DDoS 공격에 대한 사전탐지 기법을 이용한 지역적인 방어 모델

박성욱*, 예홍진*
*아주대학교 정보통신전문대학원
e-mail:{mabus666, hjyeh}@ajou.ac.kr

The regional defense model using early detection mechanism for against DDoS attack

Sung-Wook Park*, Hong-Jin Yeh*
*Graduate School of Information and Communication, Ajou University

요 약

본 논문에서는 DDoS 공격 패킷을 사전에 탐지하고 트래픽 제어를 하기위한 방안을 제안한다. 제안된 모델은 공격대상에서 멀리 떨어 진 라우터에서 낮은 임계치를 적용하여 탐지 하게 되며 지역 연합 모델을 통한 지역적인 방어 행동을 취하게 된다. 사전에 취해지는 방어 행동으로 인해 본 시스템은 좋은 성능을 발휘 할 것이다. 시스템의 각 지역연합들은 DDoS 공격의 악의 적인 트래픽의 양을 줄이는 것에 기여 할 것이다.

1. 서론

2000년대 이후 DOS 공격의 진화된 형태인 Distributed DOS 공격이 등장하여 네트워크 보안에 큰 이슈가 되고 있다. 지금까지 DDoS 공격에 대한 많은 연구가 이루어지고 있고 많은 대응 방안들이 제안 되었지만, 현재 네트워크 환경아래에서 완벽하게 DDoS 공격을 차단하는 방안 은 제안 되지 못하고 있다. 그 이유는, DDoS 의 특성상 대량의 트래픽을 일시에 공격 대상에게 집중 하므로 써, 네트워크의 자원을 고갈시켜 공격대상 호스트를 차단하고, 또한 한 호스트에 능력만으로는 그것을 제어 할 수 없기 때문이다. 여기서 중요한 점은, DDoS 이전의 다른 공격들은 공격대상에게 만 피해를 입히고 공격이 성공 했을 시에만 사용자에게 피해를 줄 수 있었다. 하지만 DDoS 공격은 공격 하는 그 순간부터 이미 사용자에게 피해를 입히고 있고 공격대상뿐만 아니라, 공격 대상의 주변 네트워크 까지도 심각한 피해를 입힌다. 그것은 다량의 패킷을 공격대상에게 전송함으로써, 공격대상은 물론 공격대상으로 가는 길(route)이 갖고 있는 자원을 소모하기 때문에 그 길을 공유하는 사용자에게는 이미 그것으로 공격이 가해지고 있는 것이 된다. 또한 DDoS는 공격 시작 시 많은 zombie 컴퓨터로부터 공격이 가해지기 때문에 zombie computer의 사용자등도 심각한 피해를 받으므로 중대한 공격이라 할 수 있다. 따라서 DDoS 공격의 해결책으로, 기존처럼 공격대상에서 방어의 경보와 제어를 갖기 보다는 조금 더 공격자와 가깝고, 공격목표대상에서 떨어진 쪽에서 먼저 발견하고 먼저 대응하는 쪽이 전체적인 네트워크의 피해를 줄인다는 입장에서 나은 방법이라 할 수 있겠다. 우리는 본 논문에서 이러한 방어를 할 수 있는 모델을 소개하고 어떻게 악의적인 공격자로부터 네트워크의 자원 소모를 줄이는지 그리고 어떻게 이것들이 모여 하나의 큰 DDoS 방어막이 될 수 있는지 보여줄 것이다.

2. 관련연구

2.1 Detection of DDoS

DDoS 공격이 시작 되면 네트워크 트래픽의 흐름이 그렇지 않을 때와는 다른 양상으로 변할 것이다. 여기서는 이러한 트래픽 흐름의 변화 또는 대다수 트래픽의 특징 변화를 이용하여 탐지 하는 방법을 소개 한다.

대부분의 DDoS 에서는 공격자의 위치가 드러나는 것을 막기 위해 DDoS 의 공격 packet안의 Source IP Address를 Spoofing 해서 사용한다. 여기서 Spoofing 된 IP 는 random한 특징을 갖고 있다, 따라서 이러한 특징을 이용하여 DDoS를 초기에 빠르게 탐지 할 수 있게 고안된 기법이 Kolmogorov Complexity라는 DDoS 공격 탐지 기법이다. 이 방법은 일반적인 상황에서는 지역성을 갖고 있다. 하지만 공격이 시작 되면 Source IP 의 address 가 spoofing 되기 때문에 평상시와 많은 차이를 보이는 특성을 이용하여 탐지 한다.

평상시 TCP 연결의 생성과 종료는 거의 동일한 비율로 발생한다. 따라서 SYN 플래그를 갖은 패킷과 FIN 플래그를 갖은 패키의 비율은 거의 동일하게 나타난다. 하지만 SYN Flooding 공격이 발생한다면 대량의 SYN 플래그를 가진 packet이 급격히 증가 할 것이다. 여기서 SYN 플래그의 비율이 FIN 의 비율보다 월등히 높아지는 이러한 성질을 이용해서 탐지 하는 방법이 'TCP SYN-FIN pairs' 방법과 'Intensity measure of SYN segment' 방법 등이 있다. 이러한 방법들은 여러 공격 유형 중에서 SYN Flooding 방법에 특화된 탐지 방법 들이다.

2.3 Defense mechanism

DDoS 의 공격 packet을 막는 방안은 다양하게 제안되었다.

Rate limit 방법은 ICMP flood attack 과 SYN flood attack을 막을 때 사용한다. Management 를 통해 해당 패킷의 rate limit를 미리 정해 놓고 그 이상의 패킷은 drop 시키는 방법이다. 이는 파라미터의 설정에 따라서 뛰어난 성능을 발휘할 수도 있지만, 정상적인 패킷에 대해 정상적인 service 해주지 못할 수도 있다. 현재 Cisco router 에 적용되어 사용되어 지고 있다.

Ingress and Egress filtering 방법은 border 라우터에서 들어가고 나가는 패킷을 관찰하여 들어가고 나가는 패킷들의 발생지 주소와 목적지 주소를 보고 패킷의 비정상 여부와 주소 위조 여부를 판단해서 filtering 한다. 또한 DDoS 공격 packet이 외부로 나가는 것을 Egress filtering을 통해 막을 수 있다.

Unicast RPF(reverse path forwarding) 방법은 IP address spoofing 이나 SMURF attack 을 막 을 때 사용한다. 이 방법은 라우터로 들어오는 각각의 packet을 조사해서 만약 source IP address 가 packet이 도착한 동일한 인터페이스를 지정하고 있는 CEF(Cisco Express Forwarding) 테이블 내에 routing 정보를 갖고 있지 않다면, 라우터는 해당 packet을 drop 시킨다.

이 이외에도 중간에 거쳐 온 라우터들에서 packet 의 특정 필드에 marking을 함으로써 문제가 될 packet 을 drop 시키는 packet marking 기법, 패킷의 흐름을 실시간으로 모니터링 하면서 갑작스런 트래픽의 집중을 탐지 해내고 해당 Source IP 로 부터 오는 packet 을 Class Type 으로 구분하여, 각 Class 별로 CBQ 와 ipchains 을 사용해서 비정상적인 Class Type 의 packet을 막는 방법 등 많은 기법들이 제안되었지만 이 논문에서는 최근에 가장 타당성 있는 방법으로 인식되고 있는 공격 발생 시에 라우터의 출력 대역폭(bandwidth) 을 조절함으로써 전달되는 패킷의 양을 조절하는 라우터 기반의 rate limit 기업을 사용한다고 가정한다.

3. 사전 탐지 과정

이제까지의 DDoS의 방어에서는 대부분 독립된 어떤 공격대상의 상위 node 단계에서나 아니면 그 victim 호스트 자체에서 방어를 하였다. 그 호스트나 victim의 상위 node 는 탐지 메커니즘에 의하여 탐지를 하고 그것에 맞게 공격에 대하여 rate limit 를 하거나, 필터링을 하였다. 하지만 우리가 살펴 본대로, DDoS 는 그러한 방법으로 막을 수 있는 공격이 아니다. 그 이유는 다음과 같다.

1) 자기가 소속돼있는 회선의 bandwidth 를 모두 탐지하고 대응하기 위해서는 시스템의 오버헤드가 너무 크다. 따라서 이 경우에도 DDoS 공격의 소기의 목적은 달성되었다고 볼 수 있다.

2) 충분히 큰 bandwidth 를 갖고 있는 탐지시스템이라면 하나의 독립된 시스템으로는 절대 DDoS 의 모든 트래픽을 제어 할 수 없다. 따라서 이 경우 또한 공격은 성공 한다.

3) 한 노드에서 다양한 모든 종류의 DDoS 공격을 탐지 하고 막을 수 없다.

4) victim 근처의 여러 노드들이 협력하여 하나의 특정한 공격 대상을 보호 한다 하더라도 일순간 다

량의 트래픽이 몰려 bandwidth를 점유 하고 말 것이다. 그러한 이유로 사전 탐지에 필요성이 제기 되는 것이다. 본 논문에서 제안 하는 탐지 모델은 [그림 1] 과 같다.

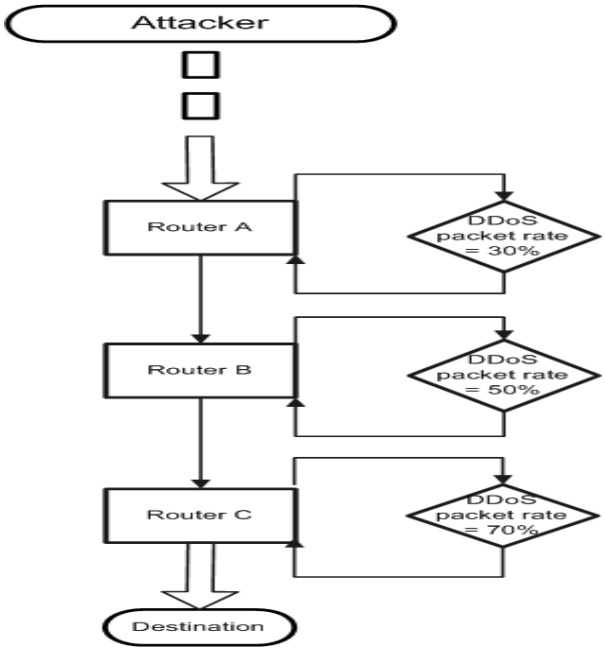

그림 1 . 단일 형태의 임계치 조정 모델

그림에서와 같이 사전 탐지 모델은 자신의 라우팅 테이블에서 알려진 대상에 대하여 홉 거리를 알 수가 있다. 따라서 이 정보를 바탕으로 남은 홉 수에 따라 차등적이 임계치를 부여하여 탐지율을 높임으로 공격 대상으로부터 먼 위치에서 사전에 탐지를 할 수가 있다.

[그림 1]에서는 단순 임계치의 부여는 사전에 탐지율을 높일 수는 있지만 그 만큼 false positive 의 비율을 높이는 결과를 낳게 된다. 따라서 false positive 의 비율을 줄일 수 있는 방안을 필요로 하게 된다. [그림 2] 는 false positive 를 줄기위한 재검증 단계를 포함한 모델이다.

DDoS 공격은 여러 방향의 목적지에서부터 소수의 공격 대상을 향해 패킷을 보내는 과정에서 생겨나는 공격 이라는 특징이 있기 때문에 실제적으로 공격 발생 시 한 방향으로부터 만 공격 패킷이 전달되는 것이 아니다. 따라서 [그림 2]에서처럼 Router D에서 또한 탐지 할 수 있을 것이다. 그림과 같이 Router A와 D에서 공격을 탐지하였다면 이 정보는 Router B로 전달되어 Router B는 더 정확한 정보를 가지고 Router A, D 에게 패킷에 전송을 막는 Rate limit 제어를 요청 할 수 있게 된다. 이와 같은 확인을 통한 기법은 빈번한 경보의 신뢰성을 재고하고 시스템의 성능을 높여 줄 것이다. 또한 정보를 받는 하부 라우터의 수가 많다면 그 만큼 정확한 정보임을 알 수 있을 것이다.

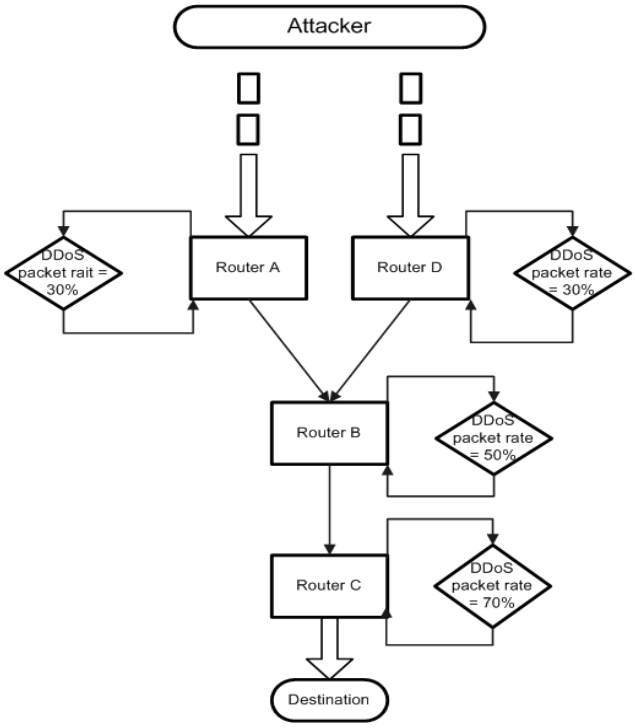

그림 2. False Positive 예방을 위한 다중 확인모델

4. 지역 연합을 통한 방어 기법

DDoS 는 다양한 종류의 아주 많은 컴퓨터가 일시에 공격을 시작하는 기법이다. 그렇다면 방어 자 또한 그러한 것을 막기 위해서는 자신만의 능력으로는 한계가 있을 것이다. 따라서 방어자 또한 공격자만 큼은 아니어도 많은 컴퓨터 끼리 연합을 하여야 한다. 이러한 연합을 지역 연합이라 부르기로 하겠다.

[그림 3] 같이 지역에 3개 이상의 지역 라우터들이 연합을 하여 [그림 2] 와 같이 경보 정보를 보내고, 그에 따른 제어 정보를 받을 수 있다면 이것을 하나의 지역 연합이라 볼 수 있다.

[그림 3] 은 한 라우터가 사전 탐지를 통한 경보 정보를 목적지 방향의 다음 라우터에게 보내 주고 다른 라우터 또한 같은 탐지를 하였을 때 경보를 받은 라우터가 이전 라우터들에게 제어를 지시하는 과정이다. 이렇게 되기 위해서는 라우터 들 끼리 서로가 신뢰 하는 인증을 이루어야만 한다. 이러한 신뢰 과정이 믿을수 없다면 또다른 DoS 공격의 빌미를 제공 할 수도 있다.

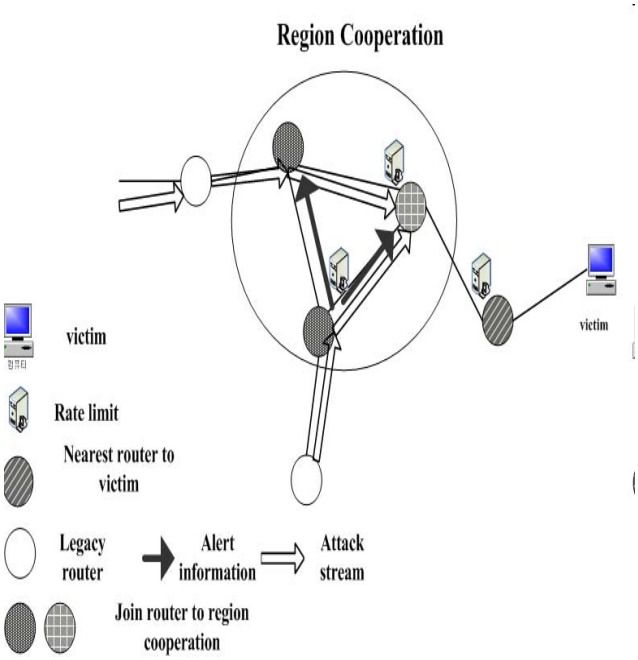

그림 3 . 지역 적인 연합을 통한 방어 모델

이러한 지역 연합은 공격 대상을 향하여 [그림 3] 같이 한 방향 뿐 만 아니라 다양한 방향으로 퍼진 형식으로 나타 날수도 있다.

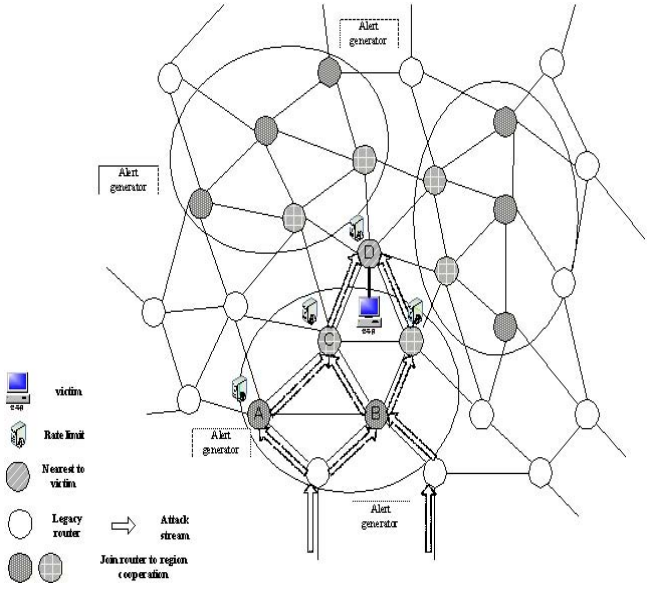

그림 4 . 지역 연합들의 자체 적인 방어 형성

목적지까지의 홉 수 만 알 수 있는 거리에 있다면 [그림 4] 와 같이 공격 대상을 감싸서 DDoS 공격 패킷으로부터 먼저 공격에 대응하고 사전에 차단할 수 있는 기능을 발휘할 수 있을 것이다.

5. 결론

DDoS 공격은 단지 공격 대상이나 대상 앞단의 장치 들이 막기에서는 역부족인 공격이다. 본 논문에서는 탐지에 관한 임계치를 조정 하여 공격 패킷이 공격대상 에게 전달되기 이전에 탐지를 통해 좀 더 초기에 방어를 하기 위한 제안 을 하였다. 따라서 많은 node 들이 공격 발생 초기부터 협동을 하여 공격 트래픽에 대하여 제어를 하여야 공격을 막을 수 있다. 이에 따라 탐지율을 높이기 위한 방안과 이러한 라우터들의 협동 관계를 모델링 하였다.

6. 향후 연구 과제

본 논문에서는 DDoS를 사전에 탐지 하고 지역 연합을 통하여 공격을 막는 방안을 제안 하였다. 향후 시뮬레이션을 통해 임의의 임계치의 가장 적합한 값을 찾는 것과. 다양한 네트워크의 구성상에서 지역연합의 자세한 규칙 또는 상호 인증에 관한 연구가 필요 할 것이다.

참고문헌

[1] J. Mirkovic., M. Robinson., P. Reiher., and G. Kuenning.: Alliance Formation for DDoS Defense. Proceedings of the New Security Paradigms Workshop, ACM, SIGSAC, August 2003.

[2] Jelena Mirkovic., Max Robinson., Peter Reiher., George Oikonomou.: Distributed Defense Against Ddos Attacks. University of Delaware CIS Department Technical Report CIS-TR-2005-02. Also submitted to INFOCOM 2005.

[3] Pete Perlegos.:DoS Defense in Structured Peer-to-Peer Networks. August, 2003, Berkeley, CA, USA.

[4] J. Mirkovic., M. Robinson., P. Reiher.: DefCOM: Defensive Cooperative Overlay Mesh. Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), 2003, IEEE.

[5] Kevin J.Houle., George M. Weaver.: Trends in Denial of Service Attack Technology. CERT Coordination Centoe, October 2001.