DDoS 공격에 대한 Pushback 기반 개선된 ICMP Traceback 기법☆

Pushback based Advanced ICMP Traceback Mechanism Against DDoS Attack

이 형 우*
Hyung-Woo Lee

요 약

근원지 IP 주소가 스푸핑된 패킷을 통해 많은 양의 DDoS 트래픽이 발생할 경우 서비스 거부 현상이 발생하게 된다. 이에 대한 대응 기술로 제시된 IP 역추적 기술은 DDoS 공격의 근원지를 판별하면서도 공격 패킷의 전달 경로를 재구성하여 역추적하는 기법이다. 기존의 기법은 크게 패킷을 중심으로한 마킹 방법과 역추적 메시지를 이용한 방법 등으로 나눌 수 있다. 기존의 기법은 현재의 인터넷 환경에서 적용하였을 경우 DDoS 공격에 대해 능동적으로 대응하지 못하고 네트워크 부하를 증가시킨다는 단점이 있다. 본 연구에서는 Pushback 기법을 적용하여 라우터를 중심으로 DDoS 공격 근원지를 역추적하는 ICMP traceback 기반 역추적 기법을 제시하였다.

Abstract

Distributed Denial-of-Service(DDoS) attack prevent users from accessing services on the target network by spoofing its origin source address with a large volume of traffic. The objective of IP Traceback is to determine the real attack sources, as well as the full path taken by the attack packets. Existing IP Traceback methods can be categorized as proactive or reactive tracing. Proactive tracing(such as packet marking and messaging) prepares information for tracing when packets are in transit. Reactive tracing starts tracing after an attack is detected. In this paper, we propose a "advanced ICMP Traceback" mechanism, which is based on the modified pushback system. Proposed mechanism can detect and control DDoS traffic on router and can generate ICMP Traceback message for reconstructing origin attack source.

Keyword : DDoS, Traceback, ICMP, ACC, Pushback

1. 서 론

현재 TCP SYN flooding[1] 공격과 같은 서비스 거부 공격(DoS: Denial of Service)[2]을 통해 TCP/IP 체계의 취약점이 노출되어 있기 때문에 네트워크 및 인터넷에서의 해킹 공격에 대응할 수 있는 방안에 대해 연구가 진행되고 있다. 대응 기술로서 우선 방화벽(firewall) 시스템은 접근 제어 기술을 적용한 것으로 해킹 공격에 수동적인 특징을 보이고 있으며, 침입탐지 시스템(IDS: Intrusion Detection System)을 통한 대응 기술은 피해 시스템에 도착한 이상 트래픽에 대한 검출 및 차단 기능만을 제공하는 수동적 해킹 대응 기술이다. 따라서 현재까지 제시된 기술은 DoS 해킹 공격 근원지에 대한 확인, 추적 등과 같이 능동적인 측면에서의 해킹 대응 기능을 제공하고 있지 못하고 있다. 그 이유는 대부분의 해킹 공격이 근원지 IP 주소를 스푸핑(IP Spoofing)하는 방식으로 수행되므로 이에 대한 능동적 대응 기술이 개발되어야 한다.

DDoS 공격과 같은 해킹 공격에 대한 대응하는

* 정 회 원 : 한신대학교 소프트웨어학과 조교수
hwlee@hs.ac.kr(제 1저자)

☆ 본 연구는 한신대학교 교내특별연구비 지원으로 수행된 연구결과입니다.

방법은 크게 백신, 침입탐지 및 침임감내 기술 등과 같은 수동적인(passive) 대응 방법과 공격 근원지 역추적(Traceback) 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.

역추적 방식은 네트워크상에 패킷이 전송되는 과정에서 사전에 라우터는 역추적 경로 정보를 생성하여 패킷에 삽입하거나 패킷의 목적지 IP 주소로 전달하여 주기적으로 관리하는 방식이다. 만일 피해 시스템에서 해킹 공격이 발생하면 이미 생성, 수집된 역추적 경로 정보를 이용하여 스푸핑된 해킹 공격 근원지를 판별하는 기법이다. 패킷에 대한 확률적 마킹(PPM : probabilistic packet marking)[4,5] 기법과 ICMP 메시지를 변형한 iTrace (ICMP Traceback)[6] 기법 등이 이에 해당한다. 오버레이 네트워크 기반 역추적[8] 기법은 역추적 라우터(TR : tracking router) 모듈을 네트워크에 별도로 설치하고 해킹 공격이 발생하였을 경우, 네트워크 위상에서의 종단 시스템과 연결된 라우터에서 전달된 정보를 사용하여 역추적 하는 방식이지만 네트워크 구성상 단일 TR로 전체 네트워크를 관리할 수 없기 때문에 소단위 네트워크에 적합한 기법이다. 해쉬 기반 역추적[9] 기법은 SPIE (source path isolation engine) 기반 역추적 서버를 구성하고 전체 네트워크를 서브 그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리/역추적 하는 방식이지만 SPIE, SCAR 및 DGA 기능을 추가적으로 구축하여야 한다는 단점이 있다. IPSec 기반 역추적[10] 기법은 IPSec 연결을 취하지 않는 네트워크에서는 역추적 경로 재구성에 어려움이 있다.

본 연구에서는 해킹 공격에 대한 능동적인 대응 방안으로 제시된 전향적/대응적 역추적 기법에서의 문제점 등을 비교 분석하였으며, 기존의 pushback [14] 기법을 개선하여 역추적 기능을 접목한 새로운 방식의 IP 근원지 역추적 기술을 제안하고자 한다. 기존의 pushback 기법은 해킹 공격지에 대한 근원지 역추적 기법을 제공하지는 못하고 있다. 라우터에서는 단순히 트래픽에 대한 판별/제어 기능을 수행하며 상위 라우터로 pushback 메시지를 전송하는 과정만을 수행하기 때문에 DDoS 공격이 발생하였을 경우 피해 시스템에서는 공격 근원지를 역추적 할 수 없다는 문제점이 있다. 따라서 본 연구에서는 해킹 피해시스템에서 공격 근원지에 대한 경로 역추적 등을 확인하기 위해 pushback 기반 개선된 ICMP Traceback 기법을 제시하였다. 제시된 기법을 통해 기존의 역추적 기법보다 관리시스템 부하, 네트워크 부하 및 역추적 기능 등을 향상시킬 수 있었다. 2장에서는 해킹 공격 근원지 역추적 기술 현황 및 대응 방안에 대해 살펴보고, 3장에서는 기존 기법에서의 문제점 등을 고찰하였다. 4장에서는 라우터 기반 pushback 기술을 개선할 수 있는 방안에 대해 제시하였으며 5장에서는 DDoS 공격 근원지에 대한 새로운 IP 역추적 기술에 대해 제시하고 성능을 비교하였다.

2. 해킹 공격 근원지 역추적

2.1 근원지 역추적의 필요성

현재 급속도로 확산되고 있는 DDoS 공격은 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 트리누 마스터는 특정한 기간에 하나 혹은 여러 개의 IP 주소를 공격하도록 하부 서버와 통신한다[2].

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 방지하거나 이를 능동적으로 실시간내에 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[4]. 역추적 기술은 해킹 공격 근원지를 실시간으로 추적함으로써 결과적으로는 해킹 공격에 대한 근본적인 억제 기능을 제공한다는 장점이 있다.

2.2 해킹 공격 근원지 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 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.

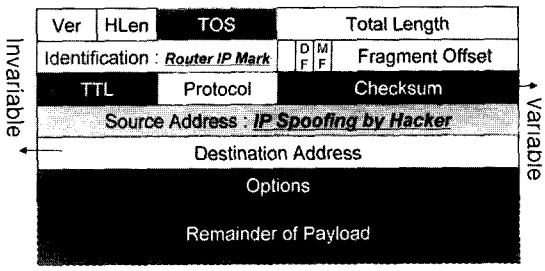
2.3 익명적 해킹 공격에 대응하기 위한 기존 기술

(1) PPM 기법[4,5]

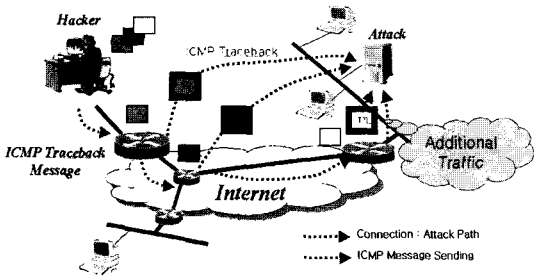
스푸핑된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해서는 IP 계층을 중심으로 네트워크 상에 전송되는 패킷에 대해 네트워크를 구성하는 주요 요소인 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달되었다는 정보를 삽입하는 방식이다. 즉, 인터넷을 통해 전달되는 패킷에 대해 라우터는 IP 계층을 중심으로 패킷 헤더 정보를 확인하여 라우팅하게 되는데 이때, IP 헤더에서 변형 가능한 필드에 대해서 라우터에 해당하는 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다.

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

각 라우터에서 전달된 정보를 마킹하는 과정에서 모든 패킷에 마킹하게 되면 전체 네트워크에 대한 지연 현상이 발생하기 때문에 일반적으로 라우터에서는 확률 p로 패킷을 샘플링하여 마킹



(그림 1) 패킷 마킹을 위한 IP 헤더 구조



(그림 2) iTrace(ICMP Traceback) 기법

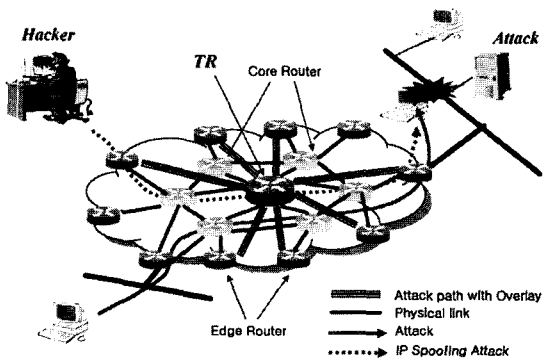
하게 된다. 이때 라우터에서 마킹하는 정보의 구성에 따라 노드 샘플링(node sampling), 에지 샘플링(edge sampling) 및 개선된 패킷 마킹 기법 등이 제시되었다.

(2) iTrace(ICMP Traceback) 기법[6]

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 전 단계 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 그림 2와 같으나 일반적으로 PPM 기법과 마찬가지로 DDoS 공격에 대응하기 위해서는 상대적으로 많은 정보가 필요하기 때문에 개선된 기법이 제시되어야 한다.

(3) 오버레이 네트워크 기반 역추적[8]

본 기법은 역추적 라우터(TR : tracking router) 모듈을 네트워크에 별도로 설치하고 해킹 공격이 발생하였을 경우, 네트워크 위상에서의 종단 시스템과 연결된 라우터에서 전달된 정보를 TR로 전송한다. 즉, 기존의 ingress 필터링 기법과 유사하게



(그림 3) 오버레이 네트워크 기반 역추적

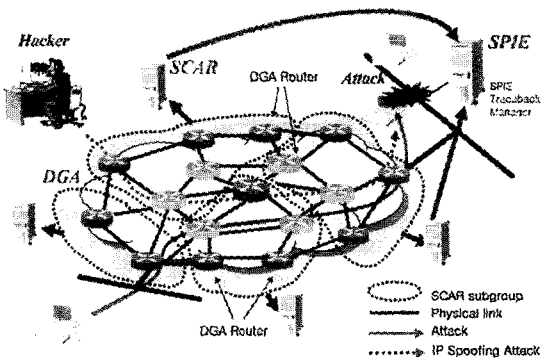
종단 라우터에서 보내진 트래픽 정보는 터널링 방식으로 TR 라우터에 전달된다. 각 패킷에 대해 20 바이트 정보의 패킷 서명(packet signature) 정보를 생성하여 TR로 전달하게 된다.

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 기간 동안에 수행될 수도 있기 때문에 전체 경로를 역추적하는데 어려움이 발생할 수도 있으며, 공격자에 의해서 터널링된 패킷이 위조될 수도 있기 때문에 보안상의 문제가 발생하게 된다.

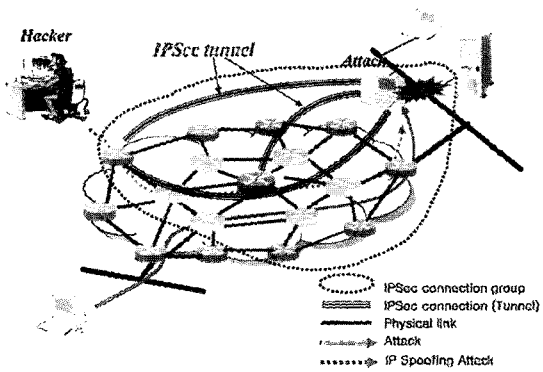
(4) 해쉬 기반 역추적[9]

본 기법은 SPIE(source path isolation engine) 기반 역추적 서버를 구성하고 전체 네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리한다. 그리고 각 라우터에는 DGA(data generation agent) 기능을 탑재하여 운영한다.

DGA에서는 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬값에 해당하는 IP 해더 정보와 8 바이트 정보의 payload 정보를 수집 관리하고 이를 bloom filter 구조로 저장하게 된다. 만일 목적지 시스템에 있는 IDS 시스템에 의해 해킹을



(그림 4) 해쉬 기반 역추적 기법



(그림 5) IPSec 기반 역추적 기법

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.

(5) IPSec 기반 역추적[10]

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. 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.

3. 기존 IP 근원지 역추적 기술에 대한 고찰

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 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.

iTrace 기법인 경우 기존의 패킷 정보에 대해 PPM과 마찬가지로 확률 p로 샘플링하여 메시지

에 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 p를 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 p에 의존하여 샘플링하지 않고 전체 네트워크의 트래픽 특성에 따라 능동적으로 확률 p를 조정할 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.

오버레이 네트워크를 이용한 역추적 기법인 경우 특정 네트워크 위상에만 적용가능하며 라우터의 구조가 동적으로 변화하는 일반적인 네트워크 환경에는 적용하기 어렵다. 또한 종단 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 라우터간에 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.

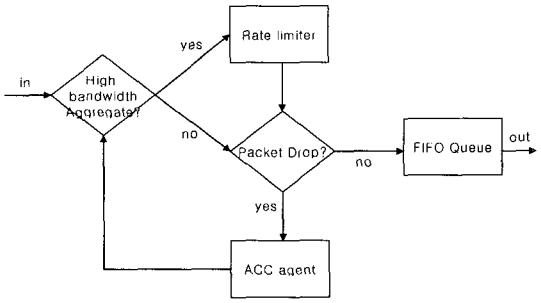
4. 라우터에서의 Pushback 기술

4.1 라우터 기반 DDoS 공격 대응 기술

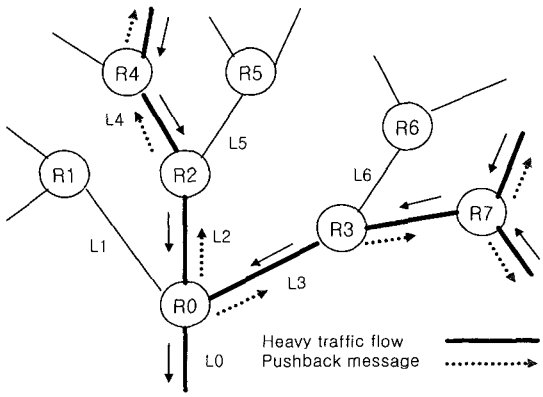
인터넷에서 발생 가능한 해킹 공격에 대한 대응 방안으로 현재까지 제시된 기법을 고찰해 보면 네트워크를 통해 지속적으로 이상적 작동 방식을 보이는 흐름에 대한 대응 방식이라고 할 수 있다. 따라서 인터넷에서 발생하는 해킹 공격은 네트워크를 구성하는 라우터에서 고찰하였을 경우 일종의 폭주(congestion) 현상으로 파악할 수 있다. 결국 해킹 공격에 대한 대응 방안으로는 종단간 폭주 제어 및 대응 기술로 접근할 수 있다. DDoS 공격인 경우 하나 이상의 호스트로부터 네트워크 상의 목적지 호스트로 많은 양의 트래픽이 전달되는 형태이기 때문에 인터넷에서의 해킹 공격에 대응하기 위해서는 DDoS 트래픽 특성을 파악하고 이를 차단하는 방식에 대한 연구가 필요하다.

4.2 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



(그림 6) ACC 기반 트래픽 판별/제어 구조



(그림 7) ACC 기반 Pushback 구조

해당하는 혼잡 시그너쳐(congestion signature)를 기준으로 트래픽을 판별하게 된다. 즉, DDoS 공격이 갖는 네트워크 트래픽의 특성을 기준으로 특정 대역폭 이상으로 폭주 현상을 보인다면 이와 같은 혼잡 시그너쳐를 기반으로 해킹 공격이 발생하였다고 판단할 수 있으며, 필터링 모듈을 접목하여 DDoS 공격 형태에 해당하는 트래픽에 대해서는 전송 방지 기능을 제공하게 된다. 그림 6은 라우터에서의 혼잡 발생시 ACC 기반 판별/제어 구조를 보이고 있다.

이와 같은 판별/제어 과정은 그림 7에서와 같이 pushback 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. 그림 7에서 L0 링크에 트래픽이 폭주되었을 경우 라우터 R0에서는 높은 대역폭을 감지(판별)하게 된다. R0에서의 ACC 모듈에 의해서 링크 L0로 가는 트래픽을 차단(제어)하고 전달 경로에 해당하는 상위 라우터 R2 및 R3로 pushback 메시지를 전달하게 된다. R2에서는 트래픽이 전달된 상위 라우터 R4로 pushback 메시지를 전달하고 R3에서는 R7라우터로 메시지를 전달하게 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 피해시스템에서 공격 근원지에 대한 경로 역추적 등을 확인하기에는 부가적인 절차를 필요로 하기 때문에 이에 대한 개선책이 제시되어야 한다.

5. DDoS 공격에 대한 Pushback 기반 ICMP 역추적

5.1 Pushback 기반 ICMP 역추적

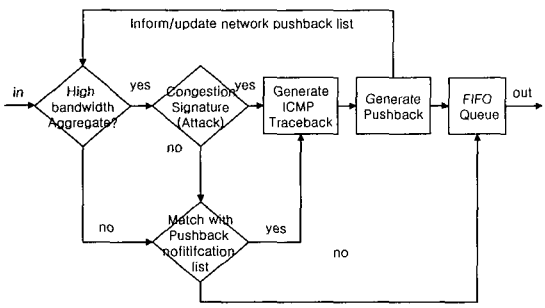
본 연구에서는 라우터에서 DDoS 공격에 해당하는 트래픽을 판별하였을 경우 전체 트래픽을 제어하는 과정은 기존의 ACC 기법과 유사한 과정을 수행하고 ICMP 역추적 메시지를 생성하여 이를 목적지에 전송한다. 기존의 pushback 기법을 적용하여 상위 라우터에 전달하며 pushback 메시지를 받은 라우터에서는 마찬가지로 ICMP 기반의 traceback 메시지를 생성하여 목적지에 전송하게 된다. DDoS가 발생하였을 경우 해당 라우터에서 pushback 기법을 통해 확인된 상위 라우터 경로로 이동하면서 역추적 관련 정보를 생성하여 목적지에 전달하는 방식이다.

그러나 기존의 ICMP 역추적 기법과 같이 일괄적으로 확률 p에 의해서 패킷을 선택하고 이에 대해 ICMP 역추적 메시지를 생성하여 목적지에 전달하는 것이 아니라, 라우터에서 혼잡 시그너쳐에 기반하여 라우터를 지나는 트래픽에서의 이상 현

상을 검출한 후에 해당 트래픽의 상위 라우터에게 이상 징후를 알린다. 또한 DDoS 공격 트래픽이 전달되는 경로를 역으로 추적하면서 ICMP traceback 메시지를 생성하게 함으로써 기존의 기법에서 고정적 확률 p로 패킷을 선정하여 전달하는 방식보다 개선된 역추적 기능을 제공할 수 있다.

5.2 Puchback을 적용한 역추적

이상 트래픽이 발견되었을 경우 단순히 pushback 메시지를 상위 라우터에 재귀적으로 전달하여 근원지 경로를 찾아가는 것이 아니라. pushback 메시지를 상위 라우터에 전달하면서 ICMP traceback 메시지를 생성하여 이를 목적지 호스트에 전송한다. 이때 생성되는 ICMP 메시지 구조는 상위 라우터 주소, 자신의 라우터 주소 및 하위 라우터 주소의 3개 주소값을 갖는 형태로 구성된다. 그리고 pushback 메시지를 받은 상위 라우터에서는 메시지 내에 포함된 해킹 트래픽 특성을 인식한 후에 마찬가지로 자신의 라우터에서 3개의 주소값으로 구성된 ICMP traceback 메시지를 생성하여 이를 목적지에 전달하게 된다. 본 연구에서 제시하는 기법에서 변형된 ACC 기반 구조는 다음과 같다.



(그림 8) 제안한 라우터 기반 DDoS 근원지 역추적 구조

5.3 개선된 ICMP Traceback 메시지 생성

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 16 비트 헤더 checksum 부분에 오류가 있게 되기 때문에 결과적으로 전체 네트워크에 대한 신뢰성을 떨어뜨리게 된다.

따라서 본 연구에서는 IP 헤더에 대한 변경을 수행하지 않으면서도 라우터에 대한 역추적 정보를 생성할 수 있는 과정을 제시한다. IP 헤더 구조에서 옵션 및 패딩 부분을 제외하고 변하지 않는 부분은 전체적으로 HLEN, TTL 및 Checksum 부분은 제외하여 옵션 이전까지를 계산하면 128 비트가 된다. 패킷에서의 128 비트 정보는 고유한 특성을 나타낼 수 있으며 결국 라우터에서는 패킷에 대한 ICMP traceback 메시지 생성 구조에 적용할 수 있다.

5.4 ICMP Traceback 기반 역추적 경로 재구성

[단계 1] 패킷에서의 Mx 128 비트 추출

라우터 Rx의 IP 주소를 Ax라고 하자. 그리고 Rx에 도착한 IP 패킷을 Px라고 하고 Px에서의 해더에서 고정 부분 128 비트를 마스크 하여 얻어낸 부분은 Mx라고 하자. Mx 값은 128비트 정보로 되어 있으며, 네트워크 패킷에 대한 특성을 대표하고 패킷에 대한 유일성을 제공하는 정보가 된다. 따라서 128 비트 정보에 대해 아래와 같이 32비트 블록 4개로 구성할 수 있다.

$$Mx = Hx_1 \mid Hx_2 \mid Hx_3 \mid Hx_4$$

[단계 2] Mx로부터 32비트 Hx 계산

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

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

[단계 3] 라우터 주소에 대한 32비트 Ax' 및 Hx'

생성

이제 라우터 자신의 주소 Ax에 대해 패킷이 전달되는 경로상에서 라우터는 패킷이 전달되는 전방위 라우터 Ry의 IP 주소 Ay와 패킷이 전달되는 다음 후방위 라우터 Rz의 주소 Az를 알 수 있다. 따라서 아래와 같이 임의의 난수 정보 32비트 Nx를 생성하여 Ax'값을 계산한다.

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

이와 같이 라우터에 도착한 패킷 Rx에서 128비트에 해당하는 Mx를 중심으로 32비트 Hx를 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.

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

[단계 4] Hx'를 ICMP traceback 메시지로 전송

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 Nx값을 bit-interleaving하여 64비트 정보를 생성한다. ICMP traceback 패킷에서의 64 비트 정보에 포함되어 목적지 IP 주소로 전달하게 된다. 물론 이때 전달되는 ICMP 메시지 Ix는 근원지 IP 주소로 전달되는 것이 아니고, 목적지 IP 주소로 전달되는 메시지이다.

[단계 5] ICMP traceback 메시지로부터 라우터 주소 Ax 추출

목적지 IP 주소에 도착한 ICMP 메시지 Ix와 패킷 Px에 대해서 이제는 피해 시스템에서는 경로 정보를 파악하게 된다. 우선 ICMP 메시지 내에 포함되어 있는 64 비트 정보에 대해서 다시 각각의 Hx'과 Nx값을 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.

[단계 6] 패킷 전송 경로 재구성

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

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

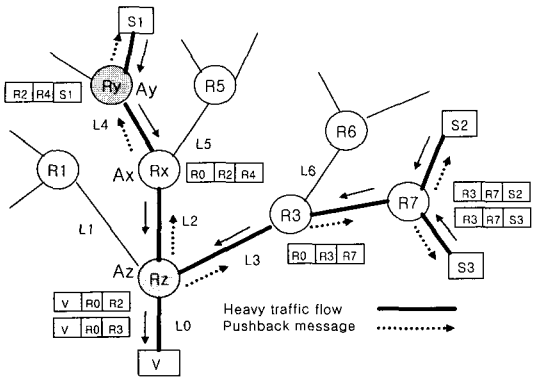
결국 피해 시스템에서는 라우터 Ry와 Rz에서도 전송된 ICMP traceback 메시지 내에 포함된 메시지에서도 동일한 과정을 통해 아래 메시지를 얻을 수 있다.

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

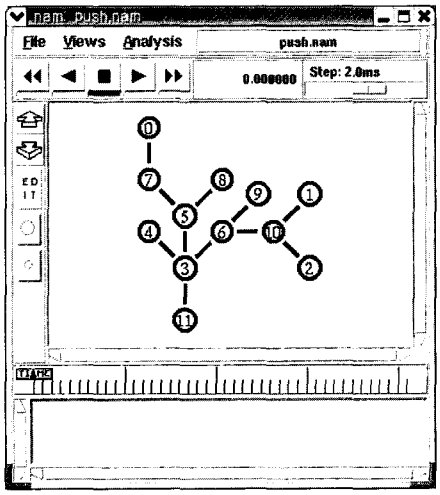
따라서 피해 시스템 V에서는 아래와 같이 계산하여 패킷이 전달된 경로 정보 $S1$을 계산할 수 있다. 즉, 아래 수식과 같이 피해 시스템에서는 전체 네트워크 구조를 모른다 하더라도 패킷 정보와 ICMP 역추적 메시지 정보만으로도 패킷에 대한 시작 위치 $S1$을 계산할 수 있다.

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

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 스푸핑된 패킷에 대한 역추적 기능도 제공할 수 있다.



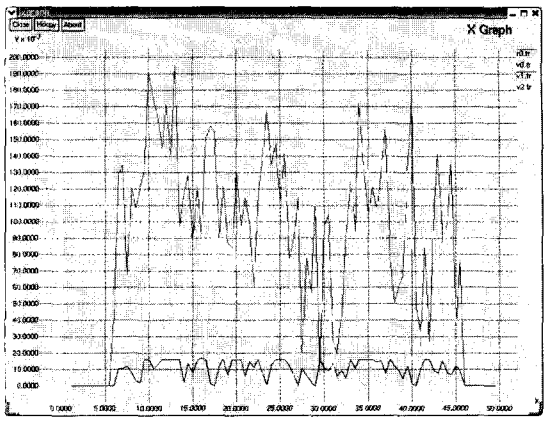
(그림 10) 제안한 방식에서의 DDoS 역추적 경로 재구성



(그림 11) ns-2 기반 시뮬레이션

5.5 제시한 기법의 성능 분석

본 연구에서는 Linux 9.0 환경에서 ns-2 시뮬레이터를 기반으로 실험하였다. DDoS 공격을 노드 0, 1, 및 2번에서 수행하기 위해 DDoS 트래픽을 발생하였으며, 라우터에서는 ICMP 메시지를 발생하여 피해시스템 11번 노드에 전송토록 하였다. 본 연구에서 제안한 기법을 적용하였을 경우, DDoS 공격 발생시 pushback 기법을 적용하게 되므로 전체 트래픽이 점차적으로 줄어드는 것을 확인할 수 있었으며, DDoS 공격 발생시 ICMP 패킷이 차지하는 비율 역시 전체 트래픽의 2% 정도인 것으로 나타났다.



(그림 12) 제안한 방식을 적용시 네트워크 트래픽 분석

제안한 기법과 [12, 13]에 제시된 기존의 IP 역추적 관련 기술들의 성능을 비교 분석하였으며 그 결과는 표 1 및 표 2와 같다. 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 보인다.

기존의 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 보인다.

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 측면

(표 1) 전향적 IP 역추적 기법과의 성능 비교 평가

특성 / 기법	네트워크부하	피해시스템부하	메모리요구	역추적기능	보안기능	DDoS 대응
Ingress filtering	×	×	×	×	×	×
SYN flooding	×	↓	×	×	×	×
Logging	×	×	↑	▽	◇	▽
PPM	↓	↑	↑	△	◇	▽
iTrace	↓	↑	↑	△	◇	▽
제안한 Pushback 기반 iTrace 기법	↓	↓	↑	△	◇	△

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

(표 2) 대응적 IP 역추적 기법과의 성능 비교 평가

특성 / 기법	네트워크부하	피해시스템부하	메모리요구	역추적기능	보안기능	DDoS 대응
Overlay Network	↓	↓	↓	△	◇	◇
Hash based TB	↓	↓	↓	△	△	◇
IPSec based TB	↓	↑	×	△	△	▽
Controlled flooding	×	×	↓	×	×	×
제안한 Pushback 기반 iTrace 기법	↓	↓	↑	△	◇	△

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

에서 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 것으로 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.

본 연구에서 제시한 기법은 기존의 iTrace 기법과 유사한 proactive 방식으로 작동하는 방식이기 때문에 관리 부하가 적으며 라우터에서 패킷에 대한 판별 및 제어 기능을 적용하였기 때문에 DDoS와 같은 해킹 공격이 발생하였을 경우 전체 네트워크의 부하를 줄일 수 있다는 장점을 제공한다. 또한 기존의 iTrace 기법에서는 임의의 확률 p로 패킷을 선정하여 ICMP 패킷을 생성하는 방식이었으나, 본 연구에서 제시한 기법은 ACC 기반 혼잡 제어 기능에 기반하여 ICMP 메시지 생성을 결정하기 때문에 피해 시스템에 도달하는 ICMP traceback 패킷의 수 역시 줄게 된다. 따라서 전체 네트워크 상의 대역폭을 향상시킬 수 있고, 적은 개수의 ICMP 메시지만을 가지고도 DDoS 공격 근원지에 대한 경로를 쉽게 재구성할 수 있다. 경로 재구성을 위해서는 네트워크에서 n개의 라우터를 거치는 경우 단지 n개의 ICMP 역추적 메시지만으로 근원지 경로를 재구성할 수 있다는 장점을 제공한다. 물론 라우터에 ACC 기반 pushback 모듈에서의 DDoS 관련 판별 기능을 추가로 수행하기 때문에 메모리 요구는 증가하지만, 전체적으로 DDoS 공

격에 효율적인 구조이기 때문에 기존의 reactive 기법의 단점을 보완할 수 있고 proactive 방식으로 대단위 네트워크 구조에 적용 가능한 기법이다.

6. 결 론

본 연구에서 제시한 기법은 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 스푸핑된 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 있다.

기존 역추적 기술의 구조와 현황, 문제점 등을 해결하기 위해 네트워크상에서 DDoS 해킹 공격에 대한 판단/제어 기능도 제공하면서도 피해 시스템에서는 스푸핑된 해킹 공격 근원지를 효율적으로 역추적할 수 있는 새로운 ICMP Traceback 기법을 제시하였다. 제시한 기법은 기존의 기법보다 부하, 성능, 안전성 및 역추적 기능에서 개선된 특징을 보인다.

최근 IPv6[11], 모바일 환경, Ad-hoc 네트워크 및 능동형 네트워크, 유비쿼터스 네트워크 등 다양한 형태의 네트워크 환경이 구축되고 있다. 따라서 앞으로는 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. 특히 기존의 방화벽 및 IDS가 담당하던 기능을 라우터가 포함하여 전체 네트워크의 안전성을 제공하면서도 패킷에 대해 개선된 역추적 기능을 제공하는 기법에 대해서도 연구가 되어야 할 것이다.

참고문헌

[1] Computer Emergency Response Team, "TCP SYN flooding and IP Spoofing attackts," 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, Departmentof 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.,

Mmgt., 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. 42~153, 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.

◐ 저 자 소 개 ◑

이 형 우

1994년 고려대학교 전산과학과 졸업(학사)
1996년 고려대학교 대학원 전산과학과 졸업(석사)
1999년 고려대학교 대학원 전산과학과 졸업(박사)
1999년~2003년 2월 천안대학교 정보통신학부 조교수
2003년~현재 : 한신대학교 소프트웨어학과 조교수
관심분야 : 정보보호, 네트워크 보안, 해킹/바이러스, 스테가노그래피, 컴퓨터 포렌식스
E-mail : hwlee@hs.ac.kr