TTL 기반 패킷 마킹 방식을 적용한 IP 패킷 역추적 기법☆

Advanced TTL based Packet Marking Mechanism for IP Traceback.

이 형 우*
Hyung-Woo Lee

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 PPM 기반 역추적 기법인 경우 패킷 내에 라우터 라우터 정보 또는 라우터 에지 경로 정보를 마킹하는 방식을 사용하였지만 효율적인 경로 역추적 기능을 제공하지 못하기 때문에 DDoS 공격에 능동적으로 대응하지 못하고 있다. 이에 본 연구에서는 DDoS 공격 패킷에 대해 TTL 기반의 개선된 패킷 마킹 기법을 제시하여 스푸핑된 IP 패킷의 근원지 정보를 재구성할 수 있음을 보였으며, 실험 결과 네트워크 부하를 줄이면서도 역추적 성능을 향상시킬 수 있었다.

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 PPM based tracing scheme(such as router node appending, sampling and edge sampling) insert traceback information in IP packet header for IP Traceback. But, these schemes did not provide enhanced performance in DDoS attack. In this paper, we propose a "TTL based advanced Packet Marking" mechanism for IP Traceback. 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.

⌐ Keyword : Packet Marking, DDoS attack, IP Traceback, Network Security

1. 서 론

서비스 거부 공격(Dos: Denial of service)[2]을 통해 손쉽게 TCP/IP 프로토콜의 취약점을 이용한 공격이 가능하기 때문에 해킹 공격에 대응할 수 있는 방안에 대해 연구가 필요하다. 현재의 대응 기술을 살펴보면 방화벽(firewall) 시스템은 접근 제어 기술을 적용한 것으로 해킹 공격에 수동적인 특징을 보이고 있으며, 침입탐지 시스템(IDS: Intrusion Detection System)을 통한 대응 기술 역시 피해 시스템에 도착한 이상 트래픽에 대한 검출 및 차단 기능만을 제공하는 수동적 해킹 대응 기술이다. 따라서 이는 DoS 해킹 공격 근원지에 대한 확인, 추적 등과 같이 능동적인 측면에서의 해킹 대응 기능을 제공하고 있지 못하고 있다. 특히 대부분의 해킹 공격이 근원지 IP 주소를 스푸핑(IP Spoofing)하는 방식으로 수행되므로 이에 대한 능동적 대응 기술이 개발되어야 한다. tracert 기술을 이용하여 근원지 주소를 판별하는 과정을 적용한다 할지라도 분산 서비스 거부 공격(DDoS: Distributed Denial of service) 패킷 내에 포함되어

* 종신회원 : 한신대학교 소프트웨어학과 조교수
hwlee@hs.ac.kr(제1저자)
[2003/12/03 투고 - 2004/01/03 심사 - 2004/10/04 심사 완료]
☆ 본 연구는 한신대학교 교내특별연구비 지원으로 수행된 연구결과입니다.

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.

본 연구에서는 DDoS 공격에 대한 판단 기능을 기반으로 역추적 기능과 접목하여 스푸핑된 DDoS 패킷에 대한 IP 근원지를 역추적하는 기술을 제안하고자 한다. 라우터에서 트래픽에 대한 판별/제어 기능이 수행된다면 DDoS 공격이 발생하였을 경우 라우터는 역추적 정보를 해당 패킷의 헤더에 마킹하여 전달할 수 있다. 이를 위해 본 연구에서는 기존의 PPM 기법의 단점을 보완하기 위해 TTL 필드 정보를 이용하여 라우터에 대한 에지 정보를 마킹하는 새로운 기법을 제시하였다. 제시된 기법은 기존의 역추적 기법보다 관리시스템 부하, 네트워크 부하 및 역추적 기능 등을 향상시킬 수 있었다.

2절에서는 관련연구로 기존 DDoS 공격에 대한 대응 방안과 패킷 마킹 기반의 대응 기술을 고찰하고, 3절에서는 역추적 기술에 대한 분류를 기반으로 기존 PPM 기반 패킷 마킹 기법에서의 문제점 등을 고찰하였다. 4절에서는 DDoS 공격 근원지를 역추적하기 위해 TTL 기반의 새로운 패킷 마킹 기법을 제시하였으며 5절에서는 제시한 기법에 대한 성능을 비교 평가하였다.

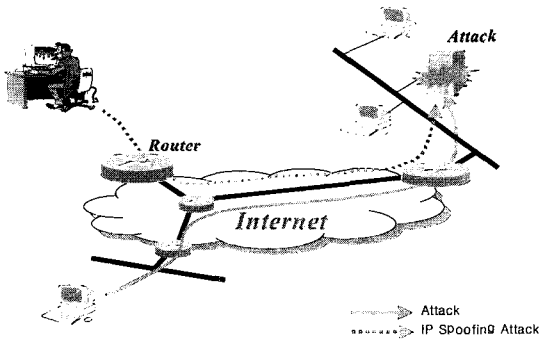
2. 관련 연구

2.1. 기존의 DDoS 공격 대응

기존의 DDoS 공격 대응 기술은 해킹 피해 시스템에서의 로그 분석을 통해 공격 시스템을 파악하고 로그 분석 과정을 반복적으로 적용하여 해킹 경로를 추적하는 수동적인 방식이다. 이는 DDoS 공격에 대한 실시간 추적이 불가능하고 DDoS 트래픽에 대한 능동적인 대응이 어렵기 때문에 결국에는 전체 네크워크가 손쉽게 마비될 수 있는 위험성을 갖고 있다.

또한 기존의 기법은 추적 경로상에 있는 일부 시스템에서의 로그 정보 등이 삭제된다면 전체적인 로그 분석 자체가 불가능하게 되며 특히 스푸핑된 IP 패킷에 대해 실제 전송 경로를 효율적으로 역추적하기에 어려움이 있다.

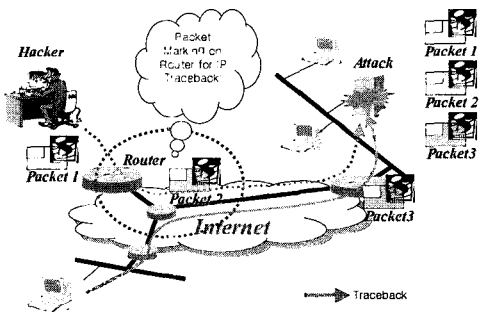
아래 [그림 1]과 같이 해커가 IP 스푸핑 방식을 통해 공격하였을 경우 역추적 경로를 찾아 해커의 위치 또는 접속 경로 등을 파악하기 위해서는 역추적 경로를 효율적으로 찾을 수 있는 기법이 제시되어야 하며, 기존 라우터에 대한 별다른 수정/변경 없이 DDoS 공격에 능동적으로 대응할 수 있는 기술이 제시되어야 한다.



〈그림 1〉 IP 스푸핑 기법을 통한 공격 형태

2.2. 패킷 마킹 기반 DDoS 대응

인터넷에서의 DDoS 공격에 대응하기 위해서는 아래 [그림 2]에서와 같이 네트워크를 구성하는 각각의 라우터에서 IP 스푸핑된 패킷에 대해 일정한 확률 P로 패킷을 선택하여 라우터 자신의 ID 정보와 IP주소 정보를 패킷 헤더에 마킹하는 방식을 사용하고 있다. 피해 시스템에서는 마킹된 정보가 도착하면 패킷에 기록되어 있는 라우터 관련 마킹 정보를 추출하여 스푸핑된 패킷의 실제적인 공격 경로를 재구성하는 방식을 사용하고 있다.



〈그림 2〉 공격 근원지 역추적을 위한 패킷 마킹 기술

패킷 전달 과정에서 각각의 라우터는 IP 계층에 해당하는 패킷 헤더 정보에서 라우터가 수정 가능한 부분을 선택하여 라우터 자신의 IP 주소 정보를 마킹하게 된다. 현재까지 제시된 기법에서는 일반적으로 IP 헤더 구조에서 ID 필드에 해당하는 16비트 필드 정보에 라우터 자신의 IP 주소 정보를 마킹하는 방식을 사용하고 있다.

3. IP 역추적 기술

3.1. 역추적 기술 분류

역추적 기술을 시스템 측면에서 분류하면 크게 IP 패킷 역추적 기술과 연결 역추적 기술로 분류할 수 있다. IP 패킷 역추적 시스템인 경우 DoS 공격에서 IP 주소가 변경된 경우 이를 찾아내기 위한 방법을 제공한다. Host B에 패킷을 보낸 시스템의 실제 위치를 추적하는 방식으로 패킷에 대한 마킹 기법(Marking)을 적용한다.

역추적 기술을 다시 세분화하면 호스트 기반 역추적, 네트워크 기반 역추적으로 구분할 수 있다. 호스트 기반 역추적 시스템(Host-based traceback system)은 모든 호스트에 역추적 모듈을 설치하는 방식이다. 따라서 모든 역추적 경로상의 호스트들로부터 정보를 얻어야 역추적이 가능한 기법이다. 기존의 모든 시스템에 역추적 모듈을 설치한다는 것이 상당히 어렵기 때문에 현재의 라우터에 환경에 많은 부분 수정을 가해야 한다는 단점이 있다.

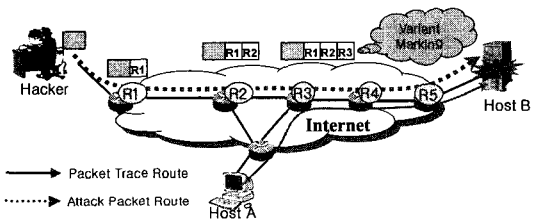
네트워크 기반 역추적 시스템(Network-based traceback system)은 네트워크 상에 송수신되는 패킷들로부터 정보를 추출하여 존재하는 연결 정보들 간의 연관성을 파악하여 역추적 경로를 파악하는 방식이다. 예를들어 해커가 ls 및 cd라는 명령어를 계속적으로 입력하였을 경우 이와 같은 명령어가 흘러가는 경로를 분석하여 전체적인 해킹 및 바이러스 경로를 분석하는 방식이다. 역추적 기법 등 중에서 기존의 패킷 마킹 기반 역추적 기법은 다음과 같다.

3.2. 기존의 확률적 패킷 마킹 기반 역추적 기법

확률적 마킹 기법(PPM: Probabilistic Packet

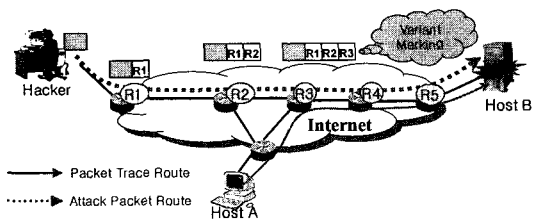
Marking)은 라우터에서 패킷에 대해 확률 p로 샘플링 과정을 수행하고 패킷 헤더에 라우터 자신의 IP 주소 정보를 마킹하여 전송한다. 라우터에 대한 IP 주소를 마킹하는 방식에 따라서 NA (Node Appending), NS(Node Sampling) 및 ES (Edge Sampling) 기법 등이 제시되고 있다.

NA(Node Appending) 방식에서는 [그림 3]과 같이 가변적인 필드에 라우터 자신의 IP 주소 정보만을 추가하는 방식이다. 이는 간단하다는 장점이 있으나, IP 헤더 구조에서 가변적인 필드에 라우터 경로 정보를 마킹하는 과정을 수행하기 때문에 결국에는 패킷의 크기가 홉 거리에 따라서 유동적으로 변화하기 때문에 실제적으로 구현하기에는 문제점이 많은 기법에 해당한다.



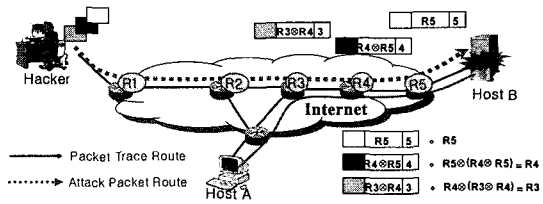
〈그림 3〉 NA(Node Appending) 기법

[그림 4]와 같은 NS(Node Sampling) 기법은 고정된 헤더 필드에 각각의 라우터에서 일정한 확률로 자신의 ID 정보를 마킹하여 전달하는 방식이다. 이는 간단히 구현할 수 있다는 장점은 있으나, 라우터에 의해 반복적으로 마킹되어 전달될 경우 삭제될 수 있으며, 전체적인 경로를 재구성하는데 있어서 많은 패킷에 대해 마킹 과정을 수행해야 전체 경로를 재구성할 수 있다는 단점이 존재한다.



〈그림 4〉 NS(Node Sampling) 기법

위 두 가지 기법을 보완하기 위해 제시된 ES (Edge Sampling) 기법은 아래 [그림 5]와 같이 고정된 헤더 필드에 라우터간의 에지 정보를 XOR 과정을 수행하여 마킹하는 방식이다. 이 방식은 최종적으로 피해 시스템에서 수집된 정보에 대해 역으로 공격 경로를 재구성하게 되어 IP 스푸핑된 공격 근원지를 역추적할 수 있다는 장점이 있다. 그러나, DDoS 공격과 같은 분산 서비스 거부 공격과 같은 대단위 공격에 대해서는 근원지를 역추적하는데 있어서 효율적이지 못하다는 단점이 있다.



〈그림 5〉 ES(Edge Sampling) 기법

2.3. 기존 패킷 마킹 기반 역추적 기술의 문제점

일반적으로 패킷 마킹 기법은 기존의 다른 IP 역추적 기법과 달리 관리 부하가 적으며, 네트워크에 대한 부하 및 분산 처리 기능이 우수하다고 할 수 있다. 그러나 확률 p로 샘플링하여 마킹하는 과정에서 상대적으로 많은 패킷을 샘플링해야 하고 경로 재구성 과정에서도 완전한 경로를 재구성할 수 없다는 단점이 있기 때문에 라우터에서의 부하가 크며 보안 기능도 취약하다.

기존의 기술은 네트워크 패킷 중심에서 각 트렌젝션간의 연계성을 이용한 연결 중심 방식의 네트워크 기반 역추적 기술이다. 그러나, 해킹 및 바이러스에 대처하기 위해 지금까지 제시된 방식에서는 현재의 인터넷 네트워크 구조를 전체적으로 변경하고 새롭게 개선된 환경을 구축한 다음에 적용 가능하다는 단점을 갖고 있다. 따라서, 본 연구에서는 기존의 환경적 변화를 최소화하면서도 능동적인 역추적이 가능하도록 하기 위해

새로운 접근 방식을 제시하고자 한다.

기존의 패킷 마킹 기법은 패킷을 확률 p로 샘플링하여 마킹 후에 전송하는 과정에서 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 있다. 물론 트랜젝션에 대한 연결 중심 방식으로도 접근할 수 있으나, 이 경우 마찬가지로 역추적 경로 재구성 과정에서 중간에 트랜젝션에 대한 정보를 상실할 경우 공격 근원지를 찾을 수 없다는 단점이 있다.

또한 기존의 PPM 기법인 경우 패킷에 대해 일정 확률 p를 만족할 경우 샘플링하여 전송하는 기법을 사용하는 과정에서 DDoS 공격 트래픽에 대해서 마킹하지 않고 보내는 경우도 발생한다. 이 경우 DDoS와 같은 해킹 공격이 발생하였을 경우 스푸핑된 공격 근원지를 재구성할 수 없다는 단점이 있다.

4. TTL 기반 DDoS 패킷 마킹 기법

4.1. 패킷 마킹을 위한 네트워크 구조

네트워크는 노드 집합 V와 에지 집합 E로 구성된 그래프 $G=(V,E)$로 정의할 수 있다. 다시 네트워크 노드 집합 V는 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 $t \in V/G$를 피해 시스템이라고 정의한다.

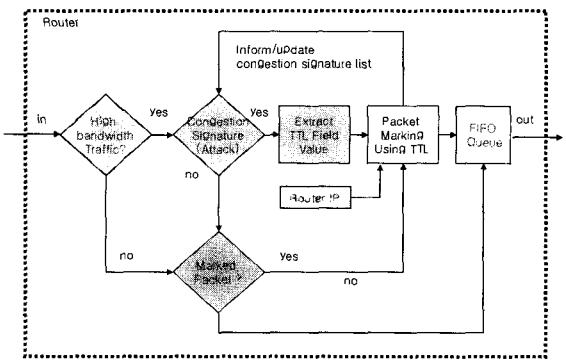
만일 $|S|=1$일 경우 단일 공격자에 의한 해킹 공격을 의미하고 공격 경로 정보 $P=(s,v_1,v_2,\ldots,v_d,t)$인 경우 공격 시스템 s에서 피해 시스템 t로 d개의 라우터를 통해 전달된 공격 경로를 의미한다. 이때 전달된 패킷의 수를 N이라고 하자. 만일 패킷내에 라우터에 대한 링크 정보 $(v,v') \in E$를 마킹할 수 있는 필드가 있다면 이를 확률 p로 샘플링하여 전달하게 된다. 패킷에 대해서 라우터에서는 일정한 확률로 패킷을 선택하여 에지에 대한 정보와 라우터에 대한 거리 정보를 패킷내에 포함시켜 전달할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

기존의 기법에서는 임의의 확률 p로 패킷을 선택하여 여기에 라우터에 대한 링크 정보를 마킹하여 전달하게 된다. 만일 네트워크 상에서 노드 v_i에서 마킹하였을 경우 다른 라우터에 의해서는 재마킹되지 않고 전달될 확률 α_i을 계산하면 다음과 같다.

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

따라서 확률 α_i는 공격자에 해당하는 패킷 정보가 다른 라우터에 의해서는 재마킹되지 않고 피해 시스템에 전달될 확률을 의미한다. 결국 피해 시스템에서 α_i값을 높이기 위해서는 p값을 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 p로 패킷을 샘플링하여 마킹하지 않고 이상 트래픽이 발견되었을 경우 패킷에 대한 마킹 과정을 수행하게 된다. 본 연구에서 제안한 구조는 아래 [그림 6]과 같다.



〈그림 6〉 제안한 라우터 기반 DDoS 근원지 역추적 구조

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 전단계 라우터에게 전송토록 한다. 만일 대역폭 조건을 만족하지 않을 경우에는 이전에 트래픽에서 유사한 패킷이 있었는지를 확인하고 만일 해당된다면 마찬가지로 패킷에 대한 마킹 과정을 수행한다. 위 조건을 만족하지 않을 경우 일반적인 트래픽으로 간주하여 다음 라우터로 전달한다. 본 연구에서 제시한 구조는 기존의 ACC 기반의 Pushback 기법에서 제공하지 못하는 IP Traceback/Marking 구조를 개선한 것으로 특정 형태(signature)의 패킷이 일정 트래픽 이상의 폭주 형태로 도착하였을 경우 해당 패킷에서의 TTL 값을 추출하고 [그림 8]에서와 같은 패킷 마킹 과정을 수행하여 전송하는 과정을 수행한다.

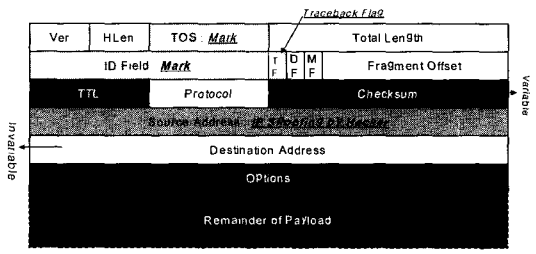
4.2. TTL 필드 정보를 이용한 패킷 마킹 기법

4.2.1 패킷 헤더 마킹 필드 M_x

라우터 R_x의 IP 주소를 A_x라고 하자. 아래 [그림 7]과 같이 R_x에 도착한 IP 패킷을 P_x라고 할 때, P_x에서의 해더에서 마킹 정보를 저장할 수 있는 25 비트를 M_x라고 하자.

- 라우터 : R_x - 라우터의 IP 주소 : A_x
- 라우터 R_x에 도착한 패킷 : P_x
- 패킷에서의 변형 가능한 헤더 25 비트 : M_x

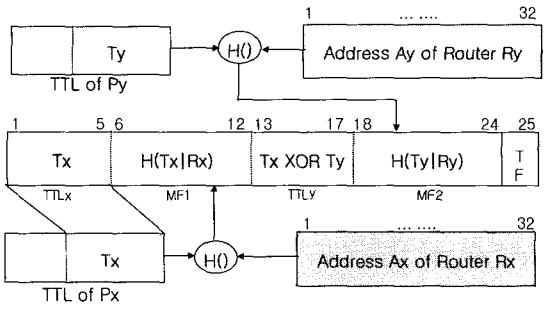
패킷 P_x에서 M_x는 아래 [그림 7]과 같이 TOS (type of service) 필드 8비트와 ID 필드 16비트 및 Fragmentation 필드에서 사용하지 않는 1비트로 구성된다. TOS 필드인 경우 현재 필드에 대한 정의만 되어 있을 뿐 실제적으로 사용하고 있지 않다. 따라서 TOS 필드 값을 사용한다고 하더라도 전체 네트워크에 영향을 미치지 않는다. 현재의 TOS 필드는 상위 3비트가 우선순위 비트로 설정되어 있고, 다음 3비트는 최소지연, 최대성능 및 신뢰성 필드로 정의되어 있으나 현재는 사용하고 있지 않다.



〈그림 7〉 제안한 기법에서의 패킷 마킹 필드

4.2.2 TTL 정보를 이용한 마킹

25비트 M_x 정보에 대해서 라우터 R_x에 대한 IP 주소 A_x 값을 패킷 헤더에 마킹하는 구조는 아래 [그림 8]과 같다.



〈그림 8〉 제안한 기법에서의 패킷 마킹 구조

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. 물론 시스템에 따라서는 127로 설정되는 경우도 있고 64 또는 32로 설정되는 경우

도 있다.

임의의 라우터 R_x에 도착한 패킷 P_x의 TTL 필드에 설정되어 있는 값을 $TTL of\ P_x$라고 하였을 경우, 이 값은 근원지 호스트에서 라우터 R_x까지의 전송 거리(hop count)에 해당하는 정보를 포함하고 있다. 그리고 만일 패킷 P_x가 피해 시스템 V에 도착하였을 경우 TTL 값의 변화는 라우터에서 피해 시스템까지의 전송 거리를 의미한다. 따라서 패킷에서의 TTL 필드 값을 이용한다면 패킷에 전달된 라우터 경로 정보와 연계하여 역추적 방식에 활용할 수 있다.

현재 TTL 값은 네트워크 상에 패킷 전송시 대역폭을 확보하고 목적지에 도착하지 않는 패킷을 제어하기 위한 목적으로 사용된다. 기존의 패킷 마킹 기법에서는 TTL 값을 사용하지 않고 다만 ID 16 비트 필드 내에 별도의 hop 카운터 필드를 두어 마킹을 수행한 라우터에서 패킷이 전달된 거리 정보를 계산하도록 하였다. 기존의 기법에서는 패킷의 16비트 ID 필드 내에 5 비트 hop 카운트 필드를 설정하여 마킹 과정에서 1로 설정하여 패킷을 전달하고 다음 라우터에서는 이 값을 1씩 증가시키는 방식을 사용하였다. 그러나 이와 같은 경우 패킷이 전달되는 경로상에 있는 모든 라우터가 ID 필드내에 있는 5비트 필드 값을 반드시 1씩 증가시켜주어야 경로 계산이 정확해진다는 단점이 발생한다. 따라서 본 연구에서는 라우터 R_x에 도착한 패킷 자체에서의 TTL의 특성을 이용하여 마킹 구조에 적용하였다.

4.2.3. TTL 기반 패킷 마킹 방식

이상 트래픽이 발생하게 되면 라우터 R_x에서 패킷 P_x에 대해 마킹 과정을 수행하는 과정을 살펴보면, 위 [그림 8]과 같이 우선 이상 트래픽 패킷에 대해 라우터에서 마킹이 가능한 25 비트 필드에 정보를 삽입하여야 한다. 이때 25 비트 필드에는 패킷이 전달된 경로 정보를 모두 포함하고 있어야 하기 때문에 라우터 R_x 자신의 32 비트 IP 주소 A_x와 다음 단계 라우터 R_y의 32 비트 IP 주소 A_y에 해당하는 64 비트 정보를 패킷 내에 마킹하여야 한다.

25 비트 내에 두 개의 라우터 주소 값을 동시에 마킹하기 위해서는 해쉬 함수를 적용할 필요가 있고, 해쉬 함수를 이용하게 되면 라우터 주소 정보에 대한 무결성 검증 기능도 제공하면서 해당 패킷에 대한 전송 경로를 25 비트 내에 마킹할 수 있게 된다. 이를 위해 본 연구에서는 각각의 라우터 IP 주소 32 비트 정보에 대해 7 비트 해쉬 함수를 적용하여 생성된 값을 패킷에 마킹하는 방식을 사용하였다.

라우터 R_x에 도착한 패킷 P_x가 이상 트래픽에 해당된다면 아래와 같은 과정을 수행한다.

〔단계 1〕 TTL 필드에서 하위 5비트 정보를 추출하여 P_x^{TTLx}에 저장

패킷이 전달되는 과정에서 일반적으로 네트워크 홉 최대 거리는 일반적으로 32 홉 이상을 넘지 않기 때문에 라우터 R_x에 도착한 패킷 P_x에 대해 IP 패킷의 TTL 필드 8비트에서 의 TTL 필드 하위 5 비트 정보만으로도 패킷이 전달된 홉 거리 정보를 계산할 수 있다. 즉, 패킷 P_x에서 TTL 필드에서 하위 5비트 정보에 추출하여 이를 T_x라고 하고 [그림 8]에서의 TOS 필드에서의 상위 5비트 필드 P_x^{TTLx}에 저장한다.

$$T_x = TTL of P_x \wedge 00011111, \quad P_x^{TTLx} = T_x \quad (2)$$

T_x 값은 공격 근원지 시스템으로부터 패킷이 라우터까지 전달된 홉 거리 정보를 의미한다. 또한 T_x 값을 패킷에 마킹하여 목적지 피해 시스템 V에 전송하였을 경우, V에 도착한 패킷에서의 TTL 값과 마킹되어 전달된 T_x 값을 비교한다면 패킷이 라우터 R_x로부터 피해 시스템까지 전달

된 홉 거리 정보를 계산할 수 있다.

〔단계 2〕 $H(T_x|A_x)$ 값을 생성하여 P_x^{MF1}에 마킹하고 P_x^{TF}를 1로 설정

패킷 P_x에서의 5 비트 TTL 값 T_x과 라우터 R_x 자신의 IP 주소 A_x에 대해 해쉬 함수 $H(\cdot)$를 사용하여 7 비트 해쉬 값 $H(T_x|A_x)$를 계산하고 이를 [그림 8]에서의 P_x^{MF1}에 마킹한다. 그리고 동시에 역추적 마킹 필드 P_x^{TF} 값을 1로 설정하여 패킷 전송 경로상의 다음 라우터 R_y로 전송한다.

$$P_x^{MF1} = H(T_x|A_x), P_x^{TF} = 1 \quad (3)$$

〔단계 3〕 라우터 R_y에서 T_y를 생성하여 P_y^{TTLy}에 마킹

패킷이 전송되는 경로상에 있는 임의의 라우터 R_y는 이상 트래픽에 해당하는 패킷에 대해 우선 P_x^{TF} 필드 값을 보고 만일 1로 설정되어 있는 경우 다음과 같은 검증 과정을 수행한다. 라우터 R_y에 도착한 패킷을 P_y라고 하자. P_y에서의 8비트 TTL 필드에서 5비트 정보를 T_y를 추출할 수 있다. 이때 T_y 값과 패킷에서의 $TTLx$ 필드에 저장된 T_x 값에 대해 $T_x XOR T_y$를 수행하여 이 값을 P_y^{TTLy}에 마킹한다.

$$T_y = TTL of P_y \wedge 00011111,\ P_y^{TTLy} = T_x - T_y \quad (4)$$

이때 P_y^{TTLy} 값은 라우터 R_x와 라우터 R_y간의 홉 거리를 의미한다.

〔단계 4〕 $H(T_y|A_y)$ 값을 생성하여 P_y^{MF2}에 마킹하여 전송

이제는 라우터 R_y에 도착한 패킷 P_y에서의 TTL 필드 5비트 정보 T_y와 자신의 IP 주소 A_y에 대해 해쉬 함수 $H(\ )$를 적용하여 이를 P_y^{MF2} 필드에 마킹한다. 마킹된 패킷은 이제 최종 목적지 V로 전송된다.

$$P_y^{MF2} = H(T_y|A_y) \quad (5)$$

이와 같이 마킹 과정은 DDoS 공격이라고 판단되는 패킷에 대해 확률 p로 샘플링하여 최종 피해시스템으로 전송하게 된다. 물론 마킹 과정은 ACC 모듈에 의해 공격 패킷을 탐지한 각 라우터에서 TF 필드 값을 조사하여 해당 패킷에 대해서만 마킹을 수행하게 된다.

4.2.4. 역추적 경로 재구성

(1) DDoS 공격 패킷 역추적

네트워크를 통해 전달된 패킷에 대해 피해 시스템 V에서는 DDoS 공격 경로를 재구성하게 된다. 아래 그림과 같이 DDoS 공격을 S_1, S_2, S_3에서 수행하였다고 가정하자. 공격 패킷에 대해 라우터 R_x, R_y 및 R_z는 패킷 헤더 25 비트 정보내에 라우터 자신의 IP 정보와 패킷에서의 TTL 필드 5비트 정보를 조합하여 각각 마킹하였다. 피해시스템에서는 DDoS 공격이 발생하였을 경우 도착한 패킷에 대해 아래와 같이 경로 역추적 과정을 수행한다.

우선 피해 시스템 V에 도착한 패킷을 P_v 라고 정의하자. P_v 값은 DDoS 공격에 해당하는 패킷들로 구성된 집합이고, 이 중에서 라우터에 의해 마킹되어 전달된 패킷을 M_v라고 정의하자.

피해 시스템에 도착한 패킷 집합 P_v에서 M_v를 구별하는 방식은 다음과 같이 P_v에 속한 임의의 패킷 P_x에 대해서 TF 필드에 해당하는 P_x^{PF} 부분이 설정되어 있는 패킷을 샘플링하는 과정을 수행하면 된다.

$$M_v = P_x | P_x^{TF} \equiv 1, x \in v \quad (6)$$

피해 시스템에서 마킹되어 있는 패킷 M_v의 원소에 해당하는 임의의 패킷 M_i에 대해서 8비트 TTL 값을 $TTL of\ M_i$라고 할 때, 이를 M_i의 25비트 마킹 필드 T_M값과 비교한다면 패킷 M_i가 임의의 라우터 로 부터 마킹된 후에 전송R된 네트워크 홉 거리 $D(M_i)$를 다음과 같이 계산 할 수 있다.

$$D(M_i) = M_i^{TTLi} - (TTL of\ M_i \wedge 00011111) \quad (7)$$

만일 $D(M_i) \equiv 1$이라면 피해 시스템 바로 앞에 있는 라우터에 의해서 마킹되었다는 것을 알 수 있다. $D(M_i)$는 피해 시스템에 도착한 패킷 중에서 임의의 라우터에 의해 마킹된 정보를 포함하고 있기 때문에 이를 기반으로 아래와 같은 사항을 도출할 수 있다.

[정리] 피해 시스템 V에 도착한 패킷 M_i에서 $d \equiv M_x^{TTLx} - TTL of M_i$이라면, 이는 패킷 M_i이 피해 시스템 V로부터 홉 거리 d에 위치한 임의의 라우터 R_x에 의해 마킹되었다.

(2) TTL 기반 DDoS 공격 경로 재구성

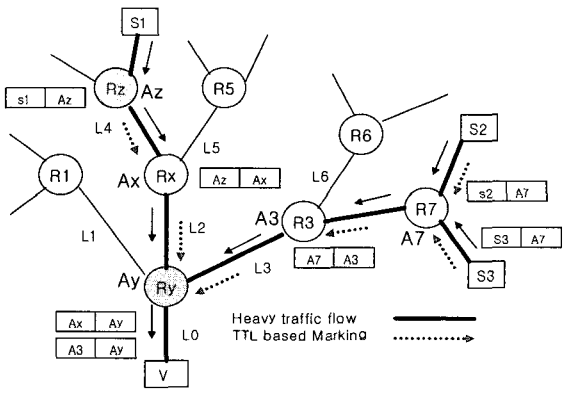
예를들어 $D(M_i)$==을 만족하는 패킷 M_i가 있다면, 이 패킷은 피해 시스템 바로 앞단에 연결되어 있는 두 홉 거리 내에 있는 라우터 R_y 및 R_x에 의해서 마킹된 패킷이라는 것을 의미한다. 즉, 패킷 M_i는 피해 시스템과 바로 연결되어 있는 라우터 R_y와 2 홉 거리에 있는 임의의 라우터 R_x에 의해 마킹되었기 때문에 $D(M_i)$ 값은 2가 된다. 따라서 패킷 M_i에서 홉 거리 d에 있는 라우터 R_x를 다음과 같이 일반화 할 수 있다.

$$M_i^{MF1} \equiv H(M_x^{TTLx} | A_x), (R_x \in D(M_i) \equiv d) \text{ and}$$
$$M_i^{MF1} \equiv H((TTL of\ M_i \wedge 00011111) + d | A_x), \quad (8)$$
$$(R_x \in D(M_i) \equiv d)$$

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

아래 [그림 9]와 같은 네트워크 구조에 대해 본 연구에서 제시한 기법을 적용하게 되면 피해 시스템 V에 대한 DDoS 공격 경로 AP를 다음과 같이 구할 수 있다. 피해 시스템 V에서는 수신된 패킷에서 TF 필드 값이 설정되어 있는 패킷들을 분류한 별도로 분류한다. 그리고, 만일 DDoS 공격이 발생하였을 경우 TF 필드 값이 설정된 패킷들에 대해 앞에서 제시한 홉 거리 판별 및 경로 재구성 과정을 수행하게 된다.

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



〈그림 9〉 제안한 기법에서의 공격 경로 역추적

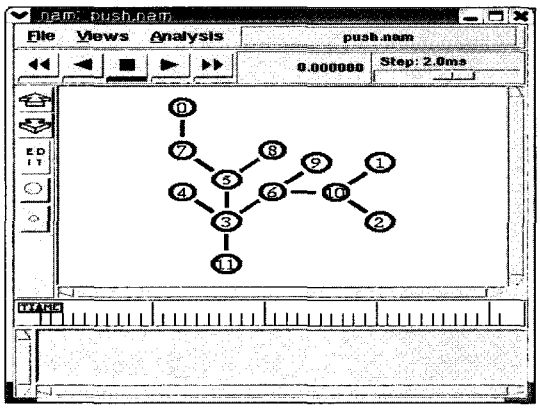
이와 같은 과정을 통해 라우터에서는 이상 트래픽이 발생하였을 경우 DDoS 해킹 경로를 역추적하기 위해서 개선된 패킷 마킹 기술을 적용하여 스푸핑된 패킷에 대한 역추적 기능도 제공하여 공격자에 대한 근원지를 재구성할 수 있다.

5. 제시한 기법의 성능 분석

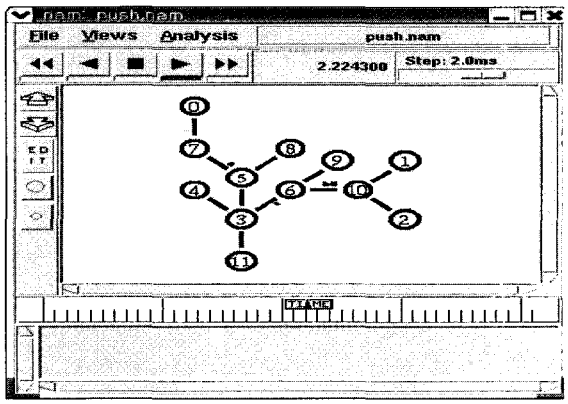
5.1. 실험결과

본 연구에서 제시한 기법에 대한 성능을 평가하기 위해서 Linux 환경에서 ns-2 시뮬레이터를 이용하여 성능을 분석하였다. 아래 [그림 10] 및 [그림 11]과 같은 네트워크를 구성하고 0 노드, 1번 및 2번 노드에서 DDoS 공격을 수행하도록 시뮬레이션 하였다.

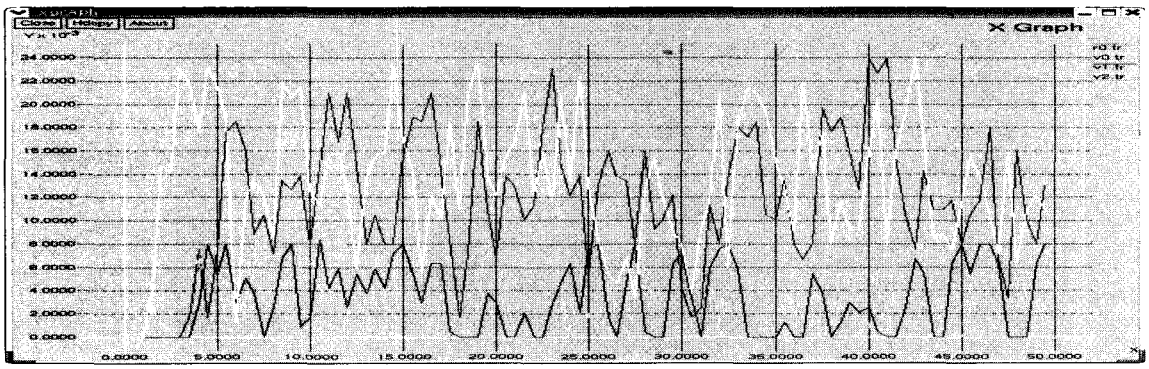
실험 결과 기존의 패킷 마킹 기법은 DDoS 공격에 대해 각 라우터에서 확률 p로 샘플링하여 마킹하는 방식이므로 전체 마킹된 패킷(파란선:v1.tr)의 수가 DDoS 트래픽(붉은선:r0.tr)에 비례하여 생성되는 것을 볼 수 있다. 본 연구에서 제시하는 기법인 경우 이상 트래픽에 대한 마킹 과정을 수행하기 때문에 기존의 PPM 기반 마킹 기법보다도 마킹된 패킷을 감소시킬 수 있다. 아래 [그림 12]는 기존 PPM 기법에서의 트래픽을 분석한 것이고, [그림 13]은 본 연구에서 제시한 기법의 트래픽을 보인다. NS-2 시스템을 통해 랜덤으로 10회 DDoS 트래픽 기반 공격 시뮬레이션을 수행하였다. 그 결과 본 연구에서 제시한 기법은 피해 시스템 V를 기준으로 기존 연구보다 마킹된 패킷이 25.3% 감소되는 것을 확인할 수 있었다. 물론 기존 PPM 기법 보다는 Pushback 모듈이 추가로 필요하다는 단점이 있으니, 전체적으로는 라우터의 성능이 부가적인 모듈의 추가를



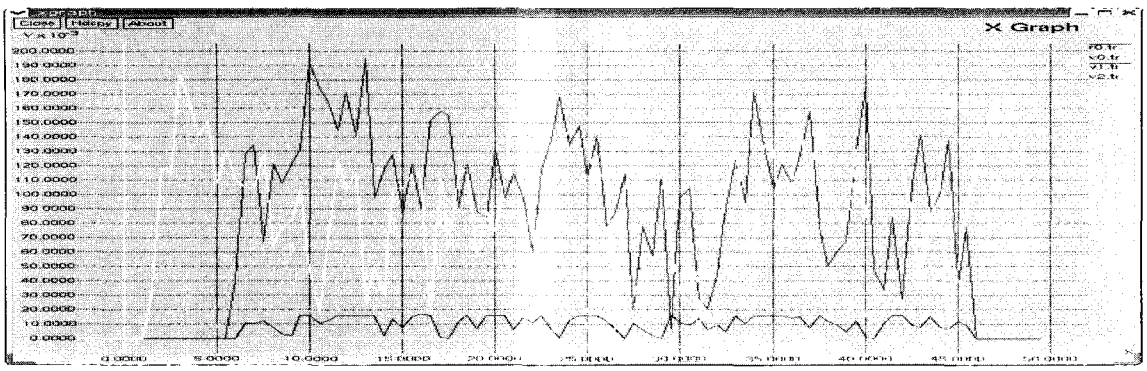
〈그림 10〉 ns-2 기반 실험환경 구축



〈그림 11〉 ns-2 기반 DDoS 시뮬레이션



〈그림 12〉 기존의 PPM 방식에서의 트래픽



〈그림 13〉 제안한 기법에서의 트래픽

허용한다고 가정하였을 경우 DDoS 공격 패킷에 대한 감소 기능을 제공하기 때문에 전체적으로 마킹된 패킷의 수도 감소되는 것을 알 수 있었다.

제안한 기법과 기존의 IP 역추적 관련 기술들의 성능을 비교 분석하면 아래 [표 1]과 같다. 라우터에서의 접근 제어 기능을 제공하는 필터링 기법은 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 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 부하

〈표 1〉 IP 역추적 기법 성능 비교 평가

특성 / 기법	관리 시스템 부하	라우터 부하	피해 시스템 부하	대역폭 부하	역추적 기능	적용 가능성	보안 기능	DDoS 대응	확장성	경로 재구성 패킷수
Ingress filtering	×	△	×	×	×	▽	×	×	△	×
Logging	↑	△	×	×	▽	▽	◇	▽	◇	1
PPM : NA	↓	◇	↑	×	▽	▽	▽	▽	×	n
PPM : NS	↓	◇	↑	×	◇	△	▽	▽	△	n
PPM : ES	↓	◇	↑	×	◇	△	◇	▽	△	n-1
iTrace	↓	◇	↑	↓	△	△	◇	△	△	n
제안한 TTL 기반 기법	↓	△	↑	×	△	△	△	△	△	n-1

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

가 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 p로 패킷을 선정하여 마킹 과정을 수행하였으나 본 연구에서 제시한 기법은 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 n개의 라우터를 거치는 경우 단지 n개의 역추적 메시지만으로 근원지 경로를 재구성할 수 있다는 장점을 제공한다.

6. 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. 패킷에서의 TTL 필드 정보가 갖고 있는 홉 거리 정보를 이용하여 라우터에서는 ID 필드 및 TOS 필드 정보에 마킹하여 피해 시스템에 전달하도록 하였으며 이를 통해 기존의 PPM 기법보다 개선된 역추적 성능을 제공할 수 있었다. 본 연구에서는 기존 역추적 기술의 구조와 문제점 등을 고찰하여 네트워크상에서 DDoS 해킹 공격에 대한 판단 기능에 기반하여 피해 시스템에서 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 모바일 네트워크 및 Ad-hoc 기반 네트워크 환경에서의 DDoS 공격에 대한 취약점이 발견되고 있다. 따라서 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. 마지막으로 기존의 방화벽 및 IDS가 담당하던 기능을 라우터가 포함하여 전체 네트워크의 안전성을 제공하면서도 패킷에 대해 개선된 역추적 기능을 제공하는 기법에 대해서도 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, 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.142-153, July, 2003.

◐ 저 자 소 개 ◑

이 형 우(Hyung-Woo Lee)

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