프로토콜과 포트 분석을 통한 유해 트래픽 탐지

Harmful Traffic Detection by Protocol and Port Analysis

신현준*, 구향옥**, 최일준**, 오창석***
충북대학교 전기전산공학과*, 충북대학교 컴퓨터공학과**, 충북대학교 전기전자컴퓨터공학부***
Hyun-Jun Shin(shinhyunjoon@korea.com)*, Hyang-Ohk Koo(ok999@hanmail.net)**,
Il-Jun Choi(cij0319@kdc.ac.kr)**, Chang-Suk Oh(csoh@nwork.chungbuk.ac.kr)***

요약

유해 트래픽의 최근 유형은 트래픽 폭주 공격에서 더 발전되어 웜, 봇과 같이 다양화, 지능화, 은닉화, 자동화되어 기존의 방법으로는 탐지하기 어렵다. SNMP 기반의 추이 분석 방법은 인터넷 사용의 큰 비중을 차지하고 있는 정상적인 P2P(메신저, 파일 공유) 및 기타 응용 프로그램 사용 시 유해 트래픽으로 분류하는 문제점과, 웜 및 봇과 같은 발전된 유해 트래픽을 분석해내지 못하는 큰 취약점을 가지고 있다. 제안한 방법은 프로토콜 추이 및 포트 트래픽 분석 방법을 적용하였다. 발생된 트래픽을 프로토콜, well-known 포트, P2P 포트, 기존 공격 포트, 특정 포트로 분류하고 이상 가중치를 적용하며, 실험 결과 P2P 트래픽 분석, 웜 및 봇 탐지, 트래픽 폭주 공격 등을 효과적으로 검출 할 수 있었다.

■ 중심어 : | 웜, 봇 | 유해 트래픽 분석 | 트래픽 폭주 공격 |

Abstract

The latest attack type against network traffic appeared by worm and bot that are advanced in DDoS. It is difficult to detect them because they are diversified, intelligent, concealed and automated. The exisiting traffic analysis method using SNMP has a vulnerable problem; it considers normal P2P and other application program to be harmful traffic. It also has limitation that does not analyze advanced programs such as worm and bot to harmful traffic.

Therefore, we analyzed harmful traffic out Protocol and Port analysis. We also classified traffic by protocol, well-known port, P2P port, existing attack port, and specification port, apply singularity weight to detect, and analyze attack availability. As a result of simulation, it is proved that it can effectively detect P2P application, worm, bot, and DDoS attack.

■ keyword : | Worm, Bot | Harmful Traffic Analysis | Traffic Flooding Attack |

I. 서 론

최근 인터넷의 사용이 급증하면서 취약점을 이용한 공격이 복잡하면서도 고도화된 기법으로 발전하고 있어 여러 사용자들이 위험에 쉽게 노출되어 있다[1]. 해킹 기술의 최근 유형은 트래픽 폭주 공격에서 더 발전되어

접수번호 : #050629-002
접수일자 : 2005년 6월 29일
심사완료일 : 2005년 07월 27일
교신저자 : 구향옥, e-mail : ok999@hanmail.net

웜, 봇과 같이 다양화, 지능화, 은닉화, 자동화되어 단순한 트래픽 분석방법으로는 탐지하기 어렵다. 기존의 SNMP를 이용한 트래픽 분석 방법은 일주 트래픽 추이 분석, 프로토콜별 추이 분석, 특정 MIB 객체 분석의 이상 가중치를 값을 통하여 유해 트래픽을 분석하였다[2]. 이러한 방법은 정상적인 P2P (메신저, 파일 공유) 및 기타 응용 프로그램의 정상 사용을 유해 트래픽으로 분류하는 문제점과, 웜 및 봇과 같은 발전된 유해 트래픽을 SNMP를 이용한 트래픽 분석으로는 찾아내지 못하는 큰 취약점을 가지고 있었다.

이에 본 논문에서는 응용 프로그램의 정상 사용 시 분석, 웜 및 봇과 같은 유해 트래픽의 분석을 통하여 성능 및 탐지율을 향상시키는 프로토콜과 포트 분석을 통한 유해 트래픽 탐지 방법을 제안한다. 2장에서는 유해 트래픽의 일반적인 내용을 기술하였고, 3장에서는 기존의 SNMP를 이용한 트래픽 분석의 문제점을 분석하였다. 4장에서는 제안된 유해 트래픽 탐지 방법으로 발생된 트래픽을 프로토콜별, 포트별 분석하였다. 5장, 6장에서는 실험 및 결과 고찰, 결론 순으로 정리하였다.

II. 유해 트래픽

웜 공격은 인터넷상에서 빠른 전파력을 통해서 자기 복제를 하는 프로그램을 말한다. 웜의 가장 큰 특징인 빠른 전파를 통해 인터넷상에서 취약점이 있는 시스템을 감염시키고, 감염된 시스템을 통해 제2의 공격을 행하는 것이다[2].

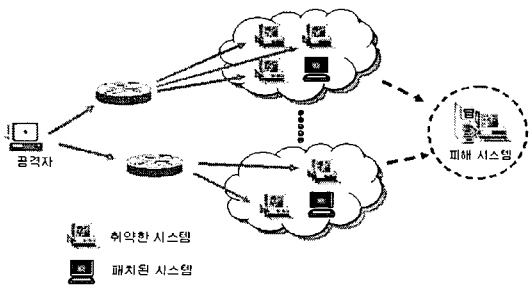


그림 1. 웜 공격의 트래픽 흐름

기존의 DDoS 공격이 트래픽 폭주 공격을 행하기 위해서는 에이전트를 확보하기 위한 해커의 노력이 필요하지만 웜을 이용할 경우 이러한 과정을 자동화시키고 또한 빠른 시간에 대규모의 에이전트를 확보할 수 있기 때문이다. [그림 1]은 웜 공격의 트래픽 흐름을 나타낸다.

[그림 1]에서 보듯이 공격자는 시스템의 취약점을 이용하여 웜을 전파하게 된다. 인터넷상에서 전파된 웜은 취약점이 있는 시스템을 검색하여 웜을 전파하게 된다. 웜의 전파로 인해 네트워크상에는 많은 트래픽이 발생하게 되며, 2차로 웜에 감염된 시스템들을 통해 특정 시스템으로 DDoS 공격을 행하게 된다.

▪ Mydoom 웜

Mydoom 웜은 메일과 P2P에 의해 감염되는 웜 공격이다. 메일에 의한 전파는 첨부파일에 웜 파일을 첨부하여 메일을 받은 사용자가 첨부파일을 실행시키게 되면 웜에 감염되게 된다. P2P에 의한 감염은 웜의 이름을 특정 소프트웨어의 이름이나 동영상 파일의 제목으로 변형하여 P2P에 게재하게 된다. 이를 다운받아 실행시킨 사용자의 컴퓨터는 웜에 감염되게 되는 것이다. Mydoom 웜도 다량의 메일을 전송시키게 됨으로써 네트워크에 큰 무리를 주며 감염된 시스템을 통해서 제 2의 공격을 행한다는 특징을 가지고 있다. 감염된 시스템들을 통해 특정 사이트로 SYN Flooding 공격을 행하게 되며 SYN Flooding 공격을 받는 시스템뿐만 아니라 공격을 행한 시스템들도 SYN에 대한 ACK의 수신으로 인해 시스템의 속도가 현저히 줄어드는 피해를 받게 된다. [그림 2]는 Mydoom 웜의 공격 형태를 나타낸다[4].

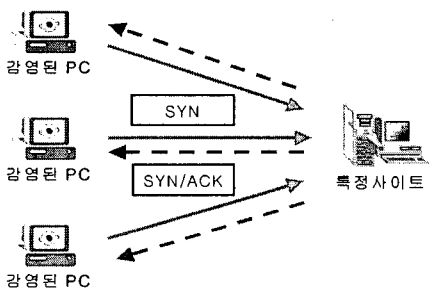


그림 2. Mydoom 웜의 공격 형태

■ Bagle.AY 웜

Bagle.AY 웜은 감염시 두 번에 걸쳐 악성코드 설치가 발생하는데, 첫 번째로 메일첨부를 클릭시 1차로 감염되고, 1차 감염이 성공할 경우 자동적으로 특정 사이트로부터 추가적인 악성코드가 다운로드 되어, 2차 감염이 발생한다. 1차 감염만으로도, 자신의 복제파일을 메일에 첨부하여 타 시스템으로 전파하는 시도를 한다. 특징으로는 1차 감염 시, 분당 메일 공격 빈도가 123회 정도이고, 악성 사이트 접속주기는 2초당 1회이다. [그림 3]은 Bagle.AY 웜의 공격 형태를 나타낸다[5].

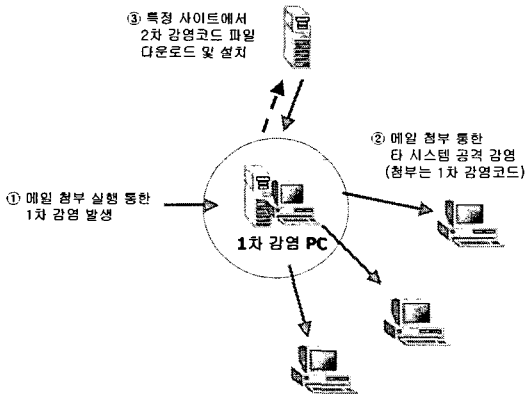


그림 3. Bagle.AY 웜의 공격 형태

■ 봇

봇은 Robot의 준말이며, 스스로 움직이지 못하고 사람에 의해 제어당하는 로봇과 마찬가지로 악성 봇은 이미 해킹당해 해커에 의해 제어당하는 시스템을 말한다. 공격자가 소유한 IRC 채널에 연결된 감염된 호스트를 봇이라고 하고, IRC 채널에 연결된 봇들로 이루어진 네트워크를 BotNet이라고 한다. 기존에는 다수의 좀비 시스템들을 관리하고 제어하기 위해서 핸들러 시스템을 별도로 두어 특정 TCP 혹은 UDP 포트를 이용하여 좀비 시스템들에게 명령을 내렸는데, 최근에는 핸들러 시스템을 별도로 두는 대신에 IRC 네트워크 제어 수단으로 많이 사용하고 있다. 봇의 종류는 대단히 다양하고 종류에 따라 감염 및 공격 절차가 서로 다르지만, 대부분 IRC를 제어 채널로 이용하고 있다. 봇은 운영체제 또는 애플리케이션의 보안 취약점, 웜과 같은 자동화된 공격도구를 이용하여 대규모의 시스템들을 해킹하고 해킹한 시스템에 봇을 설치하게 된다. [그림 4]는 봇 감염 및 공격 절차이다[4].

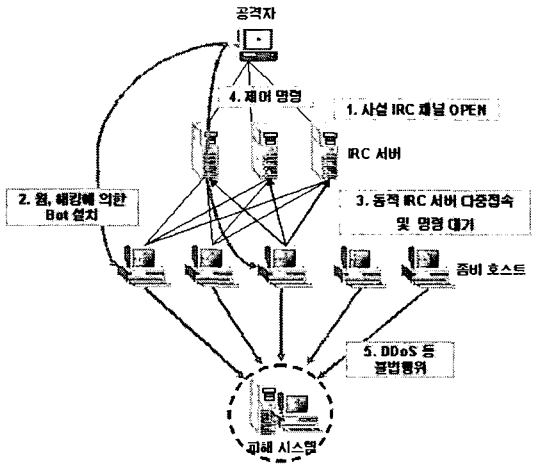


그림 4. 봇 감염 및 공격 절차

III. 기존의 SNMP 이용한 트래픽 분석

SNMP(Simple Network Management Protocol)를 이용한 트래픽 분석은 관리 객체들의 집합인 MIB(Management Information Base)를 이용하여 관리 대상 시스템으로부터 트래픽을 수집하게 된다. 이때 사용되는 MIB 객체는 일주 트래픽 추이, 프로토콜별 트래픽 발생 추이 그리고 공격에 반응하는 MIB 객체를 사용하게 된다.

수집된 트래픽 정보는 현재까지 입력된 트래픽의 총 누적치로 단위시간 동안의 트래픽 양을 알기 위해서는 현재 누적 값에서 이전 누적 값과의 차이를 통해서 구할 수 있다. [그림 5]는 SNMP 기반의 유해 트래픽 탐지 구조이다[2]. SNMP 기반의 추이 분석을 통한 트래픽 분석의 특징은 유해 트래픽에 대해서 정확한 분석을 할 수 있다는 장점을 가지고 있다. 그러나 [그림 6]과 같이 정상적인 응용 프로그램(메신저, P2P, 웹) 사용 시 유해 트래픽으로 분류하는 것과, 웜, 봇 같은 유해 트래픽을 분석해내지 못하는 단점을 가지고 있다.

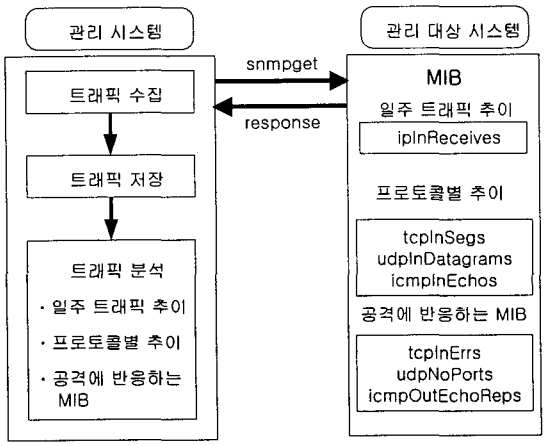


그림 5. SNMP 기반의 유해 트래픽 탐지 구조

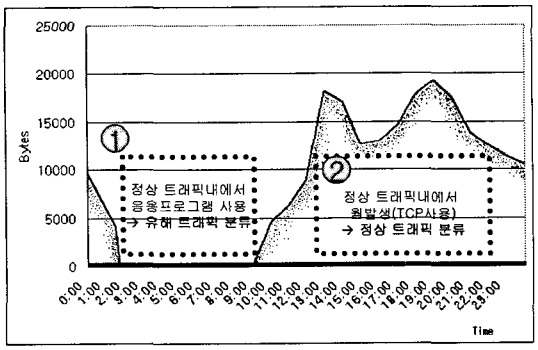


그림 6. 일주 트래픽 추이 방법의 문제점

[그림 6]은 일주 트래픽 추이 내에서 응용프로그램 및 웜 트래픽 발생시 경우의 문제점을 나타낸다.

Ⅳ. 제안된 유해 트래픽 탐지 방법

본 논문에서는 기존의 SNMP 이용한 일주 트래픽 추이 방법의 문제점을 해결하기 위해 프로토콜 추이 및 포트 트래픽 분석 방법을 사용하였다. 각 분석 방법에 대한 내용은 다음과 같다.

■ 유해 트래픽 탐지 모델

[그림 7]과 같이 트래픽을 분석하기 위해 패킷을 실시간 캡처하여 패킷 정보를 분석하는 분석기, 분석된 정보를 보여주는 윈도우즈 뷰로 구성되어 있다. 네트워크상의 패킷을 캡처한 뒤 패킷 헤더로부터 원하는 정보를 추출하여 분류하고 저장한다.

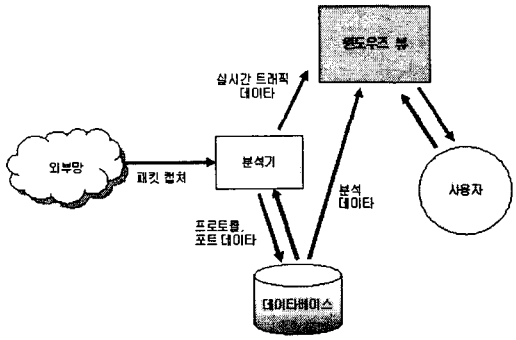


그림 7. 프로토콜 및 포트 분석의 동작 구조

네트워크 상의 패킷을 캡처한 뒤 패킷 헤더로부터 원하는 정보를 추출하여 분류하고 LogFormat에 저장한다. 이 데이터를 가지고 분석 및 비교를 하게 된다. [그림 8]은 LogFormat 정보를 추출하는 내용을 설명한다.

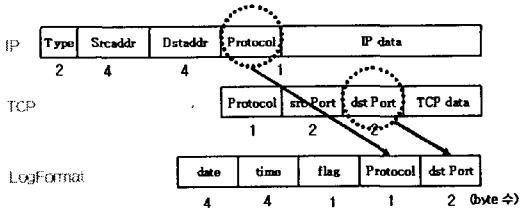


그림 8. LogFormat의 구조

Protocol 정보는 IP 프로토콜 헤더에서, dst_Port 정보는 TCP/UDP 헤더에서 가지고 온다. ICMP와 같이 IP 기반이지만 포트 정보를 사용하지 않는 프로토콜은 해당 필드를 "0"으로 저장한다.

윈도우즈 뷰는 실시간으로 캡처된 각 프로토콜, 포트별 사용량을 모니터링 할 수 있도록 보여주고, 분석기가 분석 및 통계를 내서 저장한 시간의 네트워크 트래픽 데이터를 비교 분석할 수 있도록 보여주는 모듈이다.

■ 프로토콜별, 포트별 트래픽 분석

실시간 패킷 캡처를 위해서 IpWorks 라이브러리의

promiscuous 모드를 사용했다. IpWorks 라이브러리는 윈도우즈 및 기타 운영체제에서 쓸 수 있도록 독립적인 모듈을 제공한다. 캡처한 패킷 정보는 시간 정보와 함께 데이터베이스에 저장되며, 응용 프로그램 및 관리 포트 정보는 시스템에서 과부하로 인한 패킷이 생길 수 있기 때문에 파일로 관리 하였다. 본 논문에서는 비교 기준값을 구하기 위해 각 5분대별로 얻어진 트래픽 발생 빈도에 대해서 프로토콜, 포트 트래픽을 수용할 수 있는 최대값을 기준값으로 구하였다. 구해진 기준값을 통해 시스템에 발생된 프로토콜 트래픽은 일정한 오차 범위 내에서 같은 시간대별로 규칙적으로 발생되는 것을 확인할 수 있다. 이는 정상적인 서비스를 제공하는 시스템에 접속하는 일반 사용자들은 일정한 시간대에 많은 접속을 하며 그 외의 시간에서는 접속을 하지 않기 때문이다[2]. 얻어진 프로토콜 트래픽 추이를 통해서 발생되는 트래픽량이 기준 트래픽보다 크다면 일반 사용자가 아닌 공격자에 의해 발생되는 유해 트래픽으로 간주할 수 있다.

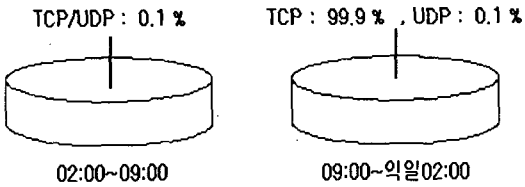


그림 9. 프로토콜별 트래픽 발생 추이

[그림 9]는 프로토콜별 트래픽 발생 추이를 나타낸다. 시스템에서 발생되는 트래픽이 시간에 따라서 비율이 다르게 나오는 것을 알 수 있다. 새벽 2시부터 9시까지는 일반적인 사용자들이 시스템에 접근하지 않는 시간대로 TCP 트래픽의 비율은 거의 0%에 가깝다. 이외의 시간대에서는 시스템에 사용자들이 접속하게 되어 TCP의 비율이 거의 100%에 가깝게 나오게 된다. ICMP 트래픽의 경우 정상적인 시스템에서는 ICMP 기반의 트래픽은 거의 발생하지 않았다[1]. 이를 통해서 ICMP 트래픽의 발생 비율이 급격하게 증가하거나 UDP 트래픽의 발생 비율이 증가할 경우 해당 프로토콜을 이용한 트래픽 폭주 공격에 의한 트래픽으로 분석할 수 있다.

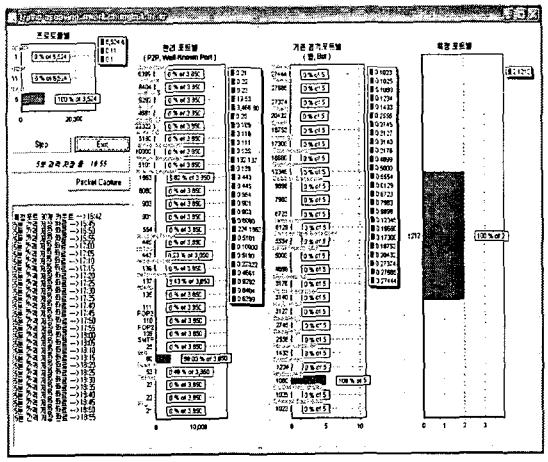


그림 10. 포트별 발생 추이

위의 [그림 10]은 각 포트별 트래픽 발생 추이를 나타낸다. 포트별 트래픽 분석은 P2P 포트, well-known 포트, 기존 공격 포트, 특정 공격 포트를 통하여, 각 종류별로 분류한 후 가중치를 적용함으로써 유해 트래픽을 탐지할 수 있다. 네트워크에서 발생되는 포트별 트래픽은 시간에 따라서 비율이 상이하게 나온다. 또한 이러한 점을 이용해 웹 응용 프로그램 및 기타 포트별 사용 현황을 실시간으로 파악할 수 있다. 관리 시스템에서는 실시간으로 패킷을 캡처하여 IP 데이터그램의 정보를 수집하며, 실시간으로 수집된 트래픽 정보는 기존 5분 단위 기준값과 비교를 하게 된다. 입력된 총 트래픽 누적치는 5분 단위로 프로토콜별 LogFormat에 저장하게 된다. LogFormat을 통해서 기준량과 비교한 후 기준량과 틀린 비율로 트래픽이 발생될 경우 이상 가중치 값 1을 부여하게 된다. 프로토콜별 발생 비율이 기준량과 같은 비율로 발생되는 경우에는 이상 가중치 값이 0을 부여하게 된다. [그림 11]은 프로토콜별 추이 분석 흐름도이다.

포트 세부 분석 과정은 Well-known 포트, P2P 포트, 기존 공격 포트, 특정 공격 포트로 나누어진다. Well-known 포트 분석 과정은, 현재 널리 알려진 서비스인 HTTP, FTP, Telnet 등 혼선을 막기 위해서 통상적으로 널리 사용되는 1024 이하의 포트를 기준 포

트로 사용한다. 그리고 이상 가중치 0을 부여하기 위한 P2P 포트 분석 과정의 중요한 점은, P2P 트래픽이 다양한 포트 번호들을 사용한다는 특성을 가지고 있고, 이 포트 번호들이 1024 이하의 well-known port가 아니라 시스템에서 자동으로 생성되는 랜덤 포트와 같은 범위라는 것이다[3]. Web이나 FTP, Telnet같은 경우는 각각 80, 21, 22, 23번의 1024 이하의 well-known 포트를 사용하고 클라이언트 포트는 1024 이상의 포트 번호를 사용한다. 따라서 P2P 트래픽의 경우는 클라이언트 포트와 서버 포트 모두 1024 이상의 포트 번호를 사용한다. 위와 같은 특성으로 알려진 대표 포트를 기준 포트로 사용하였다. 기존 공격 포트 분석은, 지금까지 국내에서 KrCERT(인터넷침해사고대응센터)에 접수된 포트 스캔 공격에 사용된 포트 번호를 기준 공격 포트로 사용하였다. 그리고 특정 공격 포트의 분석 과정에서는 정의된, P2P 포트, well-known 포트, 기존 공격 포트를 제외한 그 외의 모든 포트가 포함된다.

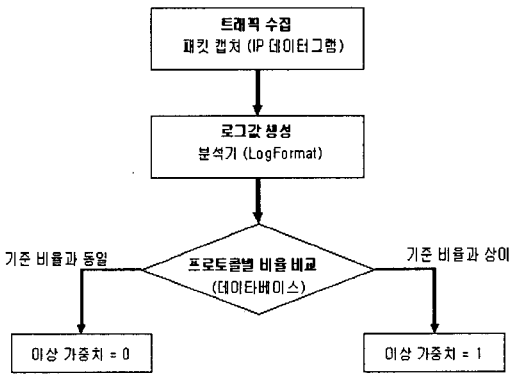


그림 11. 프로토콜별 추이 분석 흐름도

[그림 12]는 각 포트별 분류 및 트래픽 분석 흐름도를 도시하였다. 이 분석 방법에서는 수집된 트래픽의 로그값 생성 후, 각 포트별 분석에서 기존 공격 포트 및 특정 공격 포트 트래픽이 발생될 경우 이상 가중치 값을 1을 부여하게 되고, P2P 포트는 이상 가중치 값에 0을 부여하게 된다. well-known 포트는 기준 비율보다 클 경우 이상 가중치 값을 1을 부여하게 되고, 10초 단위로 기준 비율과 비교하게 된다.

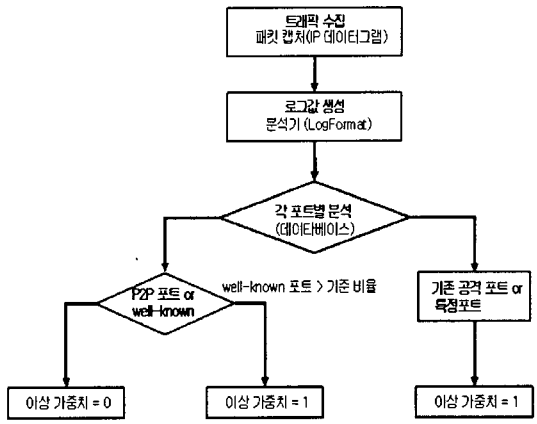


그림 12. 각 포트별 분류 및 트래픽 분석 흐름도

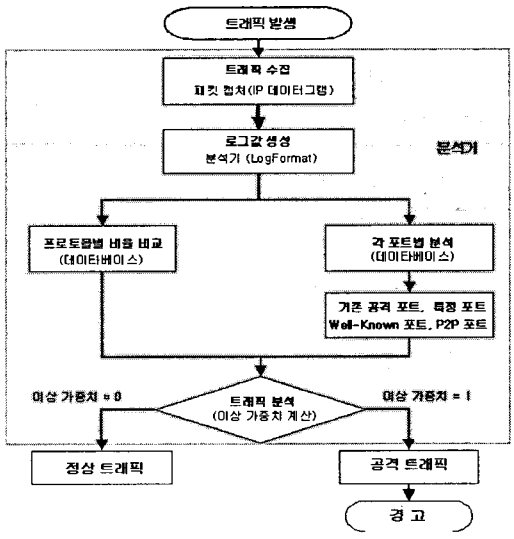


그림 13. 제안한 유해 트래픽 탐지 흐름도

각 분석 과정이 끝나면 최종적으로 이상 가중치가 0이면 정상 트래픽, 이상 가중치가 1 이상이면 유해 트래픽으로 분류하게 된다. [그림 13]은 본 논문에서 제안한 프로토콜 및 포트 분석을 통한 유해 트래픽 탐지 알고리즘을 도시화한 것이다.

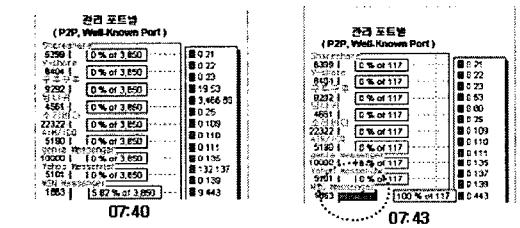
V. 실험 및 결과 고찰

본 논문에서 제안한 유해 트래픽 탐지의 실험을 위해

사용된 실험 환경은 일반 사용자들 그룹과 공격자 그리고 관리 시스템으로 구성되었다. P2P 트래픽 탐지는 MSN 메신저를 사용하였고, 웜 및 봇 공격 시 트래픽 탐지는 TFN 공격 도구 및 스팸 메일 생성기를 사용하여 분석하였다. 정상 트래픽을 발생시키기 위해 웹 서버와 메일 서버를 구동하였다. 각 공격에 대해서는 본 논문에서 제안한 알고리즘과 기존 SNMP를 이용한 트래픽 분석 방법과 비교하였다.

1. 응용 프로그램의 분석 결과

응용 프로그램이 P2P 프로그램을 사용할 때, 발생되는 트래픽의 경우 제안된 알고리즘을 통해 각 포트별 분석하였다. [그림 14]는 P2P 응용 프로그램을 사용하지 않을 경우의 트래픽 분석 결과이다.



(a) P2P 응용 프로그램을 사용하지 않을 경우 (b) 이상 가중치 = 0

그림 14. P2P 트래픽 분석 결과

특정 응용 프로그램인 P2P의 경우 사용하지 않을 때는 트래픽이 거의 없고, 사용할 때는 포트 별로 분류되어 관리되는 것을 확인 할 수 있다. 특정 P2P 포트 추가 시에는 바로 추가 적용하여 관리가 가능하다. 이상 가중치 값은 0이 발생되어 정상 트래픽으로 간주 된다. [그림 14(b)]는 P2P 응용 프로그램인 MSN 메신저를 사용할 경우의 트래픽 분석 결과이다.

본 논문에서 제안한 알고리즘에 의한 결과를 SNMP를 이용한 기존의 분석 방법과 비교하였다. [그림 15]는 SNMP를 이용한 기존의 일주 트래픽 추이 분석을 행한 결과이다. 정상적인 MSN 메신저 응용프로그램을 사용했을 경우이다.

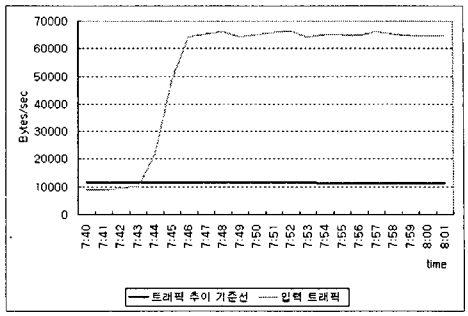


그림 15. SNMP의 일주 트래픽 추이 분석(TCP)

[그림 15]에서 보는 바와 같이 07:43분부터 기준 트래픽 선보다 큰 P2P 트래픽이 발생되고 있는 것을 확인할 수 있으며, 이상 가중치 값으로 1을 부여하게 된다.

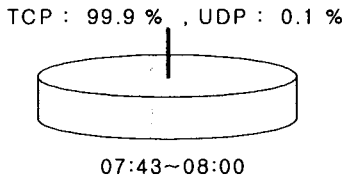


그림 16. SNMP의 프로토콜별 트래픽 발생 추이 분석(TCP)

[그림 16]은 입력된 P2P 트래픽을 프로토콜별로 분석한 결과로 TCP의 비율이 99.9%, UDP의 비율이 0.1%로 나타났다. 같은 시간대에서 프로토콜 비율은 서버 접속량이 없는 시간대로 TCP의 비율이 0.1%를 차지하는 시간대이다. 즉 TCP 트래픽의 비율이 기준량을 훨씬 초과해서 나타난 것을 확인할 수 있다. 이로 인해 이상 트래픽으로 간주하게 되고 이상 가중치 값은 1을 부여하게 된다. 특정 MIB 객체에 의한 트래픽은 발생 되지 않기 때문에 이상 가중치 값은 0을 부여한다.

표 1. 기존 SNMP 방법의 P2P 트래픽 분석 결과

분석	이상 가중치	분석 결과
일주 트래픽 추이 분석	1	이상 가중치 =2 유해트래픽
프로토콜별 트래픽 발생 추이 분석	1	
특정 MIB 객체에 의한 트래픽 발생 유무	0	

[표 1]의 결과는 P2P트래픽을 SNMP를 이용하여 분석한 결과로 정상 트래픽을 유해 트래픽으로 잘못 분석하게 됨을 알 수 있다. 실험 결과 값을 토대로 본 논문에서 제안한 알고리즘에 의한 트래픽 분석과 기존의 방법에 의한 트래픽 분석 결과를 [표 2]에 나타내었다.

표 2. 기존 방법과의 비교(응용 프로그램)

분석 방법 / 구분	제안된 방법	SNMP를 이용한 분석
분석 소요 시간	실시간	1분
탐지율	90% 이상	탐지 못함

2. 웜, 봇 공격의 분석 결과

웜, 봇 공격은 보통 1차 감염에서 특정 포트 및 취약 포트를 통하여 감염시킨다. 2차 공격에서는 대부분 DDoS 공격을 실시하는 경우가 대부분이다. 1차 감염 시 보통 well-known 포트의 취약점이나 그 이외 포트를 통하여 감염된다. well-known 포트의 경우는 정상적으로 많이 사용하는 부분과 포트 번호가 겹치므로 공격 발생시 well-known포트 기준 비율과 비교하여 공격 여부를 판단한다.

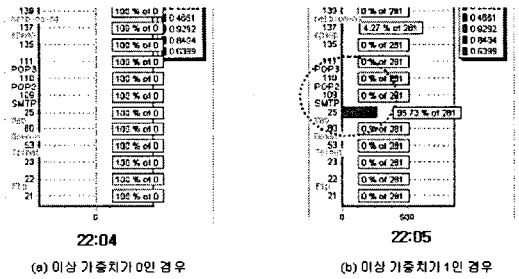


그림 17. 대량의 메일 전송 시 포트 추이 분석 결과

[그림 17]은 다량 메일 발송 시 well-known 포트의 추이 분석 결과이다. 그림에서 보는 바와 같이 22:05분 시간대에서 갑자기 대량의 메일이 발송되는 것을 확인할 수 있다. 즉 트래픽의 비율이 기준량을 훨씬 초과해서 나타난 것을 확인할 수 있다. 이로 인해 이상 트래픽으로 간주하게 되고 이상 가중치 값은 1을 부여하게 된다. Well-known 포트 이외의 경우 웜, 봇의 기존 공격 포트를 감시하여, 트래픽 발생시 실시간으로 확인 가능하다. [그림 18(a)]는 기존 공격포트 평상시 분석 결과이다.

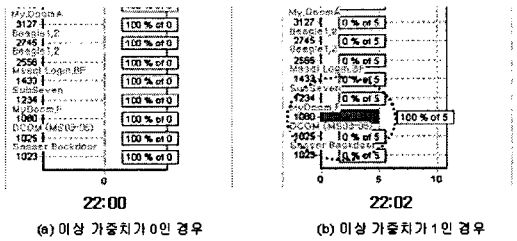


그림 18. 기존 공격 포트 트래픽 분석 결과

P2P 포트, Well-known 포트, 기존 공격 포트 이외에 발생되는 포트 트래픽에 대해서 실시간으로 분석되며, 발생 즉시 이상 가중치 값은 1을 부여하게 된다. [그림 19(a)]는 평상시 특정 포트별 분석결과이다.

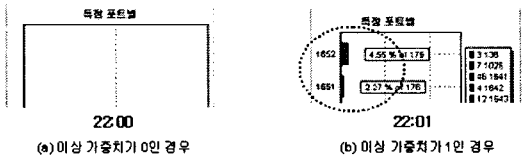


그림 19. 특정 포트 트래픽 분석 결과

[그림 19(b)]는 22:01분에 특정 포트 트래픽이 발생되어 이상 가중치 값이 적용된 분석결과이다.

본 논문에서 제안한 알고리즘에 의한 결과를 SNMP를 이용한 기존의 분석 방법과 비교하였다. [그림 20]은 SNMP를 이용한 기존의 일주 트래픽 추이 분석을 행한 결과이다.

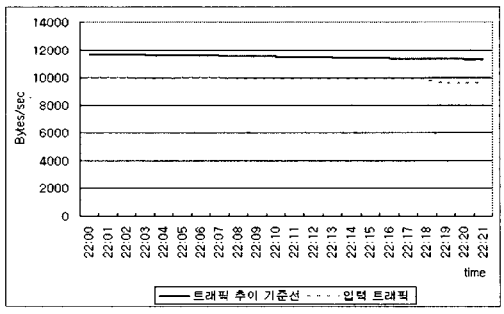


그림 20. SNMP의 일주 트래픽 추이 분석(TCP)

[그림 20]에서 보는 바와 같이 22:01, 22:05분에 발생한 공격 트래픽이 기준 트래픽 내에서 발생되고 있는 것을 확인할 수 있다. 정상 트래픽으로 분류하여 이상 가중치 값으로 0을 부여하게 된다.

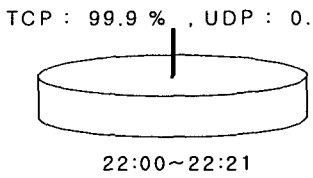


그림 21. SNMP의 프로토콜별 트래픽 발생 추이 분석(TCP)

[그림 21]은 입력된 트래픽을 프로토콜별로 분석한 결과로 TCP의 비율이 99.9%, UDP의 비율이 0.1%로 나타났다. 같은 시간대에서 프로토콜 비율을 초과하지 않는 것을 확인할 수 있다. 이로 인해 정상 트래픽으로 간주하게 되고 이상 가중치 값은 0을 부여하게 된다. 특정 MIB 객체에 의한 트래픽은 발생 되지 않기 때문에 이상 가중치 값은 0을 부여한다.

표 3. 기존 SNMP 방법의 트래픽 분석 결과

분석	이상 가중치	분석 결과
일주 트래픽 추이 분석	0	이상 가중치=0 정상 트래픽
프로토콜별 트래픽 발생 추이 분석	0	
특정 MIB 객체에 의한 트래픽 발생 유무	0	

[표 3]의 결과는 공격 트래픽을 SNMP를 이용하여 분석한 결과로 유해 트래픽을 정상 트래픽으로 잘못 분석하게 된다. 위의 실험 결과값을 토대로 본 논문에서 제안한 알고리즘에 의한 트래픽 분석과 기존의 방법에 의한 트래픽 분석 결과를 [표 4]에 나타내었다.

표 4. 기존 방법과의 비교(웜, 봇)

분석 방법 / 구분	제안된 방법	SNMP를 이용한 분석
분석 소요 시간	10초 이내	1분
탐지율	80% 이상	10 %이하

VI. 결 론

본 논문에서는 유해 트래픽 탐지율을 높이기 위해 프로토콜 추이 분석 및 각 포트별 분석을 중첩 사용하였다. 각 포트는 P2P 포트, well-known 포트, 기존 공격 포트, 특정 포트로 분류하고, 각 분석 방법마다 이상 가중치를 설정하여 유해 트래픽으로 분석해 내는 방법이다. 실험을 통해 기존의 방법보다 정확하고 빠른 분석 결과를 확인할 수 있었다.

기존의 SNMP 기반의 공격 탐지와 비교하여, 기존 방법에서는 분석해내지 못했던, 응용 프로그램, 웜 및 봇에 대해 정확하게 분석했으며, 탐지율 향상 및 분석 소요 시간을 개선시킬 수 있었다. 이를 통해 유해 트래픽에 대해 정확한 분석을 할 수 있었다. 향후 IPV6 환경에서도 적용 가능하도록 프로그램과 새로 발견되는 공격포트를 추가하면 넓은 사용범위와 여러 공격에 대해서 정확하게 탐지 할 수 있을 것으로 생각된다.

참 고 문 헌

[1] 유대성, 트래픽 분석을 이용한 SNMP 기반의 공격탐지, 충북대학교 대학원 석사학위논문, 2005.

[2] 유대성, 오창석, "공격 탐지를 위한 트래픽 수집 및 분석 알고리즘", 한국콘텐츠학회 논문지, Vol.4, No.4, pp.33-43, 2004.

[3] 김명섭, 강훈정, 홍원기, "Flow Grouping을 통한 P2P 트래픽 분석 방법에 관한 연구", 한국통신학회 KNOM, 2003.

[4] 한국정보보호진흥원, 악성 Bot 특성 분석을 통한 탐지 및 대응책, 2004.

[5] 한국정보보호진흥원, Bagle.AY(AQ)웜, 바이러스 분석 보고서, 2005.

[6] 양대일, 이승재, 정보 보안 개론과 실습, 한빛미디어, 2004.

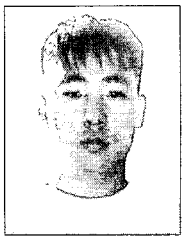
[7] 오창석, 데이터 통신 수정판, 영한출판사, 2001.

[8] 홍순화, 김재영, 조범래, 홍원기, "분산 시스템 환경에서의 로드 밸런싱을 통한 웹기반 네트워크 트

래픽 모니터링 및 분석", 한국통신학회 KNOM, 2001.

저 자 소 개

신 현 준(Hyun-Jun Shin) 준회원



- 2003년 2월 : 충주대학교 컴퓨터공학과(공학사)
- 2005년 8월 : 충북대학교 전기전산공학과(공학석사)

<관심분야> : 정보보안, 네트워크

구 향 옥(Hyang-Ohk Koo) 종신회원

- 1999년 8월 : 한밭대학교 전자계산학과(이학사)
- 2002년 2월 : 충북대학교 컴퓨터공학과(공학석사)
- 2002년~현재 : 충북대학교 컴퓨터공학과 박사과정
- 2003년 8월~현재 : 백석대학 겸임

<관심분야> : 컴퓨터네트워크, 뉴로컴퓨터, 정보보호

최 일 준(IL-Jun Choi) 준회원

- 1997년 2월 : 충주대학교 컴퓨터공학과(공학사)
- 2003년 8월 : 충북대학교 컴퓨터공학과(공학석사)
- 2004년 3월~현재 : 충북대학교 컴퓨터공학과 박사과정
- 2000년 6월~현재 : 극동정보대학 학술정보센터 네트워크관리자
- 2005년 3월~현재 : 충주대학교 컴퓨터공학과 겸임

<관심분야> : 컴퓨터네트워크, 정보보호, 네트워크보안

오 창 석(Chang-Suk Oh) 종신회원

- 1978년 2월 : 연세대학교 전자공학과(공학사)
- 1980년 2월 : 연세대학교 전자공학과(공학석사)
- 1988년 8월 : 연세대학교 전자공학과(공학박사)
- 1985년~현재 : 충북대학교 전기전자컴퓨터공학부 교수
- 1982년~1984년 : 한국전자통신연구원 연구원
- 1990년~1991년 : Stanford대학교 객원교수
- 2001년~2004년 : 한국콘텐츠학회 논문지 편집위원장
- 2004년~현재 : 한국콘텐츠학회 상임고문

<관심분야> : 컴퓨터네트워크, 뉴로컴퓨터, 정보보호