경량화된 IP 역추적 메커니즘

허 준[†] · 홍 충 선[††] · 이 호 재[†††]

요 약

네트워크를 통한 공격에 대처하는 방법 중 가장 어려운 문제는 공격자가 자신의 주소를 위장한다는 것이다. 인터넷의 근본적인 구조 때문에 자신의 주소를 위장한 패킷의 근원지를 추적하는 것은 매우 어렵다. 또한, 현재까지 제안된 방법 중 공격 근원지를 추적하는 IP 역추적(Traceback) 알고리즘은 실제 적용에 있어 한계를 가지고 있으며, 이러한 문제점을 극복하기 위한 연구가 진행되어야 할 필요가 있다. 본 논문에서는 기존 IP 역추적 기법의 문제점 해결하기 위해 마킹을 이용한 새로운 IP 역추적 메커니즘을 제안하였다. 제안된 메커니즘의 성능평가를 통해 적은 시스템 오버헤드만으로 역추적을 위한 효율적인 마킹이 가능함을 보였다.

키워드 : IP 역추적기법, 확률적 패킷 마킹, DDoS 공격

Lightweight IP Traceback Mechanism

Joon Heo[†] · Choong Seon Hong[††] · Ho Jae Lee[†††]

ABSTRACT

A serious problem to fight attacks through network is that attackers use incorrect or spoofed IP addresses in attack packets. Due to the stateless nature of the internet structure, it is a difficult problem to determine the source of these spoofed IP packets. While many IP traceback techniques have been proposed, they all have shortcomings that limit their usability in practice. In this paper we propose new IP marking techniques to solve the IP traceback problem. We have measured the performance of this mechanism and at the same time meeting the efficient marking for traceback and low system overhead.

Key Words : IP Traceback, Probabilistic Packet Marking, DDoS attack

1. 서 론

분산 시스템의 증가와 인터넷의 확산으로 인하여 네트워크를 통한 공격의 가능성은 점점 늘어나고 있다. 따라서 잠재적인 공격의 위협으로부터 시스템을 보호하기 위해 방화벽(Firewall), 침입탐지시스템(IDS : Intrusion Detection System)과 같은 보안 시스템이 설치되어 운용되고 있다. 그러나 기존의 보안 장치들은 지역 네트워크 경계를 넘어선 탐지가 불가능하고, 네트워크 차원의 효율적이고 적극적인 대응이 불가능하며, 새로운 공격 패턴이나 보안 정책 등의 변화에 대한 즉각적인 대응이 어렵다. 이러한 문제점들을 해결하기 위해서는 공격에 대해 능동적으로 대응이 가능하며, 보안 시스템들을 상호 결합하여 운용하고, 보안 정책 및 새로운 보안기술의 수용이 용이한 구조가 필요하다. 이러한 요구에 의해 DARPA에서는 능동 네트워크(Active Network)를 제안하였다. 능동 네트워크는 패킷 스위칭 네트워크를 통해 전송되는 이동 프로그램을 실행할 수 있는 라우터나 스위치를 배치하여, 전송된 능동 패킷에 포함되어 있는 이동 프로그램을 서비스 특성이나 사용자 요구에 따라 적합하게 연산, 처리할 수 있는 네트워크를 말한다. 즉, 사용자에게 네트워크를 프로그래밍 하는 능력을 부여하는 네트워크 아키텍처를 능동 네트워크라고 한다. 그러나 능동 네트워크는 동적이고 유연한 본성으로 인해 그 자체로도 심각한 보안 위협을 가지고 있다. 따라서 기존 네트워크의 보안 문제점을 해결하고 능동 네트워크의 보안 위협에 대한 자체적인 방어 능력을 가지는 보안 관리구조에 대한 연구가 필요하다.

TCP/IP 기반의 네트워크에서 현재 보안 기능을 위해 사용되고 있는 침입차단시스템, 프록시 서버, 패킷 필터 등의 기술들은 적극적으로 문제를 해결하기에는 충분하지 않다. 따라서 동적이고 재구성이 가능하며 확장가능하고 상호 운영성이 있는 보안 관리를 위한 시스템이 갖추어져야 한다. 기존의 방화벽이나 침입탐지 시스템과 같은 수동적인 보안 구조로는 공격의 근원을 차단하지 못하므로 일시적인 방어

※ This work was supported by MIC and ITRC Project.
† 준 회 원 : 경희대학교 컴퓨터공학과 박사과정
†† 종신회원 : 경희대학교 전자정보학부 부교수
††† 준 회 원 : (주)플랜티넷 솔루션 개발팀 전임연구원
논문접수 : 2006년 7월 22일, 심사완료 : 2006년 12월 26일

효과만을 기대할 수 있다. 공격자는 다양한 방법을 동원하여 공격을 시도할 것이고 현재의 보안 기술로는 다양한 공격을 막는데 한계를 가지게 된다. 현재 보안 기술들은 각각 개별적으로 연구, 개발되고 있으나, 이러한 기술들을 연동하고 보완한다면 효과적인 보안 기능을 제공할 수 있을 것이다[14,16].

대부분의 공격자는 자신의 IP를 스푸핑(spoofing) 하기 때문에 이것을 극복하기 위한 IP 역추적기법들이 제안되었다. 하지만 현재까지 제한된 기술 대부분이 제한적이거나 그들의 실용성에 문제점을 가지고 있다[1,7,8].

IP 역추적 기법의 개발에 있어 가장 중요한 사항은 현재 사용되고 있는 네트워크 및 장비에 최소한의 변경과 기능 추가로 IP 역추적기법 기술을 구현할 수 있어야 한다는 것이다. 새로운 IP 역추적기법 기술이 개발되어 공격이 발생하더라도 실시간으로 공격자를 추적하고 공격의 근원지를 차단할 수 있다면 네트워크에 대한 위협은 상당부분 사라지게 될 것이다[9,12,13].

수동적인 방어구조에서는 공격을 탐지하고 단순히 차단하는 기능만을 제공하지만, 역추적과 같은 능동적인 보안구조가 실제 네트워크에 적용된다면 공격이 발생하더라도 빠른 시간 내에 공격자를 추적, 차단하여 더 이상의 피해를 방지할 수 있고 근원적인 공격 요소를 제거할 수 있기 때문에 추후 공격의 가능성 또한 사라지게 된다.

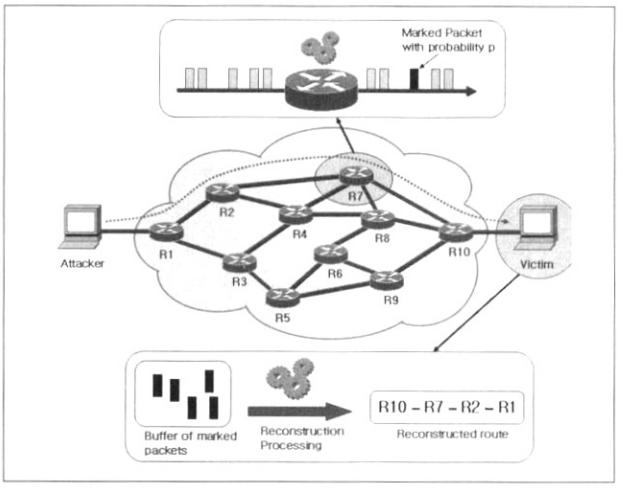
본 논문에서는 마킹(marking) 기법을 바탕으로 경량화된 IP 역추적 메커니즘을 제안한다. 본 논문은 다음과 같이 구성되었다. 2장에서는 현재까지 제안된 IP역추적 기술들을 소개하고 문제점을 살펴본다. 3장에서는 제안된 IP 역추적 메커니즘의 개념과 동작과정을 상세히 설명한다. 4장에서는 시뮬레이션을 통해 성능을 평가하고, 마지막으로 결론과 향후 과제에 관하여 논한다.

2. 관련연구

2.1 확률적 패킷 마킹(Probabilistic Packet Marking) IP 역추적기법

확률적 패킷 마킹 IP 역추적 기법[1,6]은 스푸핑된 패킷의 실제 전송경로를 알기 위해 네트워크상에 전송되는 패킷에 라우터가 패킷이 자신을 지나갔다는 정보를 삽입하는 방법이다. 라우터는 패킷의 IP 헤더에서 변형 가능한 필드에 자신의 IP 주소를 마킹하여 다음 라우터에 전달한다. 각 라우터에서 삽입된 정보가 다음 라우터에 전달되고 최종적으로 피해 시스템에 도달하게 된다. 만약, (그림 1)과 같이 구성된 네트워크에서 공격이 발행했다면 피해 시스템이 전달받은 패킷에 기록되어 있는 라우터 정보를 재구성하여 패킷의 전송 경로를 알 수 있게 된다.

하지만 라우터에서 지나가는 모든 패킷에 마킹을 하게 된다면 라우터에 엄청난 부하가 발생하여 원활한 네트워크 상태를 유지할 수 없기 때문에 패킷에 정보를 기록할 때 일정한 확률 p로 샘플링하여 마킹을 실시한다.



(그림 1) 확률적 패킷 마킹

라우터에서 패킷에 정보를 기록할 때는 패킷 헤더의 인식 필드(Identification field)에 기록한다. 이것은 IP 헤더의 분할을 위하여 패킷의 동일성을 표시하는 인식 필드(Identification field)를 사용할 확률이 0.25%정도밖에 되지 않는다는 점에 착안하여 사용하는 것이다[3,15].

라우터에서 패킷에 마킹을 하는 정보의 구성에 따라 노드 샘플링(Node Sampling), 에지 샘플링(Edge Sampling) 및 향상된 패킷 마킹 기법(Advanced Packet Marking Scheme) 등이 제안되었다[3].

2.1.1 노드 부착(Node append) 기법

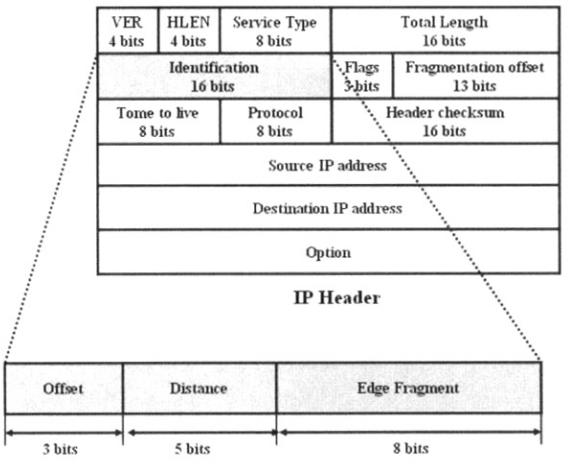
패킷 마킹 기법 중에서 가장 단순한 알고리즘으로 패킷이 경유하는 라우터의 정보를 패킷에 순차적으로 추가시키는 기법이다. 그러나 라우터의 오버헤드와 경로의 전체 길이를 알 수 없으므로 패킷의 공간 확보에 대한 불확실성, 불필요한 패킷의 단편화를 초래할 수 있다.

2.1.2 노드 샘플링(Node Sampling) 기법

노드 부착 기법(2.1.1)에서의 라우터 트래픽 증가와 패킷 공간 확보 문제를 해결하기 위하여 경로를 샘플링하여 기록하는 기법이다. 각 라우터는 확률 p를 이용하여 패킷을 샘플링해서 IP 헤더에 경로정보를 마킹한다.

2.1.3 에지 샘플링(Edge Sampling) 기법

에지 샘플링 기법의 개념은 에지 정보를 패킷에 기록한다는 것이다. 이 기술은 샘플링 되는 각 패킷의 헤더부분에 start, end, distance 3개의 필드를 만든다. 라우터가 패킷에 마킹을 결정하면 start 필드에 라우터 자신의 IP 주소를 기록하고 distance 필드에 0을 기록한다. 그렇지 않고 distance 필드가 이미 0으로 기록되어 있으면 이것은 이전 라우터가 패킷에 마킹을 했다는 것이므로 라우터의 IP 주소를 end 필드에 기록한다. 그리고 start 필드와 end 필드를 기록하지 못한다면 distance 필드 값을 하나 증가시킨다. 따라서 패킷



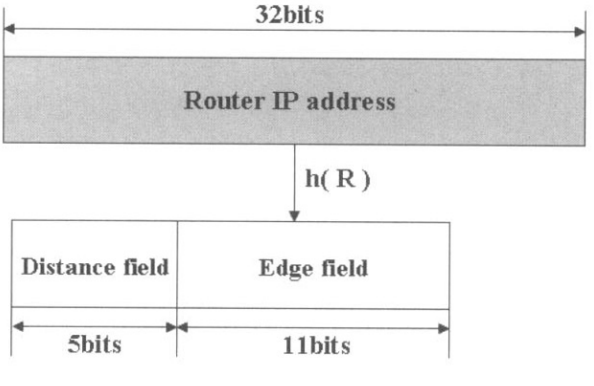
(그림 2) 인식 필드 인코딩 방법

의 distance 필드는 마킹을 시작한 라우터로부터 피해 라우터 까지 라우터의 개수를 나타내게 된다.

(그림 2)와 같이 IP 헤더의 16 비트 인식 필드(identification field)를 이용하여 에지 정보를 기록한다. 16 비트의 인식필드는 에지 정보의 순서를 나타내는 3 비트의 offset 값과 distance 필드를 기록하는 5 비트, start와 end 필드 값을 기록하는 8 비트로 구성된다. 여기서 한 개의 헤더는 8 비트의 필드 값을 기록하기 때문에 64 비트를 나타내기 위해서는 총 8개의 패킷이 필요하게 된다.

2.1.4 향상된 마킹(Advanced Marking) 기법

(그림 3)의 인코딩 구조에 나타나듯이 16비트 IP 인식 필드(identification field)를 사용하여 마킹을 하는데 라우터까지의 거리를 나타내는 5비트 distance 필드와 11비트의 edge 필드로 구분된다. 패킷의 인식필드에 32비트의 라우터 주소를 해쉬함수(h(Router))를 사용해서 11비트로 암호화 시킨 후 마킹을 하고 5비트의 distance 필드는 32홉까지 나타낼 수 있기 때문에 대부분의 인터넷 경로를 알아내는데 충분하다[4].

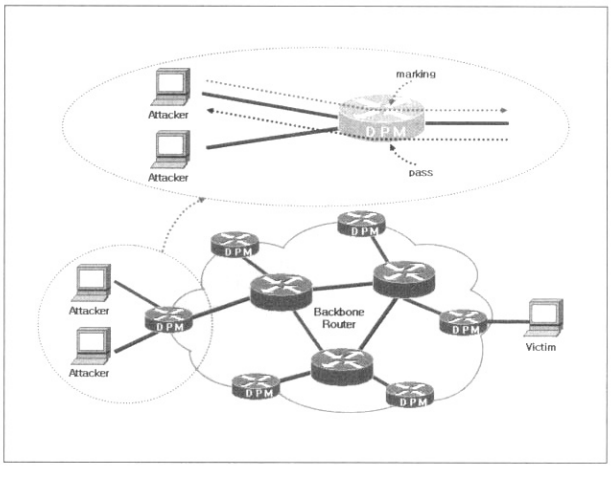


(그림 3) 향상된 마킹 기법의 인코딩 구조

2.2 Deterministic Packet Marking (DPM)

(그림 4)와 같은 구조를 가지는 DPM은 네트워크를 지나가는 모든 패킷에 마킹을 실시한다.

만약 공격자가 마킹정보를 변형시킨다 해도 DPM의 경우 변형된 정보에 다시 마킹을 하기 때문에 정확한 정보가 기록이 된다. DPM은 라우터에 들어오는 패킷에 대하여는 마킹을 하고 자신을 통해 나가는 패킷에 대해서는 마킹을 하지 않는다. DPM은 정보를 마킹하는데 2개의 패킷이 필요하다. 한 패킷당 16 비트의 패킷 ID 필드와 1 비트의 플래그(flag) 정보를 기록한다. 두 개의 패킷 ID는 라우터의 32 비트 주소를 기록하고 플래그 정보는 0과 1로 정보를 가지고 있는 두 패킷의 순서를 나타낸다[2,10,11].



(그림 4) Deterministic Packet Marking 기법

2.3 ICMP 역추적 기법

ICMP 역추적 기법[1][3]은 확률을 이용한다는 점에서 확률적 패킷 마킹 기법과 유사하지만 다른 접근 방법으로 작동한다. 라우터에서 일반적으로 1/20,000의 확률로 패킷을 샘플링하여 iTrace 메시지를 생성하고 이를 샘플링한 패킷과 동일한 목적지로 전송한다. iTrace 메시지는 일반적인 ICMP 메시지와 유사하게 전단계 라우터 정보와 다음단계 라우터 정보를 포함하고 있으며 패킷의 페이로드 정보 등을 포함하여 전달한다.

3. 제안사항

앞 절에서 설명한 다양한 IP 역추적기법들은 개선의 여지가 남아있고 현재 계속 연구가 진행되고 있다. 확률적 패킷 마킹(PPM)과 같은 기술은 설치가 간단하고 저렴하다는 장점이 있지만 피해자 측에서 공격경로를 재구성하기 위한 최소한의 패킷은 받아야 한다는 단점이 있고, ICMP 역추적기법은 역시 설치가 쉽고 현재 존재하는 프로토콜과 호환이 된다는 장점이 있는 반면 추가적으로 트래픽이 발생하는 단점이 존재한다. 해쉬 기반(Hash-based) 역추적기법은 SPIE(Source

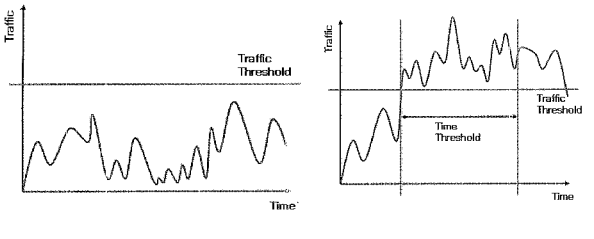
Path Isolation Engine) 기반 역추적 서버를 구성하고 전체 네트워크를 서브그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리하고 역추적 하는 방식이다. 하지만 SPIE, SCAR(SPIE Collection And Reduction Agent), DGA(Data Generation Agent) 등을 추가적으로 구축해야 하기 때문에 설치가 어렵고 설치비용 또한 상승하게 된다.

여러 IP 역추적 기법 중 현재 구성되어 있는 네트워크에 가장 간단하고 경량으로 설치할 수 있는 것은 마킹(marking) 기법을 이용한 알고리즘이다. 마킹 방법은 네트워크에 추가적인 장비를 설치할 필요 없이 현재 구성되어 있는 라우터에 마킹 관련 알고리즘을 설치하고 피해 시스템에서 공격경로를 재구성하는 알고리즘만 실행할 수 있으면 된다. 본 논문에서 사용되는 모든 라우터들은 IP 역추적(Traceback) 모듈이 지원되어 마킹 기능이 가능하다고 가정한다. 또한, 공격경로를 재구성하는 과정에서 밝혀진 공격경로상의 라우터들은 공격패킷의 정보를 피해시스템으로부터 전송받아 해당 패킷을 필터링하여 공격에 실시간으로 대응할 수 있으므로 DDoS와 같은 공격에 대응하기 적합하다고 할 수 있다. 최종 공격자를 찾았을 경우 그 공격자가 보내는 패킷을 필터링하여 더 이상의 피해가 존재하지 않도록 하는 것이 본 논문의 최종적인 연구목표라고 할 수 있다.

3.1 샘플링 확률 p의 보정

일반적인 네트워크의 트래픽을 지속적으로 관찰해보면 시간, 요일과 같은 다양한 조건에 따른 트래픽 양의 차이는 있지만 대부분 일정한 패턴을 가지고 있다.

현재 제안된 알고리즘들은 대부분 일정한 확률을 가지고 (ex. ICMP 역추적기법 : 20,000개중 1개) 샘플링을 실시하는데 이럴 경우 일반적인 트래픽과 공격시 트래픽 양의 차이에 의해 패킷이 샘플링되는 간격이 일정하지 않게 된다. (그림 5)와 같이 DDoS와 같은 공격이 시작되면 라우터를 지나가는 패킷은 일반적인 상태보다 최소한 몇 배의 양을 처리해야 하는데 샘플링 확률 p를 사용한다면 공격이 진행되는 순간 라우터의 CPU 사용률은 급격하게 증가할 것이다. 이렇게 라우터의 부하가 급격하게 늘어날 때 동일한 확률의 샘플링을 통해 패킷을 마킹한다면 라우터의 과부하가 임계치를 초과할 가능성이 있다.



(그림 5) 평상시 트래픽과 공격시의 트래픽

따라서, 본 논문에서는 이러한 라우터의 과부하 현상을 해결하고자 일정한 시간 간격을 가지고 마킹을 하는 방법을 사용하였다. 이 방법을 적용하게 되면 공격이 시작되어도 일정한 시간에 마킹하는 횟수는 변동이 없기 때문에 라우터의 부하 증가가 상대적으로 적게 된다.

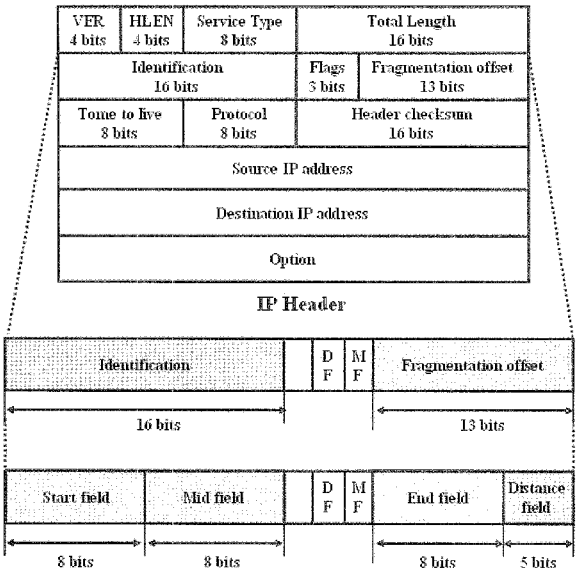
3.2 IP 헤더의 마킹 공간 확보와 향상된 에지 샘플링 기술

일반적인 마킹 알고리즘에서 사용되는 IP 헤더의 특성을 살펴보면 인식필드(identification field)의 16 비트 공간을 사용하고 있다[3,5,15]. IP 데이터그램의 단편화 및 재조립에 사용되는 인식필드를 사용하여 마킹 정보를 입력하는 이유는 실제 네트워크에서 데이터그램이 단편화되는 비율이 0.22%이하로 매우 작기 때문이다[15,17]. 더욱이 본 논문에서는 확률적 패킷 마킹방법을 사용하고 있으므로 마킹할 패킷이 단편화 되어 있을 가능성은 매우 희박하다고 할 수 있다. 이렇게 작은 가능성에도 불구하고 마킹할 패킷에 단편화 되어 있는 경우 라우터는 해당 패킷을 그대로 전달하고 다음 패킷에 마킹 정보를 입력하는 방법을 사용한다.

또한, 본 논문에서는 더 많은 마킹 공간을 확보하기 위하여 추가적인 공간을 사용하는 방법을 제안하였다. IP 헤더의 구성요소 중 13 비트의 단편화 옵셋(fragmentation offset) 필드 부분은 전체 데이터그램 내에서 단편화된 패킷의 상대적 위치를 나타내는데 사용되지만, 앞서 언급한 인식필드를 사용할 수 있는 이유로 인해 본 논문에서는 단편화 옵셋 부분까지 마킹에 사용한다.

이렇게 확보된 헤더의 사용가능 부분은 (그림 6)과 같이 인식필드의 16 비트, 단편화 옵셋의 13 비트를 사용하기 때문에 한 개의 패킷 헤더에 총 29 비트의 정보를 기록할 수 있다. 이것은 기존의 마킹 기법을 사용한 알고리즘에 비해 약 2배에 이르는 공간을 확보하는 것이다. 일반적인 에지 샘플링 기법에서 에지 정보를 기록하는데 8 비트의 start, end 필드 정보를 기록하기 때문에 8개의 패킷이 필요했다 (2.1.3절). 하지만 해쉬 함수를 사용하여 라우터의 IP 주소를 줄이게 되면 하나의 에지 정보를 전송하는데 8개의 패킷이 필요하지는 않을 것이다.

본 논문에서는 해쉬 함수를 사용하여 32 비트의 IP 주소를 8 비트 정보로 압축하여 하나의 패킷 헤더에 여러 개의 라우터 정보를 마킹하는 방법을 사용하였다. 이러한 방법을 사용해 확보한 29 비트의 IP 헤더 공간에 정보를 기록하면 5 비트의 distance 정보와 최대 3개의 라우터 정보를 기록할 수 있다. 기존의 에지 샘플링 기법은 각각 32 비트인 start 필드와 end 필드를 기록하고 5 비트의 distance 필드를 기록하기 때문에 여러 개의 패킷이 필요했지만 본 논문에서 제안하는 향상된 에지 샘플링 메커니즘은 확보된 29 비트의 공간을 (그림 6)과 같이 사용한다.



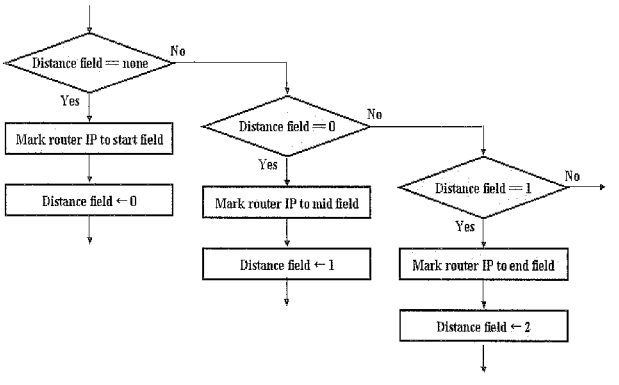
(그림 6) 제안하는 경량 IP 역추적기법의 IP 헤더부분

(그림 6)을 보면 인식 필드 16 비트와 단편화 옵셋 필드 13 비트를 합쳐 총 29 비트의 공간에 각각 8 비트인 start, mid, end 필드에 해쉬 함수로 처리된 3개의 라우터 IP를 기록하고 5 비트의 distance 정보를 기록한다. 제안된 메커니즘에서는 기존의 에지 샘플링 기법에서 2개의 에지 정보를 기록할 수 있는 반면 3개의 에지 정보를 기록 가능하고 8개의 패킷에 나누어서 정보가 기록되는 것이 아니라 하나의 패킷에 전부 기록이 가능하기 때문에 offset 값이 필요 없고, 각 패킷마다 distance 필드를 기록하기 위한 공간의 낭비도 막을 수 있다. 이렇게 하나의 패킷에 정보가 기록되게 된다면 공격이 시작되었을 경우 한 개의 패킷 헤더에 3개의 라우터 정보가 기록되어 있기 때문에 피해시스템에서 공격 패킷에 대한 정보를 얻을 확률이 높아지게 된다.

자세한 패킷 마킹 과정은 아래의 순서를 따르며, 제안된 메커니즘의 전체 순서도는 (그림 7)과 같다.

① 공격자에 의해 공격패킷이 전송

② 공격패킷이 라우터를 통과하며 일정한 시간에 의해 에지(edge) 정보가 마킹이 된다. 라우터가 패킷을 샘플링 했을 때 distance 필드에 아무것도 기록이 되지 않았다면 start 필드에 해쉬함수 처리된 라우터 IP를 기록하고 distance 필드에 0을 기록한다. 만약 distance 필드 값이 0이 아니라면 이전 라우터에서 start 필드를 마킹한 것을 의미하므로 mid 필드에 정보를 기록하고 distance 필드 값을 하나 증가시킨다. Distance 필드가 1로 기록되어 있다면 end 필드에 정보를 기록하고 distance 필드 값을 2로 하나 증가시킨다. 그리고 distance 필드에 2가 마킹된 이후에는 End 필드까지 정보가 기록되어 더 이상의 라우터 정보를 기록할 수 없기 때문에 distance 필드 값만 라우터를 지나갈 때마다 하나씩 증가시킨다.



(그림 7) 향상된 에지 샘플링 메커니즘 순서도

```
Marking procedure at router Ri

for each packet P
    when P is sampling
    if (P.distance == none) then
        P.distance ← 0
        P.edges ← h(Ri)
    else
        if (P.distance == 0) then
            P.edgem ← h(Ri)
        else
            if (P.distance == 1) then
                P.edgee ← h(Ri)
        P.distance ← P.distance + 1
```

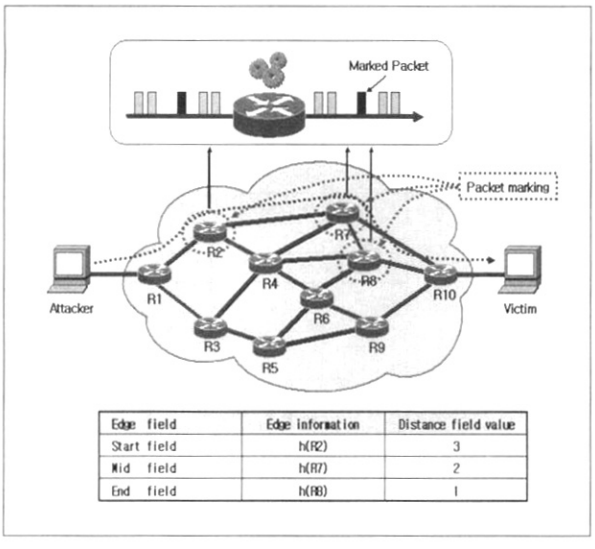
(그림 8) 라우터 Ri 에서의 마킹 순서

③ 피해시스템에서는 들어오는 패킷의 에지 정보 유무를 판단해 에지 정보가 있을 경우에는 그 정보를 저장한다.

④ 공격을 탐지했을 경우 피해시스템은 저장된 에지 정보 중 공격패킷에 해당하는 에지 정보를 선별해 공격 경로 재구성을 한다.

⑤ 공격경로가 재구성되면 공격 경로 상에 존재하는 라우터에게는 공격 정보를 전달해 해당 공격 패킷을 필터링하게 한다.

(그림 8)과 같은 마킹 기법을 사용하면 3개의 에지 정보(start, mid, end 필드)마다 distance 값을 가지게 되기 때문



Edge field	Edge information	Distance field value
Start field	h(R2)	3
Mid field	h(R7)	2
End field	h(R8)	1

(그림 9) 3개의 연속된 라우터의 마킹

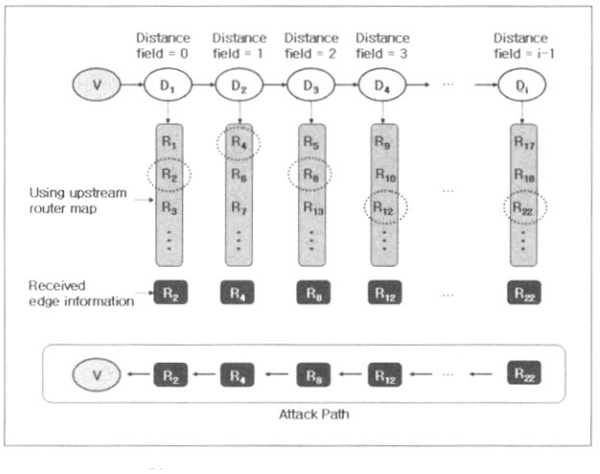
에 공격경로를 재구성하는 과정이 효과적이게 된다.

(그림 9)와 같은 시스템에서 R2에서 마킹된 패킷은 R7 → R8 → R10의 경로로 피해시스템에 도착하게 된다. 여기서 R2, R7, R8의 연속된 3개의 라우터에서 마킹이 되기 때문에 피해시스템에 도착한 마킹된 패킷의 헤더에는 해쉬 함수 처리된 R2, R7, R8의 주소와 distance 필드 값 3이 기록되어 있다.

이럴 경우 (그림 9)의 표와 같이 mid 필드의 에지 정보인 h(R7)은 바로 전 단계 라우터인 R2의 distance 필드 값보다 1이 적은 2가 되고 h(R8)의 distance 필드 값은 마찬가지의 이유로 1이 된다.

3.3 공격경로 재구성 과정

제안된 메커니즘은 피해시스템의 버퍼에 저장되어 있는 마킹된 패킷의 정보와 URM(upstream router map)을 이용하여 공격경로를 재구성한다. (그림 10)에서 피해시스템의 URM을 이용하여 distance 필드 값(max = 32)을 기준으로 라우터의 집합을 생성한다.



(그림 10) 공격경로 재구성 과정

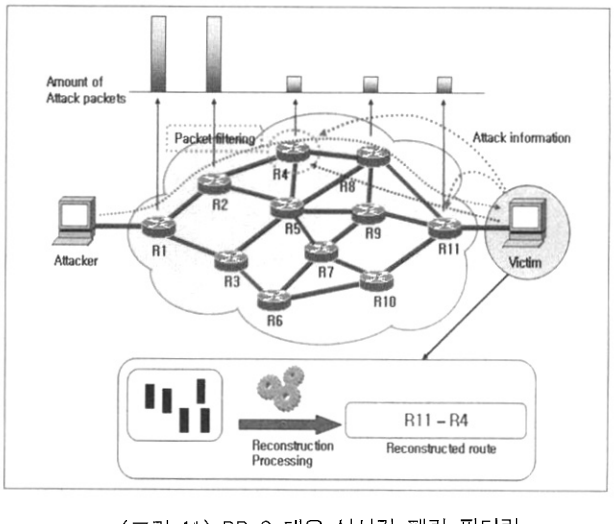
마킹된 패킷은 자신이 처음 마킹된 이후 모든 라우터를 통과할 때 마다 distance 필드값을 하나씩 증가시키기 때문에 피해노드(victim)로부터 얼마나 떨어져 있는 라우터를 통과한 패킷인지 정확한 정보를 알 수 있고 이렇게 단편화된 공격 패킷의 마킹정보를 조합하면 하나의 완전한 공격 경로를 재구성 할 수 있게 된다.

이렇게 재구성한 라우터의 공격경로를 URM을 이용한 라우터들의 경로 집합과 비교를 하여 최종적인 실제 공격경로를 재구성 하게 된다.

3.4 능동 네트워크 환경에서 DDoS 공격 대응방안

(그림 11)은 본 논문에서 제안하는 실시간 공격대응 IP 역추적기법 설명하고 있다. 이 메커니즘은 공격경로를 재구성함과 동시에 패킷필터링을 실행하는 것이다. 다시 말해, 피해시스템에서 저장된 공격패킷의 정보를 재구성함과 동시에 공격경로상의 라우터에 패킷필터링을 하게 함으로써 엄청난 양의 패킷을 전송하는 DDoS와 같은 공격에 대응할 수 있는 방법이다.

일단 공격이 탐지되면 피해시스템의 버퍼에 있는 에지 정보 중 공격패킷의 에지 정보만을 선별한 후 해당 에지 정보를 가지고 공격 경로를 재구성한다. 예를 들어 공격 경로를 재구성 하는 과정에서 (그림 11)과 같이 망이 구성되어 있고, R4와 R11의 정보가 처음으로 공격 경로로 판별되었을 경우 해당 R4와 R11 라우터에 공격 패킷에 대한 정보를 전송하고 피해시스템으로부터 더 원거리에 있는 R4 라우터가 우선적으로 공격패킷을 필터링하게 된다. 이때 경로상 자신보다 앞에 위치하는 R4 라우터에서 필터링을 실행하고 있으므로 R11 라우터에는 공격패킷이 전달되지 않아야 한다. 그럼에도 불구하고 R11 라우터에 공격패킷이 전송되고 있다면 R11도 공격패킷 필터링을 실행한다. 또한, R4 라우터를 경유하는 경로 외에 다른 경로를 통해서도 공격이 진행되고 있다는 것을 피해 시스템에 알린다. 이 경우 피해시스템은 공격이 한 개의 경로를 통해서 진행되는 것이 아니라 다양



(그림 11) DDoS 대응 실시간 패킷 필터링

한 경로를 통하여 DDoS 공격이 진행되고 있다는 것을 알 수 있게 된다.

이러한 방법을 반복하여 피해시스템에서 공격경로를 계속 재구성하게 되면 필터링은 점점 공격 근원지에 가까운 라우터에서 작동하게 될 것이다. 따라서 공격 근원지에 가장 가까운 라우터까지 역추적을 진행하며 공격을 차단할 수 있게 된다.

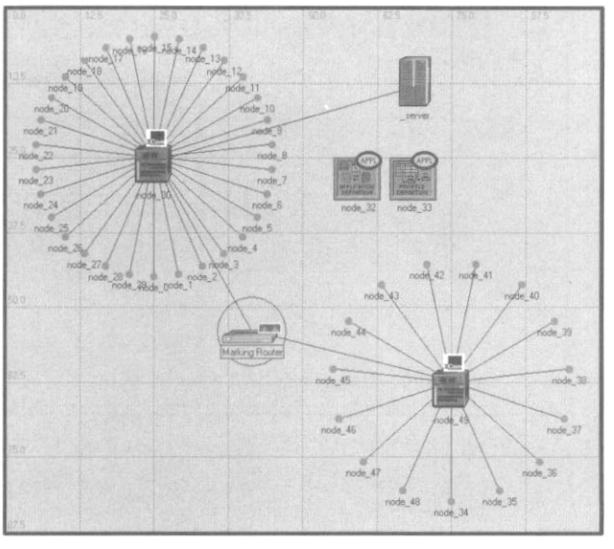
4. 성능평가

본 논문에서 제안한 메커니즘은 IP 헤더에서 확보한 29 비트의 패킷헤더 공간에 start, mid, end 에지 정보를 각각 기록하고 5 비트의 distance 필드 값을 기록하는 것이다.

성능평가 부분에서는 제안된 IP 역추적 알고리즘을 다른 IP 역추적 기법과의 정성적인 평가로 장단점을 비교하고 정량적 평가를 이용하여 제안된 IP 역추적 기법의 성능을 측정한다. 먼저, 본 논문에서 제안하는 방식을 현재까지 제안된 대표적인 기법들과 특징을 비교하여 (표 1)에 나타내었다. 비교 대상은 확률적 패킷 마킹 기법(PPM)[1][6], iTrace 기법[1][3], 해쉬기반(Hashed based) 역추적 기법[8]이다. 표 1과 같이 본 논문에서 제안하는 방식은 역추적 정보를 위한 필요 패킷의 양, 네트워크 처리 부하, 메모리 사용 등의 항목에서 효율적인 특징을 가지고 있다.

〈표 1〉 IP Traceback 기법들의 특징 비교

		Proposed Scheme	PPM	iTrace	Hashbased traceback
ISP imvolvement		Low	Low	Low	Fair
Scalbility		High	High	High	Fair
Number of attack packets required for traceback		**Hundred**	Thous ands	Thous ands	1
Network processing overhead	Every Packet	**Medium**	Low	Low	Low
	During traceback	None	None	None	Low
Victim processing overhead	Every Packet	None	None	None	None
	During traceback	High	High	High	None
Bandwidth overhead	Every Packet	None	None	Low	None
	During traceback	None	None	None	Low
Memory requirements	Every Packet	None	None	Low	Fair
	During traceback	**Low**	High	High	None
Ease of evasion		Low	Low	High	Low
Protection		High	High	High	Fair

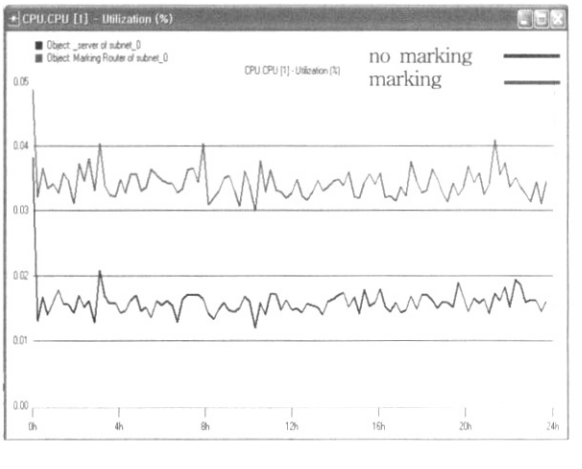


(그림 12) 시뮬레이션 시스템 구조

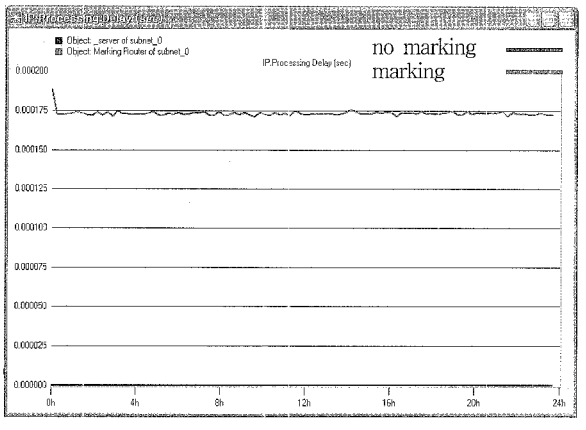
본 시뮬레이션은 마킹을 하는 과정에서 발생하는 라우터의 부하와 지연시간을 측정해서 일반적인 네트워크 상태의 라우터와 비교하여 이러한 메커니즘이 전체적인 네트워크에 어느 정도의 부하를 주는지 알아보았다. 또한, 지금까지 제안된 대표적인 역추적 기술[2][3][4][5]들은 실질적인 성능평가 결과를 포함하고 있지 않은 경우가 대부분이어서 본 논문에서 제안하는 방법을 기존의 기술들과 여러 관점에서 정량적으로 비교하기는 어렵다. 하지만, 제안하는 방법과 DPM(2.1.5절) 기술과의 효율성을 비교하는 방법을 사용하였다. (※ 시뮬레이션은 MS Windows XP Professional SP2 버전에서 OPNET modeler 10.5와 Microsoft Visual C++ 6.0 컴파일 환경을 기반으로 실행되었다.)

(그림 12)는 시뮬레이션 시스템의 구조를 표현하고 있다. 두 개의 3Com SSII 스위치를 사용하고 두 스위치 사이에 마킹을 담당하는 Cisco 2514 라우터를 배치하였다. 각 스위치에는 30개와 16개의 노드가 연결되어 다양한 종류의 패킷을 전송하고 모든 노드는 10BaseT로 연결된다.

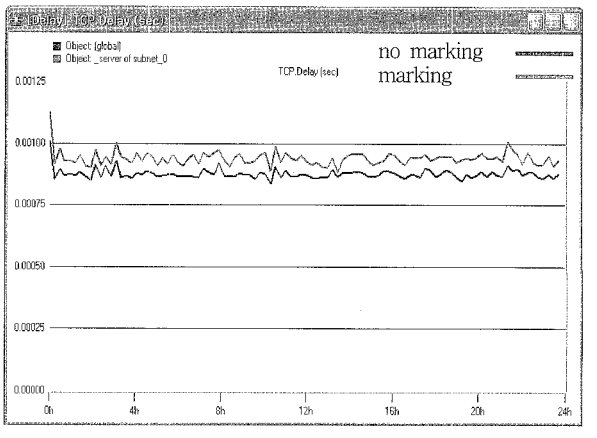
(그림 13)은 일반적인 네트워크 환경에서 라우터의 CPU



(그림 13) 일반적인 라우터와 마킹 라우터의 CPU 사용률 비교



(그림 14) IP 처리 지연(Processing Delay) 측정



(그림 15) TCP 지연(Delay) 측정

사용률과 마킹 기법을 적용했을 때의 CPU 사용률 차이를 보여주고 있는 결과이다. 시뮬레이션 결과에서 알 수 있듯이 마킹기법을 적용했을 때 CPU 사용률이 다소 증가하는 것을 볼 수 있다. 마킹을 할 경우 라우터의 CPU 사용률은 약 3.5%이고 일반적인 네트워크 상태에서의 라우터 CPU 사용률은 약 1.7%정도이므로 약 두배 정도의 차이가 나고 있으므로 마킹 기법이 라우터에 어느 정도 부하를 발생시킨다고 볼 수 있다. 하지만 3.5%의 라우터 CPU 사용률은 라우터의 패킷처리 성능에 큰 무리가 되지 않는다고 판단되므로 이러한 마킹 방법을 사용하여 IP 역추적이 가능하다면 여유 있는 라우터의 CPU 사용률을 이용한 효율적인 시스템이라고 말 할 수 있을 것이다.

(그림 14)는 라우터에서 IP를 처리하는 과정에 생기는 지연시간을 비교한 그래프이다. 마킹 알고리즘은 패킷의 헤더 부분에 라우터 정보를 마킹하기 때문에 일반적으로 라우터에서 패킷을 처리하는 것 보다는 많은 시간이 소요 된다.

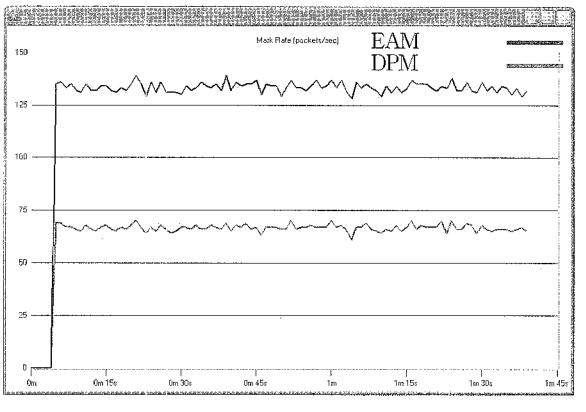
시뮬레이션 결과에서 보듯이 일반적인 네트워크 환경과 마킹 알고리즘이 적용된 환경과 패킷의 처리시간에는 0.175ms 정도의 지연시간차가 발생하는 것을 알 수 있다.

(그림 13)과 (그림 14)의 실험 결과에서 마킹알고리즘은 라우터의 추가적인 오버헤드와 처리시간 지연이 필연적으로 발생되지만 그 차이는 시스템 전체에서 우려할 만큼은 아니라고 판단할 수 있다.

(그림 15)는 TCP의 지연시간을 측정한 결과이다. 앞선 시뮬레이션 결과와 마찬가지로 지연시간의 차이가 크지 않음을 알 수 있다.

(그림16)은 본 논문에서 제안하는 메커니즘과 기존에 제안된 DPM(Deterministic Packet Marking) 기법(2.1.5절)의 Mark Detection Rate을 비교한 결과이다.

DPM은 하나의 에지 정보를 기록하는데 2개의 패킷이 필요하다. 따라서 하나의 패킷만으로 완전한 에지 정보를 가지고 있는 제안 메커니즘과 비교하면 Mark Detection Rate가 2배정도의 차이를 보이고 있다. 또한, 본 논문에서 제안된 메커니즘은 마킹이 검출될 때 마다 3개(start, mid, end)의 에지 정보를 가지고 있기 때문에 실질적으로 DPM보다



(그림 16) Mark Detection Rate

약 6배의 에지 정보를 가지게 되므로 기존의 DPM 마킹기법보다 효율적이며, 정확한 역추적 경로를 알아낼 수 있는 가능성이 크다고 볼 수 있다.

5. 결론 및 향후 과제

공격 근원지를 정확하게 찾기 위한 노력으로 IP 역추적 기술이 연구되었지만 대부분의 공격이 근원지 IP 주소를 스푸핑(IP Spoofing)하기 때문에 이러한 IP 역추적은 한계에 이를 수밖에 없다. 현재까지 제안된 IP 역추적 기법들은 단순한 추적 기능만을 제공하여 공격에 대한 근본적인 대책이 될 수 없었다. 근본적인 공격을 차단하지 않고 단순한 추적 기능만을 제공하는 것은 추후 재공격의 여지를 남겨두기 때문이다.

본 논문에서는 기존의 마킹기반 IP 역추적기법에서 사용되던 16비트 인식 필드(identification field)의 범위를 확장해 29비트까지 IP 헤더를 사용함에 따라 여러 패킷에 정보를 나누어야 했던 비효율성을 크게 개선하였다.

기존의 에지 샘플링 방법은 start 필드와 end 필드 두 개의 에지 정보와 distance 필드를 마킹해서 8개의 패킷 헤더에 기록을 해서 보내는 반면, 제안된 기법은 해쉬 함수를 사용하여 32 bits의 라우터 주소를 8 bits로 변경하여 헤더

에 3개의 라우터 정보를 마킹하는 방법을 사용하였다. 이렇게 하나의 패킷이 많은 라우터 경로정보를 가지고 있게 되면 공격 경로를 재구성할 때 보다 적은 수의 패킷으로도 완벽한 경로 재구성이 가능하게 된다. 본 논문에서 제안하는 메커니즘은 능동 네트워크를 기반으로 하고 있는 경량 IP 역추적 기법이다. 따라서 IDS와 연동하여 네트워크에서 전송되는 패킷의 헤더에 에지 정보를 마킹하고 공격 역추적 과정에서 공격패킷 필터링 기능을 라우터에게 능동적으로 실행한다면 공격을 차단하는데 더욱 효과적이라고 할 수 있다. 능동적인 대응은 일반적인 네트워크 환경에서는 복잡하고 상당한 시간이 소요되나 능동 네트워크 환경에서는 적극적이고 신속한 대응이 가능하므로 제안된 메커니즘이 더욱 효율적으로 사용될 수 있을 것이다. 향후 과제로는 제안된 메커니즘을 더욱 다양한 관점에서 시스템적 분석을 시행하여 개선되어야 할 부분을 찾아내고 이를 반영하는 것이다. 또한 기존의 IP 역추적 기법들과의 다양한 성능평가를 통해 성능을 분석하는 것이다.

참 고 문 헌

[1] Belenky A. and Ansari N., "On IP Traceback," IEEE Communications Magazine, Volume 41, Issue 7, July, 2003.

[2] Belenky A. and Ansari N., "IP traceback with deterministic packet marking," Communications Letters, IEEE, Volume 7, Issue4, pp.162-164, April, 2003.

[3] S. Savage et al., "Network Support for IP Traceback," IEEE/ACM Trans. Net., Vol.9, No.3, pp.226-237, June, 2001.

[4] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," Proc. INFOCOM2001, Vol.2, pp.878-886, 2001.

[5] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson, "Practical network support for ip traceback," in Proceedings of the 2000 ACM SIGCOMM Conference, August, 2000.

[6] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," Tech. Rep. CSD-00-013, Department of Computer Sciences, Purdue University, June, 2000.

[7] Kadobayashi Y., Yamaguchi S., "An implementation of a hierarchical IP traceback architecture," Applications and the Internet Workshops, Proceedings 2003 Symposium, pp.250-253, Jan., 2003.

[8] Minho Sung, Jun Xu, "IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks," Parallel and Distributed Systems, IEEE Transactions on, Volume 14 , Issue 9, pp. 861-872, Sept. 2003.

[9] Aljifri, H., "IP traceback: a new denial -of-service deterrent," IEEE Security & Privacy Magazine, Volume 1, Issue 3, pp.24-31, June, 2003.

[10] Belenky A., Ansari N., "Accommodating fragmentation in deterministic packet marking for IP traceback," IEEE Global Telecommunications Conference 2003, Volume 3, pp. 1374-1378, Dec., 2003.

[11] Belenky A., Ansari N., "Tracing multiple attackers with deterministic packet marking (DPM)," IEEE Communications, Computers and signal Processing 2003, Volume 1, pp.49-52, Aug., 2003.

[12] Baba T., Matsuda S., "Tracing network attacks to their sources," IEEE Internet Computing, Volume 6 , Issue 2, pp.20-26, April, 2002.

[13] Bao Tung Wang, Schulzrinne H., "An IP traceback mechanism for reflective DoS attacks," Electrical and Computer Engineering 2004, Volume 2, pp.901-904, May, 2004.

[14] Tsern Huei Lee, Wei-Kai Wu, Tze-Yau William Huang, "Scalable packet digesting schemes for IP traceback," 2004 IEEE International Conference, Vol.2, pp.1008-1013, June, 2004.

[15] Ion Stoica, Hui Zhang, "Providing Guaranteed Services Without Per Flow Management," ACM SIGCOMM Computer Communication Review archive, vol.29, Issue 4, pp.81-94, Oct., 1999.

[16] 김병룡, 김수덕, 김유성, 김기창, "마킹 알고리듬 기반 IP 역추적에서의 공격 근원지 발견 기법," 정보보호학회 논문지, 13권 1호, 2003년 2월.

[17] NLANR. Network Traffic Packet Header Traces. URL: http://moat.nlanr.net

허 준

e-mail : heojoon@khu.ac.kr

2002년 경희대학교 컴퓨터공학과(학사)

2004년 경희대학교 컴퓨터공학과 (공학석사)

2004년2월~현재 경희대학교 컴퓨터공학과 박사과정

관심분야 : 유무선 네트워크 보안, 보안 게이트웨이, 암호기술, Power Line Communication Security

홍 충 선

e-mail : cshong@khu.ac.kr
1983년 경희대학교 전자공학과(학사)
1985년 경희대학교 전자공학과(공학석사)
1997년 Keio University, Department of Information and Computer Science(공학박사)
1988년~1999년 한국통신 통신망 연구소 수석 연구원/네트워킹연구실장
1999년~현재 경희대학교 전자정보학부 부교수
관심분야 : 인터넷 서비스 및 망 관리 구조, 분산 컴포넌트 관리, IP 프로토콜, Sensor Networks, Network Security

이 호 재

e-mail : blitzguy@plantynet.com
2003년 호서대학교 전자공학과(학사)
2005년 경희대학교 컴퓨터공학과 (공학석사)
2005년~현재 (주)플랜티넷 솔루션 개발팀 전임연구원
관심분야 : 네트워크 프로그래밍, 네트워크 보안