SNMP를 이용한 트래픽 폭주 공격의 효율적 탐지

A Efficient Detection of Traffic Flooding Attack using SNMP

이홍규, 김근영, 유대성, 오창석*
충북대학교*

Lee hong-kyu, Kim guen-young, Yoo dae-sung, Oh chang-suk*
Chungbuk Univ.*

요약

본 논문에서는 최근에 빈번하게 발생하는 트래픽 폭주 공격에 대해 대응하기 위하여 기존의 SNMP를 이용하는 트래픽 폭주공격 탐지방법을 향상시키기 위해 임계값 ϵ와 임계값 θ 을 사용하였다. 임계치에 따라서 트래픽 분석을 실행시킴으로써 시스템 자원을 보다 효율적으로 이용하기 위한 방법을 제시하였다.

Abstract

In this paper, We used thresholds ϵ, θ to improve traffic flooding attack detection method using SNMP in opposition to frequent traffic flooding attack. accordingly, we can use system resourses more efficient as execute traffic analysys by threshold

I. 서 론

최근의 해킹 동향을 보면 초기의 단순히 시스템의 버그를 이용하여 루트 권한을 얻는 형태에서, 네트워크에 트래픽을 발생시켜 네트워크 자원 및 시스템을 공격 대상으로 하여 사용 가능한 자원을 모두 소비해서 실제 자원을 사용해야 하는 사용자가 자원을 사용할 수 없게 하는 DoS 형태의 공격이 주를 이루고 있다.그 중에서도 서비스 거부공격과 인터넷 웜 공격이 증가하고 있는 추세이다

그리고 이러한 트래픽 폭주 공격도 발전하여 최근에는 다수의 시스템에 에이전트를 설치하고 공격을 하는 분산 서비스 거부 공격이 일반화되어 가고 있다. 그리고 2003년 1월의 인터넷 대란 때와 같은 빠른 전파력을 갖은 웜 형태의 공격인 인터넷 웜 공격이 네트워크 보안의 이슈가 되고 있다.

기존의 SNMP를 이용한 트래픽 폭주 공격의 탐지 방법은 IP, TCP, ICMP, UDP의 입출력에 해당되는 MIB 객체의 로그값을 추출하여 트래픽을 분석하고 정상적인 트래픽인지 아니면 공격 트래픽인지를 구분하였다. 트래픽 폭주 공격에 있어서 가장 중요한 부분은 공격을 정확히 탐지하고 대응하는 것도 있지만 탐지를 위한 CPU 사용률, 메모리 사용량 등의 시스템 자원을 효율적으로 사용해야 하는 것도 중요한 부분이다. 기존의 방법에서는 많은 MIB 객체여 광법위한 트래픽 분석에서의 장점이 있지만 트래픽을 탐지하기 위하여 많은 자원을 사용하여 공격이외에도 시스템에 많은 부하가 발생하게 되었다.

본 논문에서는 시스템 자원을 효율적으로 이용하여 트래픽 폭주 공격의 탐지를 하기 위하여 MRTG를 생성한 ipInReceives의 로그값을 사용하여 시스템이 정상적인 서비스를 할 수 있는 값을 찾아내서 임계치 ε을 생성한 후 트래픽이 발생하였을 때 그 트래픽이 임계값 미만의 값을 가졌을 때는 시스템이 정상적인 서비스를 하는데 영향을 미치지 못하기 때문에 트

래픽 분석을 실행하지 않는다. 그러나 트래픽이 임계값 이상의 값을 갖는 트래픽이 발생하였을 시에는 기존의 방법과 동일한 트래픽 변화량을 이용하여 생성한 임계값으로 트래픽 폭주 공격을 탐지하였다.

Ⅱ. 기존의 SNMP를 이용한 탐지

트래픽을 분석하기 위해서는 기본적으로 에이전트와 매니저 시스템에서 SNMP데몬이 실행되어 있어야 한다. 트래픽 분석에 사용되어지는 MIB 객체는 정상트래픽과 공격트래픽을 구분할 수 있는 객체를 사용하였는데 사용되어진 MIB 객체는 다음의 표와 같다.

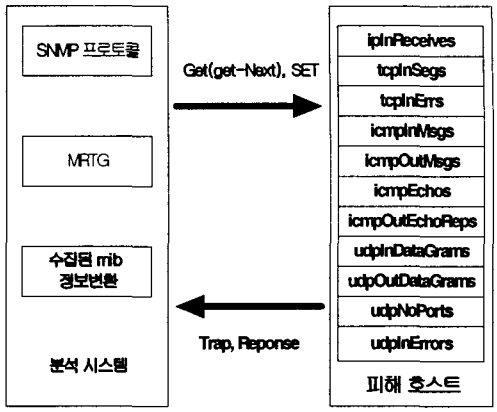
[표 1] 선정된 MIB 객체

프로토콜	MIB 객체
IP	ipInReceives
TCP	tcpInErrs
ICMP	icmpInEchos icmpOutEchoReps
UDP	udpNoPorts

Ⅲ. 시스템 자원을 효율적으로 이용한 공격 탐지

1. 트래픽 수집

트래픽 수집 방법은 선정된 MIB 객체를 통해서 이루어지며 전체적인 구성도는 다음 그림과 같다.



▶▶ 그림 1. 트래픽 수집 구성도

2. 트래픽 분석

트래픽 분석에서는 수집된 각각의 MIB 객체의 로그값을 분석하여 공격 트래픽과 정상 트래픽을 분류하게 된다. 기존의 방법은 정상 트래픽이 발생할 때도 분석 시스템을 가동하여 이로 인한 시스템 과부하를 가져오게 된다. 이러한 과부하를 줄이기 위해서 모든 MIB 객체에 대해 항시 분석을 하지 않고 입력되는 트래픽에 대한 임계값을 부여하여 기준치를 넘게 될 경우 폭주 공격을 탐지하게 된다.

다음 그림은 MRTG에 의해 생성된 로그값을 나타낸다.

```
1083309300 2047 1158 3732 1162
1083308700 2442 1154 2453 1158
1083308700 2442 1154 2453 1158
1083308400 2219 1158 2265 1174
1083308100 1457 1173 1475 1174
1083307800 1518 1159 2193 1170
1083307500 2143 1168 2193 1170
1083307200 1663 1150 4236 1154
1083306900 4141 1154 4236 1160
1083306600 2505 1160 2562 1175
1083306300 1658 1173 1673 1175
1083306000 1439 1157 1494 1169
1083305700 1532 1160 2173 1169
```

▶▶ 그림 2. MRTG로 수집된 로그 파일

첫 번째는 UTC 타임을 나타내며 패킷 수집 기본 단위인 5분을 나타낸다. 두 번째와 세 번째는 입출력

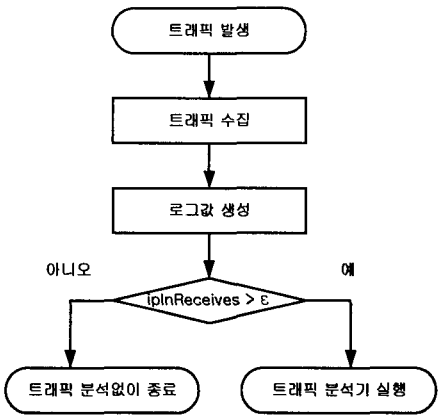
되는 트래픽의 평균값이며 세 번째와 네 번째는 입출력되는 트래픽의 최대값을 나타낸다. 위의 로그값은 tcpInSegs와 tcpInErrs의 트래픽을 수집한 값으로 입력에 해당되는 데이터는 tcpInSegs를 나타내고 출력에 해당하는 데이터는 tcpInErrs에 해당된다. TCP SYN Flooding 공격시 데이터부분이 의미없는 허위 데이터로 인해 상위 응용 프로세스로 전달되지 못하고 tcpInErrs에 트래픽이 발생하게 된다. 또한 발생된 트래픽의 양은 θ의 오차범위에서 일정하게 발생되는 것을 볼 수 있다. 이는 공격자에 의해 설정된 slave의 양에 의해 고정된 대량의 패킷을 송신하기 때문이다. 즉 공격 트래픽의 특징은 다음과 같이 정의 될 수 있다.

- 공격 트래픽에 민감하게 반응하는 MIB 객체가 존재한다
- 공격시 트래픽의 크기는 θ의 범위에서 일정하게 발생된다.

위의 2가지 특징을 가지고 본 논문에서는 공격 트래픽을 분석하였다.

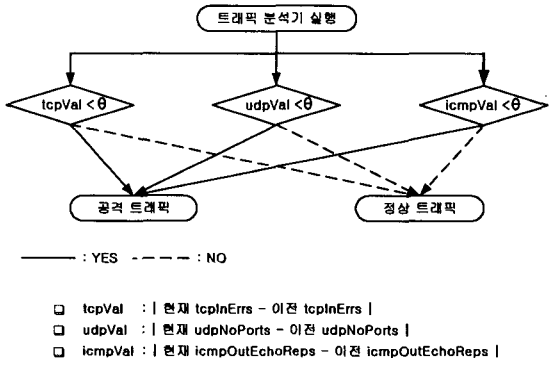
3. 트래픽 폭주 공격에 대한 트래픽 분석 알고리즘

분석시에도 시스템의 자원을 사용하게 된다. 트래픽 수집시 MIB 객체의 선정에서 시스템 자원의 사용량을 결정되듯이 기존의 분석 방법에서는 공격을 탐지하기 위해 일정 시간단위로 선정된 MIB 객체에 대해 모든 분석을 하게 되어 시스템의 사용량을 증가시켰다. 본 논문에서는 시스템의 부하를 줄이기 위해 분석 가변적인 분석을 하고자 한다. 이는 시스템의 가용성을 측정하여 가용성에 대한 임계값 ε을 선정하게 된다. 이는 트래픽 폭주 공격시 대상 시스템에 영향을 미치지 않는 트래픽이라면 분석을 하기위한 추가적인 시스템 부하를 줄이는게 더 효율적이라는 전제에서 제안되어진다. 즉 ipInReceives에서 발생되는 트래픽의 양을 ε과 비교하여 ε보다 큰 트래픽이 발생될 경우 수집된 트래픽에 대해 각 프로토콜 별로 트래픽을 분석하게 된다. 기본적인 분석 구성 흐름은 다음 그림과 같다.



▶▶ 그림 3. 트래픽 분석 흐름도

그림 3에서 트래픽 분석기에서는 입력된 트래픽에 대해서 각 프로토콜 별로 정상 트래픽과 공격 트래픽을 분류하게 된다. 분류 기준은 공격 트래픽은 3.1.1에서 도출된 특정 MIB 객체에서의 반응과 트래픽 발생이 θ의 안에서 일정하게 발생된다는 특징을 적용하여 분류하게 된다. 그림 3-8은 트래픽 분석기의 분류과정을 나타낸다.



▶▶ 그림 4. 트래픽 분석기의 트래픽 폭주 공격 분석

tcpInErrs, udpNoPorts와 icmpOurEchoReps에서 생성된 로그값을 현재값과 이전값의 차이를 이용하여 발생된 트래픽의 편차를 구하게 된다. 구해진

편차를 각각의 임계값 θ와 비교하여 θ보다 작을 경우 공격 트래픽의 특징과 일치하므로 공격 트래픽으로 판정하게 된다.

Ⅳ. 실험 결과 및 고찰

1. 임계치를 이용한 트래픽 산출방법

트래픽 분석을 시작하기 위한 임계치 ε은 시스템 성능이 저하되기 시작하는 시점의 로그값을 표본으로 산출하였다. 임계치 ε은 표본으로 선정된 ipInReceives의 로그값중에서 5분 동안의 평균값을 나타내는 로그값의 두 번째 열을 추출하였다. 조건에 맞는 로그값 중에 100개를 추출하여 그 값을 평균으로 하여 임계치를 산출하는 방식을 사용하였다. 임계치 산출 방식은 그림 6과 같다.

$$\frac{C}{N} = \varepsilon$$

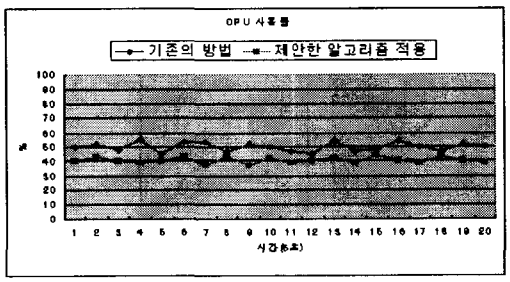
C (표본으로 선정된 로그값의 합)

N (표본으로 선정된 로그값의 갯 수)

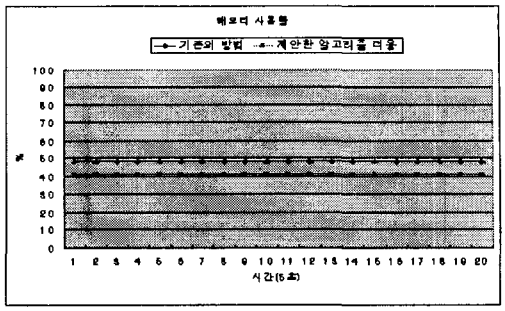
▶▶ 그림 6 임계치 ε 산출방식

3. 기존의 방법과의 비교

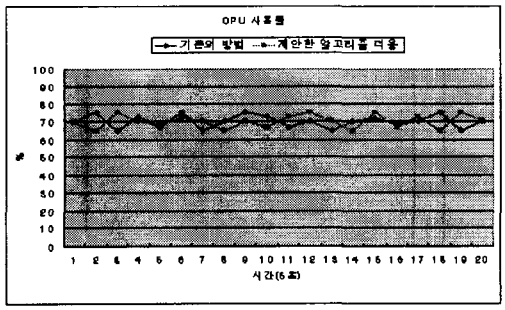
기존의 탐지 방법과 제안된 탐지 방법을 이용했을때의 CPU 사용량과 메모리 사용량의 비교는 다음 그림과 같다.



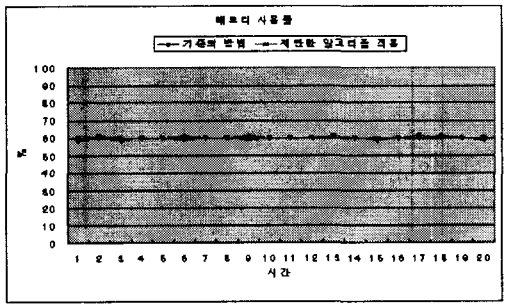
▶▶ 그림 7. 임계치 미만의 값에대한 CPU사용율 비교



▶▶ 그림 8. 임계치 미만의 값에 대한 메모리사용율 비교



▶▶ 그림 9. 임계치 이상의 값에 대한 CPU사용율 비교



▶▶ 그림 10. 임계치 이상의 값에 대한 메모리사용율 비교

[표 2] 임계치 미만의 트래픽이 발생시

탐지방법 / 비교대상	기존의 방법을 이용한 탐지	제안한 알고리즘을 이용한 탐지
분석대상	트래픽 로그	트래픽 로그
CPU 사용률	50%	42%
메모리 사용률	48%	41%

[표 3] 임계치 이상의 트래픽이 발생시

탐지방법 / 비교대상	기존의 방법을 이용한 탐지	제안한 알고리즘을 이용한 탐지
분석대상	트래픽 로그	트래픽 로그
CPU 사용률	70%	70%
메모리 사용률	61%	61%

위의 표에서 보는 바와 같이 임계치 미만의 트래픽이 발생하였을 때에 기존의 방법은 트래픽량에는 상관없이 주기 적으로 트래픽을 수집 및 분석 하였기 때문에 시스템 자원의 소비가 컸다. 하지만 제안한 알고리즘은 트래픽이 발생하더라도 시스템에 그 트래픽으로 인하여 영향을 받지 않고 정상적인 서비스를 할 수 있으면 트래픽의 분석을 시행하지 않았다. 그리고 시스템이 정상적인 서비스가 어려워지기 시작하는 시점인 임계치 이상의 트래픽이 발생하였을 때에는 기존의 방법과 동일한 방법을 사용하여 트래픽을 탐지하고 분석하였다. 제안한 알고리즘을 적용하였을 때는 표 2와 같이 임계치 미만의 트래픽이 발생하였을 때에는 CPU 사용률에서는 약 8%, 메모리 사용률에서는 약 7% 정도 자원의 활용도를 높였다

V. 결 론

본 논문에서는 SNMP MIB 객체를 이용하여 트래픽 폭주 공격을 탐지 하는데 있어서 기존의 방법 보다 시스템 자원을 효율적으로 사용하기 위한 알고리즘을 제안하였다. 기존의 SNMP를 이용한 트래픽 탐지 방법은 안정적인 정보 모델을 가지고 있고 트래픽 관리를 손쉽게 할 수 있다는 장점을 가지고 있다. 그러나 공격 트래픽이 발생하지 않았더라도 주기 적으로 트래픽을 수집 및 분석을 하기 때문에 공격 트래픽 이외에도 시스템의 성능을 저하시키는 불필요한 시스템 자원의 사용으로 인하여 더 많은 사용자에게 원활한 서비스를 제공 하지 못하는 경우가 발생하였다.

본 논문에서 제안한 알고리즘은 이러한 문제점을 보완하기 위하여 일차적으로 시스템으로 유입되는 총 트래픽량을 측정하여 시스템 자원의 고갈로 인하여 원활한 서비스의 처리가 힘들어 지기 시작하는 시점을 찾았다. 이때 생성되는 ipInReceives의 로그값의 표본을 추출하여 그 값의 평균을 임계치 ε으로 하여 그 임계치를 기준으로 트래빅 분석 여부를 결정하였다.

실험에서는 임계치 미만과 임계치 이상의 트래픽을 발생시켜서 그 결과를 측정하였고. 임계치 미만의 트래픽이 발생하였을 때에는 기존의 방법보다 CPU의 경우 약 8% 메모리의 경우 약 7%정도 시스템 자원을 적게 사용하고 정상 적인 서비스를 실행 할수 있었다.

향후 과제로는 임계값을 선정하는 과정에서 네트워크의 상태나 시스템의 상태에 따라 변화 할 수 있으므로 임계값 선정에 있어서 신뢰성을 높임과 더불어 시스템 자원을 좀 더 효율적으로 사용할 수 있는 임계값 선정이 필요하다.

▌참고문헌▐

[1] 정현철, 변대용, "트래픽 분석을 통한 서비스거부공격 추적", 한국정보보호진흥원, 2003.
[2] 조대일, 송규철, 노병규 역, 네트워크 침입탐지와 해킹 분석 핸드북, 인포북, 2001.
[3] 오창석, 데이터 통신 수정판, 영한출판사, 2001.
[4] 김선영, 박원주, 유대성, 서동일, 오창석, "SNMP를 이용한 트래픽 폭주 공격 검출", 한국콘텐츠학회 논문지 제3권 제4호, 2003.
[5] "99 정보시스템 해킹・바이러스 현황 및 대응", 한국정보보호진흥원.