

# Pushback 방식을 적용한 DDoS 공격 근원지 역추적 기술

<sup>1</sup>이형우, <sup>2</sup>최창원, <sup>3</sup>김태우, <sup>4</sup>박영준

<sup>1</sup>한신대학교 소프트웨어학과, <sup>2</sup>정보시스템공학과

<sup>3</sup>성공회대학교 컴퓨터정보통신학부, <sup>4</sup>청강문화산업대학 인터넷비즈니스과

## Pushback based DDoS Attack IP Traceback Mechanism

Hyung-Woo Lee, Chang-Won Choi, Tai-Woo Kim, Yeong-Joon Park  
Dept. of Software, Dept. of Information System, Hanshin University  
Division of Computer & Information Science, Sungkonghoe University  
Dept. of Internet Business, Chungkang College of Cultural Industries

### 요약

본 연구에서는 DDoS 공격과 같은 인터넷 해킹 공격에 대해 근원지 IP에 대한 새로운 역추적 기술을 제시하였다. 현재까지 제시된 IP 역추적 기법은 크게 패킷을 중심으로 한 마킹 방법론을 사용한 기법과 네트워크 관리 차원에서 경로 정보를 관리하는 기법 및 보안 프로토콜을 이용한 방법 등으로 나눌 수 있다. 각각의 기법은 현재의 인터넷 환경에서 적용하였을 경우 DDoS 공격에 대해 장단점을 보이고 있으며 적용 방법 및 해킹 공격의 특성에 따라서 다양한 성능을 보인다. 본 연구에서는 DDoS 공격에 대한 라우터 중심 대응 기술로 제시된 pushback 기법을 적용하여 라우터를 중심으로 해킹 공격 근원지를 역추적하는 ICMP traceback 기반 역추적 기법을 제시하였다.

### I. 서론

현재 TCP SYN flooding<sup>[1]</sup> 공격과 같은 DoS 공격을 통해 TCP/IP 체계의 취약점이 노출되어 있기 때문에 네트워크 및 인터넷에서의 해킹 공격에 대응할 수 있는 방안에 대해 연구가 진행되고 있다. 현재까지 제시된 기법은 접근 제어 기술로서 해킹 공격에 수동적인 특징을 보이고 있으며, IDS 시스템을 통한 대응 기술 역시 해킹 발생 트래픽에 대한 검출 기능을 제공하고 있다. 그러나 기존 기술은 해킹 공격 근원지에 대한 확인 기능을 제공하고 있지 못해 결국 DDoS<sup>[2]</sup> 공격자를 찾아내지 못하고 있다. 그 이유는 대부분의 해킹 공격이 근원지 IP 주소를 스판핑하는 방식으로 수행되므로 이에 대한 대응 기술이 개발되어야 한다. 본 연구에서는 해킹 및 바이러스에 대한 능동적인 대응 방안에 대해 고찰하고 현재까지 제시된 전향적/대응적 역추적 기법에 대한 비교 분석을 바탕으로, 기존의 pushback 기법을 개선하여 역추적 기능을 적목한 새로운 방식의 IP 근원지 역추적 기술을 제안하고자 한다. 2장에서는 해킹 공격 근원지 역추적 기술 현황 및 대응 방안에 대해 살펴보고, 3장에서는 라우터 기반 pushback 기술을 고찰하였다. 4장에서는 DDoS 공격 근원지에 대한 새로운 IP 역추적 기술에 대해 제시하고 5장에서 결론을 맺는다.

### II. 해킹 공격 근원지 역추적

#### 1. 근원지 역추적의 필요성

해킹사건에 사용된 수법은 분산 서비스 거부공격(DDoS: Distributed Denial of service)이며 이는 몇 개의 서버와 수많은 하부서버(클라이언트)를 생성하고 마스터 서버에 접속하여 하나 혹은 여러 개의 IP 주소를 대상으로 서비스 거부 공격을 수행하게 된다. 이럴 경우 트리뷴 마스터는 특정한 기간에 하나 혹은 여러 개의 IP 주소를 공격하도록 하부 서버와 통신한다<sup>[2]</sup>.

이는 공격자의 명령에 의해 공격 도구가 설치된 대량의 서버들을 제어해 공격 대상 시스템에 치명적인 서비스 거부 공격을 수행하기 때문에 인터넷을 교란시키려는 해커들에 의해 악용될 수 있다. 인터넷에서 해킹 공격이 발생하였을 경우 현재까지는 Firewall, IDS, scanning 및 trusted OS 기반 시스템 보안 등의 방법을 사용하는 등 수동적인 측면에서의 해킹 대응 방안을 수립·운영할 수밖에 없었다. 특히 기존의 방식은 해킹 시도 자체를 제한하거나 방지할 수 없는 방식으로서 결국에는 인터넷이 마비되거나 무용지물화되는 특성을 보이고 있다.

이러한 문제를 해결하기 위해서 제시된 기술이 바로 능동적인 해킹 방지 기술이다. 새로운 방식에서는 해킹 시도 자체를 방지

하거나 이를 능동적으로 실시간내에 추적할 수 있는 기술 등이 제공되어서 해킹 시도 자체를 방지하고자 하는 것이 주요 목적이 다. 따라서 해킹·바이러스에 대한 능동적인 대처를 위해 필수적인 기술로 최근 그 중요도가 높아지고 있는 기술이 역추적(traceback) 기술이다<sup>[4]</sup>.

## 2. 의명적 해킹 공격에 대응하기 위한 기존 기술

역추적 기술과 유사하게 스푸핑된 IP 패킷 등을 이용하여 DDoS 공격이 발생하였을 경우 이에 대한 대응 기법으로 현재까지 연구된 기법들은 크게 필터링(filtering) 기법을 통한 대응 기술과 접근 제어(access control) 기술을 적용한 대응 기술, SYN flooding 검출 기술 등으로 나눌 수 있다.

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 세부화된 역추적 기술을 분류하면 해킹 대응 방식에 따라 크게 전향적 역추적 기술과 대응적 역추적 기술로 나눌 수 있으며, 세부 기술로 나누어 본다면 라우터 중심의 역추적 기술, 패킷 정보에 대한 관리 시스템 구현 기술, 특수 네트워크 중심 기술 및 관리 기술 중심 역추적 방식으로 분류할 수 있다.

### ○ 해킹 역추적 대응 방식에 따른 분류

#### - 전향적(proactive) 역추적 기술

- 패킷 전송 과정에서 역추적 정보를 생성하여 삽입하거나 전달하는 방식으로, 만일 해킹 공격이 발생하였다면 이미 전송된 역추적 정보 등을 조합하여 공격 근원지를 판별
- 패킷 마킹 기법<sup>[4,5]</sup> 및 ICMP 역추적 메시지 기반 역추적 기법<sup>[6]</sup> 등

#### - 대응적(reactive) 역추적 기술

- 해킹 공격이 발생한 것이 확인되었다면 해킹 공격에 의한 연결이 형성되어 있는 상태에서 공격 근원지를 역추적
- 흡대홍(hop-by-hop) 역추적<sup>[7,8]</sup>, 해쉬 기반 IP 역추적 기술<sup>[9]</sup> 및 IPSec 기술을 이용한 역추적 기술<sup>[10]</sup> 등

## III. 라우터 기반 역추적 기술

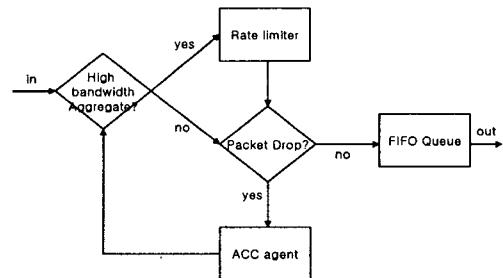
### 1. 라우터 기반 DDoS 공격 대응 기술

TCP SYN 공격이나 ICMP ECHO 패킷 등에 의한 해킹 공격을 살펴보면 많은 양의 트래픽이 네트워크를 통해 전달되고 또한 특정 목적지로 트래픽이 전달되는 특성을 보이고 있다. 따라서 이와 같은 현상에 대응하기 위해서는 우선 네트워크상에서 전달되는 트래픽에 대해서 해킹 공격에 해당하는 트래픽을 판별(identification)할 수 있는 기술이 제공되어야 하고, 이와 같은 트래픽을 제어(control)할 수 있는 기술이 접목되어 전체 해킹 관련 트래픽을 줄이거나 추후 공격 근원지 등에 대해 역추적 과정을 수행할 수 있어야 한다. 만일 라우터에 의해 해킹 트래픽 판별/제어 기능과 해킹 피해 시스템에서의 공격 근원지 역추적 기술 등이 결합될 수 있다면 DDoS 공격에 대한 효율적인 대응 방안이 제시될 수 있을 것이다.

### 2. 라우터 기반 트래픽 판별/제어

라우터에서의 DDoS 트래픽 제어 기술로 제시된 것이 ACC(aggregate-based congestion control) 및 pushback 기술이다. 이 기술은 라우터에서 주기적으로 네트워크 트래픽에 대한 모니터링 과정을 수행하면서 만일

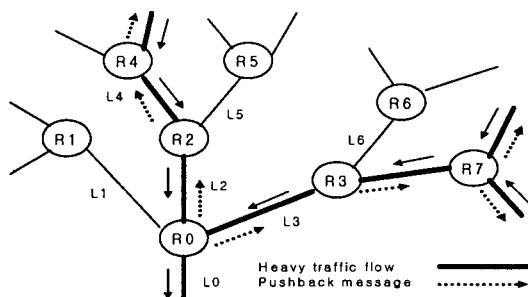
해킹 공격과 유사한 형태의 트래픽이 발생할 경우 이를 판별한다. 해킹 공격은 매우 다양하기 때문에 트래픽에서의 혼잡 특성에 해당하는 혼잡 시그너처(congestion signature)를 기준으로 트래픽을 판별하게 된다. 즉, DDoS 공격이 갖는 네트워크 트래픽의 특성을 기준으로 특정 대역폭 이상으로 폭주 현상을 보인다면 이와 같은 혼잡 시그너처를 기반으로 해킹 공격이 발생하였다고 판단할 수 있으며, 필터링 모듈을 접목하여 DDoS 공격 형태에 해당하는 트래픽에 대해서는 전송 방지 기능을 제공하게 된다. 아래 그림은 라우터에서의 혼잡 발생시 ACC 기반 판별/제어 구조를 보이고 있다.



<그림 1> ACC 기반 트래픽 판별/제어 구조

이와 같은 판별/제어 과정은 아래 그림에서와 같이 pushback<sup>[14]</sup> 모듈과 접목된다. pushback 모듈에서는 DDoS 공격을 확인한 경우 네트워크 경로상 인접한 전단계 라우터로 pushback 메시지를 전송한다. 전달된 메시지는 반복적으로 전달되어 해킹 공격 근원지까지 도달하게 된다.

그러나, pushback 기법에서는 라우터 중심으로 공격 근원지에 대한 상위 라우터로 메시지를 전송하지만 근본적으로 해킹이 발생하였을 경우 최종적인 근원지를 역추적 할 수 없다는 문제점이 있다. 즉, 해킹 피해 시스템에서 공격 근원지에 대한 경로 역추적 등을 확인하기에는 부가적인 절차를 필요로 하기 때문에 이에 대한 개선책이 제시되어야 한다.



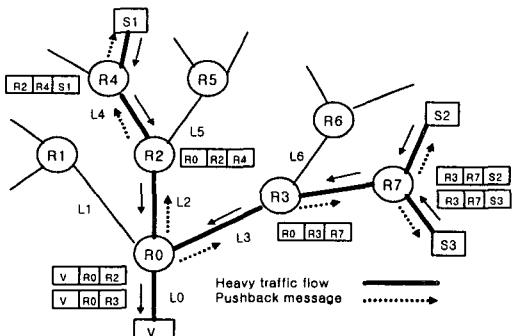
<그림 2> ACC 기반 Pushback 기술 구조

### 2. 개선된 라우터 기반 역추적

기존의 ACC 기반 pushback 기법에서는 라우터에서 인터넷 트래픽을 판별/제어하고 라우터에서 트래픽이 전달된 상위 경로로 pushback 메시지를 전달하는 방식이다. 그러나, 실제로 DDoS 공격이 발생하지 않았을 경우에도 부가적으로 라우터에서는 상위 라우터에 대한 추적 과정을 수행하기 때문에 실제적으로는 효율성 측면에서 문제점을

발견할 수 있다. 따라서 본 연구에서는 라우터에서 DDoS 공격에 해당하는 트래픽을 판별하였을 경우 전체 트래픽을 제어하는 과정은 기존의 ACC 기법과 유사한 과정을 수행하고 ICMP 역추적 메시지를 생성하여 이를 목적지에 전송한다. 그리고, 기존의 pushback 기법을 적용하여 상위 라우터에 전달하며 pushback 메시지를 받은 라우터에서는 마찬가지로 ICMP 기반의 traceback 메시지를 생성하여 목적지에 전송하게 된다. 본 기법에서 적용하는 ICMP traceback 메시지에는 DDoS가 발생하였을 경우 해당 라우터에서 pushback 기법을 통해 확인된 상위 라우터 경로로 이동하면서 역추적 관련 정보를 생성하여 목적지에 전달하는 방식이다. 개괄적인 구조를 그림으로 제시하면 다음과 같다.

본 연구에서 제시한 기법에서는 기존의 ICMP 역추적 기법에서 일괄적으로 확률  $p$ 에 의해서 패킷을 선택하고 이에 대해 ICMP 역추적 메시지를 생성하여 목적지에 전달하는 것이 아니라, 라우터에서 혼잡 시그너처에 기반하여 우선 라우터를 지나는 트래픽에서의 이상 현상을 검출한 후 해당 트래픽의 상위 라우터에게 pushback 메시지를 전송하면서 상위 라우터에게 이상 징후를 알린다. 또한 DDoS 공격 트래픽이 전달되는 경로를 역으로 추적하면서 ICMP traceback 메시지를 생성하게 함으로써 기존의 기법에서 고정적 확률  $p$ 로 패킷을 선정하여 전달하는 방식보다 개선된 역추적 기능을 제공할 수 있다.



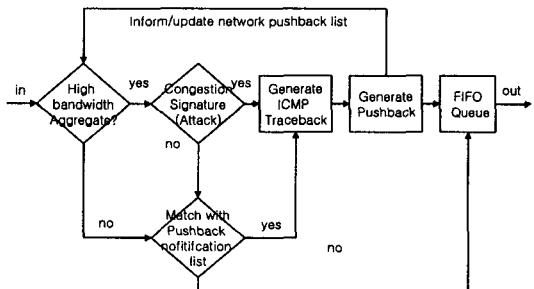
<그림 3> 개선된 Pushback 기반 경로 예측적

### 3. Pushback을 적용한 ICMP Traceback 기법

본 연구에서 제시하는 기법의 작동 구조 및 절차를 구체적으로 제시하면 다음과 같다. 기존의 ACC 및 pushback 기법과 유사하게 라우터에서 인터넷상에서의 트래픽에 대한 모니터링/필터링 과정을 수행하게 된다. 그러나 기존의 기법과는 달리 이상 트래픽이 발견되었을 경우 단순히 pushback 메시지를 상위 라우터에 재귀적으로 전달하여 근원지 경로를 찾아가는 방식을 변형하여 pushback 메시지를 상위 라우터에 전달하면서 ICMP traceback 메시지를 생성하여 이를 목적지 호스트에 전송한다.

본 연구에서 제시하는 기법에서 변형된 ACC 기반 구조는 다음과 같다. 라우터에 들어온 패킷에 대해 트래픽의 대역폭을 검사하고 일정 이상으로 도착하게 되면 공격 형태에 해당하는 혼잡 시그널인지를 판단하게 된다. 만일 공격 형태 트래픽에 해당한다면 ICMP traceback 메시지를 생성하고 동시에 해당 패킷에 대한 pushback 메시지를 생성하여 이를 라우터의 출력 큐로 하여금 전송토록 한다. 만일 대역폭 조건을 만족하지 않을 경우에는 이전에 pushback 메시지를 통해 주변 라우터로부터 전달된 정보

가 있는지를 확인하고 만일 해당된다면 마찬가지로 ICMP traceback 메시지를 생성하여 전달한다. 위 조건을 만족하지 않을 경우에는 일반적인 트래픽으로 간주하고 라우터를 통해 다음 라우터에게 전달도록 한다.



#### <그림 4> 타우터 기반 DDoS 근원지 혁주적 구조

#### 4. ICMP Traceback 메시지 구성

기존의 연구에서는 IP 헤더에서 ID 부분을 대상으로 라우터에서 라우터 자신의 IP 주소 정보를 해쉬를 적용하여 삽입하거나 아니면 단편화를 통해 몇 개의 IP 패킷에 나누어 정보를 삽입하였다. 그러나, 이와 같은 과정을 수행하게 되면 16비트 헤더 checksum 부분에 오류가 있게 되기 때문에 결과적으로 전체 네트워크에 대한 신뢰성을 떨어들게 된다. 만일 기존의 방식에서처럼 라우터가 16 비트 ID 필드에 IP 역추적 정보를 삽입하게 된다면, 실제적인 측면에서 전체 헤더에 대한 checksum 값의 변경을 가져오게 된다. 이와 같이 헤더에 대한 checksum 값에 변경이 있다는 것은 결과적으로 IP 헤더에 대한 근원지 IP 주소 값에 대해 또 다른 변경 및 수정이 가해질 수도 있다는 것을 의미하기 때문에 결과적으로 기존의 기법에서는 현실적인 측면에서 IP 패킷에 대한 신뢰성을 떨어뜨리게 된다.

따라서 본 연구에서는 IP 헤더에 대한 변경을 수행하지 않으면서도 라우터에 대한 역추적 정보를 생성할 수 있는 과정을 제시하고자 한다. 구체적으로 아래 그림에서와 같이 IP 헤더 주소에서 옵션 및 패딩 부분을 제외하고 변하지 않는 부분은 전체적으로 HLEN, TTL 및 Checksum 부분은 제외하여 옵션 이전까지를 계산하면 128비트가 된다. 따라서, 이와 같은 128 비트에 대해 라우터에서는 인증 기능을 제공하기 위해 사용한다.

### 5. DDoS 공격에 대한 ICMP Traceback 메시지 생성

라우터  $Rx$ 의 IP 주소를  $Ax$ 라고 하자. 그리고  $Rx$ 에 도착한 IP 패킷을  $Px$ 라고 하고  $Px$ 에서의 해더에서 고정 부분 128 비트를 마스크 하여 얻어낸 부분은  $Mx$ 라고 하자.  $Mx$  값은 128비트 정보로 되어 있으며, 특정 근원지 IP 주소에서 목적지 IP 주소로 전달하고자 하는 패킷인 경우 유일한 특성을 갖는다. 따라서 128 비트 정보에 대해 아래와 같이 32비트 블록 4개로 구성할 수 있다.

$$Mx \equiv Hx_1 + Hx_2 + Hx_3 + Hx_4$$

128 비트에 대한 4개의 32비트 서브 블록에 대해 아래와  
같은 과정을 수행하여  $Hx$  32비트를 그릴 수 있다.

$$Hx = Hx_1 \oplus Hx_2 \oplus Hx_3 \oplus Hx_4$$

$$Hx = Hx_1 \oplus Hx_2 \oplus Hx_3 \oplus Hx_4$$

경로상에서 라우터는 패킷이 전달되는 전방위 라우터  $Ry$ 의 IP 주소  $Ay$ 와 패킷이 전달되는 다음 후방위 라우터  $Rz$ 의 주소  $Az$ 를 알 수 있다. 따라서 아래와 같이 임의의 난수 정보 32비트  $Nx$ 를 생성하여  $Ax'$  값을 계산한다.

$$Ax' = Ax \oplus Ay \oplus Az \oplus Nx$$

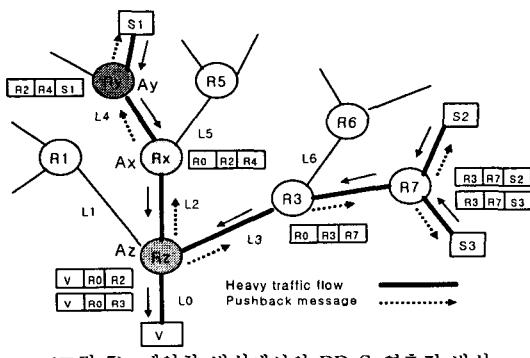
이와 같이 라우터에 도착한 패킷  $Rx$ 에서 128 비트에 해당하는  $Mx$ 를 중심으로 32비트  $Hx$ 를 계산하고, 다시 라우터 자신의 IP 주소와 패킷이 전달된 상위 라우터 및 전달하고자 하는 다음 라우터에 대한 주소값에 대해 계산된  $Ax'$  값을 가지고 다음 과정을 수행하여  $Hx$ 을 생성한다.

$$Hx' = Hx \oplus Ax'$$

이와 같이 생성된  $Hx$ '인 경우 IP 패킷에서의 고유한 정보로 구성되었으며, 여기에 라우터 자신의 32비트 IP 주소와 경로 관련 정보가 XOR 연산으로 생성된 정보이다. 위 과정을 통해 생성된 정보는 기존의 ICMP traceback 기법에 대한 변형으로 아래와 같은 ICMP 패킷의 내부에 저장하여 전송한다.

구체적으로  $Hx'$  값과  $Nx$  값을 bit-interleaving하여 64비트 정보를 생성한다. ICMP traceback 패킷에서의 64 비트 정보에 포함되어 목적지 IP 주소로 전달하게 된다. 물론 이 때 전달되는 ICMP 메시지  $Ix$ 는 근원지 IP 주소로 전달되는 것이 아니고, 목적지 IP 주소로 전달되는 메시지이다.

목적지 IP 주소에 도착한 ICMP 메시지  $Ix$ 와 패킷  $Px$ 에 대해서 이제는 피해 시스템에서는 경로 정보를 파악하게 된다. 우선 ICMP 메시지 내에 포함되어 있는 64 비트 정보에 대해서 다시 각각의  $Hx'$ 과  $Nx$ 값을 구한다. 이때  $Hx'$ 값은  $Hx \oplus Ax \oplus Ay \oplus Az \oplus Nx$ 이므로  $Hx' \oplus Nx$ 를 하게 되면 결국  $Hx \oplus Ax \oplus Ay \oplus Az$ 값을 구하게 된다.



<그림 5> 제안한 방식에서의 DDoS 역추적 방식

이제 패킷  $Px$ 에서 128 비트에 해당하는 정보  $Mx'$ 을 생성하여  $Hx$ 값을 구할 수 있으므로, 결국 피해 시스템에서는  $Hx' \oplus Nx \oplus Mx'$  연산을 통해 라우터에 대한 32비트 IP 주소  $Ax$ 와 전송 경로의 전후 주소를 얻을 수 있다.

$$Ax \oplus Ay \oplus Az = Hx' \oplus Nx \oplus Mx$$

결국 피해 시스템에서는 라우터  $R_y$ 와  $R_z$ 에서도 전송된 ICMP traceback 메시지 내에 포함된 메시지에서도 동일한 과정을 통해 아래 메시지를 얻을 수 있다.

$$V \oplus Az \oplus Ax, \quad Ax \oplus Az \oplus S1$$

따라서 피해 시스템 V에서는 아래와 같이 계산하여 패킷

이 전달된 경로 정보  $S_1$ 을 계산할 수 있다.

$$Ay = (V \oplus V \oplus Az \oplus Ax \oplus (Ax \oplus Ay \oplus Az))$$

$$S1 = (Ay) \oplus Ax \oplus Az \oplus S1 \oplus (Ax \oplus Ay \oplus Az)$$

이와 같은 과정을 통해 라우터에서는 ACC 모듈을 통해 네트워크상에 트래픽에 대한 감시 및 판단/제어 기능을 수행하면서도 변형된 pushback 기술을 적용할 수 있고, DDoS 해킹 경로를 역추적하기 위해서 ICMP traceback 기술을 적용하여 스포핑된 패킷에 대한 역추적 기능도 제공할 수 있다. 또한 보안 기능이 강화된 라우터를 기반으로 IP 역추적 과정을 수행할 경우 최종적으로 피해 시스템에서 수신된 마크에 대해 경로상에 있는 라우터를 신뢰할 수 있게 되어 공격자에 대한 근원지를 좀더 정확하게 재구성할 수 있다는 장점이 있을 것으로 예상된다.

V. 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.

최근 IPv6, 모바일 환경, Ad-hoc 네트워크 및 능동형 네트워크, 유비쿼터스 네트워크 등 다양한 형태의 네트워크 환경이 구축되고 있다. 앞으로 다양한 네트워크 환경에서 기존의 방화벽 및 IDS가 담당하던 기능을 라우터가 포함하고 패킷에 대해 개선된 역추적 기능을 제공하는 기법에 대해서도 연구가 되어야 할 것이다.

참고문헌

- [1] Computer Emergency Response Team, "TCP SYN flooding and IP Spoofing attacks," CERT Advisory CA-1996-21, Sept, 1996.
  - [2] L. Garber. "Denial-of-service attacks trip the Internet". Computer, pages 12, Apr. 2000.
  - [3] P. Ferguson and D. Senie. "Network ingress Filtering: Defeating denial of service attacks which employ IP source address spoofing", May 2000. RFC 2827.
  - [4] K. Park and H. Lee. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. In Proc. IEEE INFOCOM '01, pages 338 (347), 2001.
  - [5] D. X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback," Proc. Infocom, vol. 2, pp. 878-886, 2001.
  - [6] Steve Bellovin, Tom Taylor, "ICMP Traceback Messages", RFC 2026, Internet Engineering Task Force, February 2003.
  - [7] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback", Technical Report UW-CSE-2000-02-01, Department of Computer Science and Engineering, University of Washington
  - [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. Mngt, 1999.
  - [11] Deering, S. and R. Hinden, "Internet Protocol, Version 6, (IPv6) Specification", RFC 2460, December 1998.
  - [12] Tatsuya Baba, Shigeuyki Matsuda, "Tracing Network Attacks to Their Sources," IEEE Internet Computing, pp. 20-26, March, 2002.
  - [13] Andrey Belenky, Nirwan Ansari, "On IP Traceback," IEEE Communication Magazine, pp.142-153, July, 2003.
  - [14] S. Floyd, S. Bellovin, J. Ioannidis, K. Kompella, R. Mahajan, V. Paxson, "Pushback Message for Controlling Aggregates in the Network," Internet Draft 2001