DDoS 공격을 검출하기 위한 트래픽 분석 알고리즘

Traffic Analysis Algorithm for Detecting DDoS Attacks

유대성*, 박원주**, 김선영*, 서동일**, 오창석*
충북대학교*, 한국전자통신연구원**

Yoo Dae-Sung*, Park Won-Ju**, Kim Sun-Young*,
Seo Dong-Il**, Oh Chang-Suk*
Chungbuk National Univ.*,
Electronics and Telecommunications Research Institute.**

요약

최근의 해킹 동향은 네트워크 상의 대역폭을 목표로 하는 트래픽 폭주 공격이 증가하고 있는 추세이다, 반면 이러한 위협으로부터 네트워크 내의 공격 트래픽을 추출하는 기술은 아직 부족한 실정이다. 이에 본 논문에서는 네트워크 서비스 제공을 위협하는 트래픽을 추출하는 방법을 제시하고, DDoS 공격을 효과적으로 탐지하는 알고리즘을 제안하였다.

Abstract

The recent hacking trend is a traffic flooding attack against a bandwidth in the network grows more and more. On the other hand, technology, which extracts attack traffic in the network from these threats, is still short. Therefore, we propose methodology which can measure traffic that threaten network services, and algorithm which can detect DDoS attacks effectively.

I. 서론

최근 몇 년 사이 네트워크 기술의 급속한 발전으로 인해 초고속 네트워크 환경이 점점 실현되면서 사용자들의 요구사항은 점점 복잡하고 다양화되어 가는 추세이다. 이러한 추세와 더불어 수많은 시스템이 네트워크에 직접 연결되고 다양한 응용 프로그램들이 네트워크와 관련되어 개발되는 경우가 많아지면서 네트워크 트래픽은 점점 증가하고 있다. 현재 네트워크 트래픽의 증가는 많은 문제점을 야기하고 있고, 이러한 문제로 인해 네트워크 회선의 부족이나 응답 시간의 저하 등과 같은 많은 경제적인 문제를 불러일으키는 수준까지 이르렀다. 더불어 해커로 인한 트래픽 폭주공격은 네트워크에 수많은 트래픽을 증가시켜 정확한 서비스를 할 수 없게 되는 문제가 빈번하게 발생하고 있다. 예를 들어 1.25인터넷 대란의 경우 수십 시간동안 네트워크서비스를 제공하지 못함으로써 엄청난 경제적 문제를 야기한 대표적인 트래픽 공격이라 할 수 있다.

본 논문에서는 이러한 문제를 해결하고 좀더 정확한 트래픽 공격을 탐지하기 위해 SNMP(Simple Network Management Protocol)를 이용하여 트래픽을 분석하였다. SNMP를 이용한 트래픽 분석 방법은 먼저 에이전트 시스템의 MIB(Management Information Base) 객체를 분석한 후 공격에 이용되는 프로토콜을 중심으로 하여 DDoS공격과 일반 트래픽을 탐지하는 방법이다. 이러한 방법을 이용하여 DDoS 공격을 탐지하는 알고리즘을 제안함으로써 기존에 DDoS공격 탐지시 많은 시스템 부하와 정확하지 못한 탐지율을 향상시킬 수 있었다.[1][2]

II. 관련연구

1. 주파수를 이용한 DDoS 트래픽 분석

이 기법은 변동적인 네트워크 트래픽의 주파수 특성을 구분하여 DDoS공격이나 포트 스캔 공격을 포함하는 black-hat activity의 광범위한 공격을 다루었다. 이를 위한 트래픽 수집 방법은 IP flow data와 SNMP data의 두 data를 이용하였다. 트래픽 측정을 위하여

유동적인 트래픽에 대하여 각각의 특징을 가지고 있는 주파수 대역에 따라서 분석한다. 저주파는 원래의 매우 복잡한 데이터의 집합에서 매우 빈약한 필터링이 되어 있는 정보를 가지고 있다. 이와 반대로 고주파는 매우 세부적인 변화의 정보를 가지고 있다. 여기서는 하나의 저주파 필터와 3개의 고주파 필터를 사용하여 다음과 같은 3개의 특징적인 신호를 가지고 측정하였다.[3]

• 신호의 저주파 영역
레벨 9보다 높을 때 시스템으로부터 얻어지는 신호들의 합성으로 지속성이 크며, 데이터의 주간 패턴을 잘 캡쳐한다.

• 신호의 중주파 영역
레벨 6~8 사이에서 얻어지며, 일별 변화에 의해서 생성된다.

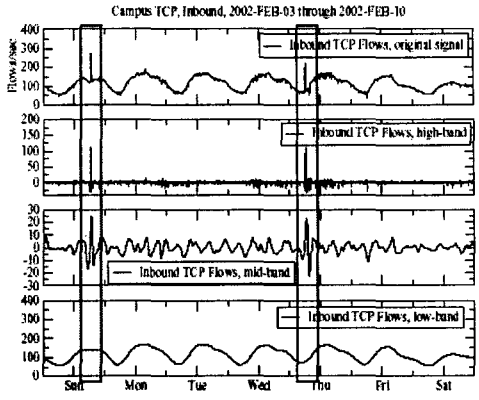
• 신호의 고주파 영역
처음 5단계의 주파수 레벨의 웨이블렛 부산물로 임계치 설정으로 얻어지는 신호. 선택되어지지 않은 값들은 임계치 적용에 의해서 0으로 초기화되며 주로 단기변화로 구성되어진다.
이 신호를 가지고 anomaly를 측정하기 위해서는 deviation score라는 방법을 사용하며 이는 다음과 같다.

• normalize the H- and M- part
일반화된 고주파와 중주파 영역을 명세된 크기의 윈도우로 움직이면서 계산. 움직이는 윈도우의 크기는 캡쳐하기를 원하는 anomaly의 지속성에 의존된다.

• 가중된 합계를 사용하는 고주파와 중주파 영역의 지역 변동성을 결합

• 편화된 신호에 임계값을 적용하여 신호변화의 최고 높이와 최고 넓이를 계산함으로써 anomaly와 그들의 지속성과 연결 강도 등을 알아낼 수 있다.

위와 같이 특징 신호와 측정조건을 이용하여 실험한 결과는 그림 1과 같다.



▶▶ 그림 1. DDoS 공격 탐지

위 그림 1에서와 같이 트래픽을 저주파, 중주파 그리고 고주파의 대역으로 분해하여 anomaly를 분석하였다. 공격에 따라 나타나지는 주파수 대역이 다른 점을 이용하여 트래픽 폭주 공격을 찾아내었으며, 더 나아가서 숨겨진 anomaly 특성까지 발견해 내었다.

Ⅲ. SNMP MIB를 이용한 DDoS 공격 검출

1. 기본 개념 정의

트래픽 분석 과정을 살펴보면 선처리되어야 할 것은 에이전트와 매니저 시스템에 SNMP 데몬이 실행되어 있어야 하며, 모니터링하고자 하는 시스템의 SNMP를 이용해 해당 시스템의 MIB정보를 가져와 분석한다. SNMP에는 수많은 종류의 MIB 객체가 있다. 그 중에서 실험을 통해 먼저 사용할 MIB객체를 선택하였다. 대부분의 DDoS 공격이 TCP, IP, UDP, ICMP를 이용한 공격이므로 그 중에서 실험을 통해 표 1과 같은 MIB를 불러들여 트래픽을 분석하였다.[4][5]

[표 1] DDoS 공격 검출을 위한 MIB객체

구분	MIB
TCP	tcpInSegs, tcpOutSegs, tcpInErrs
IP	ipInReceives, ipInDelivers, ipOutRequests, ipReasmReqds, ipFragCreates
ICMP	icmpInMsgs, icmpOutMsgs, icmpOutDestUnreachs, icmpInEchos, icmpOutEchoReps
UDP	udpNoPorts, udpInErrors

2. 공격 탐지 방법

ifInOctets, ifOutOctets에서는 관리 대상이 되는 인터페이스의 IP 데이터그램을 포함한 모든 트래픽을 감지하게 된다. 그리고 ifInUcastPkts, ifOutUcastPkts에서는 상위 계층 프로토콜에 전달되는 모든 패킷의 트래픽을 감지하게 된다. 따라서 프로토콜별로 트래픽을 분해하여 입출력되는 트래픽에 대해서 그 특징을 분석하게 된다. 분석에서 비교되는 대상은 실험에 의해서 얻어진 공격툴들의 트래픽 특성을 사용하였으며 일반적으로 다음과 같은 특징을 가지게 된다.

- 상위 대응되는 서비스가 없으므로 IP데이터그램에서 분해된 후 각 포트별 서비스에서 에러 결과 출력
- 크기가 일정한 트래픽이 지속적으로 발생

위에서처럼 2가지 특징을 각각의 MIB 객체에 이용하며, IP데이터그램 수신에 관한 트래픽을 분해하여 해당 프로토콜별로 트래픽을 추출한 후 각 서비스에 대한 정상 유무를 판별하게 된다.

3. DDoS 공격 검출 알고리즘

공격 알고리즘은 트래픽의 특성을 분석한 것을 토대로 각각의 공격에 대한 트래픽 특성과 트래픽 특성 공격 탐지 방법에 의하여 SNMP MIB를 이용한 DDoS공격 검출 알고리즘을 제안하였다. DDoS 공격 검출 알고리즘은 다음과 같은 과정으로 트래픽을 분석한다.

- ifInUcastPkts에서 각각의 프로토콜별 분해
- tcp : error check
- udp : Noport & error check
- icmp : icmpInEchos, IcmpOutEchoReps check

이러한 과정을 거쳐서 트래픽을 분석한 결과 그림 2에서와 같은 알고리즘을 도출하였다.

```
1) Traffic 수집
2) Protocol analysis
  i)tcpInSegs.
    if tcpInErrs.>0 : attack
      tcpInSegs -tcpInErrs = nomal
 ii) udpInErrs >0 or udpNoPorts>0 =>attack
     totaludpattack = udpInerrs + udpNoPorts
iii) icmpInMsg>0 and
    if icmpInEchos. >0
    and IcmpOutEchoReps >0
      if
        α≤ε1 and β≤ε2
        then  attack
α : icmpInEchosn - icmpInEchosn-1
β : icmpOutEchoRepsn - icmpOutEchoRepsn-1
ε1 : IcmpInEchos threshold
ε2 : IcmpOutEchoReps threshold
```

▶▶ 그림 2. DDoS 검출 알고리즘

DDoS 검출 알고리즘을 보게 되면 먼저 트래픽을 수집한 후 프로토콜을 분석한다. 대표적인 TCP 플로딩 공격과 같은 경우는 tcpInSegs값을 보게 되면 tcpInErrs에서 정상적인 TCP 패킷은 반응하지 않고 공격 트래픽만 반응하게 된다. 이것은 정상적인 TCP 패킷은 연결설정을 목적으로 하나 비정상적인 패킷은 완전한 쓰리웨이 핸드쉐이킹을 하지 않고 계속적으로 패킷을 보내므로 tcpInErrs에 트래픽을 발생시키게 된다. 이러한 TCP 플로딩의 경우 일정량의 유입패킷이 모두 tcpInErrs 패킷과 일치하게 된다. 따라서 tcpInErrs에 5초 이상의 동일양의 패킷이 계속 유지된다면 이것은 공격으로 탐지한다. 마찬가지로 UDP 플로딩 공격의 경우는 udpInErrs 와 udpNoPorts에서 TCP 플로딩과 같은 방법으로 공격을 탐지한다. 마지막으로 ICMP 공격 탐지는 공격 트래픽의 경우 크기가 일정하다는 특성을 근사 다항식에 적용시켜서 탐지하게 된다. icmpInEchos, imcpOutEchoReps의 트래픽을 근사 다항식에 적용시켜 임계치 안에서 트래픽이 발생된 경우 공격으로 탐지하게 된다. 여기에서 사용된 임계치는 실험에 의해서 얻어진 결과를 사용하였으면 평균값은 1이다. 알고리즘에 적용된 근사 다항식은 다음과 같다.

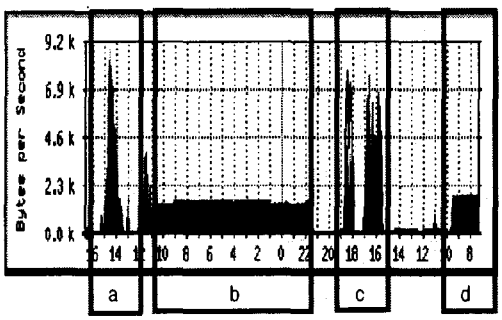
$$f(x) - p(x) = \varepsilon \qquad (1)$$

식 1에서 f(x)는 실험에 의해 얻어진 트래픽 다항식, p(x)는 공격 트래픽 다항식 그리고 ε은 임계값을 나타

낸다.

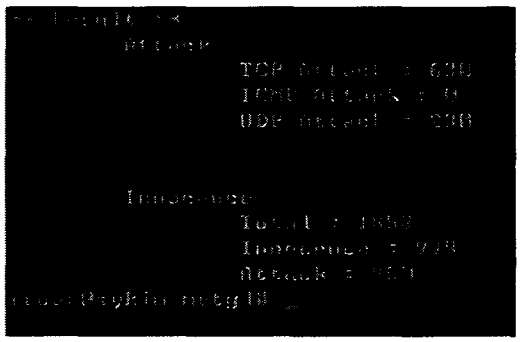
Ⅳ. 실험 및 결과

본 논문에서 제안한 알고리즘을 실험하기 위하여 공격툴로는 Trin00, Tfn, Stacheldraht[6][7][8]와 같은 DDoS 공격툴을 사용하였다. 그리고 공격이 이루어지고 있는 동안 정상적인 서비스를 병행하였을 경우 다음과 같은 트래픽을 볼 수 있었다.



▶▶ 그림 3. if객체에서의 트래픽 수집

그림 3에서 트래픽의 크기가 일정한 부분은 공격 트래픽의 단적인 특징을 그대로 보여주고 있다. 정상 트래픽을 제외하고 공격만 하였을 경우 그림 3의 b와 d부분처럼 공격의 특징을 찾아 낼 수 있다. 반면 공격이 정상 트래픽과 함께 들어올 경우 a와 같이 상위 mib 객체에서는 공격을 탐지해 낼 수 없다. 이런 경우 제안된 알고리즘에 의해서 프로토콜별로 분해한 후 탐지하게 된다. 이러한 트래픽을 DDoS공격 검출 알고리즘에 적용한 결과는 그림 4와 같다.



▶▶ 그림 4. DDoS 공격 검출 알고리즘 적용 결과

그림 4에서 보는 것과 같이 DDoS 공격툴을 이용하여 실험한 결과 총 1858개의 패킷중 정상패킷이 998개이고 공격에 해당되는 패킷이 860개로 정확한 공격을 탐지 할 수 있었다.

Ⅴ. 결론 및 향후과제

본 연구는 정보통신의 급속한 발전으로 인해 증가되고 있는 네트워크 트래픽을 분석하여 정상 트래픽과 해커로 인한 트래픽 폭주 공격을 검출하는 알고리즘을 제안하였고, 제안된 알고리즘을 실험하기 위해 트래픽 분류기를 구현하였다. 실험을 통해서 분석된 공격 트래픽 특징은 해당 포트에서 특정 MIB에 정상 트래픽과는 다른 양상의 트래픽을 발생시킨다는 사실을 알 수 있었고, 이러한 결과를 이용해 제안된 알고리즘을 적용하여 실험한 결과 정상 트래픽과 공격 트래픽을 분류해낼 수 있었다.

향후 실험을 통해 좀더 폭넓은 트래픽 폭주 공격에 대한 확장성 및 대응방법에 대한 연구를 진행할 계획이다.

▌참고문헌▐

[1] RFC 1271, "Remote Network Monitoring Management Information Base", S.Waldbusser, Febraury 1993
[2] 최재원 "웹 기반 네트워크 트래픽 분석 시스템", 한국정보처리학회 학술발표논문집, 제7권, 제2호, 2000
[3] P.Barford and D.Plonka, "Characteristics of Network Traffic Flow Anomalies," in Proceedings of ACM SIGCOMM Internet Measurement Workshop, San Francisco, CA, November 2001
[4] Tobias Oetiker, "MRTG", http://people.ee.eth.ch/~oetiker/webtools/mrtg
[5] Claffy, K. C., "Internet traffic flow profiling", http://www.caida.org/outreach/papers/1994/itf
[6] William Stallings, "SNMP, SNMPv2, SNMPv3, and RMON1 and 2 Third Edition Addison Wesley, 1999
[6] Paul J. Criscuolo "Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht" CIAC-2319
[7] Kathleen M. Moriarty, "DDoS" http://watersprings.org /pub/id/draft-moriarty-ddos-rid-01.txt
[8] Jason Barlow and Woody Thrower, Axent Secuirty Team "TFN2K-An Analysis,"