

# DDoS 해킹 공격 근원지 역추적 기술

이 형 우\*

요 약

본 연구에서는 DDoS 공격과 같은 인터넷 해킹 공격에 대해 근원지 IP에 대한 역추적 방법론에 관한 기술을 분석하였다. 현재까지 제시된 IP 역추적 기법은 크게 패킷을 중심으로한 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 지금까지 연구된 IP 역추적 방법론에 대해 고찰을 바탕으로 특히 앞으로 급속도로 확산될 것으로 예상되는 라우터를 대상으로한 네트워크 중심 해킹 공격에 대비하기 위한 새로운 역추적 방법론에 대해서도 살펴보았다.

## 1. 서 론

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. 방화벽 등과 같은 기법을 이용해 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 현재까지 제시된 기술은 해킹 공격 근원지에 대한 확인 기능을 제공하고 있지 못해 결국 DoS<sup>[2]</sup> 공격자를 찾아내지 못하고 있다. 그 이유는 대부분의 해킹 공격이 근원지 IP 주소를 스푸핑하는 방식으로 수행되므로 이에 대한 대응 기술이 개발되어야 한다. 예를 들어 traceroute 기술을 이용한 근원지 주소 판별 기법은 DDoS 공격 패킷내에 포함되어 있는 주소가 스푸핑되어 있기 때문에 실제 주소에 대한 판별 기능을 제공하지 못하고 있다. 최근의 DDoS 공격을 통한 국내 손실 및 피해 사례를 살펴보면, KT DNS 서버 다운 및 KIDC 서버의 다운으로 인해 많은 문제점을 유발하기도 하였다.

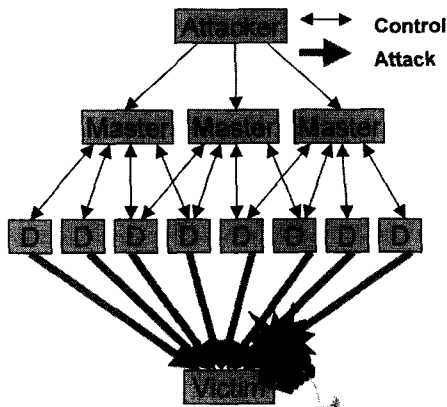
해킹 공격에 대한 대응 방법으로 백신, 침입탐지 및 침입감내 기술 등과 같은 수동적인(passive) 대응 방법과 공격 근원지 추적 기법과 같은 능동적인(active) 대응 방법으로 나눌 수 있다. 능동적인 대응 방법은 다시 해킹 공격 근원지를 검출하는 방법에 따라 전향적(proactive) 역추적 방식과 대응적(reactive) 역추적 기법으로 나눌 수 있다. 본 연구에서는 해킹 및 바이러스에 대한 능동적인 대응 방안에 대해 고찰하고 현재까지 제시된 전향적/대응적 역추적 기법의 특성을 비교 분석하고자 한다. 2장에서는 해킹 공격 근원지 역추적 기술 현황 및 대응 방안에 대해 살펴보고, 3장에서는 해킹 공격에 대한 역추적 기술을 분류하였다. 4장에서는 현재까지 제시된 IP 역추적 기술에 대해 성능을 비교 평가하고 개선된 방안 등에 대해 살펴보고, 5장에서 결론을 맺는다.

## II. 해킹 공격 근원지 역추적

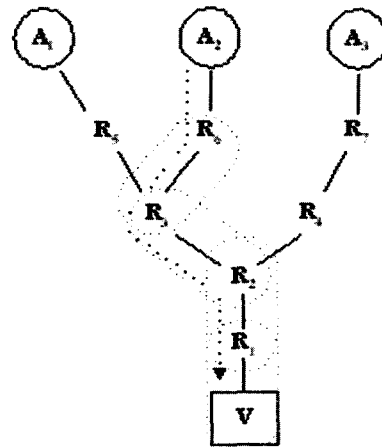
### 1. 근원지 역추적의 필요성

해킹사건에 사용된 수법은 분산 서비스 거부공격(DDoS: Distributed Denial of service)이며 이는 몇 개의 서버와 수많은 하부서버(클라이언트)를 생성

\* 한신대학교 소프트웨어학과 조교수(hwlee@hanshin.ac.kr)



DDoS Attack  
(그림 1) DDoS 공격 구조



(그림 2) 패킷의 전송경로와 공격 경로

하고 마스터 서버에 접속하여 하나 혹은 여러 개의 IP 주소를 대상으로 서비스 거부 공격을 수행하게 된다. 이럴 경우 트리누 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. 분산서비스 거부 공격은 IP 패킷에 근원지 IP 주소를 스푸핑하여 공격하기 때문에 아래 그림과 같이 공격경로와 패킷의 경로는 서로 다르다는 것을 알 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 방지하거나 이를 능동적으로 실시간 내에 추적할 수 있는 기술 등이 제공되어서 해킹 시도 자체를 방지하고자 하는 것이 주요 목적이다. 따라서 해킹·바이러스에 대한 능동적인 대처를 위해 필수적인 기술로 최근 그 중요도가 높아지고 있는 기술이 역추적(traceback) 기술이다<sup>[4]</sup>. 역추적 기술은 해킹 공격 근원지를 실시간으로 추적함으로써 결과적으로는 해킹 공격에 대한 근본적인 억제 기능을 제공한다는 장점이 있다.

## 2. 해킹 역추적 기술의 정의

역추적 기술은 능동적인 해킹 및 바이러스 대응 기법으로서 실시간으로 해커의 위치를 파악하는 것을 목적으로 하고 즉각적인 대응이 가능하도록 하는 기술을 의미한다.

기존의 수동적인 방식에서는 여러 가지 문제점이 발생한다. 실시간 추적이 불가능하고 즉각적인 대응이 불가능하여 전체 인터넷망이 마비될 수 있는 위험성을 갖고 있다. 기존의 대응 방식은 해킹 시스템에서의 로그 분석을 통해 공격 시스템을 파악하고 로그 분석 과정을 반복적으로 적용하여 해킹 경로를 추적하는 수동적인 방식이었다. 이와 같은 기법을 logging 기법이라고 하며 라우터에서 일정한 주기동안 패킷에 대한 정보를 저장하고 있다가 피해 시스템 요청시 제공하게 된다.

만일 추적 경로상에 있는 일부 시스템에서의 로그 정보 등이 삭제된다면 전체적인 로그 분석 자체가 불가능할 것으로 판단된다. 따라서 기존의 수동적인 방법인 경우 이전 단계 추적이 어려울 경우 역추적 자체가 불가능하다는 것을 의미한다. 따라서 좀더 신속하고 정확한 실시간 역추적 시스템이 필요하다.

## 3. 익명적 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.

#### 가. 필터링 및 접근 제어 기술<sup>[3]</sup>

필터링 기법은 익명적인 패킷이 도달하였을 경우 이를 필터링하여 DDoS 공격등이 발생하지 못하도록 하는 기법이다. 접근 권한 및 접속 범위 등을 지정하여 특정 조건을 만족하는 트래픽만을 허용하는 방식으로 접근 제어 기술이라고 할 수 있으나, 일반적인 인터넷 서비스의 특성상 접속 조건 등을 제한할 경우 서비스 제공의 한계가 발생하기 때문에 실제로 적용하기에는 어려움이 있다. 특히 네트워크의 구조상 라우터를 통해 전달되는 패킷 특성을 제한할 경우 전체 네트워크의 성능을 저하시킬 수 있기 때문에 필터링 기법을 역추적 기법에 적용하기에는 문제점이 있다.

#### 나. SYN flooding 검출 기술<sup>[1]</sup>

TCP 접속 과정에서 발생하는 3단계 핸드셰이크 과정을 수행하면서 과정을 마무리하지 않고 접속하는 해킹 공격에 대한 검출 기능을 제공한다. 종료되지 않은 TCP 핸드셰이크 연결이 일정 임계치를 넘어설 경우 이에 대한 조절 기능을 통해 해킹 공격을 차단하는 방식이나 SYN flooding 공격 이외의 해킹 공격에 대해서는 적용할 수 없으며, TCP 계층을 중심으로한 대응 기술이므로 제한적인 특성을 갖는다. 따라서 현재 연구되고 있는 대부분의 역추적 대응 기술은 TCP 계층보다는 IP 계층에서의 대응 기술로 발전하고 있다.

결국 익명적 패킷에 대한 해킹 공격을 방지하기 위해 제시된 위 두가지 기술은 각각 단점을 가지고 있어서 새로운 방식에서의 역추적 기술이 제시되었다.

### III. IP 근원지 역추적 기술

#### 1. 근원지 역추적 기술 분류

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 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 정보를 조합하여 공격 근원지를 판별하는 기법
- 패킷 마킹 기법<sup>[4,5]</sup> 및 ICMP 역추적 메시지 기반 역추적 기법<sup>[6]</sup> 등이 이에 해당

##### - 대응적(reactive) 역추적 기술

- 해킹 공격이 발생한 것이 확인되었다면 해킹 공격에 의한 연결이 형성되어 있는 상태에서 공격 근원지를 역추적 하는 기법
- 홉대홉(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> 등이 이에 해당

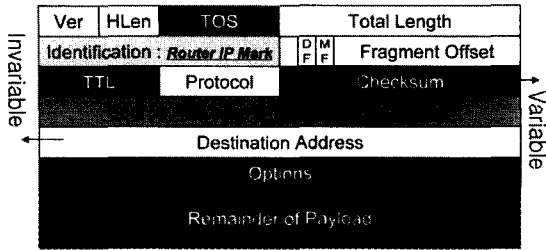
### 2. Proactive 역추적 기술

본 기술은 네트워크상에 패킷이 전송되는 과정에서 사전에 역추적 경로 정보를 생성하여 패킷에 삽입하거나 목적지로 전달하여 주기적으로 관리하면서 만일 해킹 공격이 발생하면 이미 생성, 수집된 정보를 이용하여 해킹 공격 근원지를 판별하는 기법이다. 구체적으로 분류하는 패킷에 대한 확률적 마킹(PPM : probabilistic packet marking) 기법과 전통적인 ICMP 메시지를 변형한 iTrace (ICMP traceback) 기법으로 나눌 수 있다.

#### 가. PPM 기법<sup>[4,5]</sup>

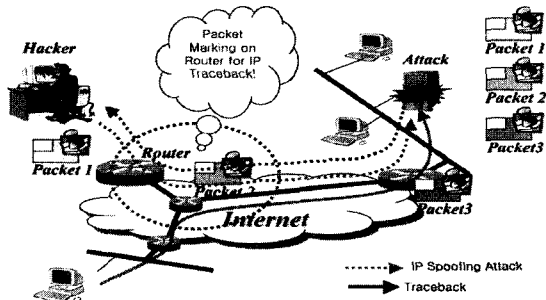
스푸핑된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해서는 IP 계층을 중심으로 네트워크 상에 전송되는 패킷에 대해 네트워크를 구성하는 주요 요소인 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달되었다는 정보를 삽입하는 방식이다.

즉, 인터넷을 통해 전달되는 패킷에 대해 라우터는 IP 계층을 중심으로 패킷 헤더 정보를 확인하여 라우팅하게 되는데 이때, IP 헤더에서 변형 가능한 필드에 대해서 라우터에 해당하는 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다. 아래 그림에서와 같이 IP 헤더에서 16비트 ID 필드에 라우터 자신의 IP 정보를 삽입하게 된다.



(그림 3) IP 헤더 형태

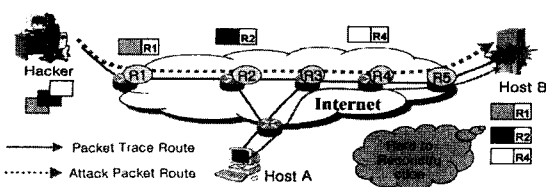
각 라우터에서 삽입된 정보는 다시 다음 라우터로 전달되고 최종적으로 목적지 피해 시스템에 전달된다. 아래 그림과 같이 각 라우터에서 마킹된 정보가 전달 되면 추후에 해킹 공격이 발생하였을 경우 해킹 공격에 해당하는 패킷에 기록된 라우터 정보를 재구성 (reconstruction)하여 실제적인 패킷의 전달 경로를 재구성하게 된다.



(그림 4) PPM 기법 구조

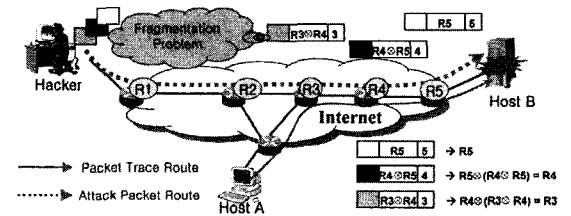
각 라우터에서 전달된 정보를 마킹하는 과정에서 모든 패킷에 마킹하게 되면 전체 네트워크에 대한 지연 현상이 발생하기 때문에 일반적으로 라우터에서는 확률  $p$  로 패킷을 샘플링하여 마킹하게 된다.

이때 라우터에서 마킹하는 정보의 구성에 따라 노드 샘플링(node sampling), 에지 샘플링(edge sampling) 및 개선된 패킷 마킹 기법 등이 제시되었다. 아래 그림과 같이 노드 샘플링 기법은 패킷이 전송된 경로 정보를 확률  $p$  로 샘플링하여 목적지에 전송하는 과정을 보인다.



(그림 5) 노드 샘플링 기반 PPM 기법

아래 그림은 에지 샘플링 방법으로 라우터에서 자신의 IP 주소 정보만을 패킷 헤더에 마킹하는 것이 아니라, 패킷이 전달된 앞단의 라우터 IP 주소까지도 같이 마킹하여 전달하는 방식이다. 이와 같은 노드 샘플링 기법은 해킹 공격 경로를 재구성하는 과정이 노드 샘플링 기법보다 뛰어나다.

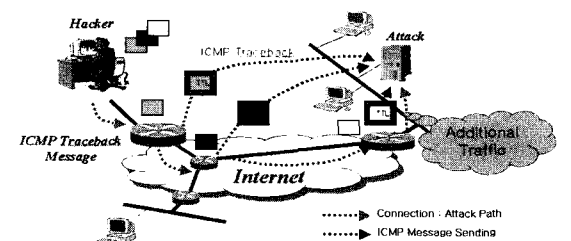


(그림 6) 에지 샘플링 기반 PPM 기법

변형된 PPM 기법으로는 라우터에서 마킹하는 패킷에 대한 인증 기능을 제공하여 마킹 과정에서 보안 기능을 제공하는 기법 등이 있다.

나. iTrace(ICMP Traceback) 기법<sup>[6]</sup>

ICMP 역추적 기법은 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. 생성시에 TTL(time of live) 필드 값은 255로 설정되어 전달되며 목적지에서는 TTL 값을 보고 네트워크 위상에서의 홉 거리 정보이기 때문에 공격 경로 재구성에 사용된다. iTraceback 기법에 대한 작동 방식은 아래 그림과 같으나 일반적으로 PPM 기법과 마찬가지로 DDoS 공격에 대응하기 위해서는 상대적으로 많은 정보가 필요하기 때문에 개선된 기법으로의 연구가 진행되고 있다.



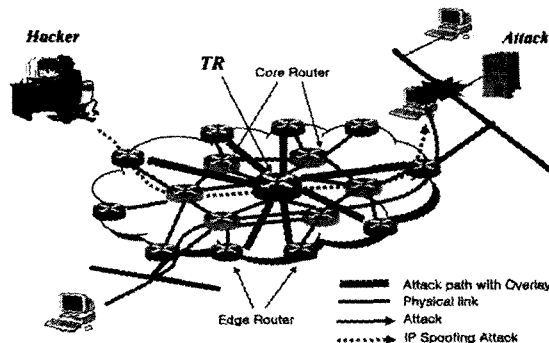
(그림 7) iTrace(ICMP Traceback) 기법

3. Reactive 역추적 기술

본 기법은 해킹 공격이 발생하였을 경우 피해 시스템에서 해킹 트래픽 연결에 대한 공격 경로를 홉 단계로 추적해 가는 방식이다. 구체적인 기법은 오버레이(overlay) 네트워크 방식, 해쉬 기반 역추적 기술 및 IPSec 기반의 역추적 기법 등으로 나눌 수 있다.

가. 오버레이 네트워크 기반 역추적<sup>[8]</sup>

본 기법은 역추적 라우터(TR : tracking router) 모듈을 네트워크에 별도로 설치하고 해킹 공격이 발생하였을 경우, 네트워크 위상에서의 중단 시스템과 연결된 라우터에서 전달된 정보를 TR로 전송한다. 즉, 기존의 ingress 필터링 기법과 유사하게 중단 라우터에서 보내진 트래픽 정보는 터널링 방식으로 TR 라우터에 전달된다. 각 패킷에 대해 20 바이트 정보의 패킷 서명(packet signature) 정보를 생성하여 TR로 전달하게 된다. TR에서 수집된 패킷 관련 정보 등을 재구성하여 실제로 패킷이 전달된 경로를 분석하는 기법이지만, 네트워크 구성상 단일 TR로 전체 네트워크를 관리할 수 없기 때문에 소단위 네트워크에 적합한 기법이다. 또한 단일 ISP 네트워크상에서 구현 가능한 기법이며 이기종의 네트워크 환경에는 적용할 수 없다. 또한 해킹 공격은 짧은 시간 동안에 수행될 수도 있기 때문에 전체 경로를 역추적하는데 어려움이 발생할 수도 있으며, 공격자에 의해서 터널링된 패킷이 위조될 수도 있기 때문에 보안상의 문제가 발생하게 된다.



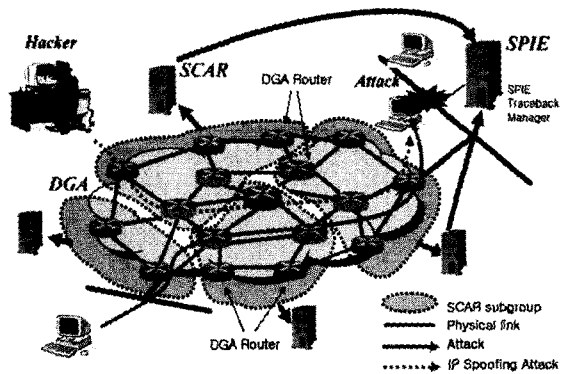
[그림 8] 오버레이 네트워크 기반 역추적

나. 해쉬 기반 역추적<sup>[9]</sup>

본 기법은 SPIE(source path isolation engine) 기반 역추적 서버를 구성하고 전체 네트워크를 서브 그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관

리한다. 그리고 각 라우터에는 DGA(data generation agent) 기능을 탑재하여 운영한다. DGA에서는 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬값에 해당하는 IP 헤더 정보와 8 바이트 정보의 payload 정보를 수집 관리하고 이를 bloom filter 구조로 저장하게 된다. 만일 목적지 시스템에 있는 IDS 시스템에 의해 해킹을 발견하였을 경우 SPIE 시스템에서는 네트워크 그룹을 관리하는 SCAR 에이전트를 통해 그룹내 DGA 라우터에 저장된 정보와 해킹 패킷 정보를 비교 분석하여 이를 다시 SPIE 시스템에 전달하게 되면 해킹 관련 패킷의 전송 경로를 재구성하게 된다.

본 기법을 적용하기 위해서는 SPIE, SCAR 및 DGA 기능을 구축하여야 하며 추가적인 모듈로 제공되기 때문에 이기종 환경의 ISP간 적용도 가능하다. 실험 결과 0.5% 정도의 추가적인 해쉬 정보가 생성되어 전달되고 SCAR에서는 주기적으로 패킷에 대한 해쉬값을 관리하기 위한 메모리가 필요하다.



(그림 9) 해쉬 기반 역추적 기법

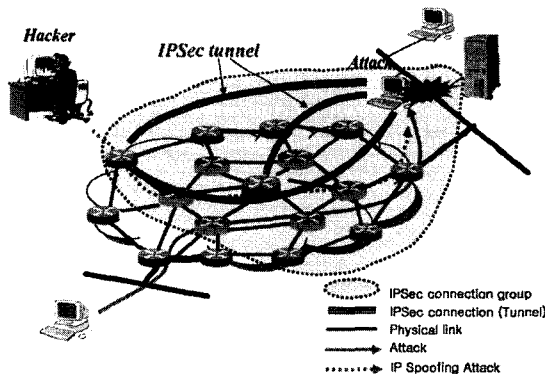
다. IPSec 기반 역추적<sup>[10]</sup>

본 기법은 오버레이 네트워크 기반 역추적 기법에서 발생하는 터널링 과정에서의 보안상 취약점을 보완하기 위해 제시된 기법이다. 전체 네트워크에 대한 위상을 각 라우터가 알고 있다는 가정하에 해킹 공격이 발생하게 되면 네트워크상의 라우터와 피해 시스템간에 IPSec 연결이 구성되어 공격자에 의한 공격 패킷이 해당 라우터를 통해 전송될 경우 IPSec 터널을 통해 경로 정보를 피해 시스템에 전달하게 된다. 다시 네트워크 위상에서의 주변 라우터를 선정하여 IPSec 터널을 구성하고 패킷에 대한 전송 여부를 판별하여 이를 피해 시스템에 전달하는 과정을 반복한다. 이와 같은 과정을 통해 해킹 공격 발생시 실제적으로 패킷이 전송된 경로상의 라우터를 판별할 수 있게 된다.

[표 1] IP 역추적 기법 성능 비교 평가

기법 \ 특성	관리 시스템 부하	네트워크 부하	피해 시스템 부하	메모리 요구	대역폭 부하	역추적 기능	적용 가능성	보안 기능	DDoS 대응	확장성	경로 재구성 패킷수
Ingress filtering	×	×	×	×	×	×	▽	×	×	△	×
SYN flooding	×	×	↓	×	↓	×	▽	×	×	△	×
Logging	↑	×	×	↑	×	▽	▽	◇	▽	◇	1
PPM	↓	↓	↑	↑	×	△	△	◇	▽	△	↑
iTrace	↓	↓	↑	↑	↓	△	△	◇	▽	△	↑
Overlay Network	↑	↓	↓	↓	↑	△	△	◇	◇	▽	1
Hash based TB	↑	↓	↓	↓	↓	△	△	△	◇	▽	1
IPSec based TB	↑	↓	↑	×	↑	△	△	△	▽	▽	↔
Controlled flooding	×	×	×	↓	↑	×	△	×	×	×	1

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



(그림 10) IPSec 기반 역추적 기법

물론 IPSec을 이용한 역추적 방식은 피해 시스템과 라우터간에 IPSec 터널 연결을 구성한 경우에는 공격 경로를 파악할 수 있으나, IPSec 연결을 취하지 않는 네트워크에서는 경로 재구성에 어려움이 있게 된다.

#### IV. IP 근원지 역추적 기술 비교 평가

##### 1. 역추적 기술 특성

현재 발표된 기존의 IP 역추적 관련 기술들의 성능을 비교 분석하면 다음 [표 1]과 같다. IP 역추적과 관련하여 기존의 기법들을 관리 시스템 부하, 네트워크 부하, 피해 시스템의 부하, 메모리 요구, 적용 가능성, 역추적 기능, 대역폭 부하, 보안 기능, DDoS 대응, 확장성 및 경로 재구성시 필요한 패킷 수 등을 기준으로 비교해 보았다.

라우터에서의 접근 제어 기능을 제공하는 필터링 기법은 SYN flooding 기법과 유사하게 전체적인 시스템의 부하 및 피해 시스템에 부하를 주는 형태가 아니라 라우터 자체에서 패킷에 대한 검사를 수행하는 기법이다. 따라서 추가적인 메모리 요구가 없으나, 역추적 기능을 제공하지 못하며 보안기능 및 DDoS 대응 기능도 제공하지 못하고 있다. 라우터에서 패킷 정보에 대한 로그 정보를 관리하는 기법은 라우터에 대해 많은 메모리를 필요로 하며 일부 역추적 기능을 제공하지만 전반적으로는 낮은 보안 구조와 DDoS 취약점을 보이고 있다.

노드 및 에지 샘플링 등에 의한 패킷 마킹 기법과 iTrace 기법은 관리 시스템 및 네트워크 부하는 적은 반면 피해 시스템에서 역추적 경로 재구성시 많은 부하를 필요로 하며, 역추적 기능 및 확장성 측면에서 적절하다고 할 수 있다. 그러나, DDoS 공격에는 조금 취약한 특성을 보이고 있다.

오버레이 네트워크와 해쉬 기반, IPSec 기반 역추적 기법인 경우 기존의 라우터에 대한 관리 시스템을 추가하거나 특정 모듈을 부가하여 역추적 기능을 제공하는 방식이기 때문에 전체적으로 관리 시스템의 부하가 크다고 할 수 있으나, 역추적 기능이 뛰어나고 보안 기능 및 DDoS 대응 측면에서 우수한 성능을 보이고 있다. 특히 기존의 네트워크를 구성하는 라우터에 추가적인 기능을 제공하는 방식으로 많은 변화 없이도 기존의 ISP와 연계하여 이기종의 네트워크 환경에도 적용 가능하다는 장점을 제공한다. 그러나, 이와 같은 기법은 특정한 환경을 구축하여 역추적을 수행하는 것

으로 일반적인 인터넷 환경에 적용하고자 할 경우 일부 적용 불가능한 경우도 발생할 수 있다.

전체적으로 현재까지 제시된 IP 역추적 기법을 검토하였을 경우 대부분 기존 라우터에 대한 변형 및 추가적인 네트워크/시스템 부하가 발생하며, reactive 기법에서는 추가적인 대역폭에 부하가 발생한다는 것을 알 수 있다. 따라서 라우터에서의 부하를 비롯하여 전체적인 관리 시스템의 부하와 대역폭 부하를 줄이면서 확장성을 제공하고 DDoS 대응 성능을 향상시킬 수 있는 기법에 대한 연구가 필요하다.

## 2. 개선된 역추적 기법 고찰

인터넷 프로토콜은 TCP/IP 프로토콜의 중심이다. IP는 OSI 참조 모델의 네트워크 계층에 해당하고, 비연결 서비스와 최선의 전달 서비스를 전송 계층에 제공한다. 특히 IP 패킷에서의 헤더는 20 바이트의 고정 길이 구성 요소와 최대 40 바이트의 가변 길이의 선택적인 구성 요소를 갖는다.

인터넷을 구성하는 물리적인 네트워크 장비인 경우 다양한 형태의 프로토콜을 사용하여 연결되어 있으며 작동 방식 역시 매우 다양하다. 따라서 인터넷을 통한 해킹 공격 역시 매우 다양한 형태로 발생하게 된다.

해킹 공격에 대한 대응 기술을 고찰할 때 우선 고려해야 하는 것은 인터넷 프로토콜 구조상 어느 계층을 중심으로 고찰할 것인가를 우선 결정해야 한다. 일반적으로 IP 계층에서의 역추적 기능을 제공하는 것이 일반적이며 TCP 계층인 경우 서비스 종류에 의존적이기 때문에 일반화하기에 어려움이 많이 있다. IP 계층에서의 역추적 기능을 제공하는 과정에서도 피해 시스템이 직접 모든 네트워크를 관리할 수 없기 때문에 결국에는 라우터에 의존하여 역추적 기능을 수행하게 된다.

이때 기존의 라우터에서 부가적인 기능을 어느 정도 추가할 것이며 어떠한 기능을 제공해야 하는 지에 따라서 여러 가지 기법으로 분류할 수 있다.

### 가. 전향적 기법에 대한 재고찰

전향적인 기법인 경우 패킷을 중심으로 IP 헤더 정보에 정보를 마킹하는 방식으로 기존의 마킹 구조에서 유발하는 문제점을 해결할 수 있는 방안이 제시되어야 한다. 즉, 기존의 기법에서는 확률  $p$ 로 패킷을 선정하게 되는데 경로 재구성을 위해서는 상당히 많은 개수의 마킹된 패킷이 필요하다. 만일 특정 라우터에서

의 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.

iTrace 기법인 경우 기존의 패킷 정보에 대해 PPM과 마찬가지로 확률  $p$ 로 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 있기 때문에 이를 해결할 수 있는 방안이 제시되어야 한다.

이와 같이 전향적 기법인 경우 패킷에 대해 일정 확률  $p$ 를 만족할 경우 샘플링하여 전송하는 기법을 사용하고 있는데, 이에 대한 구체적인 방안도 여러 가지를 생각할 수 있을 것이다. 만일 PPM 또는 iTrace 메시지를 발생하는 라우터에서 고정적인 형태의 확률  $p$ 에 의존하여 샘플링하지 않고 전체 네트워크의 트래픽 특성에 따라 능동적으로 확률  $p$ 를 조절할 수 있다면 기존 기법에 비해 네트워크 부하, 메모리 및 역추적 기능 등에서 보다 향상된 기법을 제공할 수 있을 것이다. 또한 해커에 의한 오류 경로 재구성을 방지하기 위해서는 전통적인 보안 구조를 역추적 모듈과 접목하여 제공한다면 더욱 개선된 기법을 제공할 수 있을 것이다.

### 나. 대응적 기법에 대한 재고찰

오버레이 네트워크를 이용한 역추적 기법인 경우 특정 네트워크 위상에만 적용가능하며 라우터의 구조가 동적으로 변화하는 일반적인 네트워크 환경에는 적용하기 어렵다. 또한 중단 라우터가 아닌 망 내부 라우터에 연결된 라우터를 거쳐서 전달되는 패킷인 경우 쉽게 추적할 수 없다는 문제점이 발생한다.

해쉬 기반 역추적 기법인 경우 패킷에 대한 해쉬 값을 일정한 주기로 관리 전송하는 방식이지만 네트워크가 규모가 방대한 경우 전체 성능에 많은 문제점이 발생하게 된다. 또한 IDS 시스템 등을 통해 해킹 등이 발견된 경우 역추적 과정을 수행하는 방식이므로 우선 네트워크 자체에 대한 공격이 수행된다면 본 기법 역시 작동하지 않는다는 문제점이 발생한다.

IPSec에 기반한 역추적 기법인 경우 우선 공격자는 IPSec이 가지고 있는 보안 및 인증 특성에 의해서

DDoS 공격을 수행하지는 않을 것이며 일반 네트워크 환경에서 해킹 공격을 수행할 것이다. 따라서 IPSec 기법을 적용한다는 것은 결국 목적지 시스템과 라우터 간에 IPSec으로 채널을 구성하고 트래픽에 대한 확인 과정을 수행한다는 것이다. 결국 역추적 과정에서 IPSec으로 채널이 구성된 네트워크 그룹과 공격자가 포함되어 있는 비 IPSec 기반 일반 네트워크 간의 연계 기능을 제공해야 한다.

결국 현재까지 제시된 기법을 종합적으로 비교하였을 경우 전형적 기법인 경우 라우터를 통해 패킷에 HMAC 등의 기능을 제공하고 확률  $p$ 를 다양한 기준으로 선정하여 iTrace 패킷을 생성하는 방식이 필요하며, 대응적 기법인 경우 해쉬 방식에 기반한 단일 패킷 역추적 방식이 여러 가지 측면에서 우수한 역추적 성능을 제시하고 있다.

다. 새로운 환경에 대한 고찰

최근 IPv6, 모바일 환경, Ad-hoc 네트워크 및 능동형 네트워크, 유비쿼터스 네트워크 등 다양한 형태의 네트워크 환경이 구축되고 있다. 특히 유선과 무선으로 대별되는 두가지 환경과 IPv4와 IPv6로 대별되는 프로토콜 표준에 대해 각각 역추적 기능을 어떻게 제공할 것인지에 대한 연구가 필요하다. 또한 IP 계층에서의 보안 프로토콜이 제공되는 환경인 IPSec 기반 환경과 일반 IP 계층에서의 역추적 기능도 고려해 보아야 한다. 또한 기존의 방화벽 및 IDS가 담당하던 기능을 라우터가 포함하여 전체 네트워크의 안전성을 확보하면서도 패킷에 대해 개선된 역추적 기능을 제공하는 기법에 대해서도 연구가 되어야 할 것이다.

3. 네트워크에 대한 해킹 공격에 대한 역추적 기능

현재의 네트워크 구조는 도메인에 대해 BGP 기반 라우팅 프로토콜을 사용하고 있다. 그러나, 최근 제시되고 있는 새로운 해킹 공격 방법으로는 기존 라우팅 프로토콜에서의 보안 취약점을 분석한 해킹 공격이 손쉽게 가능하다는 것이다. 현재의 네트워크를 구성하고 있는 라우터에 대해 다음 그림과 같은 간단한 공격을 통해서도 쉽게 전체 네트워크를 마비시킬 수 있다. 따라서 현재까지의 해킹·바이러스 방식과는 달리 네트워크의 단점을 악용한 공격 방식에 대한 대응 기술이 연구되어야 한다.

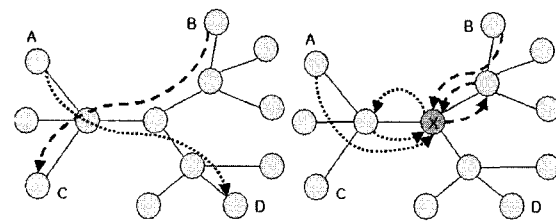
아래 그림의 (a)와 같이 일반적인 형태에서 라우팅 테이블을 통해 A에서 D 또는 B에서 C로 패킷을 전

달할 수 있다. BGP 프로토콜을 통해 라우터는 주변 네트워크 토폴로지에 대한 정보를 가지고 있어서 네트워크상에 전달되는 패킷을 전송하게 된다.

그러나, (b)와 같이 만일 라우터 X에서의 라우팅 테이블을 공격하게 된다면 A에서 D로 전달되는 패킷은 라우팅 테이블이 변경되었기 때문에 D로 전달되는 것이 아니고, 계속적으로 루프를 형성하게 될 것이다. 마찬가지로 B에서 C로 전달되는 패킷 역시 루프를 형성하면서 TTL 값이 계속 감소하게 된다.

그 결과 네트워크를 통한 전체 패킷의 양이 증가할 뿐만 아니라, 패킷 손실을 가져오게 되므로 급속도로 전체 네트워크가 다운될 수 있는 가능성이 있다. 이와 같은 라우팅 테이블 공격은 DDoS 공격보다 손쉬운 방법이지만 그 파급효과는 대단하다고 할 수 있다.

결국, 네트워크 AS 시스템에서의 해킹·바이러스를 대처하고 이를 역추적할 수 있도록 기존 라우터의 성능을 개선한 Secure Router에 대한 기술 개발이 필요하다.



(그림 11) 라우터에 대한 해킹 공격 시나리오

기존의 라우터 기반 해킹 대응 방안에서는 수동적인 방식으로 진행되며 실시간 추적과 즉각적인 대응이 불가능하여 전체 인터넷 망이 마비될 수 있는 위험성을 갖고 있다. 기존의 대응 방식은 해킹 시스템에서의 로그 분석을 통해 공격 시스템을 파악하고 로그 분석 과정을 반복적으로 적용하여 해킹 경로를 추적하는 수동적인 방식이다. 따라서 추적 경로상에 있는 일부 시스템에서의 로그 정보 등이 삭제된다면 전체적인 로그 분석 자체가 불가능하게 되며 역추적 자체가 불가능하다는 것을 의미한다.

특히 앞에서 살펴본 바와 같이 향후 해킹 방법은 네트워크의 취약점을 이용한 공격이 급증할 것으로 판단된다. 따라서 라우터에서의 해킹 공격에 대한 대응 기술이 제시되어야 하는데 가장 효과적인 방법으로는 라우터에 의한 능동적 해킹 대응 기술이라고 할 수 있다. 이를 위해서는 라우터에 대한 안전성과 함께 해킹 근원지 IP 역추적 기술이 접목되어야 한다.



## 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. 역추적 기술의 구조와 현황, 문제점 및 성능 비교 평가를 중심으로 기술하였으며, 현재까지 제시된 IP 역추적 기술에 대한 개선 방향 등에 대해 고찰하였다. 본 연구 분야는 앞으로도 네트워크를 대상으로한 해킹 공격 등에 능동적으로 대처하기 위해서는 다양한 분야에 대한 연구가 필요하다.

## 참 고 문 헌

- [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., Mgmt., 1999.
- [11] Deering, S. and R. Hinden, "Internet Protocol, Version 6, (IPv6) Specification", RFC 2460, December 1998.
- [12] Tatsuya Baba, Shigeyuki 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.

## 〈著 者 紹 介〉



**이 형 우 (Hyung-Woo Lee)**  
종신회원

1994년 2월 : 고려대학교 전산과  
학과 졸업(이학사)

1996년 2월 : 고려대학교 전산과  
학과 졸업(이학석사)

1999년 2월 : 고려대학교 전산학과 졸업(이학박사)

1996년~현재 : 컴퓨터과학기술연구소 연구원

1999년~2003년 : 천안대학교 정보통신학부 조교수

2003년~현재 : 한신대학교 소프트웨어학과 조교수

관심분야 : 정보보호, 네트워크 보안, 해킹·바이러스, 스테가노그래피, DRM, 컴퓨터 포렌식스 기술 등