

# IPv6의 공격 근원지 역추적 모델 연구

이철수<sup>0</sup>, 임인빈, 최재호

전북대학교 컴퓨터공학과

{lcstop<sup>0</sup>, cnick, wave}@chonbuk.ac.kr

## Study on Attack Source Traceback Model of IPv6

Cheolssoo Lee<sup>0</sup>, Inbin Yim, Jaeho Choi

Dept. of Computer Engineering, Chonbuk National University.

### 요약

인터넷의 급성장으로 해킹이나 Dos 공격, 웜, 바이러스 등의 사이버 범죄가 크게 증가하고 지능화되어 최근 역추적에 대한 관심이 날로 증가하고 있다. 보안 도구로 침입탐지시스템(IDS)이나 침입방지시스템(IPS) 등이 있으나 해킹이나 DoS 공격을 방어하는데 현실적으로 한계가 있다. 따라서 능동적인 해킹 방어를 위한 기본적인 기술로 해커의 실제 위치를 추적하는 역추적 시스템 기술이 필요하다. 특히 IPv4에서의 역추적 시스템에 대한 연구는 활발하게 이루어지고 있지만 IPv6에 대한 연구는 아직 미흡하다. 본 논문에서는 IPv4의 주소 고갈로 인해 앞으로 이를 대신할 IPv6에 대한 공격 근원지 역추적 시스템 개발이 시급하다고 보고, 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적할 수 있도록 IPv6 헤더 패킷의 트래픽 클래스(Traffic Class)와 플로우 라벨(Flow Label)을 이용하여 IPv6에서의 실시간 네트워크 침입자 역추적 시스템 모델을 제안하고자 한다.

### 1. 서론

역추적 기술은 네트워크상에서 사이버 범죄를 시도하는 공격자의 실제 위치를 자동화된 기법을 이용하여 탐색 및 추적하여 해커의 위치를 찾기 위해서 필요하다. 특히 Dos(Denial of Service)공격은 공격자가 시스템의 리소스를 독점해 다른 정상 사용자들이 서비스를 사용할 수 없도록 만드는 것으로, 시스템의 정상적인 수행에 문제를 일으키는 모든 행위를 DoS라 할 수 있다. DDoS(Distributed Denial of Service)공격은 DoS의 또 다른 형태로, 인터넷에 연결된 일련의 시스템들을 이용해 단일 사이트에 대한 플러드 공격을 시도하는 것이다. 해커가 일단 취약한 인터넷 시스템에 대한 액세스에 성공하면 침입한 시스템에 소프트웨어를 설치하고 이를 실행시켜 원격에서 공격을 개시한다.

역추적 기술은 해킹 및 바이러스, 웜, DoS의 대응 방법으로 실시간으로 해커의 위치를 파악하는 것을 목적으로 하고 능동적이고 즉각적으로 대응하는 기술이다. 보안업체들은 각종 침해로부터 인터넷 시스템과 네트워크를 보호하기 위해서 각종 정보보안 강화 시스템을 개발하고 있다. 그러나 현재 보급 되어있는 시스템은 대부분 해킹이나 DoS 공격, 바이러스를 막는 것이 아니라 해커의 접근을 단지 어렵게 하는 수준에서 그치고 있다. 즉 수동적인 방어만을 수행한다. 또한 인터넷상에서 동작하는 보안 강화 시스템들과의 상호 협력적인 대응이 불가능하다. 이러한 이유로 상대적으로 우수한 보안 시스템 환경에서도 해킹이나 DoS의 공격은 여전히 증가하고 있다.

역추적 기술은 크게 2가지로 분류할 수 있는데 첫 번째는 IP 패킷 역추적 기술(Connection Traceback)이고, 두 번째는 실제 위치를 추적하기 위한 연결 역추적 기술(Connection Traceback)이다. 현재의 네트워크 실시간 시스템은 해킹 당한 컴퓨터에서 해커의 컴퓨터로 나가는 응답 패킷에 해커를 찾아 낼 수 있는 정보를 실어 보낸 뒤 이 정보를 가지고 이동경로를 추적하는 방식을 사용한다. 그러나 DoS, DDoS의 경우엔 해커에게 보내지는 응답 패킷이 없어 적용할 수 없다는 단점이 있다. 또한 실제 공

격자와의 거리가 멀면, 현실적으로 실제 시스템을 확인하거나, 수동적인 역추적 과정에서 역추적 로그 파일에 대한 정보를 얻을 수 없는 경우가 있다. IPv6에서는 이러한 IP 역추적과 연결 역추적 기술의 단점을 보완하기 위해 패킷워터마킹 기법을 사용할 수 있으며, 본 논문에서는 IPv6의 헤더 패킷에서 플로우 라벨(Flow Label)과 트래픽 클래스를 이용한 실시간 역추적 시스템 모델을 제안한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 기존 역추적의 기술에 대해, 3장에서는 워터 마킹 기법들을, 4장에서는 IPv6 Header에 대해, 5장에서는 IPv6 역추적 모델을 설계하고 마지막으로 결론 및 향후 계획에 대하여 기술할 것이다.

### 2. 기존 관련 연구

역추적 기술은 크게 두 가지로 분류 할 수 있는데, 첫 번째로 DoS/DDoS 관련 역추적기술은 IP 주소 스프핑 패킷의 실제 송신자 주소를 추적하는 방법(IP Packet Traceback)으로 이는 다시 순항적 추적(Proactive tracing)과 반응적 추적(Reactive Tracing)으로 구분된다. 또, 일반 해킹 관련 역추적 기술은 우회 공격 근원지를 추적하는 방법으로 TCP연결 역추적(Connection Traceback)이 있는데 크게 호스트 기반(Host-based)과 네트워크 기반(Network-Based)으로 나뉜다. 이는 징검다리(Stepping Stones) 형태의 공격에 적용되어 진다. 그 밖에 특정 웹이나 메일 등의 특정 어플리케이션에서 수행하는 어플리케이션 역추적 기술이 있다.

#### 2.1 TCP 연결 역추적

##### 2.1.1 호스트 기반 역추적

인터넷상에 설치된 모든 시스템에 역추적 모듈을 설치하여 설치된 역추적 모듈을 이용하여 접속을 요구하는 시스템을 인증

하거나 해당 시스템 내의 각종 로그 파일을 분석하여 역추적을 수행한다. 하지만 이 방법은 한 개의 시스템이라도 문제가 생겨 역추적 정보를 얻지 못하면 역추적이 불가능하다는 단점이 있고 현실적으로 인터넷 환경에서의 적용이 거의 불가능하다.

### 2.1.2 네트워크 기반 연결 역추적

네트워크를 통해 송수신되는 패킷으로부터 정보를 추출하여 역추적을 수행하는 기법으로 송수신 패킷을 감시할 수 있는 위치에 역추적 모듈을 설치하는 기술이다. 아직까지 실제로 인터넷에 적용하여 사용할 수 있는 시스템은 제안되지 않고 있지만 패킷에서 어떤 정보를 활용해야 공격 연결에 속하는가를 판단할 수 있을지에 대한 알고리즘은 제안되고 있다.

## 2.2 IP 패킷 역추적

### 2.2.1 순항적(Proactive) 역추적

패킷을 전송하는 과정에서 역추적 정보를 생성하고 이를 삽입하여 전송하는 방법으로 만약 해킹시도가 있다면 이미 전송된 역추적 정보를 분석하여 공격 근원지를 찾는 기법으로 IP 패킷 역추적, 패킷 마킹(Packet Marking), ICMP 등이 있다. 이는 라우터에서 패킷을 수집하여 한 단계 이전의 라우터 정보와 함께 ICMP 메시지로 감사 정보를 목적지 주소로 전송하는 방식으로 패킷의 헤더 부분에 마킹을 표시하고 각 라우터에서 지역 경로 정보를 확률적으로 기록한다.

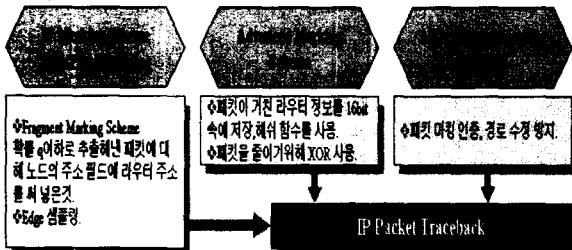
### 2.2.2 반응적(Reactive) 역추적

해킹 시도가 발견되면 연결되어 있는 상태에서 공격 근원지를 역추적 하는 방식으로 이에 해당하는 기술로는 흔히 대처 역추적, 해커 기반 IP역추적, IPSec 기반 역추적 등이 있다.

## 3. 워터마킹 기법

### 3.1 패킷 마킹 기술

패킷 마킹 기술은 DoS 또는 DDoS 등의 실제 IP를 숨기는 형태의 공격에 대하여 이를 역추적하여 실제 주소를 알아내기 위한 기술이다[1][3].



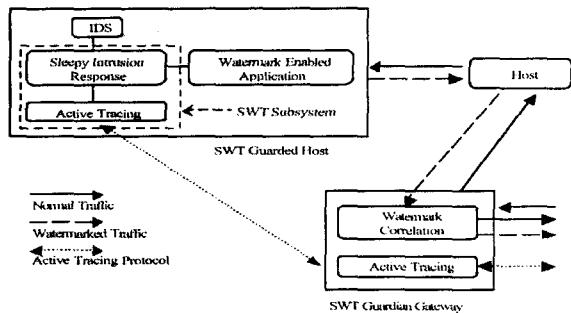
[그림 1] IP Marking Scheme

### 3.2 패킷 워터 마킹 기술

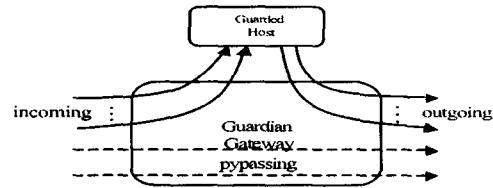
장경다리(Stepping Stones) 형태로 공격자가 여러 시스템을 경유하여 자신의 실제 IP를 공개하지 않으려는 공격을 역추적하는데 사용하는 방법으로 응답 패킷에 해커의 시스템에서는 확인할 수 없도록 패킷(Reply Packet)의 데이터 영역에 제어문자나 날 문자를 사용하여 장경다리 형식의 연결을 유지하는 공격에 대한 추적이 사용한다.

### 3.3 Sleepy Watermark Tracing(SWT)

패킷 워터 마킹의 기본적인 방법은 SWT 역추적 기법이다. 이는 침입에 대한 응답 패킷에 워터마크를 삽입하여 역추적을 수행하는 것으로 공격에 대한 응답 패킷을 이용하여 해커의 위치를 추적하기 때문에 빠르고 정확한 역추적이 가능하다.[그림 2]는 SWT의 기본 구조이다.



[그림 2] SWT의 기본 구조

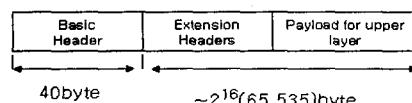


[그림 3] 보호자 게이트웨이의 상호 관계

[그림 2, 그림 3]에서 한 네트워크에는 보호 게이트웨이(Guardian Gateway)가 존재하고, 이와 연동되어 동작하는 Guarded Host가 존재한다. 최초 침입 시도에선 아무런 추가적인 동작이 진행되지 않은 일반적인 상태로 존재하지만, 침입이 발생하면 보호 호스트(Guarded Host)내의 IDS가 이를 탐지 한다. 동시에 보호 호스트(Guarded Host)의 SWT Subsystem에서 Sleepy Intrusion Response 모듈이 작동을 시작하고 이때부터 일반 host에 도착되는 패킷에 의한 응답이 Watermark Enabled Application에 의해 이루어진다. 이제 어플리케이션은 일반적인 응답패킷에 워터마크를 삽입하여 송신을 시작한다. 또한 역추적이 시작되면 어플리케이션은 보호 게이트웨이(Guardian Gateway)의 Active Tracing 모듈과 연동되어 워터마크가 삽입된 패킷을 찾기 시작한다. SWT 역추적 기법은 공격에 대한 응답 패킷을 이용하여 해커의 위치를 추적하기 때문에 빠르고 정확한 역추적이 가능하다. 그러나 모든 시스템에 Watermark Enabled Application이 반드시 설치되어야 함으로 실제 인터넷 환경에 적용하기에는 큰 무리가 있다. 또한 해커에 의해 사용되는 연결이 암호화 패킷을 사용하는 경우에는 역추적이 전혀 불가능할 수 있다는 단점이 존재한다.[2]

## 4. IPv6

### 4.1 IPv6 header



[표 1] IPv6 패킷 형식

Version (4bit)	Traffic Class (8bit)			
Payload Length (16bit)	Next Header (8bit)	Hop Limit (8bit)		
Source Address (128bit)				
Destination Address (128bit)				

[표 2] IPv6 기본 헤더 형식

[표 1, 표 2]는 각각 IPv6의 패킷 형식과 프로토콜의 기본 헤더(40byte) 구성을 보여주고 있다. IPv6의 헤더는 Version 필드(4bit), 트래픽 클래스, 플로우 라벨, Payload Length, 다음주소(Next Header), Hop Limit주소와 함께 각각 128비트의 송신측 주소, 수신측 주소로 구성되어있다. 대부분의 IPv6주소는 아래 64비트가 interface ID이고 위의 64비트는 프리픽스로 라우터에서 받은 값이거나 고정된 값을 사용한다. 따라서 IPv6는 기본으로 64비트 처리가 가능하도록 만들어졌다.

Payload Length은 현재의 헤더 뒤에 따라오는 모든 Payload의 바이트 수를 말하며, Next Header는 수신측 컴퓨터 주소 필드 뒤에 따라오는 옵션 헤더의 타입을 결정하고, Hop Limit은 라우터를 하나 거칠 때마다 1씩 줄어드는 값이다. 송신측 주소, 수신측 주소는 명확하게 정의된다. 트래픽분류(Traffic Class)의 값은 Upper Layer에서 설정하거나 읽을 수 있다는 점에서 Upper Layer(TCP/UDP)의 어플리케이션에서 요구하는 QoS를 지원하기 위해 IP Layer가 하단의 전송 계층에게 이를 요구하는 경우를 위한 배려이다. 플로우 라벨(Flow Label)은 트래픽 분류를 받아서, 이를 수신측 컴퓨터에서 수신측 컴퓨터까지의 모든 라우터들에서 만족하기 위해 지정하는 것이다. 물론 RSVP(Reservation Protocol) 등에서 미리 모든 라우터를 다니면서 플로우 라벨을 설정해야 한다. 플로우 라벨이 설정된다는 것은 어떤 QoS를 만족하는 가상 경로가 만들어졌다는 의미이다. 즉, Traffic Class 필드는 IPv6 트래픽 등급을 명시해주는 필드이며, 플로우 라벨은 IPv6 패킷이 속하는 흐름에 대한 특성을 나타내주는 필드이다.

## 5. IPv6 역추적 방법 제안

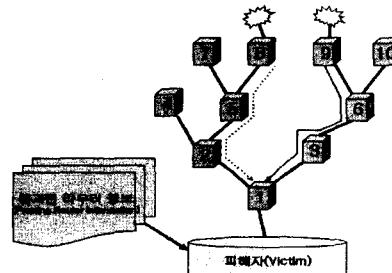
본 논문에서 사용하는 것은 트래픽 클래스와 플로우 라벨로서 이들은 QoS를 제공하기 위한 필드이다. 이 필드는 송신자가 디 플랫폼이 아닌 서비스 품질(QoS) 또는 실시간 서비스와 같은 특별한 처리를 요청하는 특정 트래픽 흐름(Flow)에 속하는 패킷을 레이블링(Labeling)할 수 있다. 이러한 특징을 이용하여 패킷 워터마킹 기법을 적용해서 각각의 필드에 특정 Signature를 워터마크를 이용해 삽입한다.

Version (4bit)	Traffic Class (8bit)	Flow Label (20bit)
5	12	32bit

[표 3] IPv6 패킷

IPv6의 플로우 라벨(Flow Label) 필드(20bit)에 역추적 메시지를 마킹한다. Traffic Class 필드에는 현재의 흐름의 라우터의 주소와 이전 흐름의 라우터의 주소를 마킹한다. 따라서 공격자의 경로를 저장하게 된다. 즉, 공격 경로를 저장하고 있으므로 저장된 공격 경로 정보를 가지고 역추적을 할 수 있다[그림 4]. Dos 공격이나 DDoS 공격은 IP 주소 스프핑을 통해 공격하기 때문에 역추적이 매우 곤란하다. 제안하는 방법은 Flow label 필드에는 발신지 주소인 IPv4의 주소와 MAC 주소를 조합해서 생성된 IPv6 주소를 플로우 라벨 필드에 패킷을 DES 암호화 알고리즘을 사용하여 암호화 한 다음 마킹하는 방법으로 IP 주소를 스프핑하지 못하도록 하여 전송한다. 피해자 측면에서는 공격을 받

은 경우 트래픽 클래스와 플로우 라벨에 암호화 되어있는 패킷에 기록된 두 가지의 정보의 분석을 통해 실시간으로 역추적이 가능한 시스템 모델을 제안하고 있다.



[그림 4] 통과된 라우터 정보

## 6. 결론 및 향후 계획

본 논문에서는 현재 급증하고 있는 해킹이나 DoS, DDoS 공격, 바이러스, 웜 등의 사이버 범죄가 발생했을 경우 스프핑된 트래픽에 대한 실체적이고 능동적으로 역추적 가능한 공격 근원지 역추적 방법에 대하여 알아보았다. 특히 기존의 IPv4에서 이루어진 연구를 중심으로 IPv6에 적용할 수 있는 메커니즘을 제시하였다.

향후 실체적인 모델 구현이 필요하며 시스템마다 어플리케이션 프로그램이 설치되는 점을 보안한다면 실시간 네트워크 역추적 시스템이 될 수 있다고 본다. 또한 Mobile IPv6에서 적용할 수 있는 방안을 제시한다면, 모바일 인터넷에서의 해킹에도 능동적으로 대처 할 수 있을 것이다.

## 참고문헌

- [1] Dawn X. Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," *Proceedings of InfoCom 2001*.
- [2] Xinyuan Wang, Douglas S. Reeves, S. Felix Wu, Jim Y uill, "Sleepy Watermark Tracing: An Active Network-based Intrusion Response Framework", Mar.2001
- [3] Stefan Savage, David Wetherall, Anna Karlin "Practical Network Support for IP Traceback," *ACM SIGCOMM Conference, Aug. 2000, pp295-306.*
- [4] Andrey Belenky and Nirwan Ansari, Senior Member, "IP Traceback With Deterministic Packet Marking," *IEEE Communications Letters, vol.7 NO.4, April 2003*
- [5] Henry C.J. Lee,Miao Ma,Vrizlyn L.L.Thing,Yi Xu,"On the Issues of IP Traceback for IPv6 and Mobile IPv6," *ISCC'03*
- [6] Y. Zhang, V. Paxson, "Detecting Stepping Stones," *Proceedings of 9th USENIX Security Symposium, 2000.*
- [7] BELLOVIN, S. M. "ICMP traceback messages," Internet Draft, IETF, draft-bellovin-itrace-05.txt, 2000
- [8] 최병월, 서동일, "인터넷 패킷 워터 검출 시스템", 정보과학회 추계학술대회, 2002.10
- [9] 이형우, "DDoS 해킹 공격 근원지 역추적 기술", 정보보호학회지, 제13권5호, 2003.10
- [10] 여운영, 김성환, "모바일 네트워크", 2003
- [11] S. Deering, R. Hinden, "Internet Protocol Version 6 (IPv6) Specification", Request for Comments 2460, Internet Engineering Task Force, December 1998.
- [12] Andrey Belenky and Nirwan Ansari, "on Ip Traceback", *IEEE Communications Magazine, July.2003*