공격 탐지를 위한 트래픽 수집 및 분석 알고리즘

Traffic Gathering and Analysis Algorithm for Attack Detection

유대성*, 오창석**

충북대학교 컴퓨터공학과*, 충북대학교 전기전자컴퓨터공학부**

Dae-Sung Yoo(dsyoo@nwork.chungbuk.ac.kr)*, Chang-Suk Oh(csoh@nwork.chungbuk.ac.kr)**

요약

본 논문에서는 기존 SNMP를 이용한 트래픽 분석 방법의 문제점을 개선시킨 SNMP 기반의 트래픽 추이 분석 알고리즘을 제안하였다. 기존 방법에서는 임계치를 적용함으로써 분석 시간이 많이 걸리며, 초기 공격 트래픽에 대해 탐지하지 못하는 취약점을 가지고 있었다. 본 논문에서는 임계치를 사용하지 않고 일주 트래픽 추이 분석, 프로토콜별 추이 분석 그리고 특정 MIB에서의 트래픽 발생 유무를 분석함으로써 기존 방법에서의 문제점을 해결할 수 있었다. 트래픽이 발생하게 되면 이 세 가지 분석 방법을 통해 이상 여부를 분석하고, 이상 트래픽이 중첩적으로 발생될 경우 현재 입력된 트래픽을 유해 트래픽으로 분석해 낼 수 있다. 제안한 알고리즘을 통해서 유해 트래픽을 빠르고 정확하게 분석해 낼 수 있으며, 이를 통해 트래픽 폭주 공격에 의한 피해를 줄일 수 있을 것이다.

■ 중심어 : | SNMP | MIB | 임계치 | 트래픽 추이 분석 | 트래픽 폭주 공격 |

Abstract

In this paper, a traffic trend analysis based SNMP algorithm is proposed for improving the problem of existing traffic analysis using SNMP. The existing traffic analysis method has a vulnerability that is taken much time in analyzing by using a threshold and not detected a harmful traffic at the point of transition. The method that is proposed in this paper can solve the problems that the existing method had, simultaneously using traffic trend analysis of the day, traffic trend analysis happening in each protocol and MIB object analysis responding to attacks instead of using the threshold. The algorithm proposed in this paper will analyze harmful traffic more quickly and more precisely; hence it can reduce the damage made by traffic flooding attacks. When traffic happens, it can detect the abnormality through the three analysis methods previously mentioned. After that, if abnormal traffic overlaps in at least two of the three methods, we can consider it as harmful traffic. The proposed algorithm will analyze harmful traffic more quickly and more precisely; hence it can reduce the damage made by traffic flooding attacks.

■ Keyword : | SNMP | MIB | Threshold | Traffic Trend Analysis | Traffic Flooding Attack |

* 이 논문은 2004년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음

접수번호 : #041030-002

접수일자 : 2004년 10월 30일

심사완료일 : 2004년 11월 17일

교신저자 : 오창석, e-mail : csoh@nwork.chungbuk.ac.kr

I. 서 론

인터넷의 발달은 생활의 다방면에서 삶의 질을 높여주는 긍정적인 효과를 제공하고 있다. 그러나 인터넷은 근본적으로 개방적인 네트워크 특성과 프로토콜 및 정보 시스템의 보안 취약성으로 인해서 불법 침입에 대한 취약점이 있다. 최근에는 이러한 문제점들을 악용한 트래픽 폭주 공격에 의해 많은 피해를 보고 있으며, 이로 인해 트래픽 분석의 중요성이 날로 증대되고 있다.[1] 기존의 SNMP를 이용한 트래픽 분석 방법은 MIB 객체를 통해 트래픽을 수집하고, 분석에 있어 현재 값과 이전 값의 차이를 임계치에 적용하여 유해 트래픽을 분석하였다. 이러한 과정으로 인해 탐지하는데 많은 시간이 걸리며 유해 트래픽이 발생되는 과도기적 시점에서는 유해 트래픽을 탐지해내지 못했다. 이에 본 논문에서는 시간의 단축과 탐지율을 높인 SNMP 기반의 트래픽 추이 분석 방법을 제안하였다.

II. 트래픽 폭주 공격

1. DDoS 공격

DDoS 공격은 인터넷의 구조적인 취약성을 악용하여 정상적인 서비스의 지연 및 마비상황을 일으키는 공격이다. DDoS 공격의 동작 원리는 TCP/IP 프로토콜의 구조적인 보안 취약점을 이용한다. 이는 모든 인터넷 사용자는 TCP/IP 프로토콜을 이용하여 임의의 데이터 패킷을 발송자의 IP 주소를 가지고 목적지의 IP 주소로 발송하며, 이때 이 IP 주소에 대한 특별한 인증 절차 없이 무제한적으로 대규모의 데이터 패킷을 전송할 수 있다는 것이다. 그림 1은 DDoS 공격의 동작원리를 나타낸다.

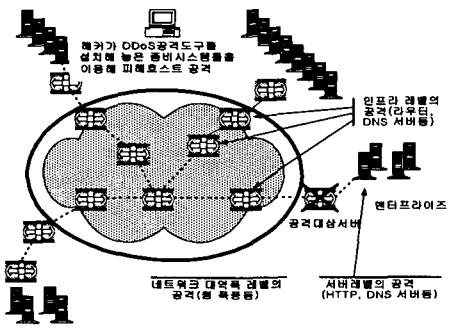


그림 1. DDoS 공격의 동작 원리

DDoS 공격은 수많은 좀비 시스템들을 이용하며, 이때 좀비 시스템들은 자신에게 어떠한 일이 일어나고 있는지 인식하지 못한 채 공격이 행해지게 된다. 이러한 DDoS 공격은 대역폭 공격과 애플리케이션 공격으로 분류된다.

1.1 대역폭 공격

대역폭 공격은 엄청난 양의 패킷을 전송해서 네트워크의 대역폭이나 장비 자체의 리소스를 모두 소진시켜 버리는 형태이다. 라우터, 서버, 방화벽 같은 주요 장비들은 모두 자신만의 제한적인 처리용량을 가지고 있기 때문에 그 용량을 초과하는 이런 형태의 공격을 받게 되면 정상적인 서비스 요청을 처리하지 못하거나 아예 장비 자체가 다운되어서 네트워크 전체가 마비되는 사태를 초래할 수 있다. 이 형태의 대표적인 공격은 패킷 오버플로우 공격으로 정상적으로 보이는 엄청난 양의 TCP, UDP, ICMP 패킷들을 특정한 목적지로 보내는 것이다. 이러한 공격은 발송지의 주소를 스푸핑해서 발송하기 때문에 공격의 탐지가 쉽지 않다.

▶ TCP Flooding 공격

TCP Flooding 공격은 TCP의 연결 지향성의 취약점을 이용한 DoS 공격이다. 이는 TCP를 이용하여 데이터를 보낼 때는 먼저 연결을 설정하게 된다. 즉 TCP의 연결 과정인 three-way handshaking을 이용하여 공격자가 피해 호스트에 근원지 IP주소를 스푸핑하여 SYN 패킷을 특정 포트로 전송하게 되면 이 포트의 대기 큐를 가득 차게 하여 이 포트에 들어오는 연결 요청을 큐가 빌 때까지 무시하도록 하는 방법이다. 그림 2는 TCP Flooding 공격을 나타낸다.

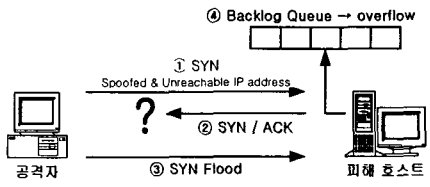


그림 2. TCP Flooding 공격

▶ UDP Flooding 공격

UDP를 이용한 패킷 전달은 비연결형 서비스로서 포트 대 포트로 전송한다. UDP Flooding 공격은 UDP의 비연결성 및 비신뢰성 때문에 공격이 용이한 방법이다. UDP는 근원지 IP 주소와 근원지 포트를 스푸핑하기 쉽다. 이러한 약점들을 이용해 많은 트래픽을 피해 호스트에 전송함으로써 시스템 자원과 네트워크를 마비시킨다. 그림 3은 UDP Flooding 공격을 나타낸다.

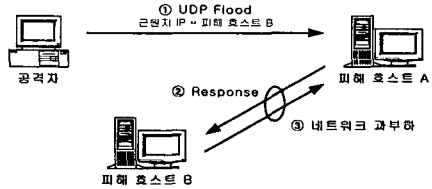


그림 3. UDP Flooding 공격

▶ ICMP Flooding 공격

ICMP는 호스트간 혹은 호스트와 라우터간의 에러 상태 혹은 상태 변화를 알려주고 요청에 응답을 하는 기능을 담당하는 네트워크 제어 프로토콜이다. ICMP는 활성화된 서비스나 포트가 필요하지 않는 유일한 프로토콜로 이러한 특징을 악용한 공격 방법이 ICMP Flooding 공격이다. 공격자는 대량의 ICMP echo request 메시지를 근원지 IP 주소를 피해 호스트의 IP 주소로 변환하여 보내게 된다. 변형된 ICMP echo request 메시지를 받은 호스트들은 피해 호스트로 ICMP echo reply 메시지를 전송하여 피해 호스트에 큰 트래픽을 발생시키게 된다. 그림 4는 ICMP Flooding 공격을 나타낸다.

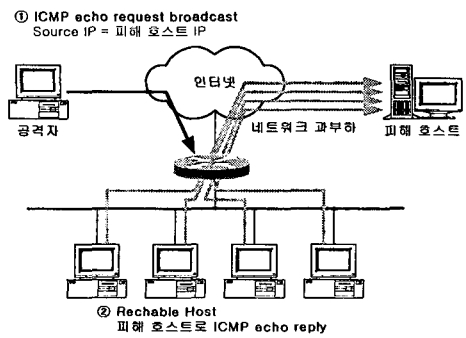


그림 4. ICMP Flooding 공격

1.2 애플리케이션 공격

애플리케이션 공격은 TCP, HTTP와 같은 프로토콜을 이용해서 특정한 반응이 일어나는 요청 패킷을 발송하여 해당 시스템의 연산처리 리소스를 소진시켜서 정상적인 서비스 요청과 처리가 불가능한 상태로 만드는 것이다. 이 형태의 대표적인 공격은 HTTP half-openattack과 HTTP error attack 등이 있다.

2. 웜 공격

웜 공격은 인터넷 상에서 빠른 전파력을 통해서 자기 복제를 하는 프로그램을 말한다. 1980년대 이전까지는 웜 공격이란 말보다는 단지 웜이란 표현으로 쓰였으며, 바이러스와 달리 시스템에 해를 끼치지는 않았었다. 이러한 웜이 최근 트래픽 폭주 공격에 있어 가장 큰 해를 입히는 공격으로 대두되고 있다.[2] 웜의 가장 큰 특징인 빠른 전파를 통해 인터넷상에서 취약점이 있는 시스템을 감염시키고 감염된 시스템을 통해 제2의 공격을 행하기 때문이다. 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. 최근 2003년 1월 25일의 인터넷 대란의 주범 역시 웜을 이용한 트래픽 폭주 공격이었다. 그림 5는 웜 공격시 트래픽 흐름을 나타낸다.

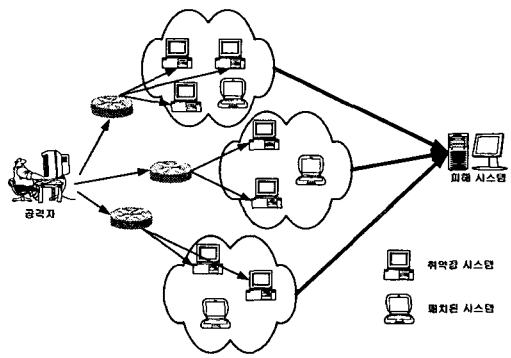


그림 5. 웜 공격의 트래픽 흐름

Ⅲ. 기존의 트래픽 분석

SNMP(Simple Network Management Protocol)를 이용한 기존의 트래픽 분석은 관리 객체들의 집합인 MIB (Management Information Base)를 이용하여 트래픽을 수집하고 임계값을 적용하여 유해 트래픽을 분석하는 방법이다.[3][4] 크게 트래픽 수집 단계와 분석 단계로 이루어지며 트래픽 수집 단계에서는 관리 시스템과 대상 시스템간에 SNMP를 활성화시킨 후 관리 하고자 하는 MIB를 선정하여 정보를 얻게 된다.[5] 그림 6은 SNMP를 이용하여 트래픽을 수집하는 구성도이다.

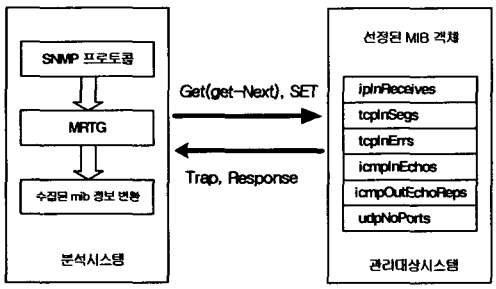


그림 6. SNMP를 이용한 트래픽수집

관리 시스템은 각 선정된 MIB 객체에 대해 snmpget을 통해 단위 시간별로 정보를 획득하게 된다. 그림 6에서 보듯이 관리 시스템은 대상 시스템과 SNMP 프로토콜을 통해 주기적인 상호 통신을 하며 대상 시스템은 관리 시스템의 요청에 대해 해당 정보를 전송하게 된다. 전송된 관리 정보는 관리 대상 시스템에 로그값으로 저장되며 이 로그값을 토대로 트래픽을 분석하게 된다.

수집된 각 MIB 객체에 대한 트래픽 양은 로그값으로 저장된 임계치를 적용하여 유해 트래픽 여부를 분석하게 된다. 이때 사용되는 분석 방법은 실험을 통해 선정된 공격에 반응하는 MIB 객체에서의 트래픽 발생이 임계치 안에서 일정하게 발생되는지를 통해서 분석하게 된다. 공격에 반응하는 MIB 객체는 tcpInErrs, udpNoPorts, icmpOutEchoReps이다. 그림 7은 기존의 SNMP를 이용한 트래픽 분석 방법의 흐름도이다.

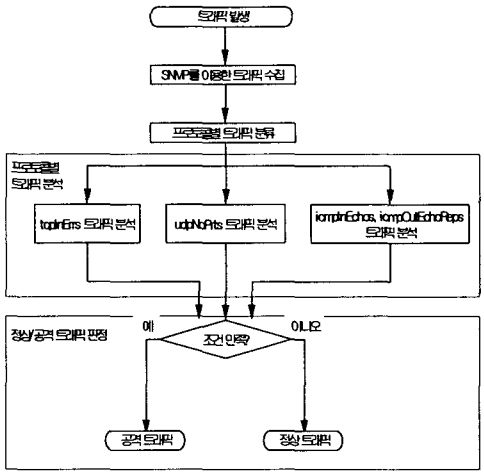


그림 7. SNMP를 이용한 기존의 공격 탐지 흐름도

Ⅳ. SNMP 기반의 트래픽 추이 분석

기존의 SNMP를 이용한 유해 트래픽 분석 방법에서는 SNMP MIB를 사용하여 트래픽을 수집하고 수집된 정보에 임계치를 적용하여 분석하였다.[6] SNMP MIB를 사용할 경우 유해 트래픽을 정확하게 분석해 낸다는 장점을 가지고 있지만, 트래픽을 분석하는데 있어 현재 트래픽과 이전 트래픽의 오차에 임계값을 적용시켜 트래픽을 분석함으로써 분석 시간이 오래 걸린다는 단점을 가지고 있다. 또한 유해 트래픽이 발생되는 과도기 시점에서는 유해 트래픽을 정상 트래픽으로 분류하는 큰취약점을 가지고 있다. 이는 유해 트래픽이 발생되기 전에는 해당 MIB에서 발생되는 트래픽이 없으므로 현재 트래픽과 이전 트래픽의 차이가 임계치보다 훨씬 크기 때문이다. 그림 8은 현재 값과 이전 값의 차이에 임계치를 적용할 경우의 문제점을 나타낸다.

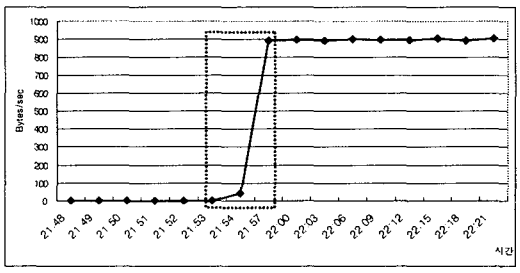


그림 8. 기존의 SNMP를 이용한 방법의 문제점

다른 문제점으로는 임계치를 적용하기 위해 수집된 트래픽의 값을 임계치를 적용하기 위해서 변형하여야 한다는 것이다. snmpget으로 수집된 로그값은 현재 시간까지의 입력된 트래픽의 누적치이기 때문이다. 또한 임계치를 적용하기 위해서 다시 초당 입력된 바이트 단위로 변환해주는 과정이 필요하였다. 이는 임계치의 값이 커지면 트래픽을 분류하는데 있어 신뢰도가 떨어지기 때문이며, 이를 보완하기 위해 현재 입력된 트래픽을 초당 입력된 트래픽으로 변환해 주어야 한다. 즉, 트래픽 분석이 끝난 후 현재 유해 트래픽량을 구하기 위한부수적인 과정이 필요하였다. 그림 9는 기존의 방법에서 로그값의 변환과정이 없을 경우의 문제점을 보여준다.

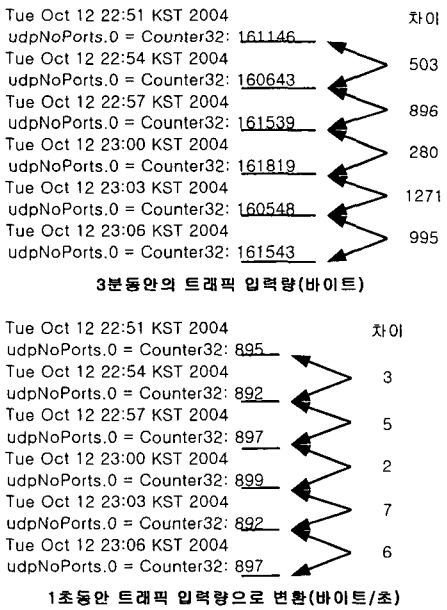


그림 9. 기존 방법에서의 임계치로 인한 문제점

또한, 최근 웜의 확산성을 이용해 단기간에 트래픽 폭주 공격이 이루어진다는 점에서 기존의 방법으로는 유해 트래픽을 분석하는데 있어 시간이 많이 걸린다는 한계가 있다. 따라서 본 논문에서는 기존의 SNMP MIB를 이용한 트래픽 분석 방법에 트래픽 추이 분석과 프로토콜별 트래픽 분석을 같이 적용하여 트래픽 분석에 있어 임계치에 의존적인 문제점을 보완하고, 트래픽 분석에 필요한 시간의 단축과 유해 트래픽를 정상 트래픽으로 잘못 분석하는 단점을 보완하였다.

1. SNMP 기반의 트래픽 추이 분석 제안

본 논문에서는 기존의 임계치로 인한 문제점을 해결하기 위해 일주 트래픽 추이 분석, 프로토콜별 추이 분석 그리고 특정 MIB에 의한 분석 방법을 중첩적으로 사용하였다. 각 분석 방법에 대한 내용은 다음과 같다.

▶ 일주 트래픽 추이 분석

일주 트래픽 추이 분석이란 대상 시스템에서 발생되는 하루 동안의 트래픽의 흐름을 예측하여 예측된 값과 현재 발생되는 트래픽을 비교하여 이상 징후를 분석하는 방법이다.[6] 본 논문에서는 ipInReceives 객체를 통해 관리하고자 하는 시스템으로 입력되는 트래픽을 지속적으로 분석하였다. 각 날짜별로 일분 단위로 트래픽을 수집한 후 한 달 동안 수집된 트래픽에 대해서 모든 트래픽을 수용할 수 있는 기준값을 설정하게 된다. 이 기준선과 입력된 트래픽을 비교하여 이상 징후를 분석해 낼 수 있다. 분석결과 본 논문에서 얻어진 일주 트래픽 추이 분석을 위한 기준선은 그림 10과 같다.

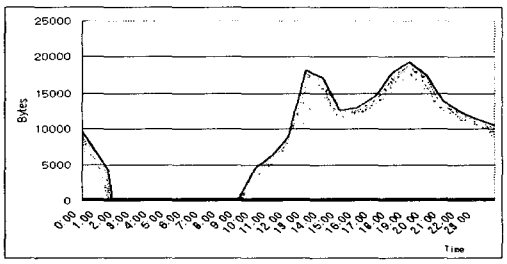


그림 10. 일주 트래픽 추이

▶ 프로토콜별 추이 분석

프로토콜별 추이 분석이란 시스템에서 발생되는 트래픽에 대해서 프로토콜별 발생 비율을 예측하여 이 기준값과 비교하여 예측된 값과 현재 발생되는 프로토콜별 비율을 비교하여 이상 징후를 분석하는 방법이다.[6] 프로토콜별 추이 분석을 위해 사용된 MIB 객체는 표 1과 같다.

표 1. 프로토콜별 트래픽 발생 추이에 사용된 MIB 객체

MIB 객체	설명
tcpInSegs	오류로 수신된 것을 포함하여, 수신된 세그먼트의 총 개수
udpInDatagrams	UDP 사용자들에게 전달되는 UDP 데이터그램의 총 개수
icmpInEchos	수신된 ICMP 요청 메시지의 총 개수

본 논문에서 실험을 통해 얻어진 프로토콜별 트래픽 발생 비율은 그림 11과 같다.

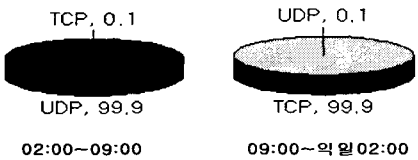


그림 11. 프로토콜별 트래픽 발생 비율

위의 그림에서 새벽 시간대에는 실제 접속자가 없는 시간대로 관리 시스템과 관리 대상 시스템간의 SNMP 통신에 의한 UDP 프로토콜 비율이 대부분을 차지하였다. 그 외의 시간대에서는 실제 접속자들에 의해 TCP의 비율이 대부분을 차지하게 된다.

▶ 특정 MIB 객체를 통한 분석

특정 MIB 객체를 통한 분석에서는 기존의 방법에서 실험을 통해 얻어진 공격에 반응하는 MIB 객체에서의 트래픽 발생 유무를 통해 이상 징후를 분석하게 된다. 이 분석 방법에서 사용된 MIB 객체는 표 2와 같다.

표 2. 특정 MIB 객체를 통한 분석에서 사용된 MIB

MIB 객체	설명
tcpInErrs	오류로 수신된 세그먼트의 총 개수
udpNoPorts	목적지 포트에 응용 프로그램이 없는 경우 수신된 UDP 데이터그램의 총 개수
icmpOutEchoReps	송신된 ICMP 요청 메시지의 총 개수

TCP Flooding 공격은 TCP의 three-way handshaking 방식을 악용한 공격으로 근원지 주소를 허위로 기재한 후 SYN 패킷을 피해 호스트로 보내게 된다. 이에 대해 ACK 신호를 허위로 기재된 근원지 주소로 전송하게 되지만 ACK 신호에 대한 SYN 신호를 받지 못함으로써 에러 트래픽으로 발생하게 되는 것이다.

UDP Flooding 공격은 대량의 UDP 패킷을 피해 호스트로 전달하여 시스템의 자원을 모두 소모하게 만드는 공격이다. 이때 피해 호스트로 전송되는 UDP 패킷은 허위로 작성된 데이터들로 피해 호스트까지 전송된 후 상위 계층의 응용 계층으로 전달될 때 에러로 처리되게 된다. 이는 이에 해당하는 응용 프로세스가 존재하지 않기 때문이다. 이러한 트래픽은 모두 udpNoPorts 객체에서 탐지하게 되며, 이로 인해 udpNoPorts를 통해 UDP Flooding 공격을 분류해 낼 수 있다.

마지막으로 ICMP Flooding 공격은 대량의 ICMP echo 패킷을 피해 호스트로 보내게 되고 피해 호스트는 이에 대한 응답 패킷을 발송하면서 시스템에 많은 과부하를 주게 되는 공격이다. 입출력에 해당하는 모든 트래픽의 양이 커서 피해 호스트의 자원을 모두 소모하게 만들게 된다. 이러한 공격 특성으로 인해 ICMP 공격이 발생될 때 많은 트래픽을 발생시키게 되는 icmpInEchos에 대한 응답을 하게 되는 icmpOutEchoReps 객체를 통해 ICMP Flooding 공격을 분류해 낼 수 있다.

2. SNMP 기반의 트래픽 추이 분석 알고리즘

본 논문에서 제안한 SNMP 기반의 트래픽 추이 분석을 통한 공격 탐지 구조는 그림 12와 같다. 관리 시스템에서는 주기적으로 snmpget 명령어를 이용하여 관리 대상 시스템으로부터 트래픽을 수집하게 된다.

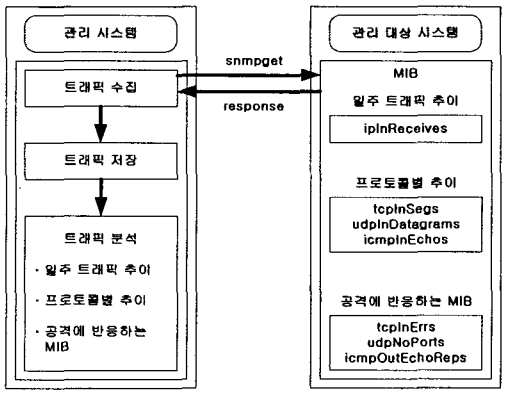


그림 12. SNMP기반의 트래픽 추이 분석 구조

수집된 로그값에 대해서 각 분석 방법별로 이상 트래픽이 발생할 경우에는 이상 가중치 값을 1을 부여하게 되며, 이상이 없을 경우에는 이상 가중치 값을 0을 부여하게 된다. 일주 트래픽 추이 분석에서는 실험을 통해 얻어진 각 시간대별 입력 트래픽의 최대 상한선과 비교하게 된다. 프로토콜별 추이 분석에서도 각 시간대별로 발생된 트래픽의 비율을 통해 이상 징후를 검사하게 된다. 기준값과 상이한 비율로 트래픽이 발생될 경우 이상 가중치 값으로 1을 부여하게 된다. 특정 MIB를 통한 분석 방법에서는 선정된 MIB 객체에서 트래픽이 발생될 경우 이상 트래픽으로 간주하고 이상 가중치를 1을 부여하게 된다. 그림 13은 각 분석 방법에서 이상 가중치를 계산하는 과정을 나타낸다.

```
Traffic analysis procedure of traffic analysis daily
  let Log() be a reading a log's value
  let a be a weight
  let daily_trend() : standard of daily trend
  let protocol_trend() : standard of protocol trend
  let special_trend() : standard of special trend
  let T() : current log value
  let T be a table for storing
    T(ip) <- Log(ipInReceives)
          T(tcpIn) <- Log(tcpInSegs)
          T(udpIn) <- Log(udpInDatagrams)
          T(icmpIn) <- Log(icmpInEchos)
          T(tcpInErrs) <- Log(tcpInErrs)
          T(udpNoPorts) <- Log(udpNoPorts)
          T(icmpOutEchoReps) <- Log(icmpOutEchoReps)
    call daily traffic trend analysis function
    if T(ip) > daily_trend() then
      a_daily = 1
    else
      a_daily = 0
    call protocol trend analysis function
    total = T(tcpIn) + T(udpIn) + T(udpIn)
    if T(tcpIn) / total ≠ protocol_trend() ||
      T(udpIn) / total ≠ protocol_trend() ||
      T(udpIn) / total ≠ protocol_trend() ||
      a_protocol = 1
    else
      a_protocol = 0
    call special MIB trend analysis function
    if T(tcpInErrs) > 0 || T(udpNoPorts) > 0 ||
          T(icmpOutEchoReps)
      a_special = 1
    else
      a_special = 0
    a = a_daily + a_protocol + a_special
    return a
```

그림 13. 이상 가중치 계산

위의 세 가지 분석 방법을 통해 얻어진 이상 가중치의 총합을 통해 최종적으로 유해 트래픽 유무를 분석한다. 이때 이상 가중치 총합이 2 또는 3일 경우 유해 트래픽으로 분류하게 되며 그 외의 경우에는 정상 트래픽으로 분류하게 된다. 이는 공격 트래픽 발생시 독자적으로 이상 징후를 나타내지 않고 최소한 위의 3가지 분석 방법중에서 2가지 분석 방법에 중첩되어 이상 트래픽을 발생시키기 때문이다. 그림 14는 본 논문에서 제안한 SNMP 기반의 트래픽 추이 분석 흐름도이다.

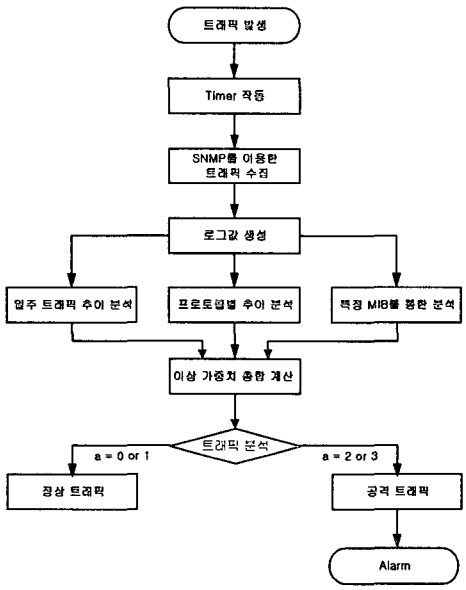


그림 14. SNMP 기반의 트래픽 추이 분석 흐름도

V. 실험 및 결과 고찰

본 논문에서 제안한 알고리즘의 실험을 위해 사용된 실험 환경은 일반 사용자들 그룹과 공격 그룹 그리고 관리 대상 시스템과 관리 시스템으로 구성되었다. TCP Flooding 공격, UDP Flooding 공격 그리고 ICMP Flooding 공격을 행한 후에 기존의 방법과 본 논문에서 제안한 알고리즘을 통해 얻어진 결과값을 비교하였다.

1. TCP Flooding 공격 탐지 결과

TCP Flooding 공격을 행한 후에 본 논문에서 제안한

알고리즘에 의해 공격 트래픽을 분석하였다.

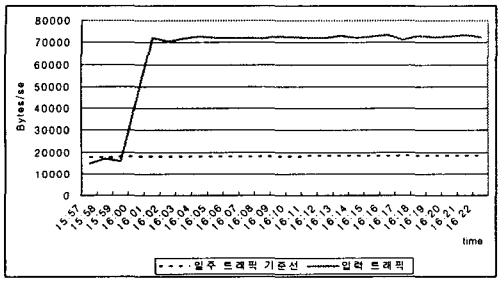
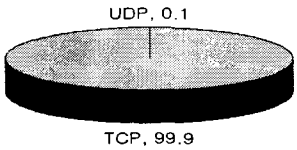


그림 15. 일주 트래픽 추이 분석(TCP)



15:59 ~ 16:22

그림 16. 프로토콜별 추이 분석(TCP)

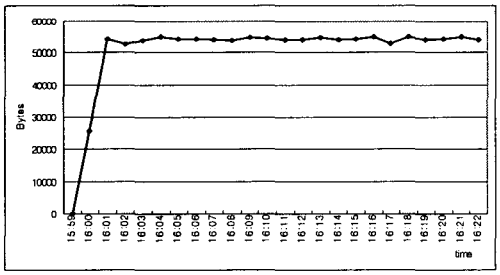


그림 17. tcpInErrs에서 트래픽 발생 분석

그림 15에서 보듯이 일주 트래픽 추이 분석을 통해 기준선보다 많은 트래픽이 현재 발생하고 있는 것을 볼 수 있다. 기준량보다 많은 트래픽이 발생되므로 이상 가중치 값은 1을 부여한다. 그림 16과 17은 프로토콜별 추이 분석과 tcpInErrs에서의 트래픽 발생을 분석한 그림으로 프로토콜별 추이 분석에서는 TCP의 비율이 기준량과 같게 나타났으며, 이상 가중치 값은 0을 부여한다. 특정 MIB를 통한 트래픽 발생에서는 대량의 트래픽이 발생되고 있는 것을 확인할 수 있다. 이로 인해 이상 가중치 값은 1을 부여한다. 위의 각 분석 결과를 통한 최종 분석 결과는 표 3과 같으며 총 이상 가중치 값이 2로 현재 발생되는 트래픽에 대해서 유해 트래픽으로 분석하였다.

표 3. 이상 가중치 결과(TCP)

분석 방법	이상 가중치	결과
일주 트래픽 추이 분석	1	총 이상 가중치 = 2 유해 트래픽
프로토콜별 추이 분석	0	
특정 MIB를 통한 분석	1	

본 논문에서 제안한 알고리즘을 기존의 SNMP를 이용한 방법과 비교한 결과는 표 4와 같다. 기존 방법에서는 임계치 적용에 의해 초기 트래픽을 분석해내지 못했지만 본 논문에서 제안한 알고리즘을 통해 일분 단위로 정확하게 분석해 낼 수 있었다.

표 4. 기존 방법과의 비교(TCP)

구분 \ 분석 방법	제안된 방법	기존 5분 단위	기존 3분 단위
분석 소요 시간	1분	15분	12분
미탐지	없음	초기 10분	초기 9분

2. UDP Flooding 공격 탐지 결과

UDP Flooding 공격을 행한 후에 본 논문에서 제안한 알고리즘에 의해 공격 트래픽을 분석하였다. 그림 18은 일주 트래픽 추이 분석 결과로서 기준선보다 많은 트래픽이 발생되고 있는 것을 확인할 수 있으며, 이상 가중치 값은 1을 부여한다.

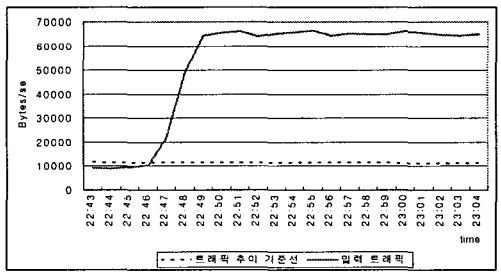


그림 18. 일주 트래픽 추이 분석(UDP)

그림 19는 프로토콜별 추이 분석으로 같은 시간대에 프로토콜별 트래픽 발생 비율과 비교하여 UDP의 트래픽 발생이 82%로 상이한 것을 확인할 수 있다. 이로 이

상 가중치 값은 1을 부여한다. 그림 20은 udpNoPorts를 통해 트래픽이 발생을 분석한 결과이다. 그림에서 보듯이 udpNoPorts를 통해 대량의 트래픽이 발생되고 있는 것을 확인할 수 있다. 분석 결과로 인해 이상 가중치 값은 1을 부여한다.

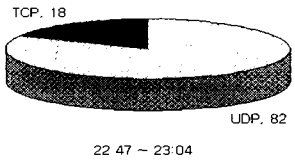


그림 19. 프로토콜별 추이 분석(UDP)

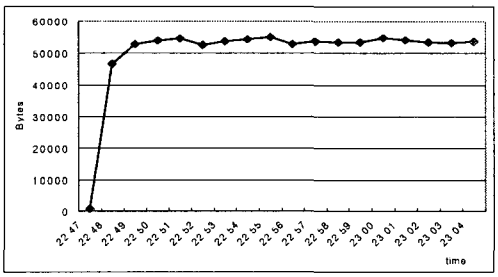


그림 20. udpNoPorts에서 트래픽 발생 분석

위의 각 분석 결과를 토대로 이상 가중치의 총합을 구한 결과는 표 5와 같으며 총 이상 가중치 값이 3으로 유해 트래픽으로 분석한다.

표 5. 이상 가중치 결과(UDP)

분석 방법	이상 가중치	결과
일주 트래픽 추이 분석	1	총 이상 가중치 = 3 유해 트래픽
프로토콜별 추이 분석	1	
특정 MIB를 통한 분석	1	

본 논문에서 제안한 알고리즘을 기존의 SNMP를 이용한 방법과 비교한 결과는 표 6과 같다. 이상 가중치 값이 총 3으로 현재 발생되는 트래픽에 대해 유해 트래픽임을 분석해내었다. 기존 방법과의 비교는 표 6과 같다.

표 6. 기존 방법과의 비교(UDP)

분석 방법 / 구분	제안된 방법	기존 5분 단위	기존 3분 단위
분석 소요 시간	1분	10분	9분
이탐지	없음	초기 5분	초기 6분

3. ICMP Flooding 공격 탐지 결과

ICMP Flooding 공격을 행한 후에 본 논문에서 제안한 알고리즘에 의해 공격 트래픽을 분석하였다. 그림 21은 일주 트래픽 추이 분석 결과로서 기준선보다 많은 트래픽이 발생되고 있는 것을 확인할 수 있다. 이로 인해 이상 가중치 값은 1을 부여한다. 그림 22는 프로토콜별 추이 분석 결과로서 ICMP 트래픽의 발생 비율이 85%로 같은 시간대의 프로토콜별 트래픽 발생 비율과 비교하여 상이한 것을 확인할 수 있다. 이로 인해 이상 가중치 값은 1을 부여한다. 그림 23은 icmpOutEchoReps에서의 트래픽 발생을 분석한 결과이다. 그림에서 보듯이 대량의 트래픽이 발생되고 있는 것을 확인할 수 있으며, 이상 가중치값은 1이 된다.

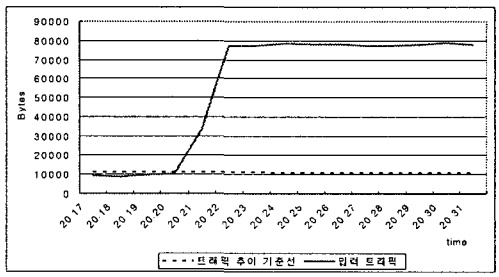


그림 21. 일주 트래픽 추이 분석(ICMP)

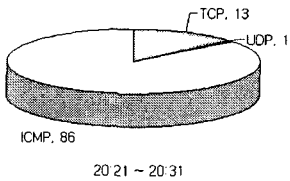


그림 22. 프로토콜별 추이 분석(ICMP)

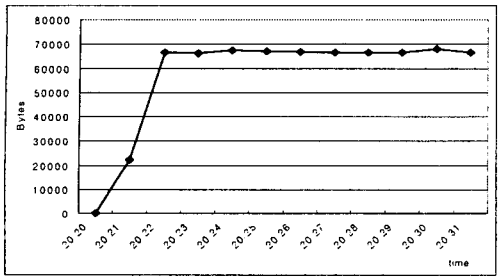


그림 23. icmpOutEchoReps에서 트래픽 발생 분석

각 분석 방법에서 모두 기준량과 비교하여 상이하게 트래픽이 발생되고 있는 것을 확인할 수 있다. 이를 통한 이상 가중치 결과는 표 7과 같다.

표 7. 이상 가중치 결과(ICMP)

분석 방법	이상 가중치	결과
일주 트래픽 추이 분석	1	총 이상 가중치 = 3 유해 트래픽
프로토콜별 추이 분석	1	
특정 MIB를 통한 분석	1	

이상 가중치 값이 총 3으로 현재 발생되는 트래픽에 대해 유해 트래픽임을 분석해내었다. 기존 방법과의 비교는 표 8과 같다.

표 8. 기존 방법과의 비교(ICMP)

분석 방법 / 구분	제안된 방법	기존 5분 단위	기존 3분 단위
분석 소요 시간	1분	15분	12분
미탐지	없음	초기 10분	초기 9분

VI. 결 론

본 논문에서는 유해 트래픽을 분석함에 있어 탐지 시간의 향상과 탐지율을 높이기 위해 일주 트래픽 추이 분석, 프로토콜별 트래픽 발생 추이 분석 그리고 특정 MIB 객체에 의한 트래픽 발생 분석 방법을 중첩하여 사용하였다. 각 분석 방법마다 이상 가중치를 설정하여 값이 2 이상인 경우 유해 트래픽으로 분석해 내는 방법으로 실험을 통해 기존의 방법보다 정확하고 빠른 분석 결과를 확인할 수 있었다.

기존의 SNMP를 이용한 분석 방법과 비교하여 기존 방법에서 분석해내지 못했던 초기 유해 트래픽에 대해 정확하게 분석했으며, 시간을 1분대로 크게 향상시킬 수 있었다. 이를 통해 트래픽 폭주 공격에 대해 빠른 분석을 할 수 있었다. 향후 변동하는 네트워크의 특성에 적응하기 위해 추이 분석에 사용되는 기준 데이터의 업데이트와 포트별 추이 분석 방법을 추가하면 여러 공격에 대해서 정확하게 탐지할 수 있을 것으로 생각된다.

참 고 문 헌

[1] http://data.dt.co.kr/special_report/downadd.asp?wp_id=158

[2] 오창석, 데이터 통신 수정판, 영한출판사, 2001.

[3] 김선영, 박원주, 유대성, 서동일, 오창석, "SNMP를 이용한 트래픽 폭주 공격 검출", 한국콘텐츠학회 논문지, 제3권, 4호, pp. 48-54, 2003.

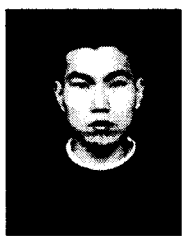
[4] 유대성, 오승희, 김선영, 서동일, 오창석, "SNMP MIB를 이용한 트래픽 분석", 한국통신학회 COMSW 2004, pp. 113-117, 2004.

[5] J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol (SNMP)," RFC1157, 1990.

[6] http://www.securitymap.co.kr/files/TrendMap_intro.pdf

저 자 소 개

유 대 성(Dae-Sung Yoo) 준회원



- 2003년 2월 : 충북대학교 컴퓨터공학과(공학사)
- 2003년 3월~현재 : 충북대학교 컴퓨터공학과 석사과정

<관심분야> : 정보보호, 컴퓨터 네트워크

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 : 미국 Stanford대학교 객원교수

<관심분야> : 컴퓨터네트워크, 뉴로컴퓨터, 정보보호