네트워크 분산반사 서비스 거부 공격(DRDoS)에 대한 역추적 시뮬레이터 설계 및 구현

이형우†

요 약

본 연구에서는 DDoS/DRDoS 공격과 같이 Zombie 및 Reflector 기반의 네트워크 기반 해킹 공격에 대해 스푸핑된 공격 패킷의 근원지 IP를 역추적 할 수 있는 시뮬레이터를 설계/구현하였다. 현재까지 제시된 IP 역추적 기법에 대한 분석을 수행하여 각 기법의 장단점을 파악하고 특히 근래에 많은 피해를 주고 있는 Reflector 기반의 DRDoS 공격에 대한 역추적 시뮬레이션을 수행하였다. NS-2 기반의 패킷 IP 역추적 모듈 개발 구조를 제시하였고 이를 설계/구현하였으며 직접 DRDoS 공격 트래픽에 대한 역추적 과정을 수행하였다. 제시한 기법에 대한 시뮬레이션 결과 DRDoS 공격에 효율적으로 대응하였으며 개선된 역추적 성능을 제공하였다.

키워드 : 정보보호, 네트워크보안, 반사서비스거부공격, 시뮬레이터

Design and Implementation of Traceback Simulator for Distributed Reflector DoS Attack on Computer Network

Hyung-Woo Lee†

ABSTRACT

In this study, we suggest a new mechanism on the design and implementation of IP Traceback system against DDoS/DRDoS by Zombie and Reflector attack based on spoofed IP packets. After analysis and comparing on the state-of-arts of several IP traceback mechanisms, we can find their own pros and cons primitives. And then we performed simulations on reflector based DRDoS network packets. In first, we suggest a NS-2 based IP traceback module and implement it for finding its real DRDoS attacker. As a results, we can find advanced new IP traceback scheme for providing enhanced proactive functionality against DRDoS attack.

Keywords : Information Security, Network Security, DRDoS Attack, Simulator

1. 서 론[1)]

인터넷은 정보 교류를 활성화하는 순기능과 함께 인터넷을 통해 시스템 해킹 및 정보유출, 불법 침입, 악성 바이러스 유포 등의 역기능도 점차 확대되고 있다. 최근에는 분산 서비스 거부 공격(Distributed Denial of Service :DDoS)[1]을 통해 호스트 및 네트워크 자원을 급격히 소진하여 성능 저하 및 서비스 불가를 초래하게 된다. DDoS 공격 툴은 인터넷을 통해 손쉽게 구할 수 있으며, 효율적인 방어 기술 및 추적 기법이 제시되지 못하고 있다. 그 이유는 DoS 공격자가 손쉽게 IP 패킷의 송신자 주소를 변경(스푸핑)하여 피해 시스템에게 보낼 수 있기 때문이다[2]. 이럴 경우 실제 IP 패킷이 보내

† 정 회 원: 한신대학교 소프트웨어학과 교수(교신저자)
논문접수: 2004년 9월 15일, 심사완료: 2004년 12월 6일
* 본 논문은 한신대학교 교내연구비 지원에 의해 수행되었음

진 송신자 주소가 아니기 때문에 DoS 패킷에 기록된 송신자 주소만을 가지고는 스푸핑된 패킷의 실제 공격근원지를 알아내기 어렵다.

IP 패킷의 헤더에는 전송 근원지에 해당하는 32비트 IP 주소를 포함하고 있다. 그러나 TCP/IP 환경에서 패킷에 기록된 송신자 IP 정보는 손쉽게 위조/변경될 수 있다. 현재 사용되는 라우터 역시 성능 측면에 중점을 두고 있어서 스푸핑된 IP 패킷에 대한 필터링, 판별 기능을 제공하지 못하고 있다. 따라서 공격자는 스푸핑된 패킷을 생성하여 손쉽게 DDoS 공격을 수행할 수 있다.

대응 기술로 제시된 기법을 살펴보면, IP 패킷에 대한 변형을 판별하기 위해 전통적인 필터링 및 분산 필터링 기법 등도 제시되었으며 라우터의 성능을 개선하여 IP 주소에 대한 검증 기능을 포함하기도 하였다. 하지만 DoS 공격과 같은 대단위 패킷에 대한 효율적 역추적 기능을 제공하지 못하여 한계점을 갖는다.

IP 역추적(IP Traceback) 기법은 DDoS 공격 대상 시스템의 관리자에게 DDoS 공격의 실제적인 공격 근원지 IP 주소를 알려주는 기능을 제공한다[3]. 대부분의 DDoS 공격은 Zombie를 통한 간접적인 공격 형태를 보인다. 따라서 IP 역추적 기법에서는 Zombie에 해당하는 라우터를 대상으로 실제 DDoS 공격 패킷이 전송된 경로를 재구성하게 된다. IP Traceback 기법은 기존의 필터링 기법과 달리 능동적인 방식으로 피해 시스템에서 공격 근원지를 판별할 수 있는 기법이다[4].

본 연구에서는 DDoS 공격에 대한 능동적인 대응 기술에 해당하는 IP 역추적 기법에 대한 시뮬레이터를 설계/구현하였다. 최근 강력한 공격 기법으로 밝혀진 Reflector 기반의 DRDoS 공격 기술의 구조와 대응 방안에 대해 살펴보고, NS-2[5] 기반의 시뮬레이션 환경을 이용하여 IP 패킷에 대한 마킹 모듈을 설계/구현하여 기존의 DRDoS 공격에 대응할 수 있는 새로운 IP 역추적 기법을 제시하였다. NS-2 기반의 시뮬레이션 과정을 수행하여 피해 시스템에서의 트래픽을 비교 분석하여 DRDoS 공격에 대한 기술 개발 방향에 대해 고찰할 수 있었다.

2. Reflector 기반 공격 기술

2.1. DDoS 공격 기법

일반적으로 DoS 공격은 공격자의 컴퓨터로부터 피해 시스템과 해당 네트워크에 과다한 데이터를 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 피해 시스템에서 제공하는 서비스들을 인터넷 사용자들이 이용하지 못하도록 하는 것이다.

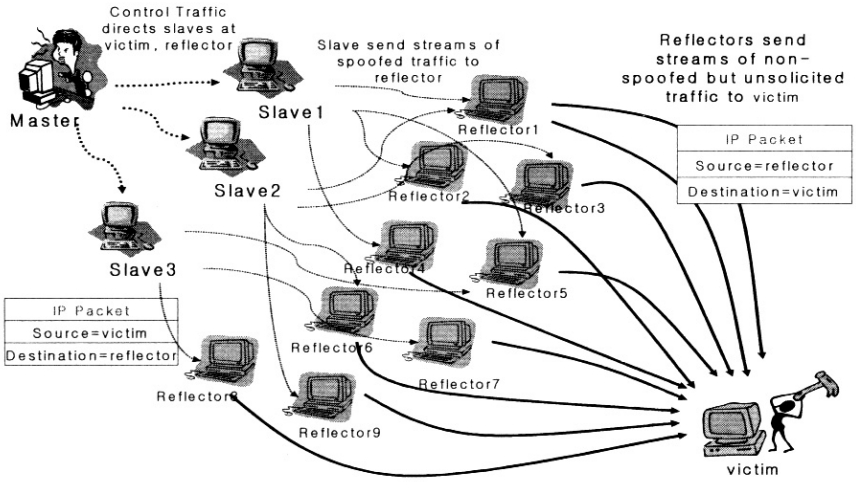
DDoS(Distributed Denial of Service) 공격은 분산된 다수의 Zombie 기반의 DoS 공격 형태로 원격으로 조정되는 Zombie 공격프로그램이 설치되어 있는 머신은 Zombie Master에 의해 공격을 지시 받게 되며 구체적으로 TCP 프로토콜의 취약점을 이용하게 된다. TCP 프로토콜은 SYN 메시지, SYN/ACK 및 ACK 패킷을 송수신하는 "three-way handshake" 방식으로 작동한다.

- 1단계 [SYN] : 웹브라우저, FTP, telnet 클라이언트와 같은 TCP 클라이언트는 TCP 서버의 포트와 TCP 클라이언트의 ISN_{Client}(Initial Sequence Number)가 명시된 SYN 패킷을 TCP 서버에게 보냄으로서 TCP 서버와 접속을 초기화한다. SYN 패킷은 일반적으로 1024~65535사이의 클라이언트 포트에서 1~1023사이의 서비스 포트로 보내진다.
- 2단계 [SYN/ACK] : 서버는 사용 가능한 TCP 서비스 포트를 통해 서버 자신의 ISN_{Server} 값과 $ISN_{Client}+1$ 의 값을 SYN/ACK 패킷으로 생성하여 클라이언트에게 전송한다.
- 3단계 [ACK] : 다시 TCP 클라이언트는 TCP 서버의 SYN/ACK에 대한 응답으로 $ISN_{Server}+1$ 의 값을 ACK로 설정하여 패킷을 전송한다.

DDoS 공격은 TCP 프로토콜에서의 SYN Flooding 방식으로 수행된다. 공격자는 피해 시스템에 자신의 IP를 Spoofing한 후에 TCP 연결을 요청하는 SYN 메시지를 보면, 피해 시스템에서는 위조된 IP로 SYN/ACK를 보내어 연결 준비를 알리고 응답을 기다리게 된다. 만일 이와 같은 과정이 무수히 반복될 경우 피해 시스템의 메모리 버퍼에 대한 오버플로우가 발생하고 결국에는 bandwidth consumption 방식으로 공격하게 된다.

2.2. Reflector 공격 기법[11]

2001년 미국에서 DRDoS(Distributed Reflection Denial of Service) 가 처음 발견되었으며 공격의 대상인



<그림 1> Reflector 기반 DDoS 공격 기법

된 깁슨리서치사 서버는 일반적인 DDoS 공격 패턴과는 달리 정상적으로 동작하고 있는 베리오(Verio.net), 퀘스트(Qwest.net), 어보브(Above .net)의 라우터와 야후의 웹 서버들로부터 공격을 당했다. 즉, 기존의 DDoS 공격이 여러 서버에 설치된 특정 에이전트에 의해 공격이 진행되는 반면, DRDoS 공격은 정상적인 서비스를 운영하고 있는 서버를 에이전트로 활용하기 때문에 해커들이 손쉽게 이용할 수 있다. 또한 DDoS 공격과 달리 공격의 근원지를 추적하기 어렵고 공격을 막을 수 있는 방법이 그리 용이하지 않다. DRDoS 공격은 다음과 같은 과정을 통해 수행된다.

- 1단계 [Master] : 공격자는 Master 시스템에서 DRDoS 공격 스크립트를 생성한다.
- 2단계 [Slave] : Master는 다수의 Slave에 스크립트를 설치한다. 설치된 스크립트에 의해 Slave는 ($SrcAddress = Victim$, $DstAddress = Reflector$)로 출발지 주소가 Spoofing된 SYN 패킷을 생성하여 Reflector에게 전송한다.
- 3단계 [Reflector] : Reflector는 SYN 패킷의 근원지 주소로 설정되어 있는 $SrcAddress = Victim$로 SYN/ACK 패킷을 전송한다. 결국 대량의 SYN/ACK 패킷이 생성되어 피해 시스템으로 전송된다.

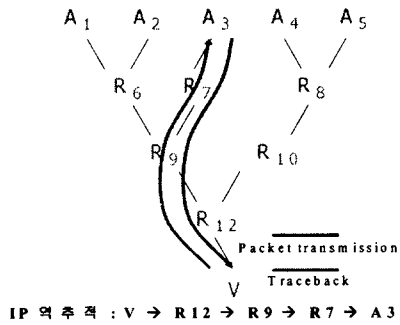
이와 같이 기존의 DoS 공격은 Zombie 기반의 분산 공격 형태로 발전하면서 더욱 강력한 공격 형태를 보이게 되고, <그림 1>과 같이 한단계 더 진보된 reflector 기반의 DRDoS 공격 형태로 발전하였다. 이와 같이 다단계 공격 형태를 보이면서 실제 DoS 공격 근원지에 대해 역추적이 더욱 어려워지고 있다. 따라서 대단위 네트워크에서 DRDoS 공격에 대한 효율적인 대응을 위해서는 공격 근원지에 해당하는 Slave 및 Master에 대한 역추적(traceback) 기법이 제시되어야 한다.

Reflector 기반의 공격에 대한 대응 기법으로 제시된 것은 Reverse iTrace 기법이 있다. 이 기법은 iTrace 기법이 ICMP 패킷을 피해 시스템으로 전송하는 것을 다시 역으로 적용하여 중간 라우터에서는 ICMP 패킷을 패킷의 근원지 주소로 보내는 방식을 사용한다. 물론 개선된 기법으로 제시된 것은 기존의 Pushback[12] 기법을 적용하여 Reflector 공격에 대응하는 방식이 제시되었다. Reflector 기반의 DRDoS 공격에 대응하기 위해서는 기존의 IP 역추적 기술에 대해 고찰할 필요가 있다.

3. Reflector 기반 공격 대응 기술

3.1. 근원지 역추적 기술

IP 역추적(IP Traceback) 기술은 <그림 2>와 같이 피해 시스템 V에서 패킷의 실제 전달 경로를 재구성하는 기술이다.



<그림 2> IP 역추적 기술 개념도

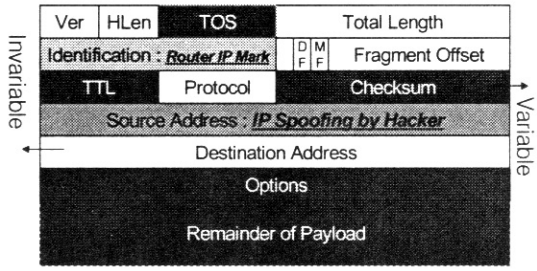
인터넷에서의 패킷 특성상 TCP 계층을 중심으로한 서비스 중심의 역추적 기능 보다는 패킷 자체의 네트워크 전송 과정을 다루는 IP 계층에서의 역추적 기능을 제공하기 위한 연구가 활발히 진행되고 있다. 따라서 IP 계층을 중심으로 현재까지 제시된 역추적 기술을 분류하면 해킹 대응 방식에 따라 크게 전향적 역추적 기술(proactive IP traceback)과 대응적 역추적 기술(reactice IP traceback)로 나눌 수 있으며 IP 역추적 기술이 갖추어야 하는 요구사항으로는 다음과 같다[3].

- 기존 네트워크 프로토콜과의 호환성
- 네트워크 부하 최소화
- 구현 가능성
- 기존 라우터 및 네트워크 구조와의 호환성
- DDoS 공격 대응력과 시간/자원 활용의 효율성

일반적인 IP 역추적 기법으로 패킷에 대한 확률적 마킹(PPM : probabilistic packet marking) 기법과 전통적인 ICMP 메시지를 변형한 iTrace (ICMP traceback) 기법이 있다.

PPM 기법[6]은 스푸핑된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해서는 IP 계층을 중심으로 네트워크 상에 전송되는 패킷에 대해 네트워크를 구성하는 주요 요소인 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달되었다는 정보를 삽입하는 방식이다. 아래 <그림 3>과 같이 IP 헤더에서 16비트 ID 필드에 라우터 자신의 IP 정보를 삽입하게 된다.

기존의 PPM 기법에서는 확률 p로 패킷을 선정하게 되는데 경로 재구성을 위해서는 상당히 많은 개수의 마킹된 패킷이 필요하다. 만일 특정 라우터에서의 에지 정보 또는 노드 정보 등이 마킹되지 않고 전달된다면 나머지 마킹된 정보를 가지고는 완벽한 공격 경로를 재구성할 수 없다는 문제점도 발견할 수 있으며, 최소한 하나의 노드 또는 에지 정보를 마킹하는데 알고리즘에서는 최소한 8개의 패킷을 선정하여 마킹해야 하기 때문에 전체적인 효율 면에서도 비효율적이다.

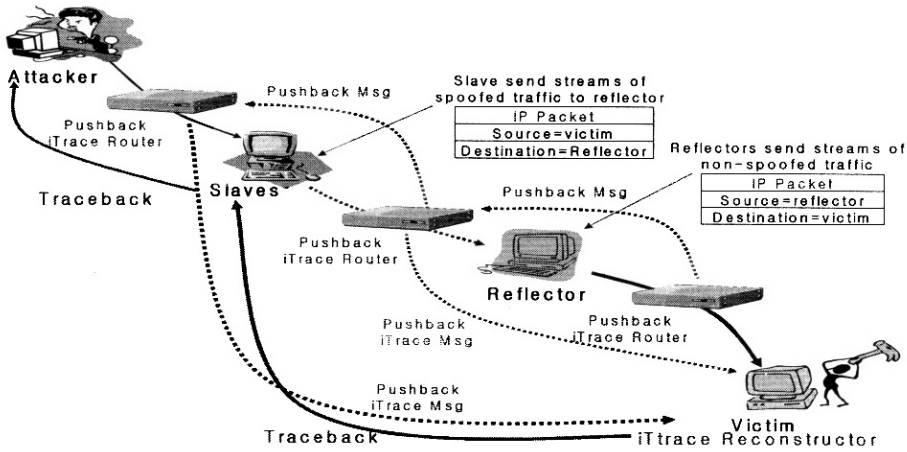


<그림 3> PPM 기법에서의 IP 헤더 마킹

iTrace(ICMP Traceback) 기법[7]은 PPM 기법과는 다른 접근 방법으로 수행된다. 라우터에서는 일반적으로 $\frac{1}{20,000}$의 확률로 패킷을 샘플링하여 iTrace 메시지를 생성하고 이를 패킷의 목적지 IP로 전송한다. iTrace 메시지는 일반적인 ICMP 메시지와 유사하게 전단계 라우터 정보와 다음 단계 라우터 정보를 포함하고 있으며 패킷의 payload 정보 등을 포함하여 전달하게 된다. iTrace 기법인 경우 기존의 패킷 정보에 대해 PPM과 마찬가지로 확률 p로 샘플링하여 메시지에 대한 iTrace 메시지를 생성하고 이를 목적지 IP로 전송하는 방식이다. 그러나 현재 DDoS 공격 기법 중의 하나로 ICMP 기법을 이용한 방식이 발견되고 있어서 결국에는 iTrace 기법 역시 목적지 피해 시스템 측면에서 보았을 경우에는 또다른 하나의 DDoS 공격으로도 보일 수 있다는 단점이 있다.

3.2. Reflector 공격에 대한 대응 기술

기존의 Pushback 기법은 라우터에서 패킷 폭주가 발생하였을 경우 ACC 기반의 모듈을 적용하여 해킹 패킷의 형태와 비교하고 만일 해킹으로 판단될 경우 라우터에서는 패킷이 전송된 앞단의 라우터에게 Pushback 메시지를 전송하여 라우터로 하여금 패킷 필터링 모듈을 작동시키도록 한다. 따라서 일반적인 Pushback 기법은 해킹 등의 DoS 공격이 발생할 경우 다량의 패킷이 전송되게 되므로 이를 라우터에서 제어



<그림 4> Reflector 기반의 DDoS 공격에 대한 대응 기술

할 수 있는 기능을 제공한다.

하지만 기존의 Pushback 기법은 DoS 공격 등에 대한 제어/판단 기능은 제공하지만, 피해 시스템에게 공격 근원지에 대한 역추적 기능을 제공하지는 못한다. 따라서 개선된 역추적 기법으로는 패킷에 대한 제어/판별 기능을 제공하는 Pushback 기법의 장점을 PPM/iTrace 등의 IP 역추적 모듈과 접목하는 방법이 있다.

제시하는 Pushback 기반의 역추적 기법인 경우 <그림 4>와 같은 과정을 수행하여 DRDoS에 대한 공격 근원지를 역추적하게 된다.

- 1단계 : 라우터에 Pushback 기반 패킷 마킹 모듈 설치
  - 각 라우터에는 본 연구에서 제시하는 Pushback 기능을 제공하는 패킷 마킹 모듈을 탑재하고 있다고 가정
  - 라우터 i에서 패킷 P_i 전송 함수 $R_i(P_i)$
  - 패킷에 대한 Pushback 기반 마킹 함수 $M_{R_i}(P_i)$
- 2단계 : 라우터에서의 패킷 마킹
  - 각 라우터에서는 확률 p로 패킷을 선택하여 패킷 마킹 과정을 수행한다.
  - 마킹된 패킷에 대해서는 패킷의 다음 라우팅 경로로 전송된다. $(R_i(P_i^*)\ when\ P_i^* = M_{R_i}(P_i))$
- 3단계 : ACC 기반의 트래픽 모니터링
  - 일반적으로 iptable/snort-inline 등의 오픈 소스를 이용하여 end 시스템에서는 트래픽을 모니터링
  - 라우터 i에서 시점 T에 ACC 모듈이 판단한 이상 트래픽의 평균 임계치 $Sig(T)$보다 클 경우 IP Traceback 모듈을 가동
  - Pushback 모듈에 의해 주변 라우터에 이상신호 메시지를 전송

$$if\ ACC(P_j) > Sig_j(T)\ then\ Alarm = 1$$

$$else\ P_j^* = M_{R_j}(P_j), Alarm = 0$$

$$where\ Sig_j(T) = (\sum_{n=1}^{j} P_n)\ /\ T_j$$

$$if\ Alarm \equiv 1\ then\ R_j^{-1}(P_{Pushback})$$

- 4단계 : ICMP 메시지 생성 및 발송
  - 각 라우터 R_x에서는 패킷에 대한 ICMP 메시지 $ICMP_{P_{pushback}}$를 생성하여 패킷의 목적지로 전송

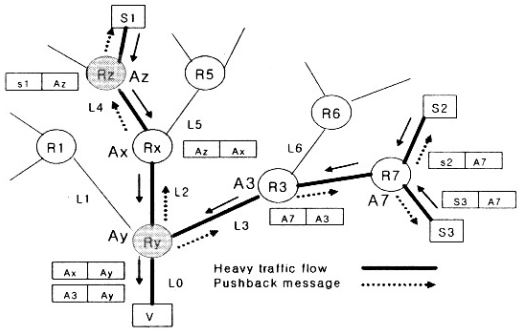
$$if\ P_{pushback}\ then\ R_x(ICMP_{P_{pushback}})$$

이와 같은 과정을 통해 피해 시스템 V에서는 수신된 패킷과 ICMP 정보를 이용하여 공격 근원지 경로를 재구성하게 된다.

이와 같은 과정을 통해 라우터에서는 ACC 모듈을 통해 네트워크상에 트래픽에 대한 감시 및 판단 기능을 수행하면서도 변형된 pushback 기술을 적용하여 네트워크 제어 기능을 수행할 수 있고, DDoS 해킹 경로를 역추적하기 위해서 개선된 패킷 마킹 기술을 적용하여 스푸핑된 패킷에 대한 역추적 기능도 제공하여 공격자에 대한 근원지를 재구성할 수 있다.

아래와 같은 네트워크 구조에 대해 본 연구에서 제시한 기법을 적용하게 되면 피해시스템에 대한 DDoS 공격 경로 AP를 다음과 같이 구할 수 있다.

$AP_1 = R_y \rightarrow R_x \rightarrow R_z \rightarrow S1$, $AP_2 = R_y \rightarrow R_3 \rightarrow R_7 \rightarrow S2$,
$AP_2 = R_y \rightarrow R_3 \rightarrow R_7 \rightarrow S2$



<그림 5> 제안한 기법에서의 공격 경로 역추적

제시된 기법을 활용할 경우 기존의 IP 역추적 기법과 같이 공격 근원지에 대한 IP 역추적 기능을 제공할 뿐만아니라, 전체적인 DDoS 패킷에 대한 감소/제어 기능까지도 제공하기 때문에 효율적인 것으로 나타났다. 또한 앞에서 제시한 iTrace 기법을 적용할 경우 Reflector 등에 기반한 다단계 DRDoS 공격에서의 근원지 역추적 기능도 제공할 수 있는 장점을 제공한다.

4. NS-2 기반 IP 역추적 시뮬레이터

4.1. NS-2 기반 시뮬레이션

앞에서 제시한 Reflector 기반의 공격에 대한 대응기술의 성능을 평가하기 위해서는 시뮬레이션 도구를 사용할 수 있다. 네트워크 공격 등에 대한 대응 기술로 제시된 IP Traceback 기술의 성능을 실험하기 위해서는 일반적으로 네트워크 공격 형태를 모의적으로 구성하고 현재의 DDoS 공격과 유사한 형태를 시뮬레이션하여 대응 기법의 성능을 비교 분석할 수 있다.

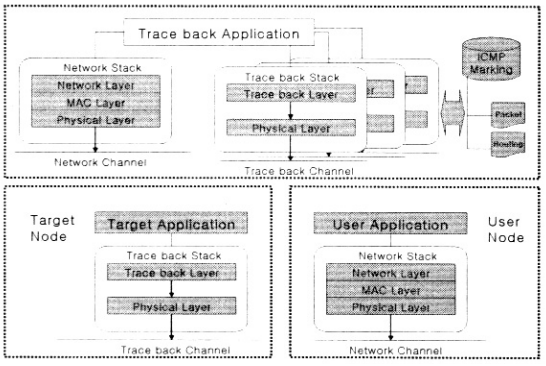
현재 IP 역추적에 대한 시뮬레이션 기법으로 가장 많이 사용되는 것은 NS-2[5] 기반의 시뮬레이터를 기반으로 실험하는 것이다. 유선 네트워크 형태를 랜덤하게 구성하여 DDoS 공격 네트워크 형태를 구축하고 이를 통해 패킷을 전송하여 피해 노드에서의 경로 역추적 과정을 모의 실험할 수 있다.

본 연구에서는 NS-2를 이용하여 대규모 DDoS 공격 네트워크를 구성하고 이를 기반으로 현재까지 제시된 IP 역추적 기법들에 대해 시뮬레이션하여 전체적인 트래픽량을 비교 분석하였다.

NS-2 시뮬레이션을 수행하면 각 노드별 전체 트래픽의 양을 분석할 수 있으며, 개별적인 패킷의 양도 측정이 가능하다. 따라서 NS-2 시뮬레이션을 기반으로 실험할 경우 제시한 알고리즘에 대한 성능을 효율적으로 실험할 수 있으며 제시한 알고리즘과 기존 알고리즘을 효율적으로 비교/분석할 수 있는 특징을 제공한다. 본 연구에서는 기존의 IP 역추적 기법들과 본 연구에서 제시한 기법들에 대해 DDoS 공격 발생시 피해 시스템 및 중간 라우터에서 발생하는 전체 트래픽의 양을 비교 분석하였다.

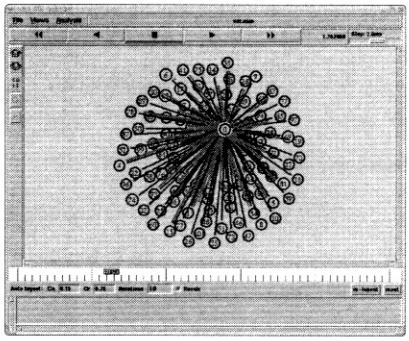
4.2. IP 역추적 시뮬레이션 시스템 구성도

본 연구에서는 <그림 6>과 같이 NS-2에서의 IP 역추적 시뮬레이터를 설계하였다. NS-2에서는 각 노드에 대한 설계를 기반으로 IP 역추적 기능을 탑재한 모듈을 설계할 수 있다. 각 노드에서는 CBR 방식의 패킷을 생성하여 목적지 시스템에 랜덤 형태의 트래픽을 발생하여 전송할 수 있다.

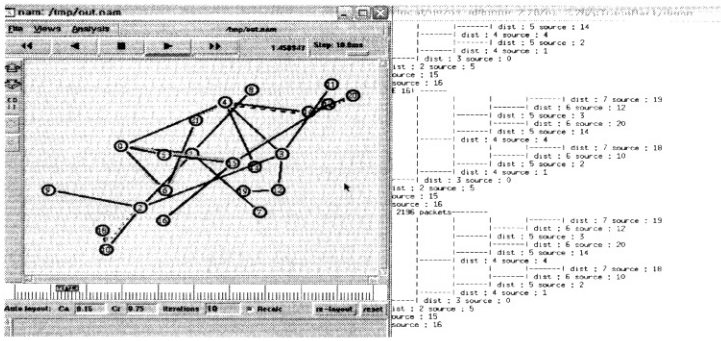


<그림 6> NS-2 기반 IP 역추적 시뮬레이터 구성도

제시한 NS-2 기반 IP 역추적 시뮬레이터에서는 최근 연구가 되고 있는 Reflector 기반의 DDoS 공격에 대응하기 위한 IP 패킷 마킹 알고리즘을 설계하여 실험하였다. 제시한 기법에서는 Pushback 기법과 ICMP 메시지를 접목하여 라우터에서 이전 라우터에게 메시지를 전송하고 DDoS 공격 패킷에 대해서는 마킹하여 피해 시스템에 전송하게 된다. 최종적으로 피해 시스템에서는 마킹된 패킷 정보와 ICMP 패킷 정보를 조합하여 실제 DDoS 공격 근원지를 검출하게 된다.



<그림 7> NS-2 기반의 DDoS 공격 구조 설계

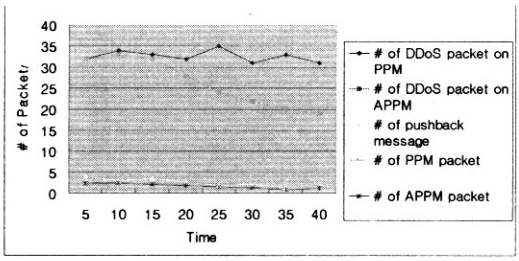


<그림 8> NS-2 기반의 IP 역추적 시뮬레이션 실험 결과

4.3. IP 역추적 시뮬레이션 실험 결과 분석

본 연구에서 제시한 구조에서는 임의의 형태의 네트워크를 구성할 수 있으며 이를 통해 다양한 형태의 토폴로지를 구성할 수 있다. <그림 7>과 같은 구조를 기반으로 본 연구에서는 <그림 8>과 같은 공격 구조를 설계하고 실제적으로 IP 패킷에 대한 역추적 구조를 실험할 수 있었다.

본 연구에서는 기존에 제시된 PPM 기법과 본 연구에서 개발한 새로운 Pushback 기반의 Reflector DDoS 공격 IP 역추적 기법의 성능을 비교 분석하였다. <그림 9>와 같이 본 연구에서 제시한 기법은 기존의 역추적 기법보다 DDoS 공격이 발생하였을 경우 피해 시스템에서의 트래픽을 감소시키는 효과을 얻을 수 있으며 결과적으로 DDoS 공격에 대한 효율적인 대응 구조를 제공한다는 것을 확인할 수 있었다.



<그림 9> IP 역추적 기법의 트래픽 비교 분석

본 연구에서 제시한 DRDoS 대응 모듈은 기존의 PPM 및 iTrace 기법과 비교하였을 경우 아래 (표 1)과 같다. 본 연구에서 제시한 기법에 의해 발생하는 역추적 패킷 개수(네트워크 부하) 및 피해 시스템의 부하 측면을 비교하였을 경우 기존의 PPM 및 iTrace 기법보다도 증가한다는 단점은 있다. 이는 본 연구에서 제시한 기법이 Reflector 기반의 다단계 역추적 기능을 제공하기 위해 패킷 마킹과 ICMP 패킷을 발생시키며, ACC 모듈 등을 필요로 하기 때문이다. 하지만, 본 연구에서 제시한 기법은 ACC 기반의 공격 트래픽 제어/판별 기능을 제공하며, DRDoS 공격에 효율적으로 대응할 수 있다는 장점을 제공하고 있다.

5. 결 론

본 연구에서는 인터넷을 통해 급격히 확산되고 있는 해킹·바이러스에 대한 대응 기술로서 DDoS 공격 등이 발생하였을 경우 스푸핑된 트래픽에 대한 실제적인 공격 근원지 IP를 피해 시스템에서 역추적하는 기술에 대해 살펴보았다. NS-2 기반 시뮬레이터를 설계/개발하여 성능에 대해 비교/평가한 결과 기존 역추적 기술의 구조와 현황, 문제점 등을 발견할 수 있었으며 이를 바탕으로 새로운 IP 역추적 기술에 대해서도 고찰하였다.

IP 계층에서의 보안 프로토콜이 제공되는 환경인 IPSec 기반 환경과 일반 IP 계층에서의 역추적 기능도 고려해 보아야 한다. 특히 IPv6[13] 환경으로 급격히 변화하면서 IPv6 환경에서의 DDoS 공격 등에 대한 대응 기술에 대해 연구가 필요하다. 물론 IPv6는 기존의 IPv4보다도 성능, 보안 및 안전성이 개선된 구조를

(표 1) 제안한 기법과 IP 역추적 기법과의 비교

특성 / 기법	역추적 패킷개수	피해시스템부하	트래픽제어	DDoS 대응	DRDoS 대응
PPM[6]	↓	↓	×	◇	×
iTrace[7]	↓	↓	×	◇	×
제안한 방식	↑	↑	△	△	△

×:N/AT ↑:high, ←:middle ↓:low △:good ◇:moderate ▽:bad

제공하고 있다. 하지만 IPv6 구조의 복잡성 및 난해성으로 인해 마찬가지로 기존 IPv4 환경과 유사한 방식의 DDoS 공격이 가능하다. 특히 IPv6에서는 이동성을 지원하는 과정에서 보안 취약점이 발견되는 등 더욱 더 심각한 문제를 유발할 수도 있다. 따라서 앞으로는 IPv6 환경에 기반한 DDoS 대응 기술에 대한 연구가 수행되어야 할 것이다.

참 고 문 헌

[1] L. Garber. "Denial-of-service attacks trip the Internet". Computer, pages 12, Apr. 2000.

[2] Computer Emergency Response Team, "TCP SYN flooding and IP Spoofing attackts," CERT Advisory CA-1996-21, Sept, 1996.

[3] Andrey Belenky, Nirwan Ansari, "On IP Traceback," IEEE Communication Magazine, pp.142-153, July, 2003.

[4] John Elliott, "Distributed Denial of Service Attack and the Zombie and Effect", IP professional, March/April 2000.

[5] K. Fall, "ns notes and documentation", The VINT Project, 2000.

[6] D. X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback," Proc, Infocom, vol. 2, pp.878-886, 2001.

[7] Steve Bellovin, Tom Taylor, "ICMP Traceback Messages", RFC 2026, Internet Engineering Task Force, February 2003.

[8] R. Stone, "CenterTrack: an IP overlay network for tracking DoS floods," Proc, 9th Usenix Security Symp., Aug., 2000.

[9] A.C. Snoeren, C. Partridge, L.A. Sanchez, W.T. Strayer, C.E. Jones, F. Tchakountio, and S.T. Kent, "Hash-Based IP Traceback", BBN Technical Memorandum No. 1284, February 7, 2001.

[10] H. Y. Chang et al., "Deciduous : Decentralized Source Identification for Network-based Intrusions," Proc, 6th IFIP/IEEE Int'l Symp., Integrated Net., Mmgt., 1999.

[11] Vern Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", ACM Comp. Commun. Rev., vol.31, no.3, July 2001, pp. 3-14.

[12] S. Floyd, S. Bellovin, J. Ioannidis, K. Kompella, R. Mahajan, V. Paxson, "Pushback Message for Controlling Aggregates in the Network", Internet Draft, 2001.

[13] Deering, S. and R. Hinden, "Internet Protocol, Version 6, (IPv6) Specification", RFC 2460, December 1998.

이 형 우

1994 고려대학교 컴퓨터학과 (이학사)
1996 고려대학교 컴퓨터학과 (전산학 석사)
1999 고려대학교 컴퓨터학과 (전산학 박사)
1999~2003 천안대학교 정보통신학부 교수
2003~현재 한신대학교 소프트웨어학과 교수
관심분야: 정보보호, 네트워크보안, 시뮬레이션
E-Mail: hwlee@hs.ac.kr