Journal of Korea Multimedia Society Vol. 7, No. 8, August 2004(pp. 1120-1130)

# Pushback 방식을 적용한 패킷 마킹 기반 역추적 기법

이형우[†], 최창원[††], 김태우[†††]


## 요 약

해킹 공격자는 공격 근원지 IP 주소를 스푸핑하여 대량의 트래픽을 발생시켜 DDoS 공격을 수행하게 된다. 이에 대한 대응 기술로 제시된 IP 역추적 기술은 DDoS 공격의 근원지를 판별하고 공격 패킷이 네트워크상에서 전달된 경로를 재구성하는 기법이다. 기존의 역추적 기법인 경우 패킷내에 경로 정보를 마킹하거나 별도의 역추적 메시지를 생성하여 역추적 과정을 수행하지만 네트워크 부하가 증가한다는 단점이 있고, DDoS 공격에 대한 판별 과정 없이 임의의 패킷에 대해 역추적 정보를 생성하기 때문에 결과적으로 DDoS 공격에 능동적으로 대응하지 못하고 있다. 이에 본 연구에서는 pushback 기능을 적용하여 라우터에서 DDoS 트래픽에 대한 판별 기능을 제공하고 DDoS 공격 패킷에 대해 개선된 마킹 기법을 제시하였으며, 실험 결과 네트워크 부하를 줄이면서도 역추적 성능을 향상시킬 수 있었다.


# Pushback Based Advanced Packet Marking Mechanism for Traceback

Hyung-Woo Lee[†], Chang-Won Choi[††], Tai-Woo Kim[†††]


## 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. Existing proactive tracing scheme(such as packet marking and messaging) prepares information for tracing when packets are in transit. But, these scheme require additional network overhead. In this paper, we propose a "advanced Traceback" mechanism, which is based on the modified Pushback system with secure router mechanism. Proposed mechanism can detect and control DDoS traffic on router and can generate marked packet for reconstructing origin DDoS attack source, by which we can diminish network overload and enhance Traceback performance.


**Key words:** Pushback, IP Traceback(역추적), DDoS, Packet Marking(패킷마킹)

## 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 있

※ 교신저자(Corresponding Author) : 이형우, 주소 : 경기도 오산시 양산동(447-791), 전화 : 031) 370-6436, FAX : 031) 370-6984, E-mail : hwlee@hs.ac.kr
접수일 : 2003년 11월 24일, 완료일 : 2004년 1월 26일
[†] 종신회원, 한신대학교 소프트웨어학과 조교수
[††] 한신대학교 정보시스템공학과 부교수
(E-mail : won@hs.ac.kr)
[†††] 성공회대학교 정보통신공학과 부교수
(E-mail : ktw@mail.skhu.ac.kr)
※ 이 논문은 2003년도 한국학술진흥재단의 신진교수연구지원사업에 의하여 연구되었음. (KRF-2003-003-D00444)

지 못하고 있다. 그 이유는 대부분의 해킹 공격이 근원지 IP 주소를 스푸핑(IP Spoofing)하는 방식으로 수행되므로 이에 대한 능동적 대응 기술이 개발되어야 한다. traceroute 기술을 이용하여 근원지 주소를 판별하는 과정을 적용한다 할지라도 분산 서비스 거부 공격(DDoS: Distributed Denial of service) 패킷 내에 포함되어 있는 주소가 스푸핑되어 있기 때문에 실제 주소에 대한 판별 및 추적 기능을 제공하지 못하고 있다.

DDoS 공격과 같은 해킹 공격에 대한 대응하는 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.

DDoS 해킹 공격이 발생하였을 경우 우선 네트워크상에서 라우터 등에 의해서 악성 정보라고 판단되는 패킷을 제거(dropping malicious packets)하는 방식은 ingress filtering[3] 기법 등과 같이 라우터에 의한 제거 및 필터링(filtering) 기법 등에 해당하며 DDoS 공격에 수동적인 특성을 보인다. 따라서 효율적인 해결 방법으로는 DDoS 공격이 발생하였을 경우 피해 시스템에서는 스푸핑된 DDoS 공격 근원지에 대한 실제 주소를 역추적하는 방법이다.

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.

또한 최근 제시된 pushback[14] 기법은 DDoS 공격이 발생하였을 경우 패킷에 대한 판단 기능을 제공하며 패킷 전달 경로를 따라서 패킷에 대한 전송 제어 기능을 제공한다. 이 기법은 DDoS 공격 트래픽에 대한 제어 기능을 제공하지만 DDoS 해킹 공격 근원지를 역추적하는 기능은 제공하지 못하고 다만 패킷 전달 경로를 따라 패킷에 대한 전송 제어 기능을 제공하여 전체적인 네트워크 성능을 높여주고 있다.

따라서, 본 연구에서는 기존의 DDoS 공격에 대한 제어 기능을 제공하는 pushback 기법을 역추적 기능과 접목하여 스푸핑된 DDoS 패킷에 대한 IP 근원지를 역추적하는 기술을 제안하고자 한다. 라우터에서는 pushback 기법을 적용하여 트래픽에 대한 판별/제어 기능을 수행하며 만일 DDoS 공격이 발생하였을 경우 상위 라우터로 pushback 메시지를 전송하고 역추적 정보를 해당 패킷의 헤더에 마킹하여 전달한다. 제시된 기법을 통해 기존의 역추적 기법보다 관리시스템 부하, 네트워크 부하 및 역추적 기능 등을 향상시킬 수 있었다.

2장에서는 해킹 공격 근원지 역추적 관련 기존 기술에서의 취약점과 개선방향을 고찰하고, 3장에서는 기존 pushback 기법에서의 취약점 등을 고찰하였다. 4장에서는 DDoS 공격 근원지를 역추적하기 위해 pushback 기술을 적용한 새로운 패킷 마킹 기법을 제시하였으며 5장에서는 제시한 기법에 대한 성능을 비교 평가하였다.

## 2. 관련 연구

### 2.1 기존의 DDoS 해킹 공격 대응 기술

스푸핑된 DDoS 패킷에 대한 역추적을 위해서는 TCP 계층을 중심으로한 서비스 중심의 역추적 방식보다는 패킷 자체의 네트워크 전송 과정과 관련된 IP 계층에서의 역추적 기능을 제공하기 위한 연구가 활발히 진행되고 있다. IP 계층을 중심으로 현재까지 제시된 역추적 기술을 분류하면 해킹 대응 방식에 따라 크게 전향적(proactive) 역추적 기술과 대응적(reactive) 역추적 기술로 나눌 수 있으며, 좀더 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.

전향적 역추적 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. 패킷에 대한 확률적 마킹(PPM : probabilistic packet marking) 기법과 전통적인 ICMP 메

시지를 변형하여 역추적 기능을 제공하는 iTrace (ICMP traceback) 기법으로 나눌 수 있다.

2.1.1 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. IP 헤더에서 16비트 ID 필드에 라우터 자신의 IP 정보를 삽입하게 된다.

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 마킹할 경우 전체 네트워크에 대한 지연 현상이 발생하기 때문에 일반적으로 라우터에서는 확률 $p$로 패킷을 샘플링하여 마킹하게 된다. 이때 라우터에서 마킹하는 정보의 구성에 따라 그림 1 및 그림 2와 같이 노드 샘플링(node sampling), 에지 샘플링(edge sampling) 기법 등이 제시되었다. 노드 및 에지 샘플링 방법은 라우터에서 자신의 IP 주소 정보만을 패킷 헤더에 마킹하는 것이 아니라, 패킷이 전달된 앞단의 라우터 IP 주소까지도 같이 마킹하여 전달하는 방식이다. 에지 샘플링 기법은 해킹 공격 경로를 재구성하는 과정이 노드 샘플링 기법보다 뛰어나다.

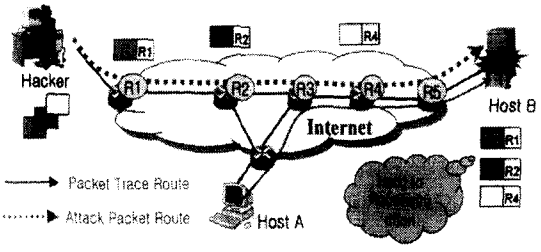



그림 1. 노드 샘플링 기반 PPM 기법

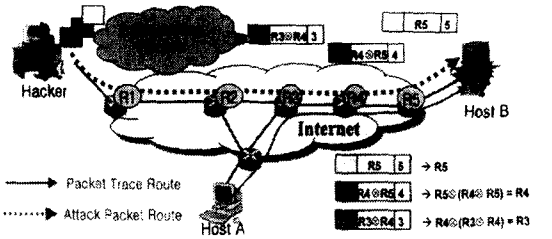



그림 2. 에지 샘플링 기반 PPM 기법

2.1.2 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 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 일반적으로 PPM 기법과 마찬가지로 DDoS 공격에 대응하기 위해서는 상대적으로 많은 정보가 필요하다.

## 3. 기존 PPM 기술의 취약점 및 개선방향

PPM 기법인 경우 기존의 패킷 정보에 대해 확률 $p$로 샘플링하여 메시지 헤더에 라우터 자신의 IP 주소 정보를 마킹하고 이를 패킷의 목적지로 전송하는 방식이다. 즉, 라우터에서는 확률 $p$로 패킷을 선정하여 전송하는데 DDoS 공격에 대한 근원지 경로를 재구성하기 위해서는 상당히 많은 수의 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.

또한 기존의 PPM 기법인 경우 패킷에 대해 일정 확률 $p$를 만족할 경우 샘플링하여 전송하는 기법을

사용하는 과정에서 해킹 트래픽에 대해서 마킹하지 않고 보내는 경우도 발생한다. 이 경우 일반적인 패킷에 대해 역추적 경로 정보를 마킹하여 보내기 때문에 DDoS와 같은 해킹 공격이 발생하였을 경우 스푸핑된 공격 근원지를 재구성할 수 없다는 단점이 있다. 따라서 라우터에서 PPM 방식을 수행하는 과정에서 고정적인 형태의 확률 $p$에 의존하여 샘플링하지 않고 전체 네트워크의 트래픽 특성에 따라 능동적으로 확률 $p$를 조정할 수 있다면 기존 기법에 비해 네트워크 부하, 메모리 및 역추적 기능 등에서 보다 향상된 기법을 제공할 수 있다.

기존의 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. 결국 라우터를 통해 패킷에 해쉬 함수를 통한 무결성/인증 기능을 적용하고 트래픽의 특성에 따라 DDoS 트래픽에 대해서만 선정하여 역추적 정보를 마킹하는 새로운 방식이 제시되어야 한다.

## 4. DDoS 공격에 대한 패킷 마킹 기반 역추적

### 4.1 Pushback 기반 DDoS 공격 트래픽 판별/제어

라우터에서의 DDoS 트래픽 제어 기술로 제시된 것이 ACC(aggregate-based congestion control) 기법을 적용한 pushback 기술[14]이다. 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.

pushback 모듈에서는 DDoS 공격을 확인한 경우 네트워크 경로상 인접한 전단계 라우터로 pushback 메시지를 전송한다. 전달된 메시지는 반복적으로 전달되어 해킹 공격 근원지까지 도달하게 된다.

### 4.2 기존 Pushback 기법의 취약점 및 개선방향

기존의 ACC(aggregate-based congestion control) 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 패킷에 대한 마킹 과정을 수행하여 경로 정보가 마킹된 패킷을 목적지에 전송한다. 그리고, 기존의 pushback 기법을 적용하여 상위 라우터에 전달하며 pushback 메시지를 받은 라우터에서는 마찬가지로 패킷에 대해 마킹하여 목적지로 전송한다. DDoS가 발생하였을 경우 해당 라우터에서 pushback 기법을 통해 확인된 상위 라우터 경로로 이동하면서 역추적 관련 정보를 생성하여 목적지에 전달하는 방식이다.

본 연구에서 제안한 기법은 라우터에서 일괄적으로 확률 $p$에 의해서 패킷을 선택하고 마킹 과정을 수행하여 목적지에 전달하는 것이 아니라, 라우터에서 혼잡 시그너처에 기반하여 우선 라우터를 지나는 트래픽에서의 이상 현상을 검출한 후에 해당 트래픽의 상위 라우터에게 pushback 메시지를 전송하면서 상위 라우터에게 이상 징후를 알린다. 이와 같이 DDoS 공격 트래픽이 발생하였을 경우 역으로 추적하면서 해당 패킷에 대한 마킹 과정을 수행함으로써 기존의 기법에서 고정적 확률 $p$로 패킷을 선정하여 전달하는 방식보다 개선된 역추적 기능을 제공할 수 있다.

또한 기존의 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 패킷 마킹 기반 역추적

### 5.1 Puchback을 적용한 역추적 구조

네트워크는 노드 집합 $V$와 에지 집합 $E$로 구성된 그래프 $G=(V,E)$로 정의할 수 있다. 다시 네트워크 노드 집합 $V$는 종단 시스템과 내부 노드에 해당하는 라우터로 나눌 수 있다. 에지는 $V$ 집합 내에 있는 노드들에 대한 물리적인 연결에 해당한다. $S\subset V$를 공격자라고 정의하고 $t\in V/S$를 피해 시스템이라고 정의한다.

만일 $|S|=1$일 경우 단일 공격자에 의한 해킹 공격을 의미하고 공격 경로 정보 $P=(s,v_1,v_2,\ldots,v_d,t)$인 경우 공격 시스템 $s$에서 피해 시스템 $t$로 $d$개의 라우터를 통해 전달된 공격 경로를 의미한다. 이때 전달된 패킷의 수를 $N$이라고 하자. 만일 패킷내에 라우터에 대한 링크 정보 $(v,v')\in E$를 마킹할 수 있는 필드가 있다면 이를 확률 $p$로 샘플링하여 전달하게 된다. 패킷에 대해서 라우터에서는 일정한 확률로 패킷을 선택하여 에지에 대한 정보와 라우터에 대한 거리 정보를 패킷내에 포함시켜 전달할 수 있다.

기존의 기법에서는 임의의 확률 $p$로 패킷을 선택하여 여기에 라우터에 대한 링크 정보를 마킹하여 전달하게 된다. 만일 네트워크 상에서 노드 $v_i$에서 마킹하였을 경우 다른 라우터에 의해서는 재마킹되지 않고 전달될 확률 $\alpha_i$을 계산하면 다음과 같다.

$$\alpha_i=\Pr(x_d=(v_{i-1},v_i))=p(1-p)^{d-1}(i=1,2,\ldots,d)$$

따라서 확률 $\alpha_i$는 공격자에 해당하는 패킷 정보가 다른 라우터에 의해서는 재마킹되지 않고 피해 시스템에 전달될 확률을 의미한다. 결국 피해 시스템에서 $\alpha_i$ 값을 높이기 위해서는 $p$ 값을 크게 해야 하는데, 이는 라우터에서 빈번하게 마킹 과정을 수행해야 한다는 것을 의미하므로 기존의 기법에서는 결과적으로 네트워크 성능을 저하시키게 된다.

본 연구에서 제시하는 기법은 라우터에서 임의의 확률 $p$로 패킷을 샘플링하여 마킹하지 않고 pushback 기반 ACC 모듈에 의해서 이상 트래픽이 발견되었을 경우 패킷에 대한 마킹 과정을 수행하게 된다. 물론 기존의 ACC 기법에서 사용하는 방법과는 달리 이상 트래픽이 발견되었을 경우 단순히 pushback 메시지를 상위 라우터에 재귀적으로 전달하는 것이 아니라, 상위 라우터에 pushback 메시지를 전달하면서 해당 패킷에 마킹 과정을 수행한다. pushback 메시지를 받은 상위 라우터에서는 메시지 내에 포함된 해킹 트래픽 특성을 인식한 후에 마찬가지로 자신의 라우터에서 2개의 라우터 주소값으로 마킹 과정을 수행하여 이를 목적지에 전달하게 된다. 본 연구에서 제안한 구조는 그림 3과 같다.

제안한 구조에서는 라우터에 들어온 패킷에 대해 트래픽의 대역폭을 검사하고 일정 이상으로 도착하게 되면 공격 형태에 해당하는 혼잡 시그너쳐인지를 판단하게 된다. 만일 공격 형태 트래픽에 해당한다면 패킷에 마킹과정을 수행하고 동시에 해당 패킷에 대한 pushback 메시지를 생성하여 이를 라우터의 출력 큐로 하여금 앞단의 라우터에게 전송토록 한다. 만일 대역폭 조건을 만족하지 않을 경우에는 이전에 pushback 메시지를 통해 주변 라우터로부터 전달된 정보가 있는지를 확인하고 만일 해당된다면 마찬가지로 패킷에 대한 마킹 과정을 수행한다. 위 조건을 만족하지 않을 경우 일반적인 트래픽으로 간주하여 다음 라우터로 전달한다.

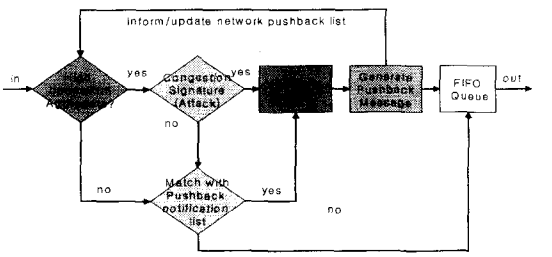



그림 3. 제안한 라우터 기반 DDoS 근원지 역추적 구조

### 5.2 Pushback을 적용한 역추적 마킹 기법

#### 5.2.1 패킷 헤더 마킹 필드 $M_x$

라우터 $R_x$의 IP 주소를 $A_x$라고 하자. 그리고 $R_x$에 도착한 IP 패킷을 $P_x$라고 할 때, $P_x$에서의 해더에서 마킹 정보를 저장할 수 있는 24 비트를 $M_x$라고 하자.

- 라우터 : $R_x$
- 라우터의 IP 주소 : $A_x$

- 라우터 $R_x$에 도착한 패킷 : $P_x$
- 패킷에서의 변형 가능한 헤더 24 비트 : $M_x$

패킷 $P_x$에서 $M_x$는 그림 4와 같이 TOS(type of service) 필드 8비트와 ID 필드 16비트로 구성된다. TOS 필드인 경우 현재 필드에 대한 정의만 되어 있을 뿐 실제적으로 사용하고 있지 않다. 따라서 TOS 필드 값을 사용한다고 하더라도 전체 네트워크에 영향을 미치지 않는다.

현재의 TOS 필드는 상위 3비트가 우선순위 비트로 설정되어 있고, 다음 3비트는 최소지연, 최대 성능 및 신뢰성 필드로 정의되어 있으나 현재는 사용하고 있지 않다. 다만 최근에 RFC2474에 의하면 Differentiated Service 필드(DS field)로 재정의하였으며 TOS 8비트 중에서 상위 6비트만을 사용하고 하위 2 비트는 사용하지 않고 있다. 따라서 본 연구에서는 TOS 필드 중에서 현재 사용하고 있지 않은 2비트에 대해서 PF(pushback flag)와 CF(congestion flag)로 정의한다. 특히 CF인 경우 RFC2474에서도 네트워크상에서 혼잡 현상이 발생하였을 경우 1로 설정하도록 정의되어 있다.

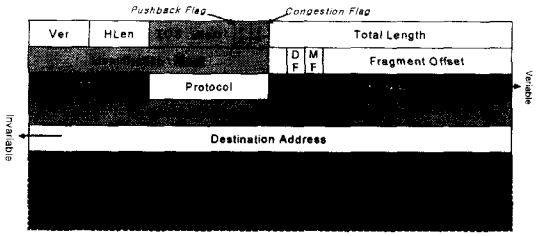



그림 4. 제안한 기법에서의 패킷 마킹 필드

### 5.2.2 TTL 정보를 이용한 마킹 구조

24비트 $M_x$ 정보에 대해서 라우터 $R_x$에 대한 IP 주소 $A_x$ 값을 패킷 헤더에 마킹하는 과정은 다음과 같다.

패킷에서 마킹이 가능한 24비트 정보에 대해서 pushback 과정을 통해 이상 트래픽이 발생하였을 경우 이에 대한 마킹을 위해 라우터 $R_x$ 자신의 IP 주소 $A_x$와 pushback에 의한 전단계 라우터 $R_y$의 IP 주소 $A_y$를 패킷에 마킹한다. 24비트 내에 두개의 라우터 주소값을 마킹해야 하기 위해서 라우터에 대한 해쉬 값을 적용하여 인증 기능도 제공하는 주소값을 마킹하게 된다.

모든 패킷의 TTL(time to live) 필드는 8비트 정보로 구성되며 패킷 전송시 일반적으로 255로 설정되어 전송된다. 라우터에 의해 전송되는 과정에서 TTL 값은 1씩 감소되어 최종적으로 목적지에 전달된다.

현재 TTL 값은 네트워크 상에 패킷 전송시 대역폭을 확보하고 목적지에 도착하지 않는 패킷을 제어하기 위한 목적으로 사용된다. 기존의 연구에서는 TTL 값을 사용하지 않고 다만 별도의 hop 카운터 필드를 두어 패킷이 전달된 거리 정보를 계산하도록 하고 있다. 그러나, 본 연구에서는 라우터 $R_x$에 도착한 패킷의 TTL 값에서 일부 정보를 사용하여 패킷 마킹 과정에 사용한다.

구체적으로 TTL 필드 8비트에서 일반적으로 네트워크 홉 거리는 최대 32 정도로 되어 있기 때문에 라우터 $R_x$에 도착한 패킷 $P_x$의 TTL 필드 하위 6비트 정보만으로도 패킷이 전달된 거리 정보를 계산할 수 있다. 즉, 패킷 $P_x$에서 TTL 필드에서 하위 6비트 정보에 추출하여 이를 $T_x$라고 하고 패킷의 TOS 6비트 필드 $P_x^{TF}$에 저장한다.

$$T_x = TTL of P_x \wedge 00111111$$

$T_x$ 값은 현재 패킷이 공격지 시스템으로부터 전달된 거리 정보를 나타내며, 만일 이를 패킷에 포함시킨다면 목적지 시스템 $V$에 패킷이 도달하였을 경우 $V$에서 마찬가지로 계산된 $T_v$ 값을 비교하여 패킷이 라우터 $R_x$로부터 전달된 거리 정보도 계산할 수 있다.

### 5.2.3 라우터에서의 역추적 경로 마킹

앞에서 제시한 ACC 기반 pushback 모듈을 통해 이상 트래픽이 발생하였다는 것을 통보받게 되면 이제 라우터 $R_x$에서는 pushback 메시지 내에 포함된 혼잡 시그너쳐에 해당하는 패킷 $P_x$에 대해서 마킹 과정을 수행한다.

우선 pushback 메시지를 받았기 때문에 TOS 필드에서의 PF 필드를 1로 설정한다. 그리고 현재 패킷 $P_x$에서의 TTL 필드 8 비트에 대해 $T_x$값을 계산하고 이를 TOS 필드 6비트에 저장한다. 그리고 라우터 $R_x$의 주소 $A_x$와 앞에서 계산된 $T_x$ 값에 대해 해쉬 함수 $H(\cdot)$를 사용하여 8비트 해쉬 값을 계산하고 이를 ID 필드 처음 8비트인 $P_x^{MF1}$에 마킹한다. 마킹

된 패킷은 패킷의 목적지 주소에 해당하는 라우팅 경로의 다음 라우터 $R_y$에게 전달된다.

이제 라우터 $R_y$는 패킷의 PF 필드값 $P_x^{PF}$을 보고 1로 설정되어 있는 경우 패킷에서의 TOS 필드 6비트에 해당하는 $P_x^{PF}$에서 1을 뺀 값과 라우터 IP 주소 $A_y$에 대해 마찬가지로 해쉬 함수를 적용하여 $P_x^{MF2}$에 마킹한다.

$$P_x^{MF1} = H(T_x | A_x), P_x^{MF2} = H(P_x^{TF} - 1 | A_y)$$

마킹과정을 수행한 후에는 CF 필드 값을 1로 설정하여 다음 라우터로 전송하게 되며 다음 라우터는 PF 필드 값과 CF 필드 값이 1로 설정되어 있는 경우에는 이전 라우터에 의해 마킹된 패킷이므로 더 이상 마킹 과정을 수행하지 않는다. 본 연구에서 제안하는 마킹 구조는 아래 그림 5와 같다.

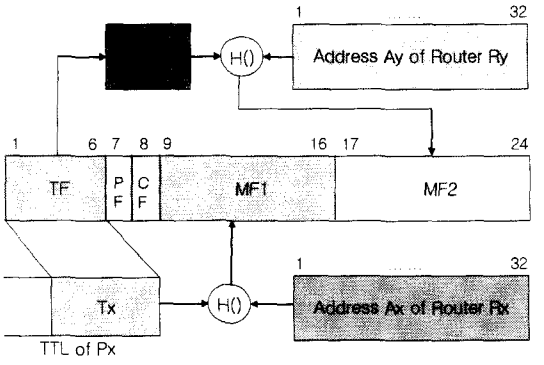



그림 5. 제안한 기법에서의 패킷 마킹 구조

### 5.3 역추적 경로 재구성

#### 5.3.1 DDoS 공격 패킷 역추적

네트워크를 통해 전달된 패킷에 대해 피해시스템 $V$에서는 DDoS 공격 경로를 재구성하게 된다. 그림 6과 같이 DDoS 공격을 $S1, S2, S3$에서 수행하였다고 가정하자. 공격 패킷에 대해 라우터 $R_x$, $R_y$ 및 $R_z$는 패킷 헤더 24비트 정보내에 라우터 자신의 IP 정보와 패킷에서의 $TTL$ 필드 6비트 정보를 마킹하였다. 피해시스템에서는 DDoS 공격이 발생하였을 경우 도착한 패킷에 대해 아래와 같이 경로 역추적 과정을 수행한다.

우선 피해시스템 $V$에 도착한 패킷을 $P_v$ 집합이라고 정의하자. $P_v$ 값은 DDoS 공격에 해당하는 패킷들로 구성된 집합이고, 집합내에서 라우터에 의해 마킹되어 전달된 패킷의 집합을 $M_v$라고 하자.

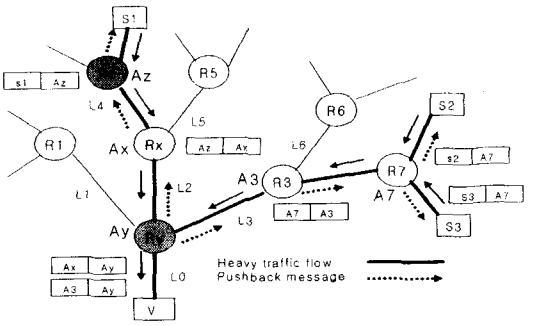



그림 6. 제안한 기법에서의 공격 경로 역추적

피해시스템에 도착한 패킷 집합 $P_v$에서 $M_v$값을 구별하는 방식은 아래와 같이 패킷에서의 TOS 필드 값중에서 임의의 패킷 $P_x$에서의 패킷 PF 필드에 해당하는 $P_x^{PF}$와 CF 필드 $P_x^{CF}$ 부분이 설정되어 있는 패킷을 선택하는 과정을 수행하게 된다.

$$M_v = P_x | P_x^{PF} \equiv 1 \wedge P_x^{CF} \equiv 1, x \in v$$

즉, 피해시스템에서 마킹되어 있는 패킷 $M_v$의 원소에 해당하는 임의의 패킷 $M_i$에 대해서 8비트 $TTL$ 값을 $TTL of M_i$라고 정의할 수 있고, TOS 필드에 패킷된 정보 $T_{Mi}$값과 비교여 패킷 $M_i$가 라우터로부터 마킹된 후에 전송된 네트워크 홉 거리 $D(M_i)$를 다음과 같이 계산 할 수 있다.

$$D(M_i) = M_i^{TF} - (TTL of M_i \wedge 00111111)$$

만일 $D(M_i) \equiv 1$이라면 피해시스템 바로 앞에 있는 라우터에 의해서 마킹 되었다는 것을 알 수 있다. 그러나 본 연구에서 제시하는 기법은 pushback 기법과 연계하였기 때문에, $D(M_i) \equiv 2$인 패킷을 대상으로 바로 역추적 경로 재구성 과정을 수행할 수 있다.

#### 5.3.2 DDoS 공격 경로 재구성

$D(M_i) \equiv 2$을 만족하는 패킷 $M_i$는 피해시스템 바로 앞단에 연결되어 있는 두 홉 거리 내에 있는 라우터 $R_y$ 및 $R_x$에 의해서 마킹된 패킷이라는 것을 의미한다. 즉, 패킷 $M_i$는 피해시스템과 바로 연결되어 있는 라우터 $R_y$와 2 홉 거리에 있는 임의의 라우터 $R_x$에 의해 마킹되었기 때문에 $D(M_i)$ 값은 2가 된다. 따라서 패킷 $M_i$에서 우선 2 홉 거리를 갖는 라우

터 $R_x$를 다음과 같이 판별할 수 있다.

$$M_i^{MF1} \equiv H(M_i^{TF} | R_x), (R_x \in D(M_i) \equiv 2) \text{ and}$$
$$M_i^{MF1} \equiv H((TTL\ of M_i \wedge 00111111) + 2 | R_x), \quad (R_x \in D(M_i) \equiv 2)$$

물론 패킷 $M_i$는 피해시스템과 홉 거리 1에 해당하는 라우터 $R_y$에 의해 마킹되었다는 것 역시 아래과 같은 방식으로 검증이 가능하다.

$$M_i^{MF2} \equiv H(M_i^{TF} - 1 | R_y), (R_y \in D(M_i) \equiv 1) \text{ and}$$
$$M_i^{MF2} \equiv H((TTL\ of M_i \wedge 00111111) + 1 | R_y), \quad (R_y \in D(M_i) \equiv 1)$$

이제는 $D(M_j) \equiv n, (n \geq 3)$를 만족하는 $M_j$에 대해서 위와 같은 과정을 반복하게 되면 DDoS 공격 패킷 집합 $P_v$에서 패킷이 전달된 실제 공격 경로를 재구성할 수 있다.

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

$$AP_1 = R_y \rightarrow R_x \rightarrow R_z \rightarrow S1,$$
$$AP_2 = R_y \rightarrow R_3 \rightarrow R_7 \rightarrow S2,$$
$$AP_3 = R_y \rightarrow R_3 \rightarrow R_7 \rightarrow S3$$

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. 또한 해쉬 방식을 적용하여 공격자에 의한 마킹 정보 검증 구조도 제공하였다.

## 6. 제시한 기법의 성능 분석

본 연구에서 제시한 기법에 대한 성능을 평가하기 위해서 Linux 환경에서 ns-2 시뮬레이터를 이용하여 성능을 분석하였다. 그림 7과 같은 네트워크를 구성하고 그림 8과 같이 0 노드, 1번 및 2번 노드에서 DDoS 공격을 수행하도록 시뮬레이션 하였다.

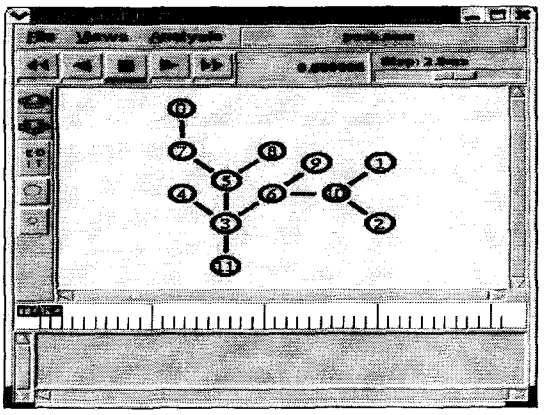


그림 7. ns-2 기반 실험환경 구축

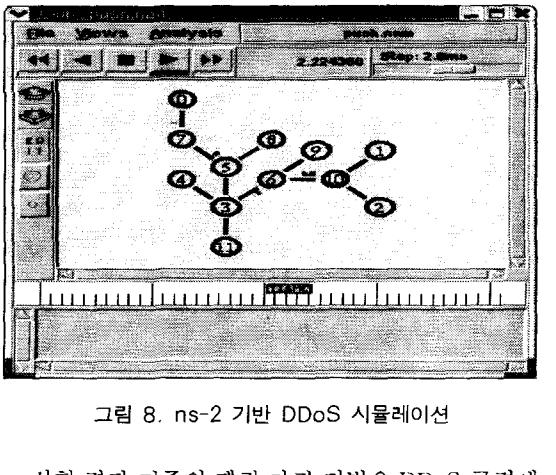


그림 8. ns-2 기반 DDoS 시뮬레이션

실험 결과 기존의 패킷 마킹 기법은 DDoS 공격에 대해 각 라우터에서 확률 $p$로 샘플링하여 마킹하는 방식이므로 전체 마킹된 패킷(파란선:v1.tr)의 수가 DDoS 트래픽(붉은선:r0.tr)에 비례하여 생성되는 것을 볼 수 있다. 그림 9, 그림 10과 같이 기존 기법과 본 연구에서 제시하는 기법을 비교하였을 경우 DDoS 트래픽에 대한 pushback 과정을 수행하기 때문에 DDoS 트래픽을 25% 정도 감소시키면서 역추적을 수행하게 된다.

제안한 기법과 기존의 IP 역추적 관련 기술들의 성능을 비교 분석하면 아래 표 1과 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 제

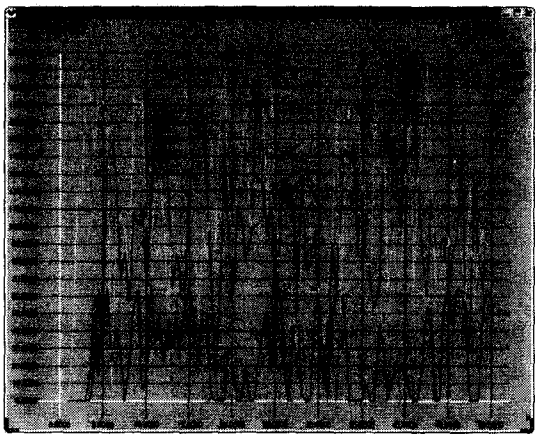


그림 9. 기존의 PPM 방식에서의 트래픽

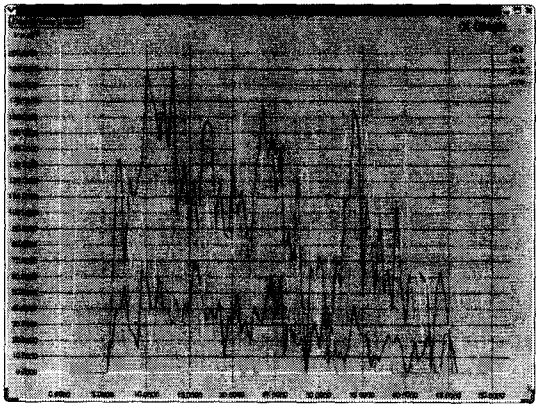


그림 10. 제안한 기법에서의 트래픽

공하지 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 취약한 특성을 보인다. 전체적으로 현재까지 제시된 IP 역추적 기법을 검토하였을 경우 대부분 기존 라우터에 대한 변형 및 추가적인 네트워크/시스템 부하가 발생한다는 것을 알 수 있다.

본 연구에서 제시한 기법은 기존의 PPM 기법과 유사한 방식으로 작동하기 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 PPM 기법에서는 임의의 확률 $p$로 패킷을 선정하여 마킹 과정을 수행하였으나 본 연구에서 제시한 기법은 ACC 기반 혼잡 제어 기능을 사용하고 TTL 필드 값을 이용하여 경로 정보를 마킹하기 때문에 피해 시스템에 도달하는 역추적 경로 재구성에 필요한 패킷의 수를 줄일 수 있었다.

따라서 전체 네트워크 상의 대역폭을 향상시킬 수 있고, 적은 개수의 마킹 패킷만을 가지고도 DDoS 공격 근원지에 대한 경로를 재구성할 수 있다. 경로 재구성을 위해서는 네트워크에서 $n$개의 라우터를 거치는 경우 단지 $n$개의 역추적 메시지만으로 근원지 경로를 재구성할 수 있다는 장점을 제공한다. 물론 라우터에 ACC 기반 pushback 모듈에서의 DDoS

표 1. IP 역추적 기법 성능 비교 평가

| 특성 / 기법 | 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 | ↓ | ↓ | ↑ | ↑ | ↓ | △ | △ | ◇ | ▽ | △ | ↑ |
| 제안한 기법 | ↓ | ↓ | ↓ | ↑ | ↓ | △ | △ | △ | △ | △ | n |

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

관련 판별 기능을 추가로 수행하기 때문에 메모리 요구는 증가한다는 단점이 있다.

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

근래 Ad-hoc 기반 네트워크 환경에서의 DDoS 공격에 대한 취약점이 발견되고 있다. 앞으로는 무선 환경에서 패킷에 대한 필터링 기능을 제공하고 공격 근원지에 대한 역추적 기능을 제공할 수 있는 방안에 대해 연구할 필요가 있다. 또한 IP 계층에서의 보안 프로토콜이 제공되는 환경인 IPSec 기반 환경과 일반 IP 계층에서의 역추적 기능도 고려해 보아야 한다. 기존의 방화벽 및 IDS가 담당하던 기능을 라우터가 포함하여 전체 네트워크의 안전성을 제공하면서도 패킷에 대해 역추적할 수 있는 기법도 연구되어야 할 것이다.

## 참 고 문 헌


[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, 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., 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.142-153, July, 2003.

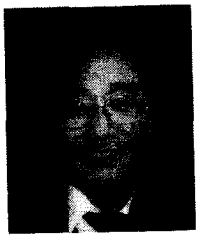
[14] S. Floyd, S. Bellovin, J. Ioannidis, K. Kompella, R. Mahajan, V. Paxson, "Pushback Message for Controlling Aggregates in the Network," Internet Draft, 2001.

**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

**최 창 원**

1990년 고려대학교 전산과학과 졸업(학사)
1992년 고려대학교 대학원 전산과학과 졸업(석사)
1995년 고려대학교 대학원 전산과학과 졸업(박사)
1996년~현재 한신대학교 정보시스템공학과 부교수
관심분야 : 정보보호, Ad-hoc 네트워크, 멀티미디어, 네트워크 성능평가



**김 태 우**

1984년 인하대학교 전자공학과 졸업(학사)
1990년 인하대학교 대학원 전산학과 졸업(석사)
1996년 고려대학교 대학원 전산과학과 졸업(박사)
1984년~1986년 (주)LG전자 시스템엔지니어
1986년~1997년 한국전자통신연구소 선임연구원
1997년~현재 성공회대학교 정보통신공학과 부교수
관심분야 : 컴퓨터네트워크, 정보보호, 네트워크 보안, 리눅스, 분산시스템