P2P 프로그램 또한 발전하여 TCP/80 포트를 사용하기 시작하였다. P2P 프로그램은 평상시 주기적인 데이터 확인을 위하여 메시지 교환을 하게 되는데, 이를 분석하여 P2P 트래픽으로 분류한다. 그림 9의 P2P 트래픽은 PM 12:30분 ~ PM 12:51분까지 MSN 메신저, 네이트온 메신저 P2P 트래픽 분석 결과이다. 기존의 방법인 그림 8에서, TCP/80 포트의 평균 트래픽이 81.8 KByte/sec으로 분류가 되지 않아서 탐지가 어려운 것에 비해 제안한 방법은 P2P 트래픽이 분류되어 평균 50.5 KByte/sec의 트래픽이 탐지가 되었다.

4.2 DDoS/DoS와 스팸 메일 트래픽 분석 결과

본 논문에서 제안한 방법을 사용하여, 그림 8의 동일 트래픽을 같은 시간대에 분석하였을 경우, TCP/80 트래픽 중에서 DDoS/DoS와 스팸 메일 트래픽에 대해서 분석 할 수 있었다. 트래픽 폭주 공격의 대표적인 DDoS/DoS 공격은 피해 호스트로 대량의 네트워크 트래픽을 발생시켜 네트워크의 기능 및 시스템 자원을 고갈시켜 서비스를 일시적 또는 완전히 정지 시키는 공격유형이다. 그런데 이런 공격에 앞서 공격자, 마스터, 에이전트 사이에 제어 메시지가 포함 되게 되는데, 트래픽 발생시 페이로드에 메시지가 포함된 유해 트래픽을 분석한 결과 이다. 그림 10의 DDoS/DoS 트래픽은 PM 12:30분부터 PM 12:51분까지 주기적으로 메시지가 교환된 경우 탐지된 경우이다. PM 12:38분에는 평균보다 145 Byte/sec 보다 높은 DDoS/DoS 트래픽의 900 Byte/sec의 탐지를 볼 수 있다. 기존의 방법인 그림 8에서, TCP/80 포트의 평균 트래픽이 81.8 KByte/sec으로 분류가 되지 않아서 탐지가 어려운 것에 비해 제안한 방법에서는 탐지가 되는 것을 볼 수 있다. 기존의 DDoS/DoS의 대량 공격 트래픽은 전체 트래픽에서 갑자기 증가하기 전체 트래픽 추이 방법으로는 탐기가 가능했으나, 위와 같이 작은 양의 공격 전 트래픽에 대해서는 탐지가 어려웠다.

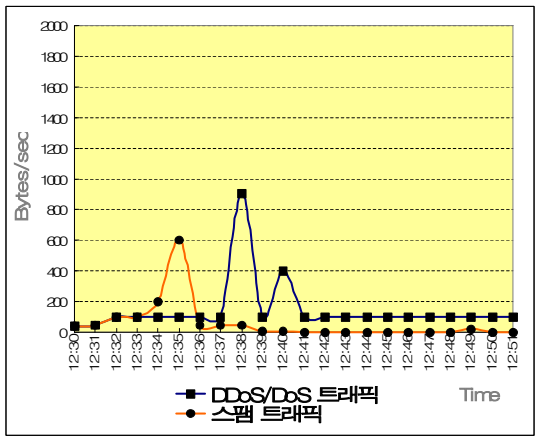

그림 10. DDoS/DoS 트래픽 탐지
Fig. 10. Detection of DDoS/DoS Traffic

웹 메일 트래픽 발생시 제목과 본문 부분의 필터링을 통하여, 제목과 본문내용에 스팸 단어가 포함 되었을 경우 유해 트래픽으로 분석하였다. 스팸 단어가 포함 되었을 경우 첨부 파일 트래픽에 대해서도 같은 트래픽으로 간주한다. 또한 스팸 단어 검색 효율을 높이기 위해 스팸 단어 사이의 특수 문자나 공백 포함 시 제거 후 분석한다. 그림 10의 스팸 트래픽은 PM 12:30분 ~ PM 12:51분 사이에 발생된 스팸 트래픽의 분석 결과이다. 기존의 방법인 그림 8에서, TCP/80 포트의 평균 트래픽이 81.8 KByte/sec으로 분류가 되지 않아서 탐지가 어려운 것에 비해 제안한 방법에서는 스팸 트래픽 평균 58.2 Byte/sec로 탐지가 되는 것을 볼 수 있다. 제안된 방법에서는 각 서비스 별로 분류가 가능한 것을 확인 할 수 있으며 분석 소요 시간 또한 대등하여 탐지 성능이 높아진 것을 확인 할 수 있다. 위의 실험 결과 값을 토대로 본 논문에서 제안한 알고리즘에 의한 트래픽 분석과 기존의 방법에 의한

트래픽 분석 결과를 표 4에 나타내고 있다.

표 4. 탐지 시간 분석 결과
Table 4. Result of Detection Time Analysis

탐지 기법 \ 트래픽 유형	HTML 트래픽	DDoS / DoS 트래픽	스팸 메일 트래픽	P2P 트래픽
기존 방법	1초 이내 (전체 트래픽)	·	·	·
제안한 분석 방법	1초 이내	1초 이내	1초 이내	1초 이내

표 4의 기존 방법의 탐지 시간 분석은 TCP/80 포트의 전체 트래픽 추이로 실시간으로 분석되기 때문에 1초 이내에 탐지가 가능하다. 단 기존 방법에서는 TCP/80 포트의 트래픽을 HTML 트래픽으로 간주한다[13][14]. 제안한 분석 방법의 HTML, DDoS/DoS, 스팸 메일, P2P 트래픽 탐지 시간 모두 실시간 분석으로 1초 이내에 탐지가 가능하다. 따라서 기존 분석 방법에 비해 탐지율 향상에 따른 분석 시간 저하는 없는 것을 표 4에서 확인 할 수 있다.

V. 결 론

유해 트래픽은 정상적인 네트워크 운용이나 서비스 운영을 방해하는 악의적 공격성 패킷과 웜/바이러스, 그리고 P2P 애플리케이션 등으로 분류할 수 있는데, 이와 같은 트래픽의 급속한 확산은 네트워크에 직접적인 피해를 유발할 뿐 아니라, 최근에는 내부 정보 유출로까지 이어지고 있어 심각성이 계속 증가하고 있는 실정이다[13][15]. 본 논문에서는 기존 프로토콜 및 포트 분석 기반의 TCP/80 포트의 전체 트래픽 추이 방법의 문제점을 해결하기 위하여, 실시간으로 TCP/80 포트의 트래픽을 캡처하여 응용 서비스 별로 분류하였다. 분류한 트래픽을 가지고 각 응용 서비스별 유해 트래픽 가중치를 적용 후 유해 트래픽을 탐지 할 수 있도록 방법을 제안하고 구현하였다. 실험을 통하여 유해 트래픽에 대하여 빠른 대응을 할 수 있고, 기존의 방법들과 비교하여 분석하지 못했던 TCP/80 트래픽을 세부적으로 분석하므로 HTML, DDoS/DoS, 스팸 메일, P2P 트래픽을 분류 할 수 있다. 또한 유해 트래픽을 조기에 검출할 수 있으므로 탐지율 향상을 개선시킬 수 있다. 향후 페이로드 분석 시 많은 트래픽 처리량으로 인한 낮은 시스템 효율 및 성능을 개선한다면 넓은 사용범위와 여러 유해 트래픽에 대해 네트워크의 효율적인 관리와 안정적인 서비스를 제공할 수 있게 될 것으로 기대된다.

참고문헌

[1] 박광청, “트래픽 모니터링과 플로우 기반 분석 방법론”, 온더넷, 2006. 1.
[2] 신동윤, “웹 서비스시대의 보안 솔루션”, 온더넷, 2007. 1.
[3] 김한기, “네트워크 인텔리전스 측면의 보안”, 온더넷, 2006. 1.
[4] Brian Caswell, Jay Beale, Andrew R. Baker, “Snort Intrusion Detection and Prevention Toolkit”, SYNGRESS, 2006.
[5] George J. Lee, Lindsey Poole, "Diagnosis of TCP Overlay Connection Failures using Bayesian Networks", SIGCOMM Conference, Sep. 2006.
[6] Changhee Joo, Saewoong Bahk, "Increasing TCP Capacity in Wireless Multihop Networks", S.Shinmojo et al. HSI 2005, LNCS 3579, pp.37-44, 2005.
[7] Tilman Wolf, Shulin You, and Ramaswamy Ramaswamy, "Transparent TCP acceleration through network processing," in Proc. of IEEE Global Communications Conference (GLOBECOM), St. Louis, MO, vol. 2, pp. 750-754, Nov. 2005.
[8] 김기환, 박대우, “Tokenless OTP를 활용한 인증

모델", 컴퓨터 정보학회 논문지, Vol. 12, No. 1, pp.107~116, 2007. 4.
[9] NTOP. http://www.ntop.org/download.html, 2006. 11
[10] Feng Qiu, Zhenyu Liu, Junghoo Cho, "Analysis of User Web Traffic with a Focus on Search Activities", University of California, Sep. 2005.
[11] 유대성, "트래픽 분석을 이용한 SNMP 기반의 공격 탐지", 충북대학교 대학원 석사학위논문, 2005. 2.
[12] 박주기, 최은복, "세션화 방식을 통한 퍼지기반 네트워크 침입탐지 시스템", 컴퓨터 정보학회 논문지, Vol. 12, No. 1, pp.127~135, 2007. 4.
[13] 이종일, "웹 애플리케이션 공격의 이해", 온더넷, 2006. 3.
[14] Kevin Borders, Atul Prakash, "Detecting Covert Web Traffic", University of Michigan, Oct. 2004.
[15] Jeffry R. Williams, "The Ten Most Critical Web Application Security Vulnerabilities," OWASP, Jan, 2004.

저 자 소 개

신 현 준

2003년 2월 충주대학교 컴퓨터공학과 (공학사)
2005년 8월 충북대학교 전기전산공학과 (공학석사)
2006년 3월 ~ 현재 충북대학교 컴퓨터공학과 박사과정
<관심분야> : 정보보안, 네트워크

최 일 준

1997년 2월 충주대학교 컴퓨터공학과 (공학사)
2003년 8월 충북대학교 컴퓨터공학과 (공학석사)
2004년 3월 ~ 현재 충북대학교 컴퓨터공학과 박사과정
<관심분야> : 컴퓨터 네트워크, 정보보호

추 병 균

1999년 2월 충주대학교 컴퓨터공학과 (공학사)
2004년 8월 충북대학교 컴퓨터공학과 (공학석사)
2005년 3월 ~ 현재 충북대학교 컴퓨터공학과 박사과정
<관심분야> : 정보보안, 네트워크

오 창 석

1978년 2월 연세대학교 전자공학과 (공학사)
1980년 2월 연세대학교 전자공학과(공학석사)
1988년 8월 연세대학교 전자공학과(공학박사)
1985년~현재 충북대학교 전기전자컴퓨터 공학부교수
1982년~1984년 한국전자 통신연구원 연구원
1990년~1991년 Stanford 대학교 객원교수
<관심분야> 컴퓨터네트워크, 뉴로컴퓨터, 정보보호