DDoS 공격 탐지에 효율적인 트래픽 비율 분석법(ETAM)

최광열*, 최현상,**, 이희조**
*고려대학교 컴퓨터정보통신대학원 디지털정보공학과
** 고려대학교 컴퓨터• 통신공학부
e-mail : choikwy, realchs, heejo@korea.ac.kr

Effective Traffic Analysis Method(ETAM) in Detecting DDoS Attacks

KwangYeol Choi*, Hyunsang Choi, HeeJo Lee**
*Dept. of Digital Information Technology, Korea University
**Dept. of Computer Science & Engineering, Korea University

요 약

DDoS 공격은 인터넷 환경에서 네트워크나 개인 호스트를 위협하는 대표적인 공격 트래픽이다. DDoS 공격은 간단한 Tool 로 공격이 가능하면서 네트워크 기반 구조에 큰 피해를 입힐 수 있기 때문에 그 심각성이 크다. DDoS 공격의 효과적인 방어와 대응을 위해서는 DDoS 공격 트래픽에 대한 정확한 분석과 탐지가 선행되어야 한다. 본 논문에서는 DDoS 공격 징후를 신속하게 탐지해 낼 수 있는 효율적인 트래픽 비율 분석법(ETAM)을 제안하고, ETAM 기법을 통해 공격을 빠르고 신속하게 탐지할 수 있음을 보인다.

1. 서 론

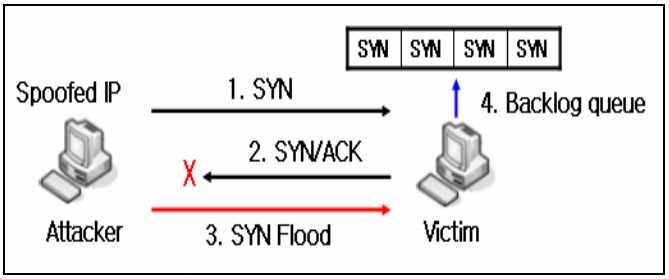
네트워크 환경의 급속한 발달과 함께 DDoS (Distributed denial of service) 공격이 증대되고 있다. DDoS 공격은 인터넷에 개방되어 있으면서 동시에 한정된 자원을 가진 모든 시스템을 쉽게 공격의 대상으로 하여 피해를 입힌다[1,2]. 뿐만 아니라 간단한 공격 Tool 만으로도 특정 서비스를 중지시키거나 네트워크 관리에 큰 혼란을 줄 수도 있다. 효율적인 네트워크 관리를 위해서 DDoS 공격이 발생했을 때 이를 정확하게 감지하여 방어자에게 알려주는 것을 탐지라 하며, 이를 기반으로 적절한 대응을 수행하는 것을 DDoS 방어라 한다. 본 논문에서는 DDoS 의 공격이 발생하고 있음을 신속하게 탐지할 수 있는 효율적인 트래픽 비율 분석법(Effective Traffic Analysis Method, ETAM)을 제안 하고자 한다.

2 장에서는 DDoS 공격의 과정 및 구조를 살펴보고 기존의 공격 탐지를 위한 트래픽 비율 분석법을 소개한다[3]. 3 장에서는 DDoS 탐지를 위한 트래픽 비율 분석법을 제안 하고. 4 장에서는 실험을 통해 DDoS 공격이 발생했을 때 트래픽 비율 분석법으로 DDoS 트래픽 탐지 결과를 분석한다. 마지막으로 5 장에서는 결론 및 향후 연구방향에 대해 언급한다.

2. 관련연구

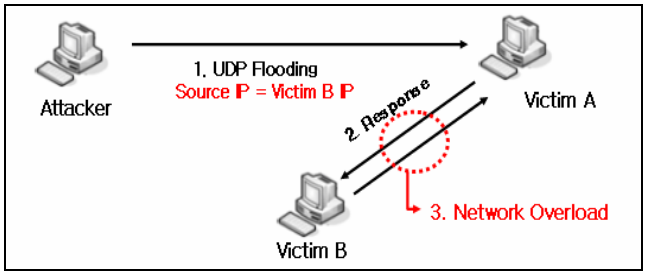
2.1 DDoS 공격 분석

DDoS 공격에 대처하려면 우선 DDoS 의 유형을 알아보고 그 특성을 파악하는 것이 중요하다. 대표적인 DDoS 공격은 SYN Flooding[4], UDP Flooding[4], ICMP Flooding[4] 등이 있고, 대표적인 공격 프로그램으로는 TrinOO, TFN, TFN2K, Stacheldraht 외에 다양한 공격 Tool 들이 있다.



(그림 1) SYN Flooding Attack

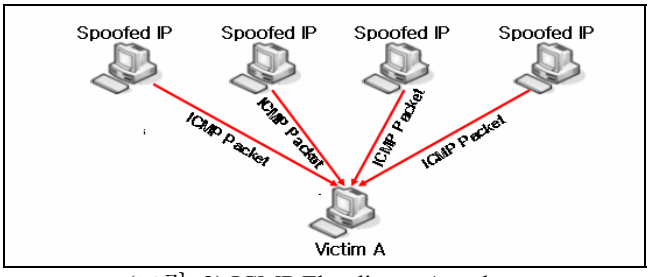
(그림 1)의 SYN Flooding 은 서버에 접속을 요청하는 패킷을 보낸 후 정보를 보내지 않아 서버가 열린 상태로 기다리고 있는 경우 연결 설정이 초기화되기 전에 위조된 패킷을 flooding 하여 포트의 대기 큐에 더 이상 저장할 수 없는 상태로 만드는 공격이다.



(그림 2) UDP Flooding Attack

UDP Flooding 은 UDP 의 비연결성 및 비신뢰성 때문에 공격이 용이한 방법이다. UDP 는 소스 주소와 소

스 포트를 스푸핑(spoofing)하기 쉽다. 이러한 약점들을 이용해 (그림 2) 와 같이 과다한 트래픽을 희생자에게 전송함으로써 희생자간(Victm A, Victm B)네트워크를 마비시킨다.



(그림 3) ICMP Flooding Attack

(그림 3)의 ICMP Flooding(Ping Flooding)은 다수의 ping 패킷을 공격대상에게 전송함으로써, 공격대상의 네트워킹을 불가능하게 만드는 공격이다. 네트워크의 bandwidth 가 과거에 비해 크고, 상당 수의 서버들은 ping 패킷의 수신을 차단하고 있기 때문에, 치명도가 낮다고 볼 수 있으나, 다량의 ping 패킷이 서버 앞단의 라우터나 스위치까지의 대역폭을 과도하게 차지하기 때문에 서비스 지연이나 중단되는 사례가 많이 발생하고 있다.

2.2 DDoS 공격의 탐지를 위한 트래픽 비율 분석법

트래픽 비율 분석법[3]이란 전체 트래픽에서 특정한 형태를 가진 트래픽 비율(Rate)을 이용하여 분석하고 DDoS 공격의 탐지를 수행하는 기법이다. 트래픽 비율 분석법은 TCP 플래그 비율(TCP flag rate)과 프로토콜 비율(protocol rate)로 구분된다. 다음 (수식 1,2)는 TCP 플래그 비율을 정의하고 있다.

$$Rtd[Ki] = \frac{\sum flag(K)}{\sum TCP\ packets} \quad (inbound) \quad (수식\ 1)$$

$$Rtd[Ko] = \frac{\sum flag(K)}{\sum TCP\ packets} \quad (outbound) \quad (수식\ 2)$$

(수식 1,2)의 TCP 플래그 비율법은 TCP 패킷만을 대상으로 하며, 특정한 TCP 플래그를 가진 패킷 개수를 전체 TCP 패킷 개수로 나눠서 구할 수 있다. 여기서 td 는 트래픽 비율을 측정한 시간 간격을 의미하고, K 는 TCP 플래그 S(SYN), F(FIN), R(RST), A(ACK), P(PSH), U(URG), N(NULL) 을 각각 의미한다.
(수식 3,4)에서는 프로토콜 비율을 정의하고 있다.

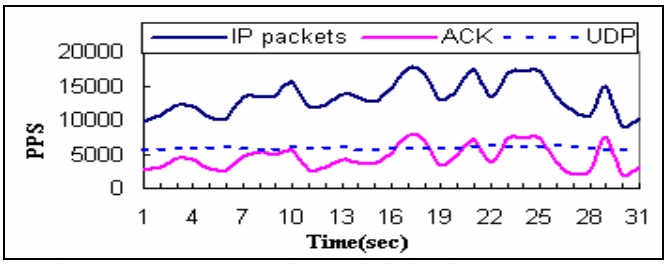
$$Rtd\{(TCP|UDP|ICMP)\,i\} = \frac{\sum (TCP|UDOP|ICMP)\ packets}{\sum IP\ Packtets} \quad (inbound) \quad (수식\ 3)$$

$$Rtd\{(TCP|UDP|ICMP)\,o\} = \frac{\sum (TCP|UDOP|ICMP)\ packets}{\sum IP\ Packtets} \quad (outbound) \quad (수식\ 4)$$

프로토콜 비율은 특정한 프로토콜(4 계층 TCP, UDP, ICMP)을 갖는 패킷 개수를 전체 IP 패킷 개수로 나눠서 구할 수 있다[3].
TCP 플래그 비율법은 TCP SYN Flooding 탐지에 효과적이지만 UDP, ICMP 공격 탐지를 하지 못하는 취약점이 있다. 프로토콜 비율법은 이를 일부 보완 하지만 다양한 공격유형을 가지는 DDoS 공격을 탐지하고 특성을 분석하기에는 충분하지 않다. 기존의 트래픽 비율 분석법은 정상적인 응용 프로그램(메신저, P2P, 웹) 사용시 TCP 플래그 변화를 유해 트래픽으로 오탐을 한다. 또한 웜(Worm),봇(Bot) 같은 유해 트래픽을 분석해내지 못하는 단점이 있다. 또한 기존의 트래픽 비율 분석법은 parameter 값인 TCP flag 7 개와 포로토콜 3 개, inbound 와 outbound 각각 20 개의 그래프로 표현된다. 그래서 공격을 판별하는데 복잡하고 어려움이 있다.

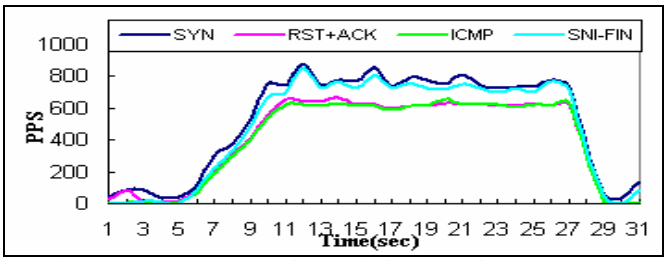
3. DDoS 공격 탐지를 위한 효율적인 트래픽 비율 분석법(ETAM)

네트워크가 DDoS 공격을 받으면 전체적인 트래픽 양과 공격 유형에 따라 프로토콜, 패킷 분포와 헤더 플래그의 비율의 변화가 생긴다. UDP Flooding 은 일반적인 UDP 프로토콜 비율이 매우 높아진다. ICMP Flooding 도 ICMP 프로토콜 비율이 높아지게 된다. SYN Flooding 공격은 일반적인 TCP 프로토콜 비율로는 단순히 공격을 판단 하기에는 어려움이 있다. SYN Flooding 공격시 각각의 프로토콜과 Flag 변화를 관찰하기 위해 정상적인 Web 트래픽과 온라인 PC Game 트래픽에 20 초간 SYN Flooding 공격 Tool 을 사용하여 공격한 후 트래픽을 관찰 하였다.



(그림 4) SYN Flooding 에 민감하지 않은 Parameter

(그림 4)에의 IP Packet, UDP, TCP 의 ACK 의 PPS 는 SYN Flooding 공격에 민감한 반응을 보이지 않는다.
반면 DDoS 공격이 없는 경우에는 TCP 연결의 생성(Establishment)과 종료(Termination)는 재전송(retransmission)의 경우를 제외하면 거의 동일한 비율로 발생한다.
그러나 SYN Flooding 공격이 발생하면 대량의 SYN 플래그를 가진 TCP 패킷이 급증하므로, SYN 플래그 탐지비율이 FIN 플래그 탐지비율보다 많아지고 RST 패킷이 증가하게 된다.



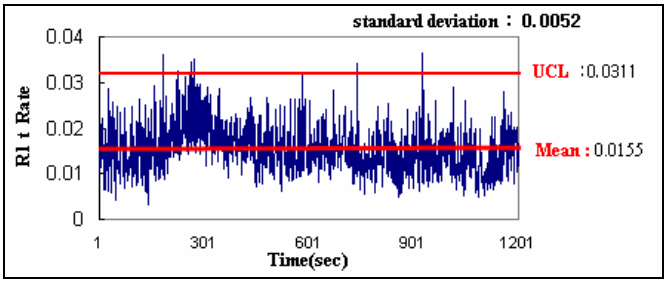
(그림 5) SYN Flooding 에 민감하게 변하는 Parameter

이러한 특성이 반영된 (그림 5)는 TCP 의 SYN, RST+ACK 이 증가 하였다. SYN 에서 FIN 을 뺀 SIN-FIN, ICMP 가 민감하게 반응함을 알 수 있다. ICMP 는 ICMP TYPE 5 Redirect 가 급격하게 증가 하였다.

$$R1\,t = \frac{\alpha\{\sum(SIN\text{-}FIN) + \sum RST\} + \beta \sum ICMP + \gamma \sum UDP}{\sum IP\ Packtets}$$

$\cdots\cdots\cdots$ (Inbound + Outbound) (수식 5)

공격시 민감하게 반응하는 특성을 고려한 개선된 트래픽 비율 분석법(ETAM)은 다음 (수식 5)와 같다.
가중치 α, β, γ 는 각각의 네트워크 상황에 따라 달라질 수 있다. 측정한 프로토콜의 양과 대역폭, 그리고 최근에 빈번히 발생하는 공격을 인지 하였다면 중점을 두고자 하는 공격에 따라서 적절한 값을 선택할 수 있다. $\alpha+\beta+\gamma=1$ 이 되며 $0 \le \alpha, \beta, \gamma \le 1$ 사이의 값이다.
트래픽 비율 ***R1 t*** 의 t 는 트래픽 비율을 측정한 시간을 의미한다. 본 논문에서는 1 초 단위로 측정을 하였다.
본 논문에서는 트래픽 비율을 고려하여 α, β, γ 를 각각 0.7, 0.1, 0.2 비율로 적용하였다.

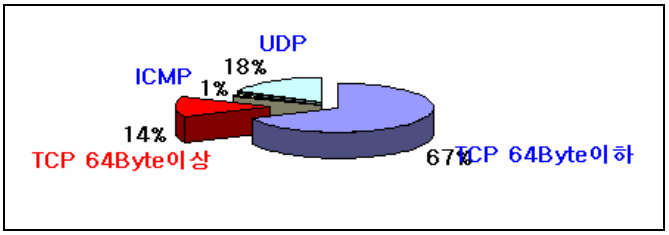


(그림 6) R1 t ETAM 결과

(그림 6)은 최번시(트래픽이 가장 많은 시간) 20 분 동안 ETAM 으로 측정한 결과이다. R1 t 의 평균은 0.0155 이며 STDEV(Standard Deviation,표준편차)는 0.0052 이다. 상한치 관리한계선인 UCL(Upper Control Limit)을 초과하여 지속적으로 발생하면 이상값으로 분류하여 공격으로 판단 한다. UCL 은 표준편차에 3 을 곱하고 평균을 더하여 산출 하였다

UCL = (STDEV X 3) + 평균
= (0.0052 X 3) + 0.0155 = 0.0311

그러나 R1 t 의 분모값인 IP Packet 의 총합과 분자값인 공격 판별에 사용되는 Parameter 값의 비율 차이가 많이 나고 있다. 분모의 값을 적당히 줄여주면 ETAM 의 결과 값이 증가하여 공격에 대한 판별이 더욱 쉬워 질 것이다.



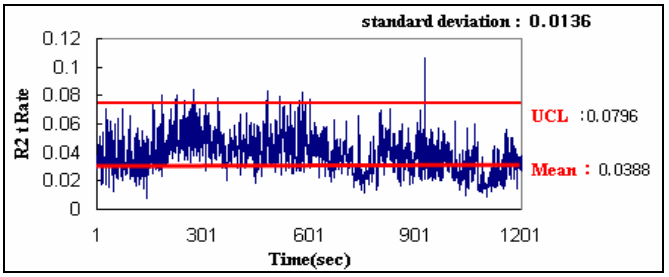
(그림 7) Packet Size 별 프로토콜 비율

(그림 7)은 최번시 20 분간 측정한 동일한 데이터중 64Byte 이하 TCP 프로토콜이 67%를 점유하고 있다. 64Byte 이상 TCP 프로토콜이 14%, UDP Packet 은 18%, ICMP 패킷은 1% 의 비율로 트래픽이 흐르고 있다. 64Byte 이상의 TCP 프로토콜의 14% 가운데 데이터 전송을 위한 정상적인 패킷이 95%이상을 점유하고 있다. 따라서 64Byte 이상인 TCP 패킷을 분석에서 제외하면 상대적으로 공격 트래픽 비율이 높아져 ETRM 결과의 비율이 더욱 높아질 것이다.

$$R2\,t = \frac{\alpha\{\sum(SIN\text{-}FIN) + \sum RST\} + \beta \sum ICMP + \gamma \sum UDP}{\sum(IP\ Packtets \le 64Byte) + \sum ICMP + \sum UDP}$$

$\cdots\cdots\cdots$ (Inbound + Outbound) (수식 6)

(수식 6)은 R1 t 의 수식을 R2 t 수식과 같이 보완 하였다.
R1 t 와 동일하게 가중치를 적용 하여 (그림 8)과 같은 결과를 얻었다.



(그림 8) R2 t ETAM 결과

UCL = (표준편차 X 3) + 평균
= (0.0136 X 3) + 0.0388 = 0.0796

즉 상한치 관리한계선인 ETAM 계산값이 UCL 0.0796 이상의 값이 지속되면 공격으로 판단 한다.

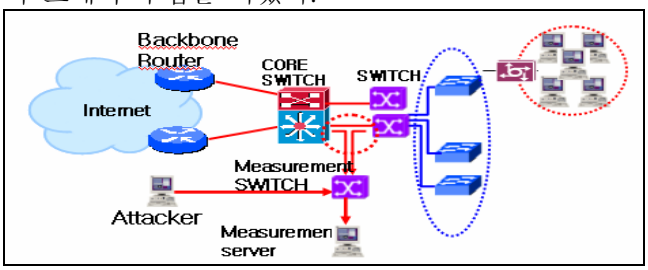
4. 실험 및 결과

본 장에서는 제안한 ETAM 을 실험하기 위하여 환경을 구축하고 DDoS 공격시 특성 변화를 관찰하여,

R1 t 와 R2 t 각각의 그래프와 결과를 비교 분석한다.

4.1 실험 환경

각각의 R1 t 와 R2 t 를 비교 분석 하기 위하여 실험 환경을 (그림 9)와 같이 구축 하였다. ETAM 측정을 위하여 Metro Ethernet PC 게임 서비스 제공을 위한 망에서 트래픽 수집을 하였다.

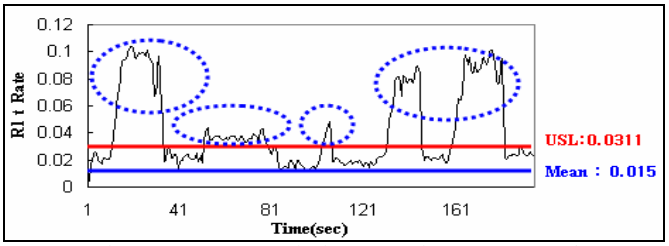


(그림 9) ETAM 시스템 구축

Giga 스위치 하위에 50Mbps 대역폭을 사용하는 15 개의 사업장이 있으며, 각 사업장 마다 60 대 정도의 PC 를 보유하고 있다. 최번시 평균 트래픽은 200Mbps 이며, 트래픽 수집과 분석을 위한 별도의 스위치로 TAP 을 설치 하여 트래픽을 유통시키고 측정용 스위치에 트래픽 분석 서버를 연결하여 트래픽을 분석 하였다. DDoS 공격을 위한 간단한 공격 Tool 이 탑재된 공격서버 1 대를 별도로 설치하여 측정용 스위치에 DDoS 공격을 하였고 측정용 스위치에서 공격 트래픽과 정상적인 트래픽을 적절히 섞이도록 하여 측정서버로 트래픽이 유통되도록 하였다..

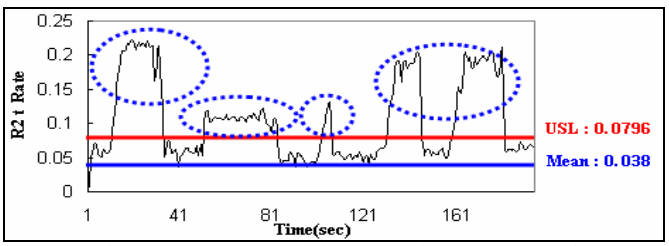
본 논문에서는 200 초 동안 정상적인 트래픽에 간단한 공격 Tool 로 공격 트래픽을 다음과 같이 SYN(80PORT), ICMP, UDP, SYN(21PORT), SYN(80PORT) 순으로 순차적으로 공격을 진행 하였다.

4.2 ETAM 의 R1 t, R2 t 결과 분석



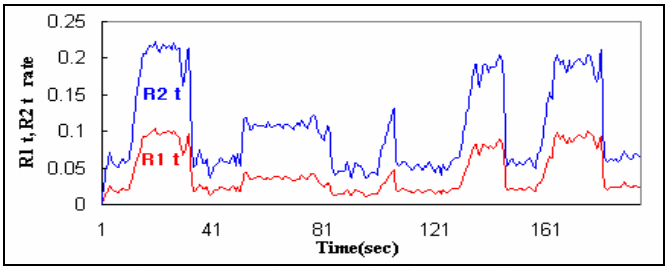
(그림 10) DDoS 공격시 R1 t 의 ETAM 결과

(그림 10)은 Time [10,30],[50,80],[100,110],[130,150] [160,180] 구간에서 관리한계선 UCL 을 초과하는 DDoS 공격이 정상적으로 탐지하였다.



(그림 11) DDoS 공격시 R2 t 의 ETAM 결과

(그림 11)은 동일한 트래픽을 R2 t 로 분석하였고 관리한계선인 UCL 을 초과하는 부분이 DDoS 공격의 시간과 일치함을 확인 할 수 있다.



(그림 12) R1 t 와 R2 t 의 비교 그래프

(그림 12)은 R1 t 와 R2 t 의 비교 그래프 이다. R1 t 보다 R2 t 의 비율이 더욱 높게 나오며 공격 판별이 용이 함을 알 수 있다.

5. 결론

본 논문에서 기존의 DDoS 공격 탐지의 트래픽 비율 분석법의 문제점을 제시 하였고. 이에 효율적인 트래픽 비율 분석법(ETAM)을 제안하였다. 그리고 실제 망 환경에서 실험을 통해 ETMA 으로 DDoS 공격을 검출해 낼 수 있음을 확인 하였다. 실제 네트워크에서 발생하는 많은 DDoS 공격에 대해 ETAM 으로 더욱 쉽게 공격을 탐지하고 이를 통한 빠른 대응이 가능할 것이다. 향후 백본망에서 ETAM 의 결과 값에 따라 지능적으로 샘플링하는 기법에 대하여 연구하여, DDoS 탐지 뿐만 아니라 공격의 근원지 추적 및 DDoS 공격을 차단하기 위한 연구를 계속 수행 할 예정이다.

참고문헌

[1] 이철호, 최경희, 정기현, 노상욱, “웹 서버에 대한 DDoS 공격의 네트워크 트래픽 분석,” 한국정보처리학회 논문지 C, 제 10-c 권, 제 3 호, June 2004.

[2] Glenn Carl, George Kesidis,Richard R. Brooks and Suresh Rai, “Denial-of-Service Attack-Detection Techniques,” IEEE Internet Computing, Jan., Feb. 2006.

[3] Cheolho Lee, Sanguk Noh, Kyunghee Choi and Gihyun Jung, “Characterizing DDoS Attacks with Traffic Rate Analysis,” In Proceeeding of the International Conference e-Society, Vol.1,pp81~88,Lisbon,Portugal, June,2003

[4] 이종엽, 윤미선, 이훈, “DoS 공격의 유형 분석 및 탐지 방법”, KNOM Review, Vol. 6, No. 2, pp.21-32, Feb. 2004