DDoS 공격 대응과정에서의 능동 라우터 성능평가

권영호*, 김영민*, 문경신O*, 안상현*, 한민호**, 나중찬**
*서울시립대학교 컴퓨터과학부, **한국전자통신연구원 정보보호기술연구본부
{ yhkwon95, blhole, ksmun96O, ahn }@venus.uos.ac.kr, { mhhan, njc }@etri.re.kr

Performance Evaluation of Active Router in DDoS Attack Response Operation

Youngho Kwon*, Youngmin Kim*, Kyoungsin MoonO* Sanghyun Ahn*
Minho Han**, Joongchan Na**
*School of Computer Science, University of Seoul, **ETRI

요 약

인터넷이 널리 보급되면서 이용자들간에는 편리하고 빠른 정보교환이 가능하게 되었지만 이를 방해하는 해커들의 활동 또한 크게 증가하고 있다. 그 중 DDoS(Distributed Denial of Service) 공격은 인터넷 서비스를 하고 있는 서버에 심각한 해를 주며 탐지와 대응이 어려운 해킹방법중의 하나이다. 본 연구에서는 DDoS 공격 대응을 위해 액티브 네트워크를 이용해 개발한 DDoS 보안시스템[1][2]을 이용할 때 얼마나 효과적인 성능을 낼 수 있는지에 대한 분석 결과를 제공한다.

1. 서 론

인터넷이 널리 보급되면서 이용자들간에는 편리하고 빠른 정보교환이 가능하게 되었지만 이를 방해하는 해커들의 활동 또한 크게 증가하고 있다. 그 중 DDoS(Distributed Denial of Service) 공격은 인터넷 서비스를 하고 있는 서버에 심각한 해를 주며 탐지와 대응이 어려운 해킹방법중의 하나이다.

이러한 DDoS 공격은 그림 1에서 보듯이 공격자(attacker)가 여러 개의 마스터를 해킹(hacking)한 후 다시 각 마스터들로부터 에이전트(agent)들을 해킹하고 DDoS 공격프로그램을 실행하여 희생자(victim)를 공격하며, 공격자에서 에이전트까지의 트리구조 단계수는 공격자에 의해 조절된다.

DDoS의 공격유형으로는 UDP Flood, SYN Flood, Smurf/Fraggle, Fragments[3] 등이 있으며, 이 중 UDP Flood는 가장 일반적인 DDoS 공격방법으로 에이전트들이 희생자에게 집중적으로 UDP 패킷을 보내어 희생자가 다른 실제 사용자들에게 인터넷 서비스를 하지 못하게 한다. SYN Flood는 TCP의 3 hand-shaking의 헛점을 이용한 공격방법으로, 에이전트들이 TCP SYN 메시지를 희생자에게 보내면 희생자는 에이전트들에게 ACK를 보내고, TCP 세션을 준비한 후 다시 ACK를 기다린다. 그러나 에이전트들이 ACK를 보내지 않으므로 희생자의 메모리가 불완전한 TCP 세션으로 가득차게 되어, 서비스가 불가능해지게 되는 상황을 만든다. Smurf/Fraggle 방법은 희생자의 주소를 소스 주소로 속여 만든 ping 요청 패킷(ICMP Echo Request)을 서브네트워크의 브로드캐스트 주소로 보내어 희생자에게 ping 응답 패킷(ICMP Echo Reply)이 몰리도록 하는 공격이다. 마지막으로 Fragments는 라우터와 같은 네트워크 장비를 주공격 목표로 하여 크기가 큰 패킷을 고의로 나누어(fragments) 보내며, 이것을 받은 호스트가 원래의 패킷을 만들어 내는데 많은 자원을 낭비하도록 만드는 공격 방법이다. 본 연구에서는 가장 일반적인 DDoS 공격방법인 UDP Flood를 사용한다.

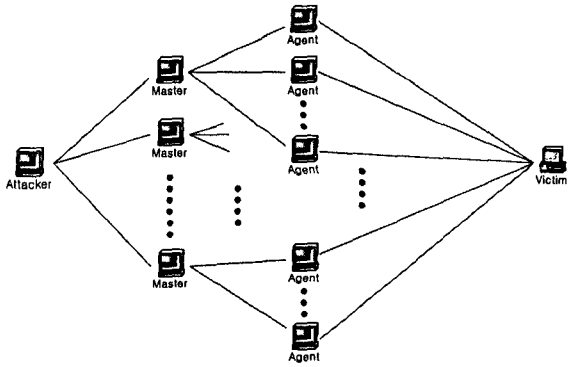

그림 1. DDoS 공격의 기본적인 모델

DDoS 공격으로부터 피해를 받지 않기 위해서는 우선 DDoS 공격을 탐지할 수 있는 기능이 필요하며, UDP Flood와 같은 DDoS 공격은 실제 데이터 트래픽과 구별하기 힘들기 때문에 어떤 상황을 DDoS 공격으로 받아들일 것인가에 대한 판단 자체가 하나의 연구분야가 된다. 그러나 본 연구에서는 공격 탐지에 대해서는 다루지 않고 대응 방법에 초점을 맞춘다. DDoS 공격 대응 방법은 공격 패킷 필터링(filtering)과 공격자 소스를 찾아내는 과정으로 이루어진다.

2. 성능 분석 시나리오

이 장에서는 DDoS 보안시스템의 구조를 간략히 살펴본 후 간단한 망을 사용한 시나리오를 보여준다.

2.1 DDoS 보안시스템의 구조[1]

DDoS 보안시스템은 시스템 우회 공격, Spoofed IP 공격, 그리고 DDoS 공격에 대응하기 위해 해당 침입자를 역추적하여 해당 공격을 무력화 시키기 위한 능동 보안 메커니즘을 구현한 시스템이다. DDoS 보안시스템으로 보호되는 도메인(Secure Domain)에는 MoSE(Mobile Security Engine), SGS_IDS(Security Gateway System - Intrusion Detection System), ASMS(Active Security Management System)들이 존재한다[2]. [그림 2]는 각 모듈들의 위치와 기능 및 역할에 대해 보여주고 있으며, 본 연구에서는 DDoS 보안시스템의 여러 기능 중 DDoS 공격 대응에 대한 부분만을 다룬다.

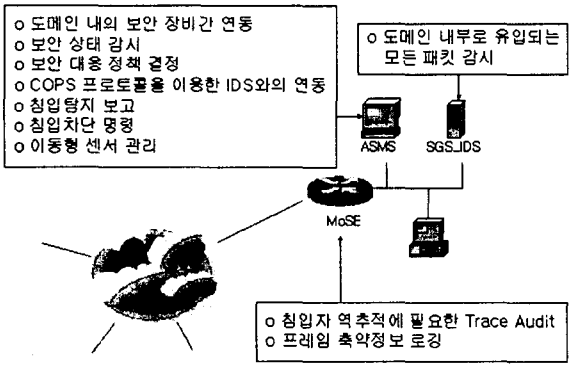

그림 2. DDoS 보안시스템의 구조

2.2 시나리오

그림 3은 시나리오에서 설정한 DDoS 보안시스템이 설치된 4개의 도메인으로 구성된 인터넷 망을 나타낸다. 각 도메인은 MoSE, ASMS, SGS_IDS를 포함하고 있으며, 공격자는 DDoS 공격을 하기 위해 먼저 에이전트로 사용할 호스트들을 해킹해서 사용권한을 얻어낸다. 에이전트들은 희생자에게 UDP Flood 공격 방법을 이용하여 DDoS 공격을 시작하며, 희생자는 서비스가 불가능한 상태가 된다.

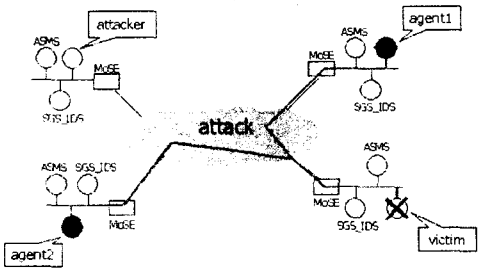

그림 3. DDoS 공격을 나타낸 시나리오 모델

도메인 내로 유입되는 모든 패킷을 감시하던 SGS_IDS가 DDoS 공격을 탐지하여 유해 패킷에 대한 축약정보 및 탐지 정보를 ASMS에게 전달한다. ASMS는 SGS_IDS로부터 보고 받은 내용을 근거로 액티브 패킷인 역추적 센서(Tracing Sensor)를 생성하여, DDoS 공격을 한 에이전트들에게 전송한다. MoSE는 TS의 정보를 분석하여 에이전트로부터 유입되는 패킷을 차단한 후 TS를 다시 원래의 목적지인 에이전트로 전송한다. 그러나 에이전트로부터 희생자로의 트래픽이 너무 많아 망에 문제가 발생하였을 경우, 역방향으로 TS 전송에 실패할 수 있으므로 일정 시간동안 ACK를 받지 못할 경우 TS를 재전송한다. 에이전트 도메인 내의 MoSE는 TS를 처리하여 에이전트로부터 나오는 패킷을 차단한 후 TS를 ASMS로 전송한다. ASMS는 에이전트에게 상위 공격자의 존재 유무에 대한 분석을 요구하여, 존재한다면 공격자의 주소를 얻어내고 도메인 내에 존재하는 에이전트의 보안상태를 점검하고 복구한다. 에이전트 도메인의 ASMS는 TS를 올바르게 수신했다는 ACK 메시지를 희생자 도메인의 ASMS에게 전송한다. 에이전트 도메인의 ASMS는 공격자를 목적지로 하여 TS를 전송하고, 이를 받은 공격자 도메인의 MoSE는 공격자로부터 밖으로 나가는 패킷을 차단한 후 TS를 공격자 도메인의 ASMS에게 전송한다. 공격자 도메인의 ASMS는 에이전트 도메인의 ASMS에게 TS를 수신했다는 ACK 메시지를 전송하고, 공격자에게 상위 공격자가 존재하는지에 대한 분석을 요구하지만 결과를 얻지 못하며 공격자를 근원지로 판단하게 된다. 공격자 도메인의 ASMS에서 역추적 결과 센서 ASMS는 에이전트도메인의 ASMS에게 TS를 수신했다는 ACK 메시지를 전송하고, 공격자에게 상위 공격자가 존재하는지에 대한 분석을 요구하지만 결과를 얻지 못하며 공격자를 근원지로 판단하게 된다. 공격자 도메인의 ASMS에서 역추적 결과 센서(Tracing-Complete Sensor, TCS)를 생성하여 에이전트 도메인의 ASMS에게 전송하며 전송과정 중 각 도메인의 MoSE는 TCS를 처리한다. 에이전트 도메인의 ASMS는 TCS를 처리하여 에이전트의 복구상태를 확인한 후, 희생자 도메인의 ASMS로 TCS를 전송한다. 희생자 도메인의 ASMS는 TCS를 처리하고, 결과를 관리자에게 통보하여 DDoS 공격에 대한 대응 조치를 정리한다.

3. 실험 및 성능 분석

DDoS 및 DDoS 보안시스템의 동작 과정을 시뮬레이션하기 위한 시뮬레이터로는 NS2(Network Simulator 2)[4]가 사용되었다. 실험에 사용되는 망은 총 52개의 노드를 가지며, 망의 종단에는 DDoS를 시뮬레이션하기 위한 일반 도메인이나 DDoS 보안시스템에 의해 보호되는 도메인이 존재한다. 망의 중앙에 위치한 네 개의 노드들과 이들로 연결된 링크들은 백본 망으로 가정하며, 공격자와 희생자는 하나씩 존재하고 에이전트는 18개 존재한다. 백본 망은 20Mbps의 대역폭을 가진 양방향 링크와 드롭 테일 큐(drop tail queue)로 구성되며, 백본 링크를 제외한 링크는 5Mbps의 대역폭을 가진 양방향 링크와 드롭 테일 큐로 구성되고, 모든 링크의 전송 지연 시간은 2ms이다. 실험에 사용되는 트래픽의 종류에는 백그라운드 트래픽, DDoS 공격 트래픽, 제어 트래픽이 있으며 모두 UDP를 사용하여 CBR(Constant Bit Rate)로 생성했다. 백그라운드 트래픽은 실험 시간동안 측정한 결과, 전체 링크 이용률의 약 20%정도를 차지하며 DDoS 트래픽은 DDoS 공격을 위해 에이전트 당 1688Kbps로 희생자에게 패킷을 전송한다.

DDoS 공격과 DDoS 보안시스템이 망의 전체 트래픽에 미치는 영향을 분석하기 위해 그림 4, 5, 6을 측정하였으며 DDoS 공격이 없는 망, DDoS 공격이 있는 상황에서 DDoS 보안시스템을 동작시킨 망과 동작시키지 않는 망의 전체 트래픽을 살펴본다. 그림 4, 5, 6은 1/100초마다 링크를 통과하는 패킷의 합을 실험시간에 걸쳐 측정한 것이다. 그림 4는 DDoS 공격이 수행되지 않는 상황에서의 트래픽, 즉 정상적인 상황에서의 백그라운드 트래픽을 측정하였으며, 그림 5는 DDoS 보안시스템이 동작하지 않는 망의 트래픽으로 백그라운드 트래픽과 DDoS 공격 트래픽을 측정함으로써 DDoS 공격이 정상적인 망에 얼마나 영향을 주는가를 보인다. 그림 4와 비교하면 전체 트래픽이 상당히 증가해서 망에 부하를 주고 있으며, 증가된 부분의 트래픽은 DDoS 공격 트래픽의 영향을 받은 것이다.

그림 6은 백그라운드 트래픽, DDoS 공격 트래픽, 제어 트래픽을 모두 포함한 그림으로, DDoS 공격이 시작된 후 DDoS 보안시스템의 제어 메커니즘에 의해 실험시간 3.1초 이후부터 전체 트래픽 중 DDoS 공격 트래픽이 사라지고 정상적인 백그라운드 트래픽과 약간의 제어 트래픽만 남는 것을 보여준다.

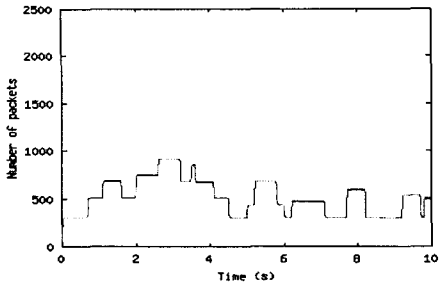

그림 4. DDoS 공격이 없는 상황에서의 전체 트래픽

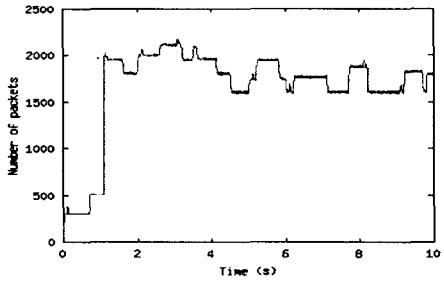

그림 5. DDoS 공격을 포함한 전체 트래픽

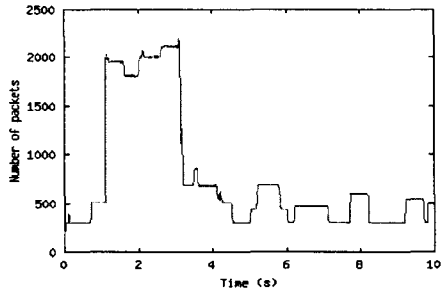

그림 6. DDoS 보안시스템이 동작하는 망에서 DDoS를 포함한 전체 트래픽

그림 7은 실험시간 10초 동안 eSMART 시스템이 동작하는 망에서 1/100초마다 각 링크를 통과했던 제어 패킷의 합을 측정한 그림으로, 총 4개의 측정 그룹이 약 1초 간격으로 나타난다. 3.1초에 시작되는 첫 번째 그룹은 희생자에서 에이전트까지 전송되는 TS를 나타내며, 두 번째 그룹은 에이전트에서 공격자까지 전송되는 TS를 나타낸다. 두 그룹의 트래픽 양에 차이가 나는 이유는 희생자에서 에이전트들까지의 홉 수의 합과 에이전트들에서 공격자까지의 홉 수의 합이 다르기 때문이다. 세 번째와 네 번째 그룹은 TS의 역방향으로 전송되는 TCS를 나타내며, 1, 2 그룹과 3, 4 그룹의 트래픽 양 차이는 TS 전송 시에만 ACK를 보내도록 했기 때문이다. 각 그룹이 1초 간격으로 나타나는 것은 ASMS에서 제어 트래픽을 처리하기 위해 1초를 소비한다고 가정했기 때문이다.

그림 8은 실험시간 10초 동안 DDoS 보안시스템이 동작하는 망에서 1/10초마다 각 링크의 이용률을 측정하여, 이용률이 40%에서 60%, 60%에서 80%, 80%에서 100%가 되는 3 구간으로 구분하고, 각 구간에 해당하는 링크의 수를 전체 링크로 나눈 후 100을 곱한 퍼센트 값을 측정하였다. DDoS 공격이 시작되는 1.1초부터 제어 트래픽이 전송되기 전까지는 높은 이용률을 갖는 링크의 수가 많지만, DDoS 보안시스템이 동작되고 난 후에는 링크 이용률이 낮아진 것을 확인할 수 있다.

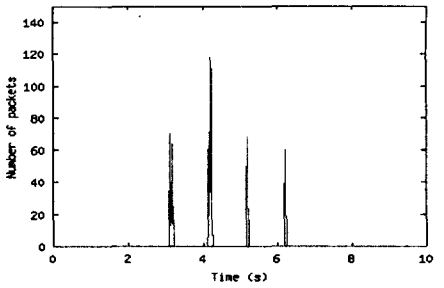

그림 7. 제어 트래픽

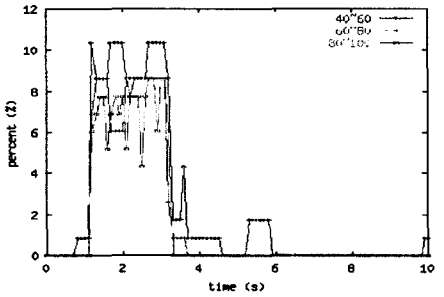

그림 8. 링크 이용률

4. 결론

본 연구에서는 DDoS 보안시스템의 성능을 분석하기 위해 NS2를 이용하여 실험하였으며, 백그라운드 트래픽과 DDoS 공격 트래픽을 정해진 기준에 의해 발생시키고 NS2로 구현한 DDoS 보안시스템을 동작시켜 DDoS 공격에 대한 대응을 관찰하였다.

DDoS 공격에 대한 DDoS 보안시스템의 대응을 분석하기 위해 망 전체에 흐르는 백그라운드 트래픽, DDoS 공격 트래픽, 제어 트래픽을 측정하여 얼마나 많은 제어 트래픽이 발생하는지, 얼마나 빨리 DDoS 공격 트래픽을 제거할 수 있는지, 망의 전체적인 부하는 어느 정도인지를 측정하였다.

DDoS 공격이 시작되고 정해진 시간(2초)후에 제어 트래픽(TS)이 발생되어 0.13초만에 DDoS 공격이 제거되었다. 링크 이용률 면에서도 DDoS 보안시스템이 동작 후 전체적인 링크 이용률이 현격하게 줄어들며, 전체 트래픽에 대한 제어 트래픽의 비율도 아주 작아 DDoS 보안시스템이 효율적으로 DDoS 공격에 대응하는 것을 보였다.

참고문헌

[1] 방효찬, 이영석, 이수형, 한민호, 나중찬, "능동보안기술 시나리오", ETRI 기술문서, 2002.

[2] ETRI 네트워크보안연구부, " 차세대 인터넷을 위한 능동 보안 기술 백서" , 2001.

[3] How a DDoS attack works, "http://www.mazunetworks.com/flash.swf"

[4] The Network Simulator - ns-2, "http://www.isi.edu/nsnam/ns/"