情報保護學會論文誌
第20卷 第3號, 2010. 6

IPv6 기반 NGN 환경에서 무결성을 제공하는 역추적 기법*

장 재 훈,† 여 돈 구, 최 현 우, 염 흥 열‡
순천향대학교

An IP Traceback "M"echanism with "E"nhanced "I"ntegrity for IPv6-based NGN Environment*

Jae-Hoon Jang,† Don-Gu Yeo, Hyun-Woo Choi, Heung-Youl Youm‡
Soonchunhyang University

요 약

현재의 인터넷 환경은 IP 기반 네트워크의 구조적인 특성상 송신지 주소를 위조하였을 경우 패킷의 근원지를 찾아내기 어렵다는 문제를 가지고 있다. DDoS 공격이 발생할 경우 또한 능동적인 방어를 하기는 어렵다. 이러한 네트워크상에서의 취약점과 공격에 대응하기 위한 역추적 기법들이 연구되어왔으나 대부분 IPv4 네트워크 환경만을 위한 기법들이며 전송된 역추적 데이터의 변조여부를 검증하기가 어렵다. IPv6 네트워크 환경에서의 역추적 기법들이 연구되어왔지만 아직 많은 연구와 발전이 필요하다. 본 논문에서 우리는 무결성을 제공하여 신뢰할 수 있는 IPv6 네트워크 환경에서의 IP 역추적 기법을 제안하며, 이 시스템을 시뮬레이션하고, 기존의 역추적 기법들과 오버헤드 및 기능성에 대해 비교한다.

ABSTRACT

It is difficult to identify attacker's real location when the attacker spoofs IP address in current IPv4-based Internet environment. If the attacks such as DDoS happen in the Internet, we can hardly expect the protection scheme to respond to these attacks in active or real-time manner. Many traceback techniques have been proposed to protect against these attacks, but most traceback schemes were designed to work with the IPv4-based Internet and found to be lack of verification of whether the traceback related information is forged or not. Few traceback schemes for IPv6-based network environment have been suggested, but it has these disadvantages that needs more study. In this paper, we propose the reliable IP traceback scheme supporting integrity of traceback-related information in IPv6 network environment, simulate it, and compare our proposed scheme with exsisting traceback mechanisms in terms of overhead and functionality.

Keywords: Traceback, IP Traceback, IPv6, NGN

I. 서 론

계속해서 발전하고 있는 인터넷상에서의 공격들을 방어하기 위해 네트워크 보안 기술들 또한 발전되어 왔다. 대표적인 보안 기술로는 방화벽, IDS(Intrusion Detection System), IPS(Intrusion Prevention System) 등을 들 수 있다. 그러나 이러한 보안 시스템은 정해진 룰에 의해서만 동작하는 매우 수동적인 보안 시스템이다. DoS 나 DDoS 공격의 경우에 IDS나 방화벽과 같이 수동적인 보안 시스템만으로는 방어하기가 쉽지 않다. 지금까지의 수동적인 보안시스템만으로는 더욱 다양화되고 지능화되는 인터

접수일(2009년 11월 9일), 수정일(1차: 2009년 12월 29일, 2차: 2010년 2월 11일), 게재확정일(2010년 3월 24일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음.
† 주저자, pure@sch.ac.kr
‡ 교신저자, hyyoum@sch.ac.kr

넷상에서의 공격을 방어하기는 더욱더 어려워 질 것이다. 게다가, 대부분의 공격은 스푸핑된 IP 주소를 이용한다. 현재 사용되는 IP 기반 네트워크에서는 IP의 구조적 특성상 송신지 주소가 변경될 경우 그 근원지를 식별할 수 없다는 매우 중요한 취약점을 가지고 있다.

인터넷상에서의 공격 및 취약점은 IPv4 뿐만 아니라 IPv6 환경에서도 많은 부분이 동일하게 해당되며 IPv6 환경의 취약점 또한 발견될지 모른다. 지금은 IPv4에서 IPv6로 넘어가는 과도기이기 때문에 IPv6에서의 취약점 등에 대응할 수 있는 방안을 마련해야 한다. 또한, ITU-T에서는 NGN(Next Generation Network)의 표준화[1]가 진행 중인데 NGN이 적용되면 PC 뿐 아니라 많은 장치들이 네트워크로 연결될 것이므로 더 많은 취약점과 그를 이용한 공격들이 발생될 것으로 예상된다.

IP를 사용하는 네트워크에서의 공격과 취약점에 대응하기 위해 IP 역추적 기술들[2]이 제안되었다. IP 역추적 기술은 이론적인 기법들과 실제 네트워크에서 적용하여 사용될 수 있도록 하는 기법들이 연구되었지만 대부분이 IPv4 네트워크 환경만을 위한 기법들이었고, 2장에서 언급할 PPM(Probabilistic Packet Marking)[3]을 포함한 기존 역추적 기법들을 개선하여 IPv6 네트워크 환경에서 이용할 수 있는 IP 역추적 기법들[4-8]이 연구되고 있지만 아직 많은 연구가 필요하다. 앞으로의 NGN 환경에서 사용될 IPv6 네트워크에 기반하여 신뢰성을 확보할 수 있는 역추적 기법이 연구 및 발전되어야 하며 이는 본 논문에서 제안하는 기법의 주요 목적이다.

본 논문에서는 확률적 패킷 마킹 기법을 기반으로 한 IPv6 네트워크 환경에서의 신뢰할 수 있는 IP 역추적 기법을 제안한다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 지금까지 연구된 역추적 기법들을 정리한 관련연구를 기술한다. 3장에서는 IPv6 네트워크 환경에서의 IP 역추적 기법을 제안한다. 4장에서는 기존 역추적 기법들과 제안하는 역추적 기법을 비교하고, 마지막으로 결론 및 연구 방향에 대해 논한다.

II. 배경연구

네트워크를 통한 공격들로부터 인프라 및 시스템을 방어하는 데에는 주로 방화벽이나 IDS등이 사용된다. 그러나 계속해서 진화하는 공격기법들로부터 기존의 보안장비 만으로 보호하는 것은 쉽지 않다. 기존의 보안 시스템을 기반으로 하여 방어할 수 있는 대책이나 기술들이 연구되고 있지만 일시적일 뿐이다. 이는 근본적인 해결책이 되기 힘들다.

2.1 네트워크에서의 공격

IP를 사용하는 네트워크에서의 공격은 오래전부터 발전되어왔다. 스푸핑과 같은 공격은 현재 사용되는 네트워크의 구조적 취약점을 이용하는 대표적인 예이다. IP를 사용하는 네트워크의 취약점을 이용하는 공격들은 계속해서 지능화되고 있다. 최근 이슈가 되고 있는 DDoS 공격의 경우 공격자는 인터넷을 통해 확보한 좀비(zombie) 호스트들을 통해 공격대상에게 원하는 방법으로 공격을 수행할 수 있다.

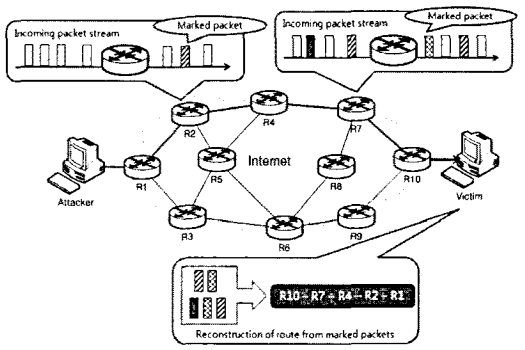
역추적 기술은 스푸핑이나 DDoS와 같은 서비스거부공격 등의 네트워크를 통한 공격이 발생 했을 경우 근원지를 추적해 낼 수 있어야 한다. 역추적 정보가 목적지로 전달되어 패킷의 전달경로를 재구성하는 경우에는 수집된 역추적 정보가 정당한 것인지 확인할 필요가 있다. 네트워크상에서의 통신은 제3자에게 노출, 수정되어질 수 있기 때문에 위조 및 변조에 주의해야 한다. 특별히 안전한 채널이나 통신 참여자 간의 키를 이용한 암호통신 등을 이용하지 않는 한 정보에 대한 정당성은 보장될 수 없다. 본 논문에서는 PPM에 기반하는 역추적 기술을 이용하여 라우터로부터 전송받은 역추적 정보에 대해 위조 및 변조 여부를 판별하여 정확한 역추적 경로를 재구성할 수 있는 메커니즘에 대해 논한다.

2.2 관련연구

인터넷을 통한 공격은 계속해서 지능화 되고 다양화 되고 있다. 이러한 공격들에 대해 능동적으로 대응하기 위한 역추적 기술들이 연구되고 있다. 대표적인 IP 역추적 기술로는 패킷을 확률적으로 샘플링하여 역추적 정보를 마킹하는 확률적 패킷 마킹 기법, 단일 패킷 역추적을 위한 Hash-based 역추적 기법, ICMP메시지를 이용한 iTrace 기법 등이 있다.

2.2.1 확률적 패킷 마킹 기법

확률적 패킷 마킹 기법은 네트워크상의 라우터가 자신을 지나는 패킷에 확률적으로 라우터 정보를 삽입



〔그림 1〕 확률적 패킷 마킹 기법 (PPM: Probabilistic Packet Marking)

하여 역추적 정보를 구성함으로써 패킷이 실제로 지나온 경로를 알 수 있게 하는 기법이다. 라우터는 어떠한 패킷이 지나갈 때 패킷의 IP 헤더에 자신을 통과했다는 표시로 IP 주소를 마킹하여 다음 라우터로 전송한다. 패킷이 지나는 라우터들이 해당 패킷에 역추적 정보를 마킹하게 되면 패킷이 스푸핑되어 있더라도 실제로 어떤 경로를 지나왔는지 알 수 있게 된다.

그러나 라우터는 엄청난 양의 패킷들을 전달한다. 역추적 정보를 모든 패킷에 대해 마킹하게 되면 라우터에는 많은 오버헤드가 발생하게 되므로 통신에 지연 및 장애가 발생할 수 있다. 이에 대한 확률적 패킷 마킹 기법의 대안은 라우터가 자신을 지나가는 패킷들 중에서 역추적 정보를 마킹하기 위한 패킷을 확률적으로 샘플링하여 라우터 본래의 역할을 수행하는 데에 걸리는 오버헤드를 줄이도록 하는 것이다.

패킷 마킹 기법은 일반적으로 PPM(Probabilistic Packet Marking)〔3〕과 DPM(Deterministic Packet Marking)〔9-11〕으로 나눌 수 있다. PPM의 경우 설정된 확률에 따라 패킷을 샘플링하여 마킹하고, DPM의 경우 모든 패킷에 마킹한다는 차이가 있다(본 논문에서는 PPM에 기반으로 하는 역추적 기법을 제안하고 있으며 DPM은 비교대상으로써는 차이가 있기 때문에 자세히 다루지 않는다). PPM 기법에서 라우터들은 확률 p로 패킷을 샘플링하여 역추적 정보를 마킹한다. 이 때 마킹하는 역추적 정보는 마킹하는 라우터의 주소 정보이며 IP 헤더의 변경 가능한 부분 즉, 변경되더라도 네트워크상에서의 통신에 지장을 주지 않는 필드에 기록하게 된다.

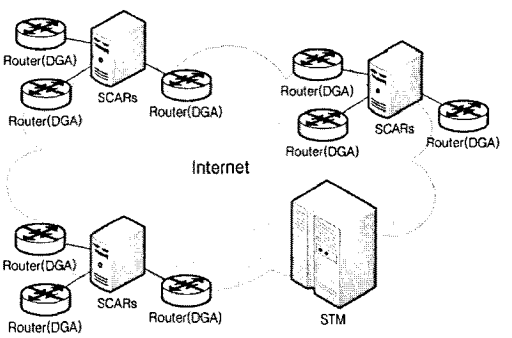
PPM 기법은 세부적으로 node append, node sampling, edge sampling 기법으로 연구되어왔다. Node append는 패킷의 끝에 각 node의 주소를 덧붙이는 방법이다. 가장 단순하고 정확하지만 높은 라우터 오버헤드와 충분한 저장 공간을 마련하기 어렵다는 큰 문제가 있다. Node sampling은 라우터 오버헤드와 저장 공간을 감소시키기 위해 연구된 기법이며, 이 후에 edge sampling 기법이 연구되었다. Edge sampling 기법은 각 네트워크 별로 edge가 되는 라우터들에서 확률적으로 패킷을 샘플링하여 마킹하는 방법이다.

Edge sampling을 이용하게 될 경우 각 네트워크의 edge가 되는 라우터들이 확률 p로 패킷을 샘플링한 후 역추적 정보를 마킹하여 목적지로 전달한다. 역추적 정보가 마킹된 패킷들을 수신한 피해자는 수집된 역추적 정보들을 근거로 패킷이 지나온 경로를 재구성할 수 있게 된다.

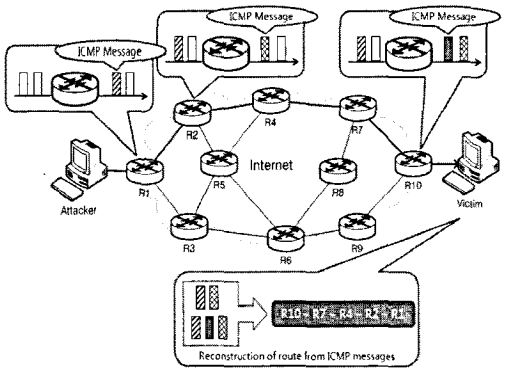
2.2.2 해쉬 기반 역추적 기법

해쉬 기반 역추적 기법〔12, 13〕은 단일 패킷을 이용한 공격을 역추적 가능하게 한다. SPIE(Source Path Isolation Engine)를 적용하여 단일 패킷 역추적을 수행할 때의 패킷 데이터 저장 공간 문제를 해결 하였다.

SPIE는 DGA(Data Generation Agent)를 가지는 라우터, SCARs(SPIE Collection and Reduction Agents), STM(SPIE Traceback Manager)로 구성된다. 패킷이 라우터를 통과 할 때 라우터에 포함되어있는 DGA가 해당 패킷의 IP 헤더 및 페이로드를 이용해 해쉬 데이터를 생성하고 bloom filter 구조로 저장한다. SCARs는 특정 네트워크 영역을 담당하고 역추적을 하기 위한 패킷 정보를 수집 및 분석한다. STM은 역추적 요청을 적절한 SCARs에 디스패치 하고 SCARs로부터 역추적 분석 결과를 전달 받아 경로를 재구성하는 등의 역할



〔그림 2〕 해쉬 기반 역추적(Hash-based traceback) 기법에서 사용되는 SPIE 시스템



〔그림 3〕 ICMP 역추적 기법인 iTrace(ICMP Traceback) 기법

을 수행한다. 해쉬 기반 역추적 기법에서 사용되는 SPIE 시스템을 IPv6 네트워크 환경에서 이용 가능하도록 개선한 SPIE-IPv6 시스템이 연구되었지만, 이는 IPv4 네트워크에서의 SPIE 시스템을 IPv6 프로토콜 및 헤더에 맞도록 조금 변경된 것이고 기본적인 구성이 동일하다.

SPIE 시스템을 이용한 해쉬 기반 역추적의 특징은 단일 패킷을 통한 역추적이 가능하다는 점이다. 그러나 각 라우터에 DGA 모듈의 탑재와 SCARs 및 STM이 설치되어야 하기 때문에 비용이 많이 들고 실제 적용이 어렵다는 단점이 있다.

2.2.3 iTrace(ICMP Traceback) 기법

ICMP 역추적 기법〔14〕은 확률적으로 패킷을 샘플링하여 ICMP 메시지에 역추적 정보를 삽입한 후 피해자에게 송신함으로써 역추적 정보를 전달하는 기법이다.

확률적으로 샘플링한다는 측면에서는 확률적 패킷 마킹 기법과 비슷하게 보일 수 있으나, 샘플링된 패킷에 역추적 정보를 마킹하는 것이 아니라 라우터가 ICMP 메시지를 발생시켜 message body부분에 라우터가 생성한 역추적 정보를 구성한 후 패킷의 목적지로 전달한다. 이 기법의 장점은 기존 IPv4에서 사용되는 ICMP나 IPv6에서 제공하는 ICMPv6를 그대로 이용하여 message body부분에 역추적 정보를 기록한 후 목적지로 전달하는 구조이기 때문에 구현이 매우 용이하고 적용이 비교적 쉽다. 그러나 라우터가 ICMP 메시지를 발생시키는 것은 네트워크 트래픽을 증가시키는 문제점을 가진다.

2.2.4 IPv6 네트워크 기반 역추적 기법

IPv6 네트워크에서 이용할 수 있는 역추적 기법들 또한 연구되어 왔으며, 해쉬 기반 역추적 및 iTrace 기법의 경우 앞서 언급 했듯이 기존의 기법들을 각각 IPv6 프로토콜 및 필드 구조에 적합하도록 SPIE-IPv6로 개선하고 ICMPv6를 이용하여 IPv6 네트워크에서 적용 가능하도록 개선한 것이다.

그 이외에 일반적으로 연구되는 IPv6 기반 역추적 기법들의 경우 대부분 확률적 역추적 기법에 기반하고 있다〔5-7〕. 이들은 PPM에 기반하는 역추적 기법들로, IPv6 네트워크에서 적용 가능한 일반적이면서 효율적인 구조들을 가지고 있다. 〔5〕의 경우 IPv6의 기본 헤더에 위치하는 Flow Label 필드를 edge hash 필드와 distance 필드로 구분하여 간결하게 역추적 정보를 구성하도록 했고, 〔6, 7〕의 경우 IPv6의 확장 헤더를 이용하여 확장성이 좋고 효율적인 역추적 기법을 제안하고 있다.

PPM을 이용한 역추적 기법은 SPIE와 같은 관리 시스템이 없기 때문에 피해자가 역추적 정보가 마킹된 패킷들을 수집하여 경로를 재구성해야 한다. 그러나 2.1절에서 언급한 것처럼 역추적 정보가 마킹된 패킷들 또한 네트워크를 통해 전달되므로 공격자가 봇 등을 이용한 DDoS공격을 수행하면서 네트워크상의 역추적 정보를 가로채 임의로 변조시키거나, 위조할 수 있게 되고, 피해자는 정확한 경로의 재구성이 매우 어려워진다. 지금까지 연구된 IPv6 기반 역추적 기법들은 효율성 및 확장성이 매우 용이 하지만 PPM에 기반한 기법임에도 위조 및 변조 여부를 검증할 수 있는 방안을 제시하지 않고 있어 문제가 될 수 있다. 이에 따라, 본 논문에서는 PPM에 기반면서 무결성 검증이 가능한 역추적 기법에 대해 제안한다.

III. 역추적 기법 제안

2장에서 지금까지 연구된 IP 역추적 기술들에 대해 간단히 언급하였다. 해쉬 기반 역추적 기법에서 필요로 하는 SPIE와 같은 시스템은 단일 패킷으로도 역추적이 가능한 기술이지만 환경 구성이 어렵고, iTrace 기법의 경우 네트워크 트래픽을 증가시켜 실제로 적용하는 데에는 어려운 점이 있다. 일반적으로, 현재 연구되는 많은 역추적 기법들이 라우터 오버헤드를 적절히 조절하고 구현이 비교적 쉬우며 확장성을 높일 수 있도록 PPM 기법의 확률적으로 패킷을 샘플

링하여 마킹한다는 점을 이용하여 개선되고 있다.

역추적 기술의 연구는 라우터 오버헤드, 구현의 용이성, 확장성 등 여러 가지를 고려해야 한다. 이와 더불어 또 한 가지 중요한 점은 마킹된 역추적 정보에 대해 신뢰할 수 있어야 한다는 것이다. PPM에 기반한 역추적 기술들이 적절히 적용될 수 있다고 해도 역추적 정보 또한 네트워크를 통해 전송되는 정보이기 때문에 위조 및 변조에 대해 고려야 해야 한다. 역추적 정보가 위조되거나 전송 도중 변조된다면 그 역추적 정보는 신뢰할 수 없는 정보이다. 위조 또는 변조된 역추적 정보는 피해자에게 잘못된 경로를 재구성하도록 할 것이다.

본 논문에서는 IPv6 기반의 NGN 환경에서 신뢰할 수 있는 IP 역추적 기법을 제안한다. 제안하는 IP 역추적 기법은 다음과 같은 사항이 전제되어야 한다.

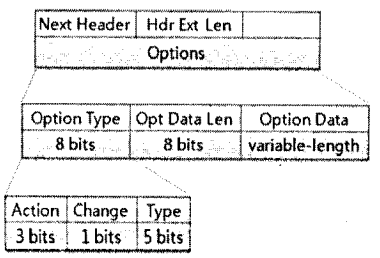
① 역추적에 참여하는 라우터는 타협되지 않아야 한다.

② 역추적에 참여하는 라우터들은 각각의 key를 가지며 keyed-hash 알고리즘을 계산할 수 있어야 한다.

③ 마킹하는 라우터는 피해자 시스템으로부터 역추적 정보 검증 메시지를 수신하여 검증 후 응답할 수 있어야 한다.

3.1 Hop-by-Hop options header

본 논문에서는 IPv6 네트워크 환경에서 역추적을 가능하게 하기위해 Hop-by-Hop options header [15]를 사용한다. 그림 4는 Hop-by-Hop options header를 나타낸 그림이다. 이 Hop-by-Hop options header는 IPv6의 확장 헤더 중 하나로 목적지로 전달되는 경로상의 모든 라우터에서 인식가능하며 모든 호스트에서 처리될 수 있다. 또한, 크기가 유동적이기 때문에 정보의 저장 및 전달이 용이하다.



[그림 4] IPv6의 Hop-by-Hop options header의 구조

3.2 역추적 정보의 구성

Type필드의 하위 5비트를 $10111_{(2)}$로 기록하여 제안하는 역추적 기법을 사용함을 나타내었다.

제안하는 역추적 기법은 Hop-by-Hop options header의 data필드에 역추적에 필요한 정보를 기록한다. 가변 데이터 필드는 다음과 같은 정보들로 구성되어 있다.

① Hop: IPv6 헤더에 있는 Hop Limit필드의 값을 그대로 쓴다.

② NetID: 라우터가 가지는 IPv6 주소의 상위 16비트 이후의 48비트 네트워크 주소를 기록한다.

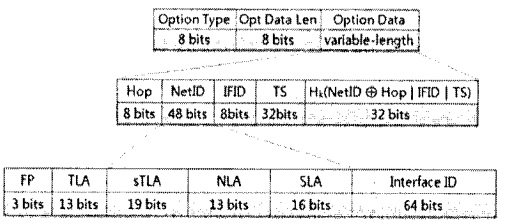
③ IFID: 라우터가 패킷을 수신하였을 때 패킷이 들어온 인터페이스의 ID를 기록한다.

④ TS: 라우터가 패킷을 수신하였을 때의 time-stamp값을 기록한다.

⑤ H_k(NetID⊕Hop|IFID|TS): 무결성을 제공하기 위한 역추적 정보들의 keyed-hash값이다.

실제로 네트워크에서 전송될 때의 Hop수가 대부분 8비트로 나타낼 만큼 크지 않음에도 Hop필드를 8비트로 할당한 것은 헤더 정보와의 호환성을 위함이다.

8비트의 IFID 필드는 라우터가 가지는 각 인터페이스에 고유 값을 할당하여 기록한다. 이는 라우터의 인터페이스가 가지는 64비트의 인터페이스 ID를 8비트로 축소시켜 데이터 크기를 줄이기 위함이다. 패킷이 입력된 인터페이스 ID를 기록하면 PPM 기법의 일정량 패킷을 수집하여 역추적 경로를 재구성한다는 특성상 중간 경유 라우터로부터 역추적 정보를 수신하지 못하더라도 이전에 어떤 네트워크를 거쳐 왔는지를 알 수 있다. 또한 공격자와 가장 근접한 라우터에서



[그림 5] Hop-by-Hop options header의 가변 길이 데이터 부분에 구성한 제안하는 역추적 기법의 필드 구조

```
Marking procedure at router R:
  Let E be a hop-by-hop options header
  Let T be a traceback information data (Hop, NetID, IFID, ts, hmac)
  Let H_k() be a keyed-Hash( (T.hop||T.IFID||T.ts) ⊕ T.NetID )
    with R.private-key
  For each packet ω marked with probability p
    Write ω.hop_limit into T.Hop
    Write R.NetID into T.NetID
    Write R.IFID matched with R.interfaceID into T.IFID
    Write time-stamp into T.ts
    Write truncated H_k() into T.hmac

    Write 10111(2) into E.low-order 5bits of option type field
    Write T into E.data

    Append E to the IPv6 header of ω
```

〔그림 6〕 제안하는 역추적 기법의 패킷 마킹 알고리즘

마킹이 되었을 경우 공격자가 속한 하위 네트워크 까지 알아 낼 수 있다.

일반적으로 역추적 정보를 기록할 때에는 시간정보를 고려하지 않지만 제안하는 역추적 기법에서는 time-stamp를 다음과 같은 목적으로 이용하고 있다. keyed-hash값에 의한 무결성 검증 시에 가변정보를 이용하여 재전송 공격을 막는데 이용된다. 또한, 경우에 따라 피해자 시스템에서의 수신시간과 비교하여 별도의 검사과정 없이 현재 네트워크의 대략적인 상태나 공격의 종류를 판별하는데 도움을 줄 수 있다.

Keyed-hash값은 앞에서 언급된 모든 역추적 정보를 이용해 라우터가 가지는 고유의 키로 계산된다. 따라서 공격자가 역추적 정보를 위조 또는 변조했을 경우 라우터가 생성한 keyed-hash 값이 아니기 때문에 올바른 검증 과정을 거칠 수 없다.

제안하는 역추적 기법은 PPM방식을 기반으로 하므로 라우터는 전송되는 패킷을 확률적으로 샘플링 하여 역추적 정보를 마킹한다. Hop필드에는 IPv6 헤더의 Hop Limit필드 값을 그대로 복사하고, NetID에는 라우터의 48비트 네트워크 주소가 기록되며 IFID에는 라우터가 패킷을 수신한 인터페이스의 ID를 8비트로 표현하여 기록한다. times-tamp는 라우터가 패킷을 수신한 시간정보를 32비트로 기록한다. 마지막 필드에는 Hop, IFID, time-stamp를 연결하여 48비트로 만든 후 48비트의 NetID와 XOR연산한 결과를 라우터의 고유키로 해쉬하여 기록한다. 일반적인 해쉬 알고리즘은 128 bits 이상의 출력을 가지기 때문에 해쉬 결과의 일부를 32비트로 취해야 한다.

해쉬 기반 역추적에서는 단일 패킷에 대한 해쉬 값을 라우터의 DGA 모듈이 계산하여 bloom filter 형식으로 저장하고 이를 이용해 역추적을 수행하는 반면, 제안하는 기법에서의 keyed-hash 값은 라우터가 라우터 고유의 키로 해쉬 한 값을 이용하여 무결성을 검증하는 용도로 사용되므로 해쉬 기반 역추적에서 사용되는 해쉬와는 용도 및 성격에 많은 차이를 가지고 있다.

3.3 경로 재구성 과정

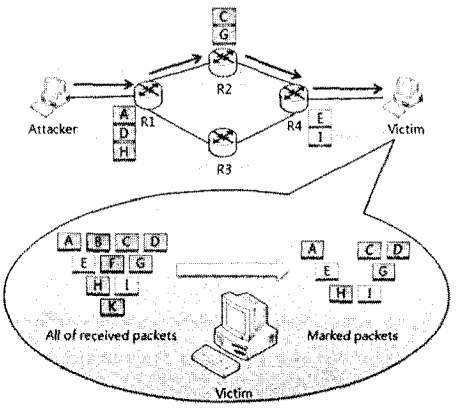
제안하는 기법은 확률적으로 패킷에 마킹하는 PPM을 기반으로 하기 때문에 충분한 양의 패킷을 요구한다. DDoS와 같은 서비스 거부 공격의 경우 많은 양의 패킷을 전달하여 네트워크 및 대상 시스템의 자원을 소모시키기 때문에 PPM 기반의 역추적 기법을 이용하면 라우터나 네트워크에 큰 오버헤드 없이 역추적이 가능하다.

공격 패킷이 라우터를 통과할 때 경로 상에 있는 경

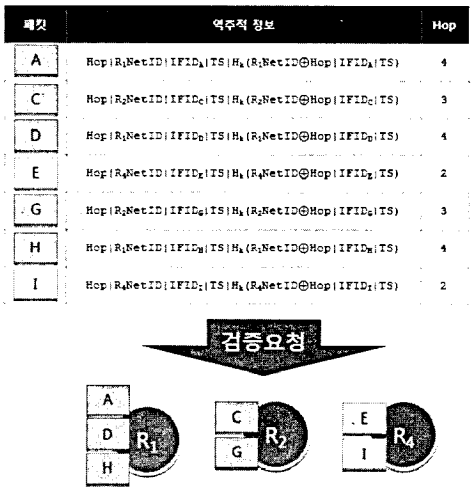
```
Path reconstruction procedure at victim V:
  Let X be a reconstructed attack path
  For each packet ω from attacker
    IF ω.low-order 5bits extention header's option type field = 10111(2) THEN
      Extract T.Hop, T.NetID, T.IFID
      Classify T by T.Hop
      Transmit T to R
        then R call traceback information data verification procedure
      Receive reply message from R
      IF replay message = verification success message THEN
        Add R into X
      ELSE
        Remove T
      ENDIF
    ENDIF

Traceback information data verification procedure at router R:
  Receive T from V
  Compute H_k()
  IF H_k() = T.hmac THEN
    Reply verification success message to V
  ELSE
    Reply verification failure message to V
  ENDIF
```

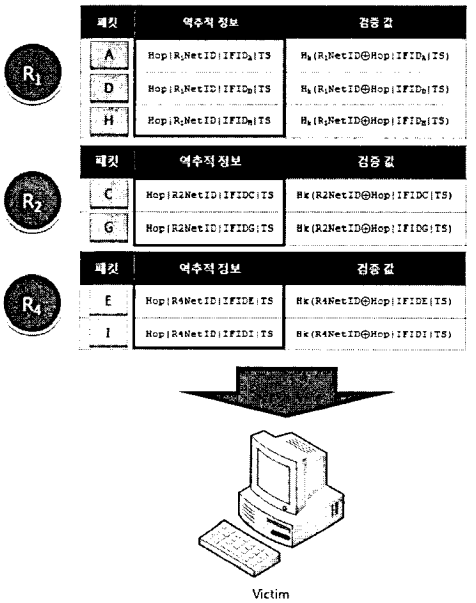
〔그림 7〕 제안하는 역추적 기법의 경로 재구성 알고리즘



〔그림 8〕 피해자가 각 경유라우터에서 마킹된 패킷을 추출



〔그림 9〕 피해자가 수집한 마킹된 패킷들을 정렬하고 각 네트워크의 라우터에 역추적 정보에 대한 무결성 검증을 요청



〔그림 10〕 라우터는 역추적 정보에 대한 무결성을 검증하여 결과를 피해자에게 통지

유 라우터들은 패킷들을 확률적으로 샘플링하여 역추적 정보를 마킹하고 목적지로 전달한다. 다수의 공격 패킷들을 수신한 피해자는 그 중에서 마킹된 패킷을 추출해야 한다. Hop-by-hop options header의 option type 필드가 제안하는 기법에서 정의한 값을 가질 경우 역추적 정보가 마킹된 것으로 판단하고 이를 수집한다.

그림 8은 공격자가 공격 패킷A~K를 전송했을 때 각각 R1에서 A, D, H, R2에서 C, G, R4에서 E, I를 마킹하고 B, F, K는 마킹이 되지 않은 일반 패킷으로 전달되된 것을 나타낸다. 결과적으로 패킷 A, C, D, E, G, H, I가 경유 라우터에서 역추적 정보가 마킹되어 확장헤더의 option type 필드 하위5비트에 10111(2)를 가지는 패킷이다.

마킹된 패킷이 충분히 수집되면 마킹했던 홉 값과 라우터 정보를 이용해 분류 및 정렬하고 라우터에게 마킹된 역추적 정보를 전송하여 역추적 정보에 대한 무결성 검증을 요청한다.

역추적 정보를 수신한 라우터는 자신이 가진 고유키를 이용해 역추적 정보의 필드들을 해쉬하여 무결성 검증을 시도하고 그에 대한 결과를 피해자에게 응답한다. 이때 라우터가 피해자에게 보내는 응답은 무결성 검증에 대한 성공 또는 실패 메시지이다. 라우터로 부터의 성공 또는 실패 메시지는 별도의 보안연계를 통해 안전하게 전달된다고 가정한다. 만약 역추적 정보가 위조 또는 변조되었다면 다음과 같은 임의로 생성된 값이 라우터 주소로 인식되기 때문에 요청자체가 불가능 하거나, 라우터가 존재할지라도 라우터가 가지는 고유키를 이용해 역추적 정보를 해쉬했을 때 같은 결과를 얻기가 쉽지 않다. 따라서 위조 또는 변조된 역추적 정보가 사용되어 공격자로의 경로 재구성이 방해되는 것을 막을 수 있다.

라우터로부터 응답을 받은 피해자는 해당 역추적 정보가 해당 라우터에서 생성되어 신뢰할 수 있는 역추적 정보인지를 확인하고 정당한 것으로 검증된 역추적 정보들을 이용해 패킷이 전송되어온 경로를 재구성한다.

IV. 제안시스템 시뮬레이션 및 특성 분석

4.1 제안시스템 시뮬레이션

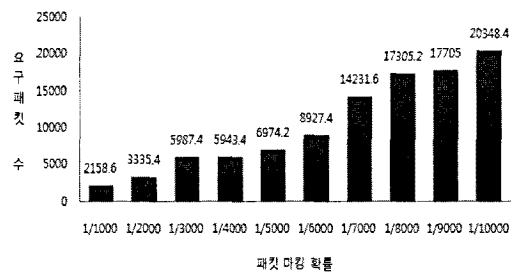
제안하는 역추적 기법은 IPv6를 기반으로 하는 NGN 환경에서 이용될 수 있도록 고안되었다. 그러나 IPv6를 지원하고 제안하는 기법에서 이용되는 keyed-hash등의 기능 구현이 용이한 실험환경을 구성하기 쉽지 않기 때문에 소규모의 IPv6 네트워크 환경을 가상환경으로 구성하였다. 가상으로 구성된 시뮬레이션 환경은 그림 8과 같이 구성되었으며, 경유 라우터를 통과하는 패킷을 다양화시키기 위해 패킷 송신지 머신이 2대 추가되었다. 각 라우터 모듈 및 피해자

〔표 1〕 기존 역추적 기법들과 제안하는 역추적 기법의 비교 및 분석

	별도 시스템 필요	확장성	IPv6 지원	무결성 지원
PPM 기법(IPv4)	낮음	낮음	지원안함	지원안함
iTrace 기법(IPv6)	낮음	높음	지원함	지원안함
Hash-based 기법(IPv6)	높음	낮음	지원함	일부지원
제안하는 기법(IPv6)	**낮음**	**높음**	**지원함**	**지원함**

의 역추적 데이터 수집 프로그램은 리눅스 운영체제에서 그림 6, 7의 알고리즘을 기반으로 C를 이용해 구현하였다.

샘플링된 패킷에 대한 keyed-hash 값을 구할 때에는 openssl 라이브러리에서 제공하는 HMAC with md5를 이용하였다. 이때 해쉬 값의 기본 출력은 128 비트이며 이중 상위 32 비트를 취해 역추적 데이터의 keyed-hash에 이용했을 때, 데이터 구성 및 파싱 과정과 HMAC with md5의 계산에 소요되는 500회 평균 실행시간은 약 46.13us였다. 그림 11은 구성된 시뮬레이션 환경에서 3대의 머신에서 송신된 패킷이 3대의 라우터를 경유 할 때 각 공격지에 대해 전체 경로 재구성시 필요한 평균 패킷 수를 계산한 것이다. 이 시뮬레이션은 각 확률별로 5회 실행되었으며, 송신된 IPv6 패킷 수는 각각 10만개이다.



〔그림 11〕 마킹 확률에 따른 전체 경로 재구성시의 평균 요구 패킷 수

4.2 비교 분석

표 1은 앞서 살펴본 기존 역추적 기법들과 제안하는 역추적 기법에 대한 특징을 비교한 것이며, 표 2는 네트워크 및 라우터에 발생하는 오버헤드를 나타내고 있다.

해쉬 기반 역추적 기법은 라우터에 탑재되는 DGA를 중심으로 전체적인 시스템을 구성하는 요소들이 요구되고 구현이 어렵다. 또한, 각 패킷에 대한 해쉬 데이터를 보관해야 하는 등 별도의 구성요소들이 각각의 역할을 수행하더라도 높은 별도로 요구되는 시스템과 그에 대한 관리 오버헤드가 예상된다.

확장성에 대해서는 PPM의 경우 IP header에서 변경되어도 통신에 지장을 주지 않는 필드에 역추적 정보를 저장하기 때문에 매우 낮다. 해쉬 기반 역추적 기법의 경우 역추적 정보의 생성, 관리, 경로 재구성까지의 모든 과정 및 구조가 정해져있기 때문에 확장성을 기대하기 어렵다.

IPv6 프로토콜을 지원하기 위해서는 PPM의 경우 IPv4의 특정 필드를 이용하므로 프로토콜이 변경될 경우 새로 고안되어야 한다. iTrace의 경우 ICMPv6를 이용할 수 있으며 이미 이에 대한 연구가 있다. SPIE 시스템의 구성이 요구되는 해쉬 기반 역추적 기법의 경우 또한 IPv6에서 이용될 수 있도록 연구된 바가 있으나, 기술의 적용이 매우 어렵다는 점은 변하지 않는다.

지금까지 제안된 역추적 기법들은 무결성에 대해 크게 중요하게 다루지 않았기 때문에 기본적으로는 무

〔표 2〕 기존 역추적 기법들과 제안하는 역추적 기법의 오버헤드 비교 및 분석

	네트워크 오버헤드 (네트워크 트래픽 량)		라우터 오버헤드 (데이터 처리량)	
	정성적 비교	정량적 비교	정성적 비교	정량적 비교
PPM 기법(IPv4)	낮음	추가 오버헤드 없음	낮음	16 bits
iTrace 기법(IPv6)	보통	가변	보통	가변
Hash-based 기법(IPv6)	낮음	추가 오버헤드 없음	높음	최소 480 bits
제안하는 기법(IPv6)	**낮음**	128 bits	**보통**	128 bits

결성을 제공하지 않는다. iTrace에서 역추적 정보에 대한 위조 방지를 위해 전자서명에 대해 언급하였으나 모든 라우터에서 전자서명을 지원할 수 없다는 문제 때문에 정의하지 않고 이후 과제로 남겨두었다. 제안하는 역추적 기법은 PPM 기법의 장점을 IPv6 네트워크에서 이용하면서 무결성을 제공할 수 있도록 하였다.

네트워크 오버헤드에서는 대부분 각 패킷에 대한 역추적 정보를 생성하는 방식을 사용하기 때문에 네트워크상에서는 크게 영향이 없지만 iTrace의 경우 라우터에서 확률적으로 샘플링된 패킷에 대해 ICMP 메시지를 생성해서 발생시켜야 하기 때문에 네트워크상에 오버헤드가 발생하여 다른 역추적 기법들에 비해 비교적 높은 편이다. ICMP 메시지의 가변길이 message body 필드에 역추적 정보를 구성하는데, 역추적 정보의 크기 또한 가변이기 때문에 네트워크상에서 증가하는 데이터 량이 커 질 수도 있다. 제안하는 역추적 기법의 경우 Hop-by-Hop options header의 가변길이 data 필드에 역추적 정보를 128 bits 크기로 구성하여 네트워크상에서 전송되는 트래픽을 크게 증가시키지 않는다.

라우터 오버헤드는 역추적 정보 처리 시에 라우터가 받는 오버헤드를 나타낸다. 해쉬 기반 역추적 기법은 라우터의 DGA 모듈 등이 요구되고 그 역할이 많기 때문에 라우터의 오버헤드가 굉장히 높다. SPIE-IPv6에서는 IPv6 헤더의 40 byte와 페이로드 부분의 20 byte를 처리하고 추가적으로 확장 헤더가 있을 경우 더 처리하기 때문에 최소 60 byte, 비트로는 최소 480 bits 이상을 처리해야 한다. iTrace는 ICMP 메시지를 생성하는 과정에서 라우터가 상당히 큰 량의 데이터를 처리해야 할 수도 있다. 제안하는 역추적 기법에서는 Hop-by-Hop options header에 구성하는 역추적 정보인 128 bits를 처리하여 라우터가 처리하는 양이 크지 않다.

V. 결론

본 논문에서는 PPM 기법에 기반을 두는 IPv6 네트워크 환경에서 무결성을 제공하는 역추적 기법을 제안하였다. 또한 제안 시스템의 동작을 시뮬레이션한 결과, 역추적 경로를 구성하기 위한 최소 패킷 수를 구했고, 이를 통해 동작 타당성을 확인했다. 제안하는 IP 역추적 기법은 마킹 정보에 대해 무결성을 제공하여 라우터가 마킹 한 패킷이 위조 또는 변조 되었는지 판별이 가능하고 Hop-by-Hop options header를 이용하여 확장성이 좋고 처리하는 데이터가 크지 않기 때문에 네트워크 오버헤드를 크게 유발하지 않는다. 무결성 정보를 생성하면서 라우터에서 발생할 수 있는 계산상의 오버헤드를 최소화하는 것이 앞으로의 과제일 것이다. 또한 많은 연구를 통해 실제로 적용 가능한 역추적 기술이 표준화될 수 있도록 해야 할 것이다.

참 고 문 헌

[1] X. Zeltsan, "Guidelines for NGN Security Release," ITU-T, FGNGN, FGNGN-OD-00254, Nov. 2005.

[2] 한정화, 김락현, 류재철, 염흥열, "역추적 기술 및 보안 요구사항 분석," 한국정보보호학회지, 18(5), pp. 132-141, 2008년 10월

[3] S. Savage, D. Wtherall, A. Karlin, and T. Anderson,, "Practical Network Support for IP Traceback," Proceedings of ACM SIGCOMM 2000, pp. 295-306, Oct. 2000.

[4] H.C.J. Lee, M. Ma, V.L.L. Thing, and Y. Xu, "On the Issues of IP Traceback for IPv6 and Mobile IPv6," Proceedings of the IEEE International Symposium on Computers and Communication, pp. 582-587, July 2003.

[5] E. Albright and X. H. Dang, "An Implementation of IP Traceback in IPv6 Using Probabilistic Packet Marking," Proceedings of International Conferencee on Internet Computing (ICOMP 05), June, 2005.

[6] 허준, 강명수, 홍충선, "IPv6 네트워크 환경에서의 경량화된 IP 역추적 기법," 한국정보보호학회 논문지, 17(2), pp. 93-102, 2007년 4월.

[7] Rack-Hyun Kim, Jae-Hoon Jang, Heung-Youl Youm, "An Efficient IP Traceback mechanism for the NGN based on IPv6 Protocol," JWIS 2009, August 2009.

[8] S. O. Amin, C. Seon, "On IPv6 traceback," ICACT 2006, Feb. 2006.

[9] S.K. Rayanchu and G. Barua, "Tracing

Attackers with Deterministic Edge Router Marking (DERM)," Distributed Computing and Internet Technology, First International Conference, Bhubaneswar, India, pp. 400?409, Dec. 2004.

[10] Shokri, Reza, A. Varshovi, H. Mohammadi, N. Yazdani, and B. Sadeghian, "DDPM: Dynamic Deterministic Packet Marking for IP Traceback," IEEE International Conference on Networks. Singapore. pp. 1 - 6, Sep. 2006

[11] Hazeyama, Hiroaki, Y. Kadobayashi, D. Miyamoto, and M. Oe, "An Autonomous Architecture for Inter-Domain Traceback across the Borders of Network Operation," Proceedings of the 11th IEEE Symposium on Computers and Communications, Cagliari, Sardinia, Italy, pp. 378?385, June, 2006.

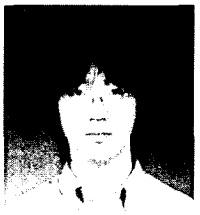
[12] A.C. Snoeren, C. Partridge, L.A. Sanchez, C.E. Jones, F. Tchakountio, B. Schwartz, S.T. Kent, and W.T. Strayer, "Single-Packet IP Traceback," IEEE/ACM Transactions on Networking, pp. 721-734, Dec. 2002

[13] W.T. Strayer, C.E. Jones, F. Tchakountio and R.R. Hain, "SPIE-IPv6: Single IPv6 Packet Traceback," Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, pp. 118-125, Nov. 2004

[14] Steve Bellovin, Marcus Leech, and Tom Taylor, "ICMP Traceback Messages", IETF Internet Draft, Version 4, February 2003

[15] S. Deering and R. Hinden "Internet Protocol, Version 6 (IPv6) Specification", RFC2460, Dec. 1998

〈著者紹介〉



장 재 훈 (Jaehoon Jang) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 역추적, IPTV 보안, USN 보안, 웹 보안

여 돈 구 (Don-Gu Yeo) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적

최 현 우 (Hyun-Woo Choi) 학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 IPTV 보안, 스마트그리드 보안, USN 보안, 역추적

염 흥 열 (Heung-Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 졸업(학사)
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
〈관심분야〉 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜