Active Edge 라우터 기반의 분산서비스거부공격 대응기법

김정태*, 김원일**, 김동규*
*아주대학교 정보통신전문대학원
**세종대학교 컴퓨터공학과
e-mail:coolpeace@ajou.ac.kr

DDoS Defense Mechanism based on Active Edge Router

Jungtae Kim*, Wonil Kim**, Dong-Kyoo Kim*
*Graduate School of Information Communication, Ajou Univ.
**Dept of Computer Engineering, Sejong University

요 약

지난 몇 년간 DDoS 공격의 기법들은 더욱 복잡해지고 효과적으로 변하였으며, 공격자를 추적하기는 더욱 힘들어지고 있다. 이러한 문제들에 대응하기 위해 다양한 패킷 필터링 기법과 공격자 추적 기법 등 많은 연구들이 진행되어 왔다. 하지만 이러한 노력에도 불구하고 DDoS 공격은 여전히 인터넷의 안정성을 위협하는 요소로 작용하고 있다. 따라서 본 논문에서는 이러한 위협에 대응하기 위하여 Active Edge 라우터 기반의 분산 서비스 거부공격대응 기법을 제안하고자 한다. 제안된 방법의 경우 기존의 중간 라우터(intermediate-router)의 오버헤더, 공격경로 재구성에 필요한 오버헤더, 재구성된 공격경로의 부정확성과 같은 기존의 기법들이 지니고 있던 단점들을 보완하고 있다. 또한 제안된 방법의 경우 공격 패킷을 공격대상 네트워크가 아닌 공격자가 위치하고 있는 네트워크에서 제거함으로서 공격패킷의 필터링 효과를 더욱 향상 시켰다.

1. 서론

분산 서비스 거부 공격(DDoS: Distributed Denial of Service attack)공격은 기존의 서비스 거부 공격과는 다른 형태의 공격방법으로, 네트워크나 대상시스템의 취약점에 의존하지 않고 단순히 많은 패킷을 대상시스템에 전송하는 방법을 통해 공격을 수행한다. DDoS 공격의 특징은 공격의 대상이 엄청난 수의 패킷들로 인해 정상적인 서비스를 제공하지 못한다는 것이다. 정상적인 상황의 경우, 서비스를 요구하는 패킷의 양이 증가 할수록 서비스를 제공하는 시스템의 효율성은 증가 하게 된다. 하지만 패킷의 양이 네트워크 혹은 시스템의 처리 용량을 초과할 경우 심각한 문제를 야기하며 심지어 시스템이 붕괴되는 심각한 상황을 초래하게 된다.

이러한 문제들에 대응하기 위하여 지난 수년간 많은 연구들이 진행되어 왔다. 예를 들어, IP 스푸핑을 이용한 DDoS 공격에 대응하기 위해서 Ingress packet filtering [1], Pi [2]와 같은 방법들이 제안되었으며, 공격자를 추적하기 위한 기술로는 확률적인 패킷 마킹에 의한 방법(PPM)[3]등이 제안되었다. 하지만 이러한 노력들에도 불구하고 DDoS 공격은 인터넷의 안전성을 위협하는 심각한 요소로 남아 있다. 더욱이 현재의 인터넷상에서는 목적지 우선의 라우팅 정책을 사용하기 때문에 공격 대상 호스트는 자신에게 전송되고 있는 패킷을 사전에 차단할 수 있는 방안을 가지 고 있지 못하다. 따라서 공격자가 다수의 패킷으로 네트워크 자원을 소모하는 방법으로 네트워크 자체에 대한 공격을 시도할 경우 기존에 제시된 필터링 방법들의 경우 적절한 해결책이 되지 못한다.

따라서 본 논문에서는 이러한 문제들을 해결하기 위해 Active Edge 라우터에 기반을 둔 분산서비스 거부공격 대응 기법을 제안하고자 한다. 제안된 방법의 경우 중간 라우터(intermediate-router)의 오버

헤더, 공격경로 재구성에 필요한 오버헤더, 재구성된 공격경로의 부정확성과 같은 기존의 기법들이 지니고 있던 단점들을 보완하고 있다. 또한 제안된 방법의 경우 공격 패킷을 공격대상 네트워크가 아닌 공격자가 위치하고 있는 네트워크에서 제거함으로서 공격패킷의 필터링 효과를 더욱 향상 시켰다.

2. 관련연구

DDoS 공격에 적절히 대응하기 위해서는 두 가지 큰 문제를 해결해야만 한다. 첫 번째 해결해야할 문제는 공격대상 시스템이 공격자를 정확히 인식하기 힘들다는 문제다. DDoS 공격의 경우 대부분 공격자는 자신의 위치를 숨기고 효율적인 공격을 하기 위하여 IP 스푸핑을 사용한다. 따라서 IP 스푸핑을 효율적으로 차단함으로써 DDoS 공격의 피해를 상당부분 줄 일 수 있다. 이에 그동안 IP 스푸핑을 이용한 DDoS공격을 차단하기 위한 많은 연구들이 진행 되어왔다. 대표적인 예로 IP 스푸핑을 사용한 패킷을 경계라우터(edge router)에서 필터링하는 Ingress Packet Filtering, 공격자가 스푸핑한 IP가 속한 네트워크와, 공격자의 네트워크가 서로 다를 경우 목적 호스트까지의 홉 수도 서로 달라진다는 사실을 이용한 Hop-count filtering, 패킷이 지나온 경로정보를 이용하는 Pi기법등이 있다.

두 번째 문제는 Link flooding 문제로 DDoS 공격을 받는 동안 공격대상 네트워크는 감당할 수 없을 정도의 패킷들로 인해 정상적인 서비스를 제공하지 못한다는 점이다. 앞서 언급한 기법들의 경우 첫 번째 문제에 대한 어느 정도의 대응책이 될 수 있지만 두 번째 문제에 대해서는 적절한 대응책이 되지 못한다. 즉, 두 번째 문제를 해결하기 위해서는 DDoS 공격으로 인한 네트워크의 대역폭 소모를 방지할 수 있는 방안이 필요하다. 이에 대한 해결방안으로 Aggregation 기반의 혼잡(congestion)제어 메커니즘인 Pushback [4]과 같은 방법들이 제안되었다.

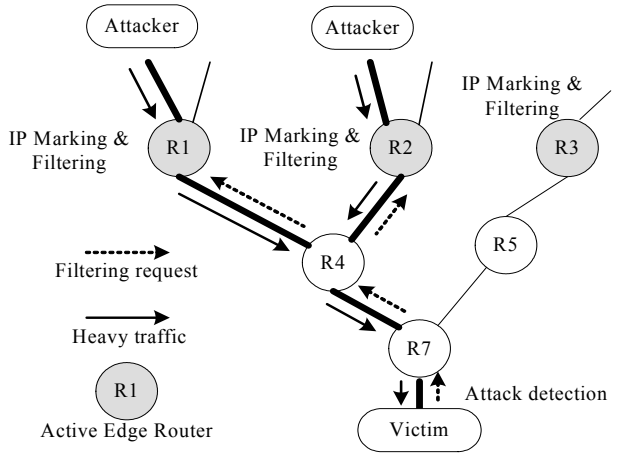
3. 제안하는 DDoS 대응 기법

DDoS 공격을 탐지하였을 때, 가장 중요한 것은 공격에 대해서 어떻게 대응하느냐 하는 문제이다. 현재까지 제안된 대부분의 방안들의 경우, DDoS 공격 패킷은 공격을 탐지한 네트워크에 위치한 라우터나 방화벽등에 의해서 제거된다. 이와 같이 Victim에서 공격 패킷을 제거함으로써, 공격대상 시스템은 공격에 대한 피해를 줄 일 수 있다. 하지만 현재 발생하고 있는 DDoS 공격들의 경우 특정 호스트뿐만 아니라 네트워크 자체를 노린다는 특징도 가지고 있다. 따라서 공격 패킷을 공격 목표가 위치한 네트워크에서 제거 시킬 경우 네트워크의 자원이 공격 패킷에 의해 소모됨으로 인해 발생하는 문제에 대해 적절히 대응할 수 없다.

이 문제에 대응하기 위해 본 논문에서는 공격의 탐지는 공격 대상 시스템에서 이루어지고, 공격 패킷의 차단은 공격자가 위치한 네트워크에서 이루어질 수 있는 방안을 제안한다. 이와 같은 방법을 사용할 경우 공격탐지의 정확성을 증가 시킬 수 있다는 장점이 있다. 즉, 공격 대상 시스템의 경우 모든 자신으로 전송되는 모든 패킷을 관찰 할 수 있고 현재 자신의 상황을 정확히 판단할 수 있기 때문에 공격여부를 정확히 판단할 수 있다. 반면 패킷 필터링의 효율은 공격자가 위치한 네트워크에서 이루어지는 것이 더욱 효율적이다. 기존의 제시된 필터링 기법들과 같이 공격 대상 시스템이 위치한 네트워크에서 필터링이 이루어 질 경우 네트워크 자원을 소비하기 위한 공격에 대해서는 적절히 대응할 수 없다. 반면 공격 패킷을 공격자가 위치한 네트워크에서 차단할 경우 공격 패킷이 인터넷으로 진입할 수 없기 때문에 DDoS 공격 패킷으로 인한 네트워크 자원의 소모를 줄일 수 있다. 따라서 본 논문에서는 DDoS 공격여부에 대한 판단은 공격대상 시스템에서 이루어지도록 하여 공격 여부의 판단에 대한 정확성을 향상시키고, 공격 패킷의 필터링은 공격자가 위치한 네트워크에서 이루어지도록 함으로서 필터링의 효율성 또한 증가 시킬 수 있다.

그림 1은 제안된 방법의 DDoS 공격 대응 방법을 나타내고 있다. 그림에서 굵은 선은 공격 패킷의 흐름을 나타내고 가는 선은 합법적인 패킷을 나타내고 있다. 그리고 화살표는 공격대상 시스템에서 전송하는 pushback 메시지를 나타내고 있다. 제안된 기법은 크게 3단계로 DDoS 공격에 대해 대응한다. 첫 번째 단계는 사전 단계로 R1, R2, R3와 같이 호스트와 직접 연결된 모든 경계라우터 들은 자신이 담당하고 있는 네트워크에서 발생한 모든 패킷에 자신의 IP를 표시한다. 이 정보는 두 번째 단계에서 공격의 탐지와 pushback 메시지의 전송에 사용된다. 두 번째 단계는 공격 탐지와 pushback 메시지 전송단계로, 공격 대상 시스템에서는 DDoS 공격을 탐지하고 공격자가 속한 네트워크의 경계라우터로 pushback 메시지를 전송한다. 현재 제안된 DDoS 공격 탐지의

대부분의 방법은 공격자가 IP 스푸핑을 사용할 경우 공격의 근원지를 알지 못하기 때문에 공격에 대한 판단을 적절히 할 수 없다는 문제점이 있다. 하지만 제안된 기법의 경우 공격자가 위치한 네트워크의 경계라우터에서 패킷이 발생한 위치를 정확히 나타내어 주기 때문에 IP 스푸핑으로 인해 발생 하는 공격 판단의 부정확성 문제를 해결 할 수 있다. 또한 공격에 대한 판단이 이루어질 경우 패킷에 포함된 경계라우터의 IP를 이용하여 pushback 메시지를 공격자가 위치한 네트워크로 직접 전송할 수 있게 된다. 세 번째 단계는 패킷 필터링 단계로 경계 pushback 메시지를 전송받은 경계 라우터들은 내부 네트워크에서 공격대상 시스템으로 전송되는 패킷을 공격대상 시스템의 요구에 의해 차단한다. pushback 메시지에는 공격대상 시스템의 주소와 공격대상 시스템이 제한하는 대역폭 정보 그리고 필터링의 기간이 명시되어 있다. 따라서 경계라우터는 이 정보들을 이용하여 내부 네트워크에서 공격대상 시스템으로 전송되는 패킷의 대역폭을 공격대상 시스템이 요구한 기간 동안 제한한다.



(그림 1) 제안하는 DDoS 공격대응 모델

3.1 Active Edge 라우터의 동작 방법

제안된 기법에서 Active Edge라우터의 첫 번째 역할은 자신의 IP 주소를 내부 네트워크에서 발생한 모든 패킷에 표시하는 것이다. 경계라우터가 자신의 IP 주소를 내부 네트워크에서 발생한 모든 패킷에 표시하는 이유는 DDoS 공격의 경우 대부분의 공격자는 자신의 위치를 숨기고 효율적인 공격을 위해 IP 스푸핑을 사용하기 때문이다. 즉, 경계라우터가 자신의 IP 주소를 패킷에 효시해 줌으로써 공격자가 IP 스푸핑을 사용하더라도 공격 대상 시스템은 그 패킷이 발생한 위치를 정확히 판단 할 수 있다. 따라서 제안된 기법에서는 모든 경계라우터는 자신의 IP 주소를 IP 헤더의 옵션 필드에 표시한다.

경계라우터의 두 번째 역할은 공격대상 시스템에서 보내온 pushback 메시지를 기반으로 공격 패킷을 차단하는 것이다. pushback 메시지에는 공격대상 시스템의 IP 주소, 허용하는 대역폭의 크기, 필터링의 기간이 포함되어 있다. 경계라우터는 공격대상시스템의 IP 주소를 통해 내부 네트워크에서 공격대상 네트워크로 전송되는 패킷은 의심스러운 패킷으로 판단한다. 패킷의 차단 비율은 pushback 메시지의 대역폭 정보에 기초하여 이루어진다. 제안된 구조에서는 공격대상 시스템으로 전송되는 플로우의 대역폭을 공격대상시스템이 지정해준 만큼만을 허용하고 나머지 패킷들은 경계 라우터에서 임의적으로 제거한다. 이와 같은 방법을 채택한 이유는 대부분의 DDoS 공격의 경우 공격자는 DDoS 공격이 이루어지는 동안 공격의 유형의 자주 변화시키기 때문이다. 즉, 대역폭이 아닌 각각의 패킷에 포함된 시그너쳐를 기반으로 하여 패킷을 차단할 경우 공격의 유형이 바뀔 경우 이에 대한 대응책이 필요하며, 각각의 패킷을 공격 시그너쳐와 비교하는데 필요한 오버헤더도 문제가 된다. 또한 DDoS 공격이 이루어지는 것과 같은 심각한 문제 상황의 경우 공격자가 위치한 네트워크에서 공격대상 시스템으로 전송되는 대부분의 패킷은 공격을 위한 패킷들이다. 따라서 공격패킷을 차단하기 위해 공격대상시스템에서 보내온 허용대역폭을 기반으로 플로우의 대역폭을 제한하는 것이 더 효율적이라고 볼 수 있다. 공격 패킷에 대한 필터링은 pushback 메시지에 지정된 시간만큼 이루어진다.

3.2 공격대상시스템에서의 공격대응을 위한 방법

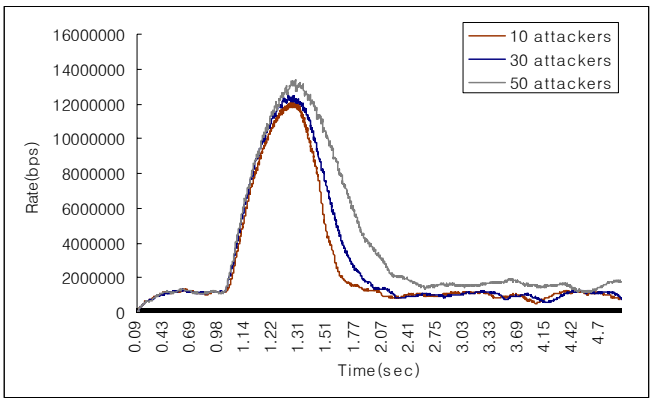
공격대상 시스템은 DDoS 공격을 탐지하고 DDoS 공격과 관련된 정보를 pushback 메시지를 이용하여 경계라우터에게 전송하는 역할을 한다. DDoS 공격에 대한 탐지는 IP 헤더의 소스 IP 정보를 이용하는 것이 아니라 경계라우터의 IP 정보를 이용하여 이루어진다. 즉, DDoS 공격의 경우 대부분 IP 스푸핑을 사용하기 때문에 DDoS 공격이 이루어지는 동안 패킷의 소스 IP 주소는 의미를 지니지 못한다. 반면 앞서 밝혔듯이 경계라우터의 주소는 공격자가 스푸핑하는 것이 불가능하기 때문에 공격의 탐지를 위해

이 정보를 이용하는 것이 더욱 효율적이다.

공격 대상 시스템에서 공격을 탐지한 경우, 공격 대상 시스템은 pushback 메시지를 공격 패킷에 표시된 경계라우터의 IP를 이용하여 공격자가 위치한 네트워크의 경계라우터로 직접 전송한다. pushback 메시지는 IP 데이터그램에 포함되며 IP는 공격자가 위치한 경계라우터를 나타내는 공격자 IP, 공격대상 시스템 자신의 IP를 나타내는 소스 IP, 공격대상 시스템으로 전송되는 패킷에 대한 대역폭 제한을 나타내는 대역폭(bandwidth), 경계라우터가 필터링 상태를 유지해야 하는 기간을 나타내는 파기시간(Expiration time), pushback 메시지라는 것을 타나내는 DDoS Filtering Request ID가 포함 된다.

4. 실험 결과

제안된 기법의 효율성을 검증하기 위하여 네트워크 시뮬레이터인 ns-2를 이용하여 가상의 네트워크를 구성하였다. 실험에서는 전체 공격 패킷의 도착 속도(15Mbps), 평균 공격 탐지 시간(100 milliseconds), 공격자와 Victim사이의 평균 거리(100 milliseconds)를 가정 하였으며, 공격자가 10(1.5Mbps)명, 30(0.5Mbps)명, 50(0.3Mbps)명인 세 가지 시나리오에 대해 실험 하였다.



(그림 2) Victim에서의 패킷 전송 속도

그림 2는 처음 5초간의 시뮬레이션 결과를 보여주고 있다. 실험 시작 후 약 1.3초까지는 Victim에 도착하는 패킷의 양이 급격하게 증가함을 알 수 있다. 이는 공격 패킷이 발생한 후 Victim에서 이를 탐지하는데 약 1초 정도의 시간이 걸리기 때문에 그동안 도착하는 패킷은 필터링 되지 않음을 나타낸다. 반면, 공격을 탐지한 후(약 1.3초) 부터는 패킷이 필터링 되기 시작하여 Victim에 도착하는 공격 패킷의 양이 급격하게 줄어듦을 알 수 있다.

실험에서 알 수 있듯이 제안된 모델의 성능은 공격자의 수 혹은 분산의 정도에는 큰 영향을 받지 않는다. Edge router가 Pushback메시지에 명시된 정보에 따라 모든 공격 패킷을 차단한다고 가정할 경우, 공격 패킷 필터링의 효과는 공격 탐지 시간과 Pushback 메시지의 도달 시간에 의해 결정된다. 즉, 공격 탐지 시간을 D_t, Pushback 메시지 도달 시간을 I_t, 공격 패킷의 전송속도를 A_r bps라 할 경우, Victim에 도달하는 전체 공격 패킷의 양은 $(D_t + 2I_t)$ A_r과 같다.

5. 결론

본 논문에서는 Active Edge 라우터에 기반한 DDoS 대응 기법을 제안 하였다. 제안된 모델은 기존의 Pushback 기법에 비해 중간 라우터들의 오버헤를 크게 줄일 수 있다는 장점과, 공격 탐지의 정확성을 향상 시킬 수 있다는 장점을 갖는다. 또한, 제안된 모델은 기존 모델에서 공격대응을 위해 중간 라우터들에서 수행하는 컴퓨팅 시간을 줄임으로서 보다 빠르게 공격에 대응할 수 있다.

참고문헌

[1] P. Frequson, D. Senie, “Network Ingress Filtering: defeating Denial of Service Attacks Which Employ IP Source Address Spoofing,” RFC 2827, May 2000.

[2] A. Yaar, A. Perrig, D. Song, “Pi: A Path Identification Mechanism to Defend against DDoS Attacks,” In IEEE Symposium on Security and Privacy, May 2003, pp. 93-109.

[3] K. Park and H. Lee, “On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack,” Tech. Rep. CSD-00-013,Department of Computer Sciences, Purdue University, June 2000

[4] R. Mahajan, M. Bellovin, “Implementing pushback: Router-based defense against DDoS attacks,” In Proceeding of the symposium on Network and Distributed Systems Security, 2002.