트래픽 분석을 통한 효과적인 DDOS공격탐지방법

*정휘석[0] *이철호 *최경희 **정기현
*아주대학교 정보통신 전문대학원, **아주대학교 전자전기공학부
kitty@cesys.ajou.ac.kr[0] cheolholee@nate.com, (khchoi, khchung)@madang.ajou.ac.kr

Detection of Distributes Denial of Service Attacks through the analysis of traffic

Hui-Suk Jung[0] Kyung-Hee Choi Gi-Hyun Jung
*The Graduate School for Information&Communication Technology, Ajou University
** Division of Electical & Electronics Engineering Ajou University

요 약

DDOS공격은 최근 인터넷 환경에서 큰 위협요소로 부각되고 있다. 하지만, DDOS 공격을 완벽하게 막아내는 것은 현재까지 알려진 방법으로는 거의 불가능하다. 그 이유는 DDOS 공격이 Vulnerability Exploit을 이용한 공격방법이 아니라 Network Resource를 고갈시켜서 공격대상 호스트의 서비스를 차단하기 때문이다. 그래서, DDOS공격을 방어하기 위해서는 DDOS공격 트래픽에 대한 정확한 분석과 탐지가 선행되어야 한다. 본 논문을 통해서 여러 가지 DDOS공격 Traffic의 특징을 살펴보고, Web traffic과의 차이를 통해 DDOS traffic을 탐지하는 방법을 제안하고자 한다.

1. 서 론

몇 해 전부터 Yahoo, eBay등과 같은 유명한 웹사이트들이 서비스거부공격으로 인해 몇 시간씩 서비스를 중단하는 사태가 종종 나타나고 있다.[10] 이러한 서비스거부공격은 대량의 트래픽을 네크웍으로 흘려서 네트웍의 자원을 고갈시키고 이로 인해 정상적인 트래픽들에 대한 서비스를 못하게 하는 것이다.

최근 분산환경에서의 서비스거부공격도구들이 많은 시스템에 불법적으로 설치되고 있다. 이 해킹도구들은 대규모 네트워크의 많은 호스트에 설치되어 서로 통합된 형태로 패킷을 범람시켜 심각한 네트워크 성능저하 및 시스템 마비를 유발한다. 최근에 발견되고 있는 이러한 서비스거부 공격도구로는 trinoo와 TFN, TFN2K, Stacheldraht가 대표적이다.[11] 이러한 공격도구를 이용한 DDOS 공격 형태로는 UDP flood attack, TCP flood attack, ICMP flood attack, Smurf 등이 있다.[2][3][4][5][6]

이러한 DDOS공격 트래픽과 정상적인 서비스를 위한 트래픽을 구분해 내는 것은 쉽지 않기 때문에 정상적인 패킷을 DDOS 패킷으로 판단하고 DDOS 공격자의 의도대로 서비스를 못하는 경우가 생길 수 있다. 그래서 DDOS공격으로부터 시스템을 보호하기 위해서는 DDOS 공격 트래픽에 대한 정확한 분석과 탐지가 우선되어야 한다. 하지만, DDOS 공격은 짧은 시간 내에 대량의 네트워크 트래픽을 발생시켜서 네트워크 리소스를 고갈시키는 방식이기 때문에 정확한 탐지가 매우 힘들다.

본 논문에서는 DDOS의 주요 공격대상인 Web 서비스를 고려한다. 우선 DDOS 트래픽과 Web 트래픽의 특징을 살펴보고, DDOS 공격 시 트래픽의 pattern을 분석한 후 두 트래픽의 차이를 제시함으로써 DDOS공격탐지 방법을 제안하고자 한다.

본 논문의 2장에서는 DDOS 트래픽과 Web 트래픽의 특징 및 차이를 살펴보고, 3장에서는 이들의 특징을 이용한 DDOS 방어방법에 대해 언급할 것이며, 4장에서는 실험을 통해 이 방법들의 타당성을 분석할 것이다.

2. Background

이 장에서는 DDOS 트래픽과 Web 트래픽에 대해 분석하고, 그 차이에 대해서 논의하고자 한다. 그리고, DDOS 트래픽 parameter중에서 공격자의 의도대로 바뀔 수 없는 특성을 중점으로 분석한다. 이는 공격자가 DDOS 공격도구의 source code를 수정하였을 경우에는 이 분석에서 사용된 parameter, 공격 기능, 기타의 특징들이 얼마든지 변형될 수 있기 때문이다. 또한, 본 논문에서는 DDOS 트래픽과 Web 트래픽의 차이를 통해서 DDOS 공격에 대응하고자 하기 때문에 Web 트래픽과 공통parameter인 IP header값과 TCP header값에 대해서만 언급하겠다.

2.1 DDOS 트래픽의 특징

DDOS 트래픽 parameter는 randomized value와 specialized value로 구분할 수 있다. 즉, IP header와 TCP header에서 각 필드는 두 가지로 구분된다. 각 필드 중 Source IP, Source Port, Window size, Seq/Ack number가 random하게 구성되는 것이다.

우선 살펴볼 parameter는 Source IP이다. 일반적으로 공격자는 자신의 존재를 숨기기 위해서 IP Spoofing을 한다. 그래서 랜덤함수를 이용해서 Source IP를 생성한다.

또한, DDOS공격의 특성상 네트웍자원을 빨리 고갈시키기 위해 패킷 Length는 보통 프로토콜에서 허용하는 최소의 크기로 정해진다. 즉, 동일한 네트웍 자원을 소모

하는 DDOS Attack이라면 작은 size의 패킷을 다량으로 전송하는 것이 큰 size의 패킷을 소량으로 전송하는 것보다 공격의 측면에서 더 큰 효과를 거둘 수 있다. 그래서, 실제로 현재 널리 사용되는 DDOS공격도구에서는 DATA size가 0인 패킷을 공격에 사용하고 있다.

여러 가지 parameter에 대한 DDOS 트래픽 분석 결과 몇 가지 특징을 찾을 수 있었지만, DDOS만의 특징을 찾아내기에는 어려움이 있었다. 따라서, Web트래픽을 분석한 후에 Web 트래픽의 뚜렷한 특징을 살펴보고, 이를 이용해서 DDOS 트래픽과의 차이를 조사하겠다. DDOS의 일반적인 특징을 찾는 것도 중요하지만, 보호하려는 시스템의 특징에 적합한 parameter를 찾는 것이 필요하다.

2.2 Web 트래픽의 특징

보통 전체 TCP 트래픽에서 Web 트래픽은 전체 바이트의 75%, 전체 패킷수의 70%를 차지한다.[8] Web 트래픽을 두 가지로 구분하면 client 트래픽과 server 트래픽으로 구분할 수 있다. client 트래픽은 전체 트래픽 중에서 패킷 fractions (30~38%), byte fractions (6~8%)이다.[8] 즉, client 패킷은 평균 67byte로 작다는 것을 알 수 있다. 이는 HTTP reply는 길지만, 이에 해당하는 HTTP request는 짧기 때문이다. 이에 비해 Server 트래픽은 전체 트래픽 중에서 패킷 fractions(30~35%), byte fractions (55~70%)을 차지한다.[8]

그리고, Web 트래픽은 HTTP protocol을 이용하고 TCP 기반으로 이루어 진다. Web Client와 Web Server는 TCP connection을 생성하고, 해당 HTTP request가 해당 Web Server에게 전달되고 그에 대한 응답으로 Web Server는 요청 받은 문서를 Client에게 전송하고 전송이 완료된 후에는 TCP connection을 종료한다[7]. 이처럼, HTTP는 TCP를 기반으로 한 프로토콜이므로, Web 트래픽에서 일정시간 내에 같은 Source IP를 가지고 들어오는 패킷들이 여러 번 나타난다. 이는 최소한 한 패킷이 들어오면 Connection을 맺어서 Data를 받기까지 해당 Source IP를 가진 패킷이 여러 번 들어온다는 것을 의미한다.

2.3 DDOS 트래픽과 Web 트래픽의 차이점

그림1에서 보듯이 Web 트래픽은 특정 Source IP대의 분포가 높게 나온다.[9] 즉, address 빈도수가 고르지 않고 특정 몇 군데의 address가 많은 빈도수를 가진 것을 알 수 있다.

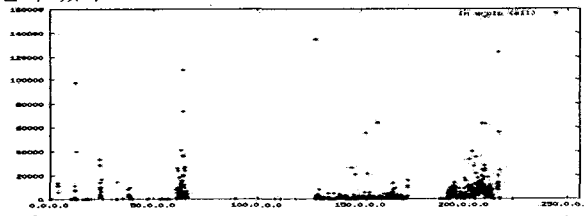

그림1. Source IP address distribution of normal incoming traffic for web site[9]

이에 비해, DDOS 트래픽의 분포는 그림 2에서 보듯이 address의 빈도수가 uniform한 형태를 보여주고 있다. 이는 DDOS 특성상 Source IP address를 random하게 생성함으로써 생기는 현상이다.

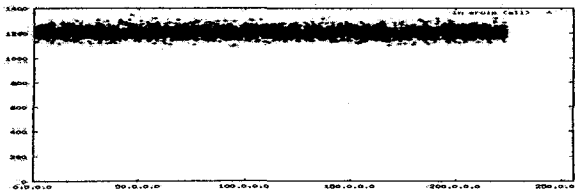

그림2. Source IP address distribution of normal incoming traffic during DDoS[9]

두 트래픽의 차이를 보면, 우선 Web 트래픽은 단위시간당 들어오는 패킷들의 source IP의 분포가 넓게 퍼져있지 않고, 그 빈도수도 DDOS 트래픽에 비해 훨씬 작다. 이에 비해 DDOS는 단위 시간당 들어오는 패킷들의 Source IP의 분포가 넓게 퍼져있고, 그 빈도수도 Web 트래픽에 비해 훨씬 많다. 이는 DDOS 트래픽에서 일정시간 내에 같은 source IP가 중복될 경우는 거의 없다는 것을 알 수 있다.

본 논문은 Source IP를 유용한 parameter로 선정했다. 그 이유는 DDOS 트래픽에서 specialized parameter는 항상 일반적인 DDOS의 특징이라고 보기 힘들다는 것이다. 왜냐하면 specialized parameter들은 언제든지 공격자의 의도에 따라 변할 수 있기 때문이다. 하지만, DDOS의 특징상 Source IP address는 특정 값으로 정해질 수 없다. 이는 분명히 공격의 목적을 달성하기 위한 속성이라 볼 수 있다. 즉, DDOS 공격은 공격자의 위치를 숨기고 victim에게 큰 피해를 주는 것. 즉, IP spoofing은 필연적으로 가질 수 밖에 없는 속성이기 때문이다. 그리고, 그림 1와 2의 분포상의 차이를 잘 이용할 수 있다.

3. 본론

본 논문에서 제안하는 방법은 단순히 프로토콜의 특징이 아닌 DDOS 트래픽과 Web 트래픽의 차이를 이용하는 것이다. 앞에서 충분히 두 트래픽의 특징을 살펴봤고 그 결과로 input packet의 source IP의 분포가 현저히 차이가 나는 것을 보았다. 여기서 우리가 이용하고자 하는 개념은 짧은 시간 동안 Web 트래픽에 비해 DDOS 트래픽은 Source IP의 분포가 넓게 퍼지고, 그 빈도수도 월등히 많다는 것이다. Router로 들어오는 패킷들의 Source IP를 monitoring하면 이러한 트래픽의 분포를 찾아낼 수 있다. 이러한 분포의 차이를 이용해서 DDOS 공격을 탐지하는 방법을 제안하고자 한다.

3.1 Source IP를 이용한 DDOS 공격 탐지

본 논문은 Source IP address의 monitoring하기 위해 LRU queue를 이용하고자 한다. LRU queue의 특성상 계속해서 다른 값이 들어오면 queue의 replacement가 자주 일어나게 된다. 즉, Web 트래픽만 있을 때에는 queue에 miss할 확률이 적고, replacement도 자주 일어나지 않게 된다. 하지만, DDOS 트래픽이 발생하게 되면 queue는 잦은 replacement를 하게 된다. 이런 LRU queue의 특성을 이용해서 DDOS 공격을 탐지할 수 있다.

DDOS detector는 PCAP library를 이용해서 패킷을 capture하고 이 패킷의 header에서 Source IP를 추출해서 이를 LRU queue로 관리한다. Watcher system은 이 queue를 monitoring하게 된다. Queue size의 변화,

replacement rate, 전체 패킷수 등을 일정시간 간격으로 분석하고, 이 통계값들은 공격탐지에 이용된다.

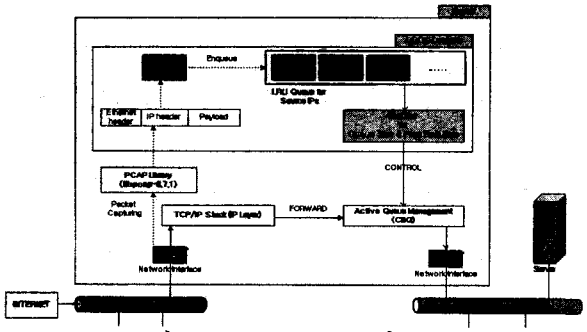

그림 3. DDOS Detector의 구조

실험을 통해 LRU queue의 단위시간당 replacement 분포의 변화를 알아보고 그 의미를 분석하겠다.

4. 실험 및 분석결과

본 논문의 실험환경은 그림 4와 같다. DDOS 공격도구로는 TFN2K를 사용했고, Web server의 앞 단에 있는 Router에서 실험을 하였다.

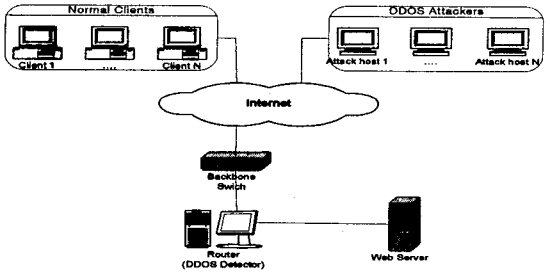

그림 4. 실험환경

4.1 Source IP를 이용한 DDOS 공격 탐지 실험 분석

이 실험에서는 LRU Queue의 최대크기를 100으로 설정했다. 하지만, 일반적인 상황에서 더 많은 사용자가 접속하는 서버에 대해서 이 방법을 적용할 경우 더 크게 설정해야 할 것이다. 주의해야 할 것은 MAX_QUEUE의 크기는 256보다는 작아야 한다. 왜냐하면, 몇몇 DDOS 공격도구에는 IP Spoofing Level 설정기능이 있기 때문이다. 이 기능은 공격자가 자신이 Spoofing할 수 있는 네트워크 주소대역을 탐지해낼 수 있으며 A.B.C.D 의 네트워크 주소에서 D영역만Spoofing 할 수 있게 하는 것이다.

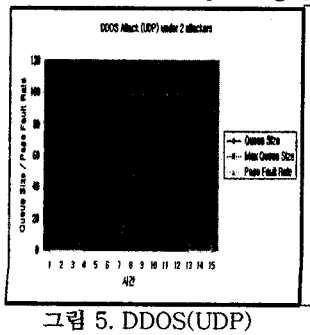

그림 5. DDOS(UDP)

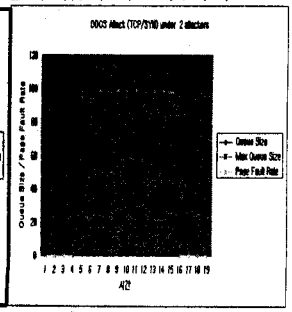

그림 6. DDOS (TCP)

그림 5,6은 각종 DDOS 공격이 발생할 때 monitoring 한 결과이다. 이 실험의 결과는 LRU queue에서 1초당 replacement 분포의 변화를 나타낸다.

DDOS공격이 없는 상황에서는 비록 많은 수의 패킷이 발생한다 하더라도 단위시간당 Source IP의 개수가 아주 작다. 이 실험에서는 20개 미만으로 나타난다. 하지만, DDOS공격이 벌어지게 되면 Spoofing된 Source IP를 가진 공격 패킷이 발생하게 되어 Source IP의 개수가 Queue의 최대크기를 초과하게 되며 Replacement가 발생한다. 이것을 통계적 수치로 살펴보면, Replacement Rate가 거의 100%에 가깝게 나타난다. 따라서, DDOS공격을 탐지하는데 매우 유용하게 사용할 수 있음을 알 수 있다.

5. 결론 및 향후 과제

본 논문에서 제안하는 DDOS 트래픽 탐지방법은 네트웍의 트래픽의 분석을 통해 나타나는 특징을 이용한 것이다. 즉, DDOS 트래픽과 Web 트래픽 각각의 분석을 통해 몇 가지 특징을 찾아보았고, 이중에서 가장 적합한 parameter로 Input 패킷의 Source IP를 선택하였다. 그리고, 각 트래픽에서 Source IP의 분포차이를 자세히 살펴보았고, 이를 이용하는 방법을 제안하였다. 우리가 제안한 방법은 우선 DDOS 트래픽 탐지를 위해 단위 시간당 LRU queue size의 변화와 replacement rate를 monitoring하고, 이러한 정보를 이용해서 DDOS 트래픽을 탐지에 이용한다. 향후에는, 본 논문에서 제안한 DDOS 탐지방법을 기반으로 하여 방어방법을 제시할 것이며 이는 DDOS 트래픽을 판정하고, DDOS 트래픽을 구분해 낼 수 있도록 해야 할 것이다. 즉, 제안된 방법으로 구한 정보를 가지고 실제 QM를 제어함으로써 트래픽 control이 가능할 것이다.

6. 참고문헌

[1] David Moore, Geoffrey M. Voelker and Stefan Savage, "Inferring Internet Denial-of-Service Activity", Usenix Security Symposium, 2001.
[2] Tribe FloodNet - 2k edition (TFN2K) by Mixter, DDOS Attack Tool.
[3] Trinoo, DDOS Attack Tool.
[4] Stacheldraht Flood Network, DDOS Tool.
[5] Syn Flooder by Zakath, DDOS Attack Tool.
[6] TFN2K - An Analysis, Jason Barlow and Woody Thrower, AXENT Security Team February 10, 2000
[7] RFC 2616, "Hypertext Transfer Protocol -- HTTP/1.1", IETF, June 1999.
[8] Kevin Thompson, Gregory J. Miller, and Rick Wilder, "Wide-Area Internet traffic Patterns and Characteristics" (Extended Version)
[9] Massimiliano Poletto, "Practical Approaches to Dealing with DDoS Attacks", May ,2001
[10] L. Garber, "Denial-of-Service Attack Rip the Internet", Computer, April 2000.