검증 IP table를 사용한 통계 기반 DDoS 대응 시스템

박필용° 홍충선
경희대학교
pypark@networking.khu.ac.kr°, cshong@khu.ac.kr

A Statistics based respond system against DDoS using the identified IP table

PilYong Park° ,Choong Seon Hong
Dept. of Computer Engineering , Kyung Hee University Graduate School

요 약

Distributed Denial of Service는 네트워크나 개인 호스트를 위협하는 대표적인 공격 트래픽이다. DDoS 공격은 특정한 패턴을 가지고 있지 않기 때문에 탐지가 어려울 뿐 아니라, TNF2K와 같은 간단한 tool로 공격이 가능하여 그 심각성은 실로 크다. 이러한 DDoS를 탐지하기 위한 메카니즘이나 알고리즘은 많이 개발되었다. 하지만 DDoS의 근원지를 판별하고 대응하는 것이 아닌, 단지 방어 지점에서 전체 threshold를 낮추거나 leaky bucket처럼 수용 능력 이상의 패킷을 폐기하는 방법으로 네트워크나 개인 호스트를 보호한다. 무분별하게 전체 트래픽을 줄이는 것은 네트워크의 resource를 고갈 시키지는 않지만, 정상적인 clients가 공격당하고 있는 호스트에 연결을 할 수가 없다. 이를 위해 여러 단계의 테스트를 통해 합법적인 검증 IP table을 만들고, 검증 IP table에 있는 source IP를 제외한 나머지 트래픽을 차단한다면, DDoS 공격에 대해서 대응을 하면서 정상적인 clients의 연결을 보호 할 수 있다.

1. 서 론

DDoS는 2000년 2월 야후, 아마존과 같은 인터넷 포털 사이트에 심각한 피해를 주면서, 주요 공격 트래픽으로 부상했다. 공격 특징은 네트워크나 개인 호스트의 리소스를 고갈 시켜, victim 네트워크나 호스트에 접속 할 수 없도록 한다. DDoS의 특징은 flash crowd와 같은 정상적인 인터넷 사용 트래픽과 구별이 되지 않고, 명확한 패턴이 없기 때문에 탐지하기가 어렵다. 또한 공격자가 좀비와 같은 감염된 호스트를 통해서 간접 공격을 하기 때문에 공격 시작지를 찾았다고 해도 실질적인 공격자는 찾을 수가 없다. 이러한 특징 때문에 DDoS에 대한 연구가 많이 이루어졌지만 아직까지도 명확한 대응 방법은 개발되지 않고 있다. 대부분의 DDoS 대응 시스템은 DDoS 방어지점에 전체적으로 트래픽을 감소시켜 네트워크를 보호하는 것이 대응책이다. 기존과 같이 공격 트래픽에 대한 무분별한 threshold 감소가 아닌, 검증된 source IP address를 사용한다면 합법적인 clients의 연결을 보호하면서 DDoS 공격을 차단할 수 있다.

2. 관련 연구

2.1 Signature 기반 탐지 방법

Snort와 같은 signature 기반의 Intrusion Detection System (IDS)은 공격 패턴을 미리 정의해 놓고 rule를 가지고 탐지한다. 이러한 탐지 기법은 rule에서 정의한 패턴에 정확히 일치해야만 탐지가 된다. 또한 여러 가지 rule 중에 네트워크에 실제 필요한 것을 설정하는 것도 중요하다. 그렇지 않으면 네트워크에 영향을 주지 않는 의미 없는 경보를 무수히 발생한다.

2.2 통계기반 탐지 알고리즘

DDoS는 여러 가지의 공격 형태를 띄고 있어서 합법적인 패킷과 구분하기 어렵고, 각각의 공격 source에서 보내는 패킷의 양이 적기 때문에 local 관리자가 쉽게 탐지할 수 없다. 따라서 이를 탐지하기 위해서는 통계적인 방법을 사용하는 것이 가장 효율적이다.

통계적인 탐지 알고리즘에는 패킷 속성값의 엔트로피(entropy)나 카이 제곱 (Chi-Square) 검증법등이 사용되고 있다.[1] 이중 엔트로피 연산법은 어떠한 네트워크 속성값에 대한 임의성(randomness)를 계산한 뒤, 그 값의 평균의 변화량을 탐지하는 방법이다.

$$H = -\sum_{i=1}^{n} \pi \log \pi$$

[수식 1] 엔트로피 연산법

수식1의 공식은 n개의 속성값(ex. Source address, destination address)에 대한 엔트로피 H를 구하는 공식이다. 여기서 pi는 i번째의 속성값이 선택될 확률을 나타낸다.

카이 제곱 검증법은 속성값에 대한 분산도를 측정하는 방법이다. 여기서는 기대값에 대한 분산도를 계산하여 그 값에 따라 비정상적인 속성값을 탐지할 수 있다. 이 방법의 구체적인 식은 다음과 같다.

$$x^2 = \sum_{i=1}^{B} \frac{(N_i - n_i)^2}{n_i}$$

[수식 2] 카이-제곱 테스트

여기서 B는 샘플 패킷들이 가질 수 있는 값들을 묶어 놓은 binning 값이다.(ex. 패킷길이는 0-64, 65-128, 129-255로 binning 될 수 있다) N_i는 N개의 샘플 패킷에서 각각의 binning 범위에 속하는 패킷의 개수고, ni는 일반적인 분포에서 binning에 속하는 기대값이다.

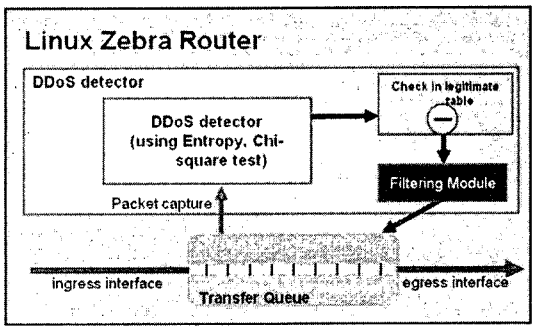
$$\sum_{i=1}^{n} PAT[i] - PAT[i-1]$$

[수식 3] Traffic volume

수식 3은 패킷이 이더넷 카드에 도착하는 시간을 계산하는 것이다. 각각의 패킷이 도착하는 시간을 측정하여 그룹단위로 패킷이 도착한 시간을 합한다. 즉 Traffic volume 값이 낮을 수록 이더넷 카드에 도착하는 패킷의 수가 증가했다는 것을 의미한다.

3. 제안 사항

3.1 Linux Zebra 라우터 기반 침입 탐지



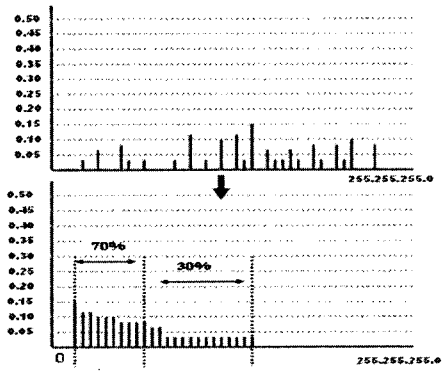
[그림 1] Zebra router기반 DDoS 탐지 대응 시스템

그림 1은 리눅스 Zebra router에 통계기반의 DDoS 탐지 모듈을 설치한 구조이다. Entropy와 Chi-square 알고리즘을 사용하여 DDoS를 탐지하고 Filtering 모듈에서을 트래픽을 차단 한다. 여기서 check in legitimate table 모듈은 검증 IP table에 있는 정보를 가지고 현재 차단하려는 트래픽에서 검증된 source IP addresss를 제외한다. 그리고 나머지 source IP address는 filtering 모듈에서 필터링한다.

3.2 검증 IP table

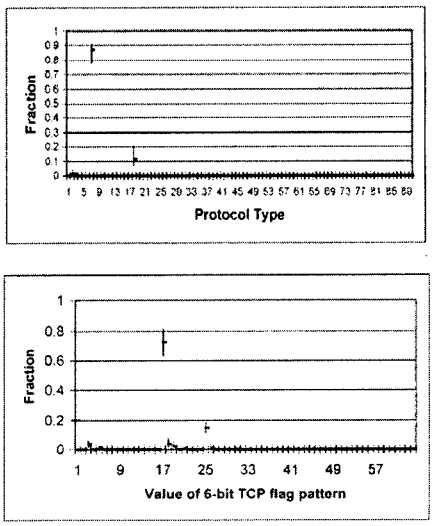
네트워크나 호스트에서 측정한 트래픽 통계를 분석하면, 전날 나타났던 IP의 80%-90% 반복해서 나타나는 것을 알 수 있다[2]. 즉 통상적으로 80%정도의 clients는 지속적으로 특정 네크워크나 호스트에 접속한다는 것을 의미한다. 이러한 통계를 가지고, IP address에 대해서 높은 발생 빈도 순으로 정렬 한다.

그림 2는 source IP address의 네트워크 prefix 별로 정렬한 것이다. 여기서 70%라는 값은 전체 트래픽에서 빈도수 별로 누적합을 의미한다. 또한 여기 70%안에 있는 네트워크 prefix는 여러 가지 검증의 대상이 되고 모든 검증이 끝났을 경우 검증 IP table에 등록된다.



[그림 2] Source IP 빈도에 의한 정렬

3.2.1 유용한 확률



[그림 3] TCP flag 값과 Protocol별 빈도

그림 3은 일정 기간 동한 측정된 전체 트래픽에서 TCP flag의 분포와 Protocol의 분표를 보여주고 있다[3]. Protocol 별로 분석해보면 7번인 TCP가 거의 대부분을 차지 한다는 것을 알 수 있고 TCP flag의 분포에서는 ack값이 가장 많고, syn 메시지는 지극히 적다는 것을 알 수 있다.

3.2.2 T-test

단순히 빈도수가 높다는 이유만으로 합법적인 source IP address라고 하기에는 지극히 위험하다. 통계를 내기 위해 측정한 트래픽의 특정 IP에서 높은 트래픽을 유발

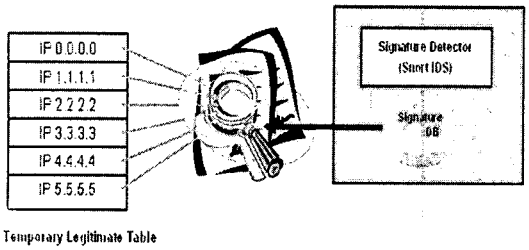
시키는 DDoS 공격이 발생했었다면 당연히 그 source IP는 높은 빈도수를 나타낼 것이다. 이러한 비정상적인 source IP를 판별하기 위해 T-test를 사용한다

$$T=\sum_{i=1}^{n}\frac{(\overline{X_i}-\mu_i)}{S/\sqrt{n}}$$

[수식 4] T-test

수식4는 T-test를 나타낸다. T-test는 통계 측정을 위해서 무작위로 추출한 표본이 전체 표본과 유사한가를 검증하는 것이다. 이는 빈도수가 높은 source IP의 속성값(udp, tcp, icmp 등)이 전체 트래픽의 속성값과 비교해서 유의성을 판단하다. 여기서 차이가 많이 날 경우 검증 IP table에서 제거한다.

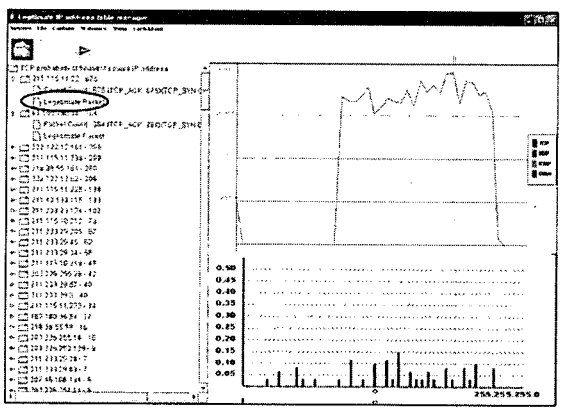
3.3 스노트 기반 abnormal IP 검사



[그림 4] 스토트 alert의 source IP address 검사

그림 4는 임시 합법 테이블에 있는 IP와 스노트[4] alert리스트에 있는 IP를 검사하는 것이다. 통계적 유의성 검증으로는 합법적인 IP로 검증 됐지만, port scan이나 tiny fragment와 같은 DDoS의 전 징후를 보이는 침입 형태에 대해서도 검증할 필요가 있다. 또한 worm이나 troian 처럼 해킹에 의한 침입에 대해서도 확인해야 한다. 이처럼 통계적인 유의성 검증과 signature의 검사에서 비정상 판정이 되지 않은 source IP address만 검증 IP table에 등록한다.

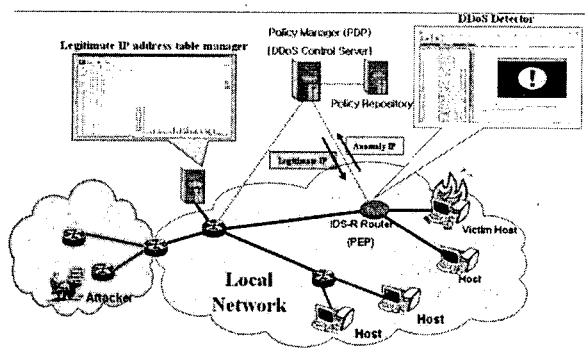
3.4 검증 IP table 모듈



[그림 5] 검증 IP table 모듈

그림 5는 검증 IP table 모듈을 보여준다. 통계적인 방법으로 분석된 source IP 목록을 높은 빈도 값을 기준으로 위에서부터 정렬되어 있다. 이렇게 정렬된 IP는 T-test와 스노트 signature 검사를 통과하여 합법적인 IP로 등록된다.

4. 검증 IP table를 사용한 DDoS 대응 시스템



[그림 6] DDoS 대응 시스템 구조

그림 6은 전체 망 구성도를 나타낸 것이다. 검증 IP table 모듈은 라우터에서 splitter를 사용하여 트래픽을 측정하고 분석한다. 여기서 만들어진 검증 IP table은 네트워크의 모든 보안 시스템을 관리하는 Policy Manager에게 보내지고 DDoS를 탐지한 라우터에게 이러한 정보를 보내준다.

5. 결론

본 논문에서는 기존의 DDoS 공격방어에서 나타날 수 있는 문제점을 제시하였고, 이에 관한 해결방안을 제시하였다. 제안한 라우터 기반의 탐지 시스템을 구현하여 보다 동적으로 침입에 대응 할 수 있고, 검증 IP table를 사용함으로써 DDoS 대응시 합법적인 clients에게 일어날 수 있는 간접피해 문제를 완화 할 수 있을 것이다. 향 후 연구 과제로는 검증 IP table을 가지고 DDoS 공격 트래픽을 필터링 할 때 실질적으로 성능 면에서 유용한가에 대해서 실험할 계획이다. 또한 리눅스 라우터에서 iptables에 능동적으로 접근 관리하는 모듈의 설계 및 성능 평가를 수행할 예정이다.

5. 참고문헌

[1] Feinstein L., Schnackenberg D, Balupari R., Kindred D., "Statistical Approaches to DDoS Attack Detection and Response", DARPA Information Survivability Conference and Exposition(DISCEX 2003), April 22-24, 2003
[2] W.A.N.D.R.group http://wand.cs.waikato.ac.nz
[3] WIDE-project http://www.wide.ad.jp
[4] http://www.snort.org