DDoS 공격에 대처하기 위한 효율적인 패킷 필터링 방안

오성민*, 홍충선*, 이대영*
*경희대학교 전자정보학부
e-mail:osmin@cvs2.khu.ac.kr

Efficient Packet Filtering against DDoS Attacks

Sung-Min Oh*, Choong-Seon Hong*, Dae-Young Lee*
*School of Electronics and Information, Kyung Hee University

요 약

네트워크의 급속한 발전으로 인해 이제는 생활의 중요한 요소로 자리 잡고 있는 현재의 시점에서, 악의적으로 네트워크에 심각한 피해를 끼치는 사례 또한 증가하고 있다. 따라서 이러한 피해로부터 네트워크나 종단 호스트를 보호해야할 필요성이 매우 높아지고 있다. 하지만, 현재의 보안 시스템으로는 DDoS 공격 시 이에 빠르게 대처하여 시스템을 보호하기에는 많은 문제점을 안고 있으므로, DDoS 공격을 받기 이전에 패킷을 필터링하고 패킷 양을 조절해 주어야 할 필요가 있다. 이에 네트워크에 유입되는 패킷을 분류하여 처리하는 보다 향상된 패킷 필터링 기법을 사용하여 DDoS와 같은 공격에 대해 유연하게 대처하기 위한 방안을 제시하고자 한다.

1. 서론

인터넷의 빠른 보급과 이용증가로 인해 네트워크 기본 프레임 또한 빠르게 성장하고 있으며, 네트워크가 구축되어 있지 않은 곳에서는 생활의 불편을 가져오는 상황이 되었다. 이러한 현실 속에서 일부 이용자들이 악의적인 목적으로 네트워크에 심각한 피해를 끼치는 사례가 급증하고 있어, 이에 따른 네트워크와 종단 호스트를 보호해야 할 필요성이 매우 높아졌다. 네트워크와 종단 호스트가 공격자로부터의 공격에 대처하지 못하고 피해를 입을 경우 정상적인 사용자들이 정당한 서비스를 받지 못하게 되기 때문이다.

현재 네트워크 구조는 이러한 Attacker들의 공격에 매우 취약하다. 그리고 이에 대응하기 위해 방화벽이나 침입탐지시스템 등을 도입하여 사용하고 있으나, 그 또한 새로운 공격 형태에 대해서는 취약한 점을 드러내고 있다. 따라서 현재 가장 큰 위험으로 부각되고 있는 DDoS (Distributed Denial of Service) 공격에 대해 좀 더 유연하게 대처해야 할 필요가 있다. 본 논문에서는 새로운 패킷 필터링 기법을 사용하여 DDoS와 같은 공격에 유연하게 대처할 수 있는 방안에 대해 논의 할 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에 제시한 방법을 논의하기 위한 배경지식과 관련 연구에 대해 설명하고 3장에서는 본 논문에서 제시하고자 하는 제안사항에 대해 논의한다. 마지막으로 4장에서 본 논문에 관한 최종 결론을 논의한다.

2. 배경지식 및 관련 연구

2.1 DDoS (Distributed Denial of Service) 공격

DoS (Denial of Service)라 함은 한 사용자가 시

스템의 리소스를 독점하거나 모두 사용, 또는 파괴함으로써 다른 사용자들이 이 시스템의 서비스를 올바르게 사용할 수 없도록 만드는 것을 말한다. 이런 의미에서 시스템의 정상적인 수행에 문제를 일으키는 모든 행위를 DoS라 할 수 있다 [1]. 그림 1은 일반적인 DoS 공격을 간략히 나타낸 그림이다.

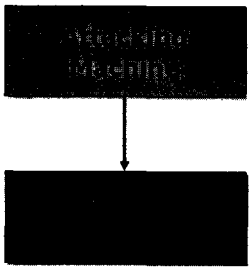

그림 1 DoS 공격

DDoS (Distributed Denial of Service)는 DoS의 또 다른 형태로, 인터넷에 연결된 일련의 시스템들을 이용해 단일 사이트에 대한 플러드 공격을 시도하는 것이다. 그림 2에서처럼 공격자가 일단 취약한 인터넷 시스템에 대한 엑세스에 성공하면 침입한 시스템에 소프트웨어를 설치하고 동시에 이를 실행시켜 원격에서 하나의 시스템에 공격을 개시한다. 공격을 받은 시스템은 공격자가 한꺼번에 보낸 패킷을 감당하지 못하고 피해를 입게 된다.

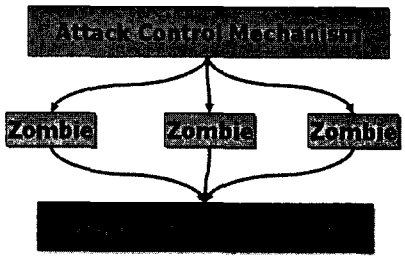

그림 2 DDoS 공격

2.2 방화벽과 침입탐지시스템

DoS와 DDoS 공격을 막기 위해 현재 가장 많이 사용하고 있는 것이 방화벽과 침입탐지시스템이다.

방화벽(Firewall)은 특정 인터넷 프로토콜을 위한 포트를 사전에 차단함으로써 이를 통한 어떠한 트래픽도 통과하지 못하게 하는 방식이다. 이 방식은 포트 차단으로 외부로부터 들어오는 공격을 막을 수는 있지만, 정상적인 서비스를 받기 위한 트래픽 또한 차단된다는 치명적인 약점이 있다. 이러한 약점을 보완하기 위하여 도입된 방식이 침입탐지시스템이다.

침입탐지시스템(Intrusion Detection System)은 네트워크상의 정보시스템에 대한 불법접속, 정보시스템 내부에서 시도되는 침입관련 행위, 정상적인 네트워크 서비스를 방해하는 침입시도 등을 네트워크 패킷 분석을 탐지, 분석하여 대응책을 알려주는 시스템이다.

하지만 시스템이 공격을 받은 후에 침입탐지가 가능하며 그 후에 대응하기 때문에 시스템이 그 사이 공격을 받아 서비스를 행하지 못하게 되는 치명적인 약점이 있다.

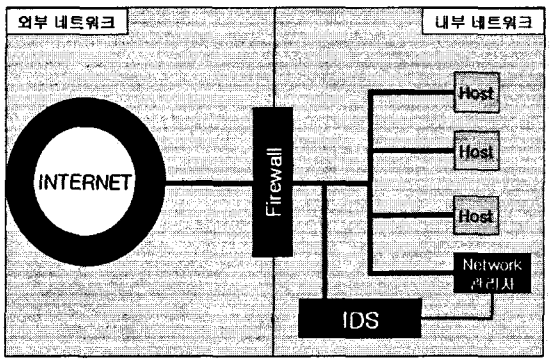

그림 3 방화벽과 침입탐지시스템

현재의 보안 시스템은 그림 3에서와 같이 방화벽과 침입탐지시스템의 약점을 서로 보안하기 위하여 두 가지 시스템을 병행하여 사용하고 있는 실정이다.

2.3 패킷 필터링 (Packet Filtering)

패킷 필터는 패킷의 헤더를 분석하여 전체 패킷의 처리를 위한 소프트웨어의 일부로써, 패킷의 '폐기(Drop)'나 '수용(Accept)'과 같은 작업을 수행하게 된다[2].

패킷 필터링을 하는 이유는 위에서 말한 것처럼 네트워크로 들어오는 패킷의 종류에 따라 패킷을 폐기하거나 수용할 수 있기 때문에 네트워크의 보안성 향상을 위해 보안 시스템에 접목되고 있는 현실이다.

2.4 DDoS 공격에 대비한 데이터마이닝 프로토콜 : NetShield

그림 4는 NetShield 구조에서 패킷 필터의 사용과 처리과정을 보여주는 그림이다[3][4]. 패킷이 들어오면 패킷필터가 자신이 가지고 있는 패킷 시그너쳐(Signature)를 가지고 패킷을 검사하여 비정상패킷

과 공격으로 간주된 패킷들을 분류해내고 나머지 패킷들만 전송한다. 비정상 패킷이나 공격으로 간주된 패킷들은 검사를 거쳐 위험을 알리고 이에 대처하여 그 방안을 패킷 필터에게 다시 알려준다. 패킷 필터는 다시 이러한 정보를 저장하여 다음 번에 들어오는 패킷들에 적용한다.

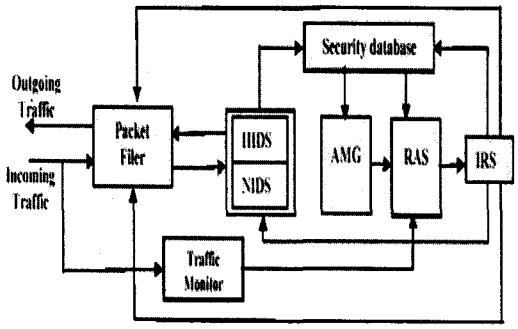

그림 4 NetShield 침입탐지시스템

3. 제안사항

이전 장에서 소개되었듯이, 기존 침입탐지 시스템은 초기에 서버나 네트워크가 공격을 받은 후에 그 공격 패킷을 탐지하여 대응하는 시스템이기 때문에 알려지지 않은 DDoS와 같은 공격을 받을 시, 효과적인 대응을 할 수 없다. 따라서 패킷 필터에서 사전에 시스템에 오버플로우가 발생하지 않도록 패킷의 양을 조절해야 할 필요가 있다[5].

본 논문에서는 이러한 패킷의 양의 조절하기 위한 패킷 필터의 새로운 구성을 위한 방법을 제시하고자 한다.

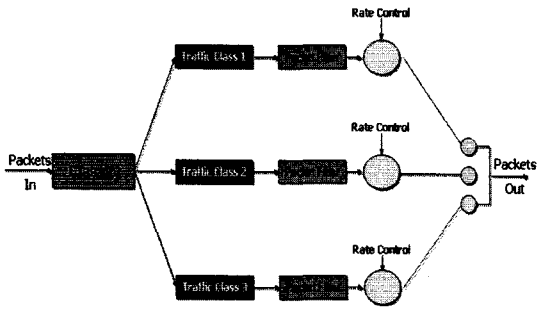

그림 5 제안된 패킷 필터

3.1 패킷 필터링 과정

그림 5는 본 논문에서 제안하고자 하는 패킷 필터이다. 패킷이 들어오면 우선 패킷을 분류한다. 패킷은 UDP 패킷, TCP 패킷, 혹은 연결 설정을 위한 TCP SYN 패킷과 ICMP 패킷 등으로 구별할 수 있기 때문에 우선 전체 들어오는 패킷들을 이러한 패킷의 종류로 분류하여 클래스를 구성한다.

구성된 클래스는 각각 패킷 필터를 거치는데, 여기서는 패킷 필터가 가지고 있는 패킷 시그너처(Signature)를 이용하여 패킷이 일반 패킷인지 공격 패킷인지를 구별하여 공격 패킷인 경우는 드롭시키고 그 정보를 네트워크 관리자에게 전송한다. 물론 알려지지 않은 공격 패킷들은 패킷 필터를 통과하여 결국 최종 목표 시스템을 공격할 것이다. 따라서 패킷 필터를 통과한 패킷들이 만일 DDoS 공격 패킷이 포함되어 과도한 패킷의 양으로 도달한다면, 패킷 필터 다음에 있는 Rate Control에서 최종 목표 시스템으로 보내지는 패킷의 양을 조절하게 된다. 네트워크 관리자는 패킷 클래스에 따라서 전송되는 패킷의 양을 상황에 맞게 정책으로 구성하여 각각의 Rate Control에게 그 정책에 따라 수행하도록 명령하고, Rate Control은 이 정책에 따라 패킷 전송량을 제한한다. 예를 들어 목적지 호스트가 처리할 수 있는 패킷의 양은 100Mbps인데, 패킷 필터를 통과한 패킷의 양이 120Mbps라고 한다면 Rate Control에서 100Mbps의 패킷만 전송 하고 나머지는 드롭시키게 되는 것이다. 물론 이 과정에서 정상적인 사용자가 전송한 패킷들도 드롭될 가능성이 많이 있지만, 시스템은 서비스를 계속할 수 있게 될 것이다. 시스템에 전송된 패킷들 중에는 패킷 필터를 통과하여 들어온 공격 패킷이 포함되어 있을지도 모른다. 이런 패킷들이 시스템을 공격하겠지만, DDoS 공격의 특성상 서버에 영향을 줄 수 있는 정도의 패킷이 들어오지 않았기 때문에 시스템은 피해를 최소화할 수 있게 되고, 이 공격 패킷을 침입탐지시스템이 탐지하여 그에 대한 정보를 분석하고 이에 대한 대응책을 다시 패킷 필터에 전송한다. 패킷 필터는 이 패킷 시그너처를 자신의 데이터베이스에 추가하고 이후에 들어오는 패킷에 대해서 적용시켜 다시금 그러한 패턴의 공격 패킷이 필터를 통과할 수 없게 만든다.

3.2 패킷 분류 목적

초기에 패킷을 분류하는 이유는 DDoS의 특성상

여러 종류의 공격형태를 가지고 공격하지 않고 한 종류의 패킷을 동시에 과도하게 전송하기 때문에, 패킷을 분류하여 다른 종류의 패킷을 가지고 서비스를 받는 사람들에게는 정상적으로 서비스를 받게 하기 위함이다. 예를 들어 UDP 플러드 DDoS 공격이 가해졌다라고 가정하자. 그렇다면 들어오는 패킷들 중에는 UDP 패킷들이 가장 많이 존재할 것이고 이 패킷들을 분류하지 않고 그대로 Rate Control로 제어하여 전송하였을 경우 UDP 패킷들이 드롭되지 않을 확률이 다분히 높다는 것이다. 따라서 패킷 분류를 하지 않을 때는 분류하였을 때보다 서비스를 받지 못하는 사용자가 더 늘어날 것이다. 그러므로 패킷을 분류하여 정상 패킷이 공격 패킷보다 더 많이 전송될 수 있게 하여 정상적인 사용자가 시스템에 DDoS 공격이 가해진 상황에서도 최대한 올바른 서비스를 받게 하기 위함이다. 그리고 패킷을 분산시킴으로써 전체 패킷을 하나의 필터로 필터링 하는 것보다 더 효율적이고 신속하게 패킷을 처리할 수 있다.

4. 결론 및 향후과제

본 논문에서는 DDoS 공격에 대해서 좀 더 효과적으로 대처할 수 있는 방법을 제시하였다.

패킷 분류를 통한 전송량 제어를 통해, DDoS 공격을 받을 경우에도 시스템이 계속 서비스를 제공할 수 있고, 패킷의 종류와 전송되는 패킷의 양에 따라 우선권을 주어 정상 패킷이 더 많이 전송되어 올바른 서비스를 받게 하기 위한 방법을 제시하였다. 또한 패킷을 분산처리 하여 필터링 함으로써 시스템 성능을 향상시킬 수 있을 것이다.

향후 연구과제로는 본 논문에서 제안한 방식을 활용하여 더 효율적인 패킷 전송방식에 대한 연구가 필요하다.

우선적으로 패킷을 분류하는데 있어 좀 더 다양한 방법으로의 접근이 필요하다. 패킷의 종류에 대한 분류뿐만 아니라 시스템이 제공하는 서비스의 종류에 따른 패킷 분류가 가능할 것이며, 종류별로 분류된 패킷들을 관리자의 정책에 따라 또다시 분류하여 전송하는 방법 또한 연구되어야 할 것이다. 또한 제안된 구조의 성능 평가가 필요할 것이다.

앞으로 본 논문의 제안사항을 Active Network에 접목시키려고 한다. 이는 공격 패킷에 대한 정보를 다른 도메인의 관리자와 공유하여 자신의 도메인에 공격 패킷이 접근하기 이전에 제어할 수 있게 하기 위함이다. 이를 위해 다른 도메인으로 공격 패킷의 정보를 전송하기 위해 사용되는 Active packet이 목적지에 도달하기 전에 누출되지 않도록 하는 보안 구조가 앞으로 연구해야할 과제이다.

참고문헌

[1] Internet Security System (ISS) White Paper "Distributed Denial of Service Mitigation", 2002

[2] P. Ferguson, D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", May 2000. rfc 2827

[3] Kai Hwang, "Proactive Intrusion Defense Against DDoS Flooding Attacks", submitted to IEEE Security and Privacy, April 14, 2003

[4] Kai Hwang, "NetShield: Protocol Anomaly Detection with Datamining against DDoS Attacks", Sixth Int'l Symp. on Recent Advances in Intrusion Detection (RAID-2003), Pittsburgh, PA. Sept. 8-10, 2003

[5] Garg, A. "Mitigation of DoS attacks Through QoS Regulation", Proc. of Int'l Workshop on Quality of Service, Miami Beach, May 15-17, 2002