情報保護學會論文誌
第17卷 第2號, 2007. 4

IPv6 네트워크 환경에서의 경량화된 IP 역추적 기법

허 준,[1†] 홍 충 선,[1‡] 강 명 수[2]
[1]경희대학교, [2](주)플렌티넷

Lightweight IP Traceback Mechanism on IPv6 Network Environment

Joon Heo,[1†] Choong Seon Hong,[1‡] Myung Soo Kang[2]
[1]Kyung Hee University, [2]Plantynet

요 약

DDoS 공격에 대처하고자 할 때 가장 어려운 문제는 공격패킷에 스푸핑된 IP 주소가 사용된다는 것이다. 인터넷의 구조적인 특성상 스푸핑된 IP 패킷의 공격 근원지를 찾아내는 것은 어려운 문제이다. 지금까지 DDoS 공격에 대응하기 위해 역추적 메커니즘을 사용하는 대부분의 연구들은 IPv4 네트워크 환경에 초점을 맞추고 있다. IPv6 네트워크 환경을 위한 몇몇 연구가 진행 되었으나 DDoS 공격에 대처하기 위한 자세한 메커니즘을 제공하지 못하고 있다. IPv6 네트워크에서 공격 근원지를 역추적하기 위한 메커니즘은 IPv4 네트워크와는 많은 부분이 상이하게 된다. 본 논문에서는 IPv6 네트워크 환경을 위한 경량화된 역추적 메커니즘을 제안한다. 역추적을 위한 마킹이 필요할 경우 라우터는 홉간 옵션을 생성하고 마킹을 실시한 후 패킷을 전송한다. 제안된 메커니즘의 성능평가를 통해 역추적을 위한 효율적인 마킹이 가능함을 보였다.

ABSTRACT

A serious problem to fight DDoS attacks is that attackers use incorrect or spoofed IP addresses in the attack packets. Due to the stateless nature of the internet, it is a difficult problem to determine the source of these spoofed IP packets. The most of previous studies to prevent and correspond to DDoS attacks using the traceback mechanism have been accomplished in IPv4 environment. Even though a few studies in IPv6 environment were introduced, those have no detailed mechanism to cope with DDoS attacks. The mechanisms for tracing the origin of attacks in IPv6 networks have so many differences from those of IPv4 networks. In this paper we proposed a lightweight IP traceback mechanism in IPv6 network environment. When marking for traceback is needed, the router can generate Hop-by-Hop option and transmit the marked packet. We measured the performance of this mechanism and at the same time meeting the efficient marking for traceback.

Keywords : *Traceback, IPv6, Probabilistic Packet Marking*

Ⅰ. 서 론

최근 IP기반 네트워크에 위협적인 요소들이 늘어나고 있으며, 그 중 관심의 대상이 되고 있는 것 중 대표적인 것이 Bot이다. Bot을 이용하게 되면 개인의 정보 유출은 물론 다량의 Bot을 이용한 DDoS 공격도 가능하다. 네트워크 위협요소의 증가와 함께 네트워크 보안 기술 또한 발전하고 있다. 대표적인 보안 기술로는 IDS(Intrusion Detection System), IPS(Intrusion Prevention System), 방화벽 등을 들 수 있다. 그러나 기존의 방화벽이나 침입

접수일: 2006년 10월 4일; 채택일: 2007년 2월 28일
* This work was supported by MIC and ITRC Project.
† 주저자, heojoon@khu.ac.kr
‡ 교신저자, cshong@khu.ac.kr

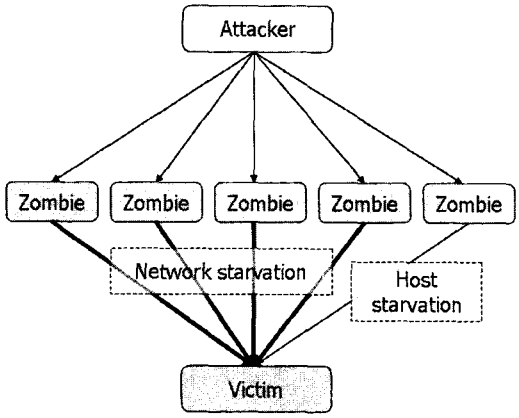
탐지 시스템과 같은 수동적인 보안구조로는 공격의 근원을 차단하지 못하므로 일시적인 방어효과만을 기대할 수 있다. 공격자는 다양한 방법을 동원하여 공격을 시도할 것이므로 수동적인 보안구조만을 사용해 공격을 막는 것은 부족하다고 할 수 있으며, 능동적인 보안기술의 추가적인 적용이 매우 중요하다고 할 수 있다. 수동적인 방어구조는 공격을 탐지하고 단순히 막아주는 기능만을 제공하게 되지만, 능동적인 보안구조가 실제 네트워크에 적용되면 공격이 발생했을 경우 빠른 시간 내에 공격자를 추적, 차단하여 더 이상의 피해를 막을 수 있다. 다시 말해 근원적인 공격 요소를 제거할 수 있기 때문에 추후 공격의 가능성 또한 사라지게 된다[2][3].

대부분의 공격들이 스푸핑된 IP 주소를 사용하는 상황에서 근본적인 공격자를 추적하기 위해 IP 역추적(Traceback) 기술들이 제안되었다. 이러한 기술들은 IP 역추적 기술의 개념을 정리하고, 실제 네트워크에서 유용하게 사용되기 위해 발전하고 있으나, IPv6 네트워크에 대한 고려는 매우 미흡한 실정이다. IPv4 네트워크에 위협을 주었던 요소들은 IPv6 네트워크에도 위협적인 요소가 될 것이며 공격방법은 오히려 발전된 형태를 가질 것이다. 이에 효율적으로 대처하기 위해서는 현재 제안된 기술들을 IPv6 네트워크 관점에서 재고하고 발전시켜야 할 필요성이 있다. IP 역추적 기법의 개발에 있어 가장 중요한 사항은 현재 사용되고 있는 네트워크 및 장비에 최소한의 변경과 기능 추가로 IP 역추적 기술을 구현할 수 있어야 한다는 것이다[11][12].

본 논문에서는 마킹 기법에 기반한 IP 역추적 기술을 IPv6 네트워크에 적용하기 위한 새로운 패킷 공간의 활용 및 경로 재구성 메커니즘을 제안한다. 본 논문은 다음과 같이 구성되었다. 2장에서는 현재까지 IP 역추적 기법으로 제안된 방법들의 특징을 정리하고 장단점을 기술한다. 3장에서는 IPv6 네트워크 환경에 적용할 수 있는 새로운 역추적 메커니즘을 마킹과 경로 재구성 기법을 중심으로 설명한다. 4장에서는 시뮬레이션을 통해 성능을 평가하고, 마지막으로 결론 및 향후 과제에 관하여 논한다.

Ⅱ. IP 역추적(Traceback) 기술

인터넷에서 발생되는 다양한 종류의 공격을 방어하기 위해 방화벽과 침입탐지시스템 같은 보안기술들이 점차 발전하고 있지만 이러한 기술들의 발전에도 불구하고 오늘날 인터넷에 대한 DoS 공격의 위협은 크게 증가하고 있는데, 그 이유 중 한 가지는 자동 공격 툴의 간단한 조작만으로도 넓게 분산된 DDoS 공격이 가능하기 때문이다. 이러한 DDoS 공격은 공격자가 하위에 수많은 좀비(zombie)를 만들어 특정한 호스트를 상대로 동시에 많은 패킷을 전송하여 서비스 불능상태로 만들게 된다.

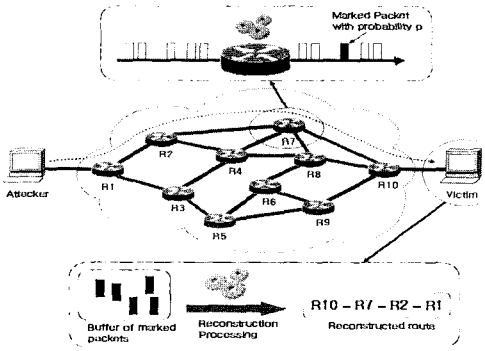


〔그림 1〕 DDoS 공격의 특징

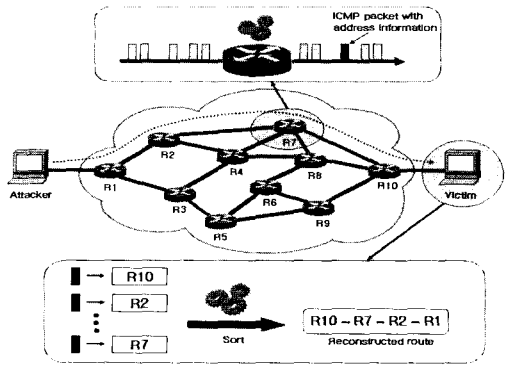
〔그림 1〕은 DDoS 공격의 일반적인 형태를 보여주고 있으며, 다수의 좀비(Zombie)들이 공격자(Attacker)의 의도에 따라 피해 시스템(Victim)에 대한 DDoS 공격을 하고 있다. 실제 DDoS 공격은 훨씬 많은 수의 공격자와 좀비들이 존재하게 되어, 피해 시스템에서 수동적인 방어만으로는 이러한 공격에 효율적으로 대처하기 어렵게 된다. 이러한 상황에서 능동적으로 공격 근원지를 찾아내기 위해 IP 역추적 기술들이 제안되었다[6][7][10]. 대표적인 IP 역추적 기술에는 확률적 패킷마킹[1][4], ICMP 역추적 기법[1][3], 해쉬 기반(Hash-based) 방식[5][14] 등이 있으며, 본 장에서는 이러한 기술들의 특징을 설명한다. 앞서 언급한 것과 같이 현재까지의 대부분의 역추적 기법들은 IPv4 네트워크에 초점을 맞추고 있으나, 기본적인 개념과 특징은 IPv6 네트워크에서도 동일하게 적용될 것으로 기대되고 있다.

2.1 확률적 패킷 마킹(PPM: Probabilistic Packet Marking)

확률적 패킷 마킹기법[1][4]은 스푸핑된 패킷의 실제 전송경로를 찾아내기 위해 라우터에서 패킷이 자신을 지나갔다는 정보를 삽입하는 방법이다. 〔그림 2〕와 같



〔그림 2〕 확률적 패킷 마킹(PPM) 기법



〔그림 3〕 ICMP 역추적 기법

이 라우터는 패킷의 IP 헤더에서 변형 가능한 필드에 자신의 IP 주소를 마킹하여 다음 라우터에 전달한다. 각 라우터에서 삽입된 정보가 경로 중 다음 라우터에 전달되고 최종적으로 피해 시스템에 도달하게 된다. 만약 시스템이 공격을 받았다면 전달받은 패킷 헤더에 기록되어 있는 라우터 정보를 재구성 하여 패킷의 전송 경로를 찾아내는 방법이다. 라우터에서 모든 패킷을 마킹하게 되면 큰 오버헤드가 발생하여 원활한 네트워크 상태를 유지할 수 없기 때문에 패킷에 정보를 기록할 때 일정한 확률 p 로 샘플링 하여 마킹을 한다. 확률적 패킷 마킹(PPM)과 기법은 설치가 간단하고 저렴하다는 장점이 있지만 피해자 측에서 공격경로를 재구성하기 위한 최소한의 패킷을 받아야 한다는 단점을 가지고 있다.

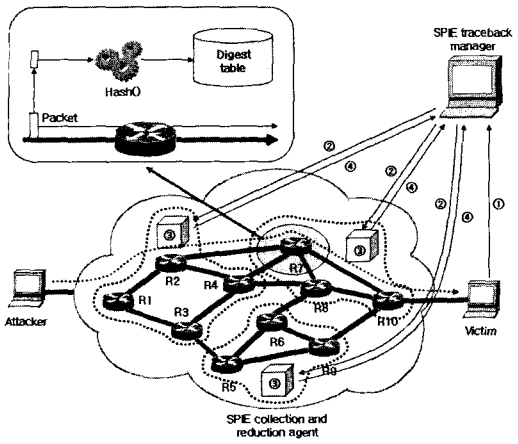
2.2 ICMP 역추적

ICMP 역추적 기법[1][3]은 확률을 이용한다는 점에서 확률적 패킷 마킹 기법(2.1절)과 비슷하지만 다른 접근 방법으로 작동한다. 〔그림 3〕에서 나타내는 것처럼 라우터에서 일정한 확률(일반적으로 1/20,000)로 패킷을 샘플링 하여 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 전달하게 된다. 메시지 생성 시에 TTL(Time To Live) 필드 값은 255로 설정되어 전달되며 목적지에서는 TTL 값이 네트워크상의 홉 거리 정보이므로 공격 경로 재구성에 사용한다.

또한, IPv6 네트워크를 위해 제안된 ICMP 역추적 기술은 IPv6 네트워크에서 모바일 노드(Mobile Node)에 DDoS 공격이 발생할 경우, MN가 HA(Home Agent)에게 ICMPv6 역추적 요구 메시지(Traceback request message)를 보냄으로서 HA가 역추적을 실행할 수 있도록 하는 메커니즘[13]이다. 역추적의 기본적인 개념은 〔그림 3〕과 동일하다. ICMP 역추적기법은 설치가 쉽고 현재 존재하는 프로토콜과 호환이 된다는 장점이 있는 반면 추가적으로 트래픽이 발생하는 단점이 존재한다. 다시 말해, 이 방식은 자체적으로 추가적인 패킷을 생성하므로 네트워크 대역폭에 영향을 줄 수 있다.

2.3 해쉬 기반(Hash-based) 역추적

해쉬 기반 역추적 기법[5][14]은 SPIE(Source Path Isolation Engine) 기반으로 역추적 서버를 구성하고 전체 네트워크를 몇 개의 서브그룹으로 나누어 각 그룹별로 SCAR(SPIE Collection And Reduction Agent)이라는 에이전트를 두어 망을 관리하게 된다. 그리고 각 라우터에는 DGA(Data Generation Agent) 기능을 탑재하여 운영한다. DGA에서는 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬 값에 해당하는 IP 헤더 정보와 8바이트 정보의 페이로드 정보를 수집 관리하고 이를 bloom filter 구조로 저장하게 된다. 만일 〔그림 4〕와 같이 목적지 IDS 시스템에 의해 공격이 발견되는 경우 (①) SPIE 시스템에서는 네트워크 그룹을 관리하는 STM(SPIE Traceback Manager)를 통해(②) 그룹 내 DGA 라우터에 저장된 정보와 공격 패킷 정보를 비교 분석하여(③) 이를 다시 SPIE 시스템에 전달(④)하게 되면 공격 관련 패킷의 전송 경로를 재구성하게 된다. 이 방식을 적용하기 위해서는 STM, SCAR 및 DGA 기능을 구축하여야 하며 추가적인 모듈로 제공되기 때문



〔그림 4〕 해쉬 기반 역추적 기법

〔표 1〕 역추적 기술들의 특징 비교

	단점	IPv4	경량화	DDoS 대응	IPv 6
PPM	- 오버헤드가 커질 수 있음 - 공격경로 재구성을 위한 최소한의 패킷 필요	○	X	X	X
ICMP	- 추가적 트래픽 발생 - 네트워크 성능에 영향을 줄 수 있음	○	X	X	○
SPIE	- 설치비용 많음 - 모든 라우터 DGA 지원 되어야 함.	○	○	X	○

에 서로 다른 환경의 ISP간 적용도 가능하다. 하지만 모든 라우터들이 DGA를 지원하도록 업그레이드되어야 하고 최소 한 개의 STM과 몇 개의 SCAR을 갖추어야 하므로 비용 상의 문제가 크다는 단점이 있다.

앞서 설명한 PPM, ICMP, SPIE 역추적 기술들의 문제점, IPv6 환경에서의 적용 가능성, 경량화 특징, DDoS 공격 대응 가능성을 비교하면 〔표 1〕과 같다.

본 논문에서는 마킹 기법을 기반으로 하는 IPv6 기반 역추적 메커니즘을 제안하고, 동시에 DDoS 공격에 대응할 수 있는 방안과 오버헤드를 줄이기 위한 경량화 방법을 제안한다.

Ⅲ. IPv6기반 경량화 역추적 제안 기법

앞서 소개한 대표적인 IP 역추적 기법 중 현재 구성되어 있는 네트워크에 가장 간단하고 경량으로 설치할 수 있는 것은 마킹(marking) 기법을 이용한 알고리즘(2.1절)이다. 마킹 기법은 네트워크에 추가적인 장비를 설치할 필요 없이 현재 구성되어 있는 라우터에 마킹 관련 알고리즘을 설치하고 피해 시스템에서 공격경로를 재구성하는 알고리즘만 실행할 수 있으면 된다. 지금까지 제안된 대부분의 마킹 기법들은 라우터에서 패킷에 정보를 기록할 때 IPv4 패킷 헤더의 인식 필드(Identification field)에 기록하는 방법을 사용하였다. 이것은 IP 헤더의 분할을 위하여 패킷의 동일성을 표시하는 인식 필드(Identification field)를 사용할 확률이 0.25%정도밖에 되지 않는다는 점에 착안하여 사용한 것이다[2][12]. 이 방법은 IPv6 네트워크에서는 사용될 수 없으며 새로운 마킹 기법과 경로 재구성 방법이 정의되어야 하며, 이 부분이 본 논문의 최종 연구 목표라고 할 수 있다.

본 논문에서 제안하는 메커니즘을 위해 다음과 같은 사항을 가정한다.

① 모든 라우터들은 IP 역추적 모듈이 지원되어 마킹 기능이 가능하다.

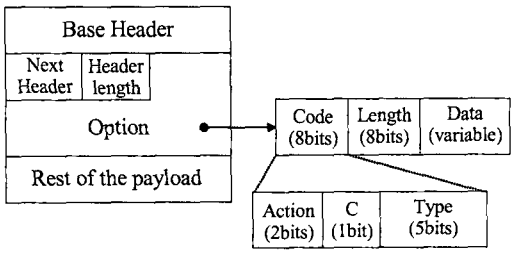
② 홉간 옵션(Hop-by-Hop Option)은 발신지가 데이터그램을 거치는 모든 라우터에 정보를 전달할 필요가 있을 경우 사용되지만, 본 논문에서는 IPv6 에서의 Router Alert 메커니즘[9]처럼 중간라우터가 호스트기능(Host Function)을 수행할 수 있다고 가정한다. 다시 말해, 중간 라우터는 역추적을 위해 IPv6 패킷에 마킹을 해야 할 필요가 있을 경우 해당 패킷에서 기본헤더(Basic Header) 정보를 복사하고, 마킹 정보를 기재한 홉간 옵션을 생성하여 복사된 주소정보를 통해 전송할 수 있다.

③ 피해 시스템(Victim)과 최종 연결된 라우터는 경로 재구성을 수행할 수 있는 에이전트(Agent) 기능을 가지고 있다.

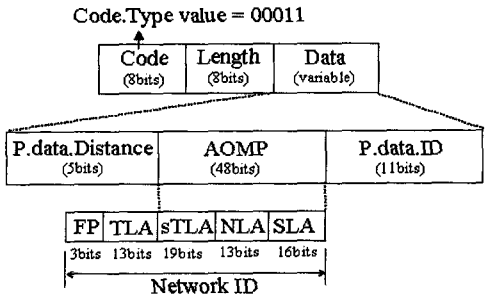
④ 공격경로를 재구성하는 과정에서 밝혀진 공격경로상의 라우터들은 공격패킷의 정보를 피해시스템으로부터 전송받아 해당 패킷을 필터링하여 공격에 실시간으로 대응할 수 있다.

3.1 IPv6 패킷에서 마킹 공간의 사용

〔그림 5〕는 IPv6 확장 헤더(Extension Header) 중의 하나인 홉간 옵션(Hop-by-Hop) 헤더[8]의 구조를 나타



〔그림 5〕 홉간(Hop-by-Hop) 옵션 헤더 구조

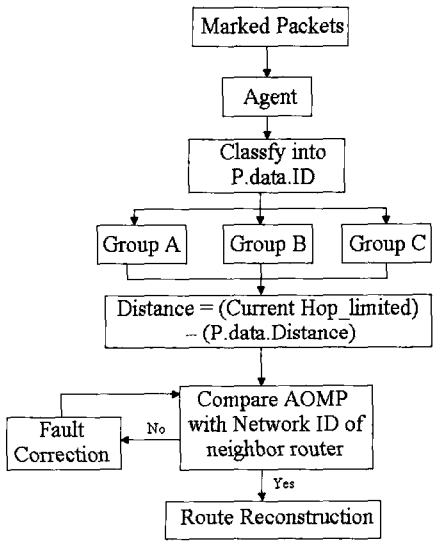


〔그림 6〕 마킹 정보 정의

내고 있다. 이 헤더는 발신지가 데이터 그램을 거치는 모든 라우터에 정보를 전달할 필요가 있을 경우 사용되며, IPv6 표준에 따라 모든 노드에서 처리가 가능하다. 앞서 가정한 내용처럼 본 논문에서는 IPv6 에서의 Router Alert메커니즘[9]처럼 중간라우터가 호스트기능(Host Function)을 수행할 수 있다고 가정한다. 따라서, IPv6 헤더 공간 중 IP 역추적에 사용하기에 가장 적합하다고 할 수 있다. 헤더의 크기 또한 자유롭기 때문에 필요한 정보를 삽입하는데 있어서 공간을 충분히 사용할 수 있다는 장점이 있다.

3.2 마킹 정보 정의 및 사용

〔그림 6〕은 홉간 옵션 필드 중 데이터(Data) 필드에 마킹에 필요한 인자들을 어떻게 정의하고 사용할 것인지에 대하여 설명하고 있다. 먼저 Code.Type을 00011로 새롭게 정의하여 역추적을 위한 패킷임을 구별할 수 있게 한다. 본 논문에서 제안하는 방법은 P.data.Distance, AOMP(Address of Marking Point), P.data.ID 라는 3가지 인자 값을 데이터 필드에 마킹한다. P.data.Distance 값은 경로 재구성시 공격자에 가까운 정도를 계산하기 위한 절차에 사용되며, 마킹 시점에서 현재 기본헤더의 홉제한(Hop_limited) 값의 뒤쪽 5비트 값을 마킹한다. AOMP 필드는 마킹된 라우터를 식별하기 위한 필드로서 라우터 주소의 Network ID 64비트 중 FP와 TLA에 해당하는 16비트를 제외한 48비트를 마킹한다. FP와 TLA는 16비트의 공간을 가지고 있지만 현재 3ffe , 2001, 2002 의 3개의 값만이 사용되고 있기 때문에 마킹 라우터 식별에 큰 영향을 주지 않는다[8]. 이러한 방법을 사용하게 되면 실제 IPv6의 주소 128bit 마킹이 아닌 48bit으로 사용하게 되고, 총 마킹 공간을 64bit으로 감소시킴으로써 마킹을 할 때 생기는 부하를 경량화 할 수

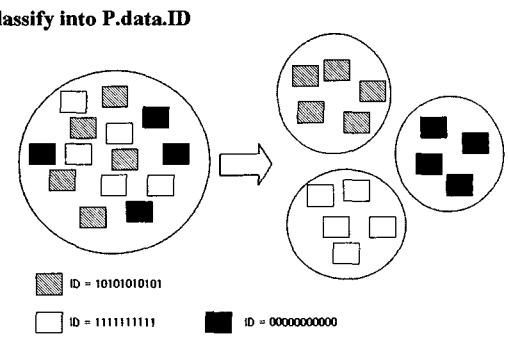


〔그림 7〕 경로재구성 절차

있다. 마지막으로 P.data.ID 필드는 DDoS 공격이 탐지되었을 때 이들의 경로를 공격자별로 분류하기 위한 것으로 패킷의 근원주소(Source Address)의 인터페이스 ID를 11비트로 해싱(hashing) 하여 마킹한다. 여기에서의 인터페이스 ID는 라우터의 MAC 주소를 의미하는 것이 아니라 라우터가 여러 개의 네트워크에 연결되어 다수의 인터페이스를 갖는 경우 해당 네트워크와 연결된 네트워크 주소를 의미한다.

3.3 경로재구성 기법

제안된 IP 역추적의 궁극적인 목표는 공격이 탐지되면 패킷에 마킹된 정보를 통해 경로를 재구성하여 공격자에 가장 근접한 지점을 찾는 것이다. 앞절(3.2절)에서 정의한 마킹 공간을 이용한 경로재구성 기법의 전체 과정은 〔그림 7〕과 같다.

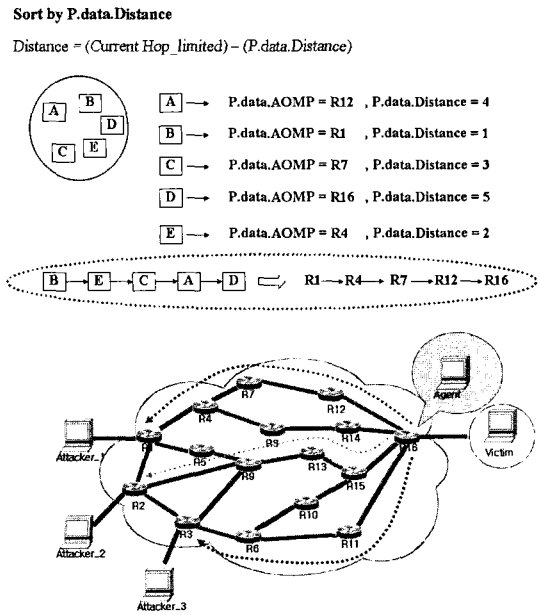


〔그림 8〕 P.data.ID 필드를 이용한 패킷의 그룹별 분류

먼저 3가지 인자(P.data.Distance, AOMP, P.data.ID) 중 P.data.ID값을 이용하여 패킷을 공격자별로 분류한다. P.data.ID값은 근원지 주소(Source Address)의 인터페이스 ID를 11bit으로 해싱한 값으로 공격자를 피해자 측에서 분류하기 위해 사용한다. 이는 경로 재구성시 DDoS처럼 여러 곳에서 분산되어 오는 공격의 경우 여러 가지 경로의 정보들이 섞이지 않게 하기 위함이다.

〔그림 8〕은 위에서 설명한 과정을 예를 들어 도식화하고 있다. 각각 P.data.ID 값이 10101010101 인 패킷과 11111111111인 패킷 그리고 00000000000인 패킷이 섞여 있으며 이를 마킹된 P.data.ID값을 기준으로 그룹화하는 것을 나타내고 있다. P.data.ID 값으로 분류된 패킷 그룹은 그룹 별로 P.data.Distance값에 의해 정렬된다. 최종 Distance값은 재구성 시점에서의 Hop_limited 값과 마킹된 P.data.Distance 값의 차이를 최종 값으로 하고 이 값에 의해 정렬을 실시한다. 홉제한(Hop_limited) 값은 Hop을 하나 지날 때 마다 1씩 증가한다. 따라서 정렬을 실행할 때 최종 값(Hop_limited - P.data.Distance)이 크면 클수록 공격자에 가깝게 위치한다는 뜻이다. 최종 Distance값에 의한 내림차순 정렬이 끝난 그룹은 정렬된 맨 마지막 값, 즉 피해 시스템에 가장 근접하다고 판단되는 라우터의 AOMP값을 자신과 인접한 라우터의 Network ID와 비교하여 같을 경우 경로의 하나로 채택한다. 그리고 이 채택된 라우터에서 가장 근접 하다고 판단되는 것의 AOMP값을 채택된 라우터의 인접한 라우터의 Network ID 와 비교하여 다음번 라우터로 채택한다. 이러한 과정을 정렬된 값의 첫 번째 값이 올 때까지 반복하여 경로를 재구성한다.

〔그림 9〕는 앞서 설명한 P.data.Distance 값에 의한 정렬과 AOMP값에 의한 경로의 구성의 예를 보여주고 있다. 여기서 에이전트(Agent)는 피해 시스템(victim)에

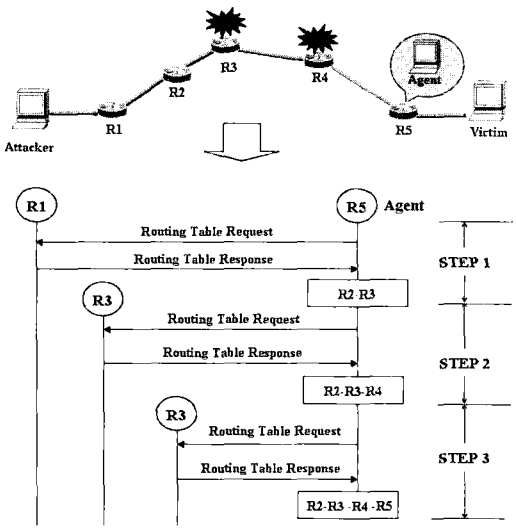


〔그림 9〕 Distance 값과 AOMP값을 이용한 경로의 재구성

연결된 라우터에서 공격이 발생하고 있는 지를 판별하고, 그럴 경우 확보된 마킹 정보에 의해 경로 재구성을 하는 기능을 담당하고 있다. 일반적인 IDS나 IPS의 모듈에 경로 역추적 기능이 추가되는 것이 가장 이상적인 에이전트(Agent)의 기능이라고 할 수 있다. 먼저 각각의 P.data.Distance 값은 A=4, B=1, C=3 D=5 E=2 의 값을 가지고 있다. 이때, 경로 재구성 시점에서의 Hop_limited 값이 5라고 하면 최종 Distance 값은 각각 A=1, B=4, C=2, D=0, E=3 이 된다. 따라서, 피해 시스템 측에 가장 근접 하다고 판단할 수 있는 것은 D이다. 이때 D가 지니고 있는 AOMP정보, 즉 라우터 주소의 Network ID 값을 D의 인접 라우터들과 비교하여 R16과 일치함을 확인할 수 있다. 다음으로 A가 지니고 있는 AOMP 정보를 R16과 인접 하고 있는 라우터들과 비교해 보면 R12의 Network ID 값과 일치함을 알 수 있다. 이러한 방식으로 C, E, B의 순으로 경로를 재구성해 나간다. 결국 B의 AOMP 값과 R4의 인접한 라우터들의 Network ID 값을 비교 하여 R1을 도출 하는 시점에서 경로 재구성이 마무리 된다.

3.4 경로 재구성시 오류정정 기법

본 논문에서 제안하는 PPM기반 마킹 기법은 경로



〔그림 10〕 경로 재구성 오류 정정 기법

재구성시 마킹이 되지 않은 라우터가 존재할 수 있다. PPM기법의 경우 마킹 빈도를 높이면 경로 재구성이 정확하게 될 확률은 높아지지만 시스템의 성능은 오히려 낮아지게 된다. 따라서, 마킹할 확률(p)을 적당한 수준에서 결정할 필요가 있다. 이러한 이유로 인해 마킹 확률이 낮아져 P.data.Distance 값이 연속되지 않을 경우 경로의 재구성은 완벽하게 이루어지지 못할 수 있다. 본 장에서는 PPM기법에서 경로가 완벽하게 재구성 되지 않았을 경우 문제를 보완할 수 있는 방법을 제시한다. 본 논문에서는 가장 일반적인 라우팅 프로토콜을 사용하는 경우를 가정하고 설명한다. 즉, IPv6에서 RIP프로토콜을 사용해 라우팅 테이블을 관리하는 경우 라우팅 테이블은 각각 Destination, Next Hop, flags, Metric, Ref, Use, interface 로 정의된다. 경로 재구성 실패 시 오류정정 기법에는 이러한 필드 중 Destination과 Next Hop 필드를 사용한다. 본 장에서 제안하는 경로 구성을 〔그림 10〕의 예를 들어서 설명 하면, 먼저 경로 재구성 중 'R3'와 'R4'에 대한 경로 정보가 없을 경우를 가정한다. 이때 피해 시스템의 Agent는 재구성시 사용한 P.data.Distance 정보를 이용하여 'R2'에서부터 'R5'사이의 정보가 없다는 것을 알 수 있다. 또한 재구성되지 않은 부분이 각각 'R2'의 다음 구간과 그 다음 구간이라는 것도 알 수 있다.

① STEP1: Agent는 'R2'에게 Destination이 'R5'인 라우팅 테이블의 Next Hop을 요청하는 Routing Table Request Message를 보낸다. 'R2'는 Destination이 'R5'인 라우팅 테이블의 Next Hop 정보를 Routing Table Response Message에 담아 피해 시스템의 Agent로 보낸다. 이를 받은 피해자 측의 Agent는 'R2'의 다음 홉이 'R3'임을 알 수 있다.

② STEP2: 피해 시스템의 Agent는 'R2'의 다음 홉이 'R5'가 아님을 확인하고 'R3' 에게 Destination이 'R5'인 라우팅 테이블의 Next Hop을 요청하는 Routing Table Request Message를 보낸다. 이를 받은 'R3'는 Destination이 'R5'인 라우팅 테이블의 Next Hop 정보를 Routing Table Response Message에 담아 피해 시스템의 Agent로 보낸다. 이를 받은 Agent는 'R3'의 다음 홉이 'R4'임을 알 수 있다.

③ STEP3: 피해 시스템의 Agent는 'R3'의 다음 홉이 'R5'가 아님을 확인하고 'R4'에게 Destination이 'R5'인 라우팅 테이블의 Next Hop을 요청하는 Routing Table Request Message를 보낸다. 이를 받은 'R4'는 Destination이 'R5'인 라우팅 테이블의 Next Hop 정보를 Routing Table Response Message에 담아 피해 시스템의 Agent로 보낸다. 이를 받은 Agent는 'R4'의 다음 홉이 재구성이 실패한 마지막 부분의 다음 라우터인 'R5'임을 알 수 있다.

Ⅳ. 성능평가

성능평가 부분에서는 제안된 IPv6 역추적 알고리즘을 다른 IPv6 역추적 기법과의 정성적인 평가로 장단점을 비교하고 정량적 평가를 이용하여 제안된 방법의 성능을 측정한다. 평가지표는 다음과 같다.

① 정성적 평가에 따른 특징 비교
② 마킹확률에 따른 역추적 정확도
③ 패킷수에 따른 역추적 정확도

〔표 2〕는 본 논문에서 제안한 방법과 기존에 제안된 방법을 정성적으로 비교한 결과이며, 비교 대상은 ICMPv6 기법[12]과 SPIEv6 기법[14]이다. 〔표 2〕와 같이 본 논문에서 제안하는 방식은 확장성 및 경로 재구성을 위한 오버헤드, 요구 메모리와 보안 강도에서 기존의 방법보다 효율적인 특징을 가지고 있음을 알 수 있다.

또한, 3.2절에서 설명한 것처럼 마킹 공간을 확보하고 정보를 마킹함에 있어 불필요한 부분을 제외함으로

〔표 2〕 IPv6 기반 역추적 기법의 비교

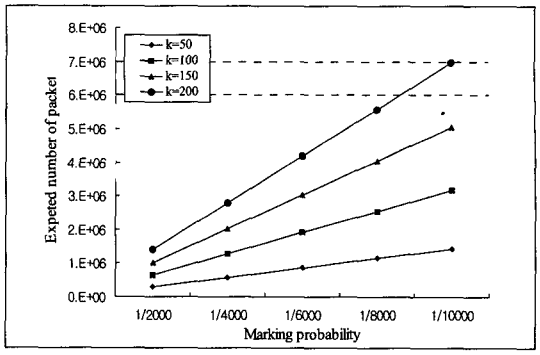
		Proposed scheme	ICMPv6	SPIEv6
ISP involvement		Low	Low	Fair
Scalability		High	High	Fair
Number of attack packets required for traceback		Thousands	Thousands	1
Network processing overhead	Every packet	Low	Low	Low
	During traceback	None	None	Low
Victim processing overhead	Every packet	None	None	None
	During traceback	High	High	None
Bandwidth overhead	Every packet	None	Low	None
	During traceback	None	None	Low
Memory requirements	Every packet	None	Low	Fair
	During traceback	High	High	None
Lightweight		○	X	X
DDoS Protection		○	X	X

〔표 3〕 시뮬레이션 변수

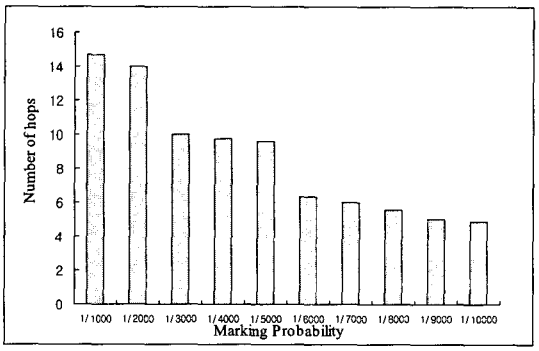
변 수	값
경로 상에 존재하는 홉(라우터)의 개수	15
각 라우터를 지나는 서로 다른 Source Address (Zombie)를 갖는 패킷의 종류	250
고정된 마킹의 확률 (p)	1/2000
고정된 정보 확보 량	1,000,000

써 역추적 기법의 경량화에 초점을 맞추었으며, P.data.ID에 따른 그룹을 형성함으로써 분산된 공격에 대응할 수 있도록 하였다. 그러나, 경로 재구성을 위해서는 어느 정도의 패킷이 확보되어야하고, 역추적을 위한 프로세스 오버헤드가 발생하는 단점을 가지고 있다. 정량적 평가의 경우 IP 역추적 방법이 가능한 네트워크를 구축하여 실험하기 어렵고, 현재 IPv6 네트워크에서 IP 역추적을 지원하는 시뮬레이터가 존재하지 않으므로 성능평가를 위한 도구로 본 논문에서 제안한 IP 역추적 경로 재구성 시뮬레이터를 Java로 구현하였다.

경로상의 전체 라우터(hop)의 개수를 15개로 지정하고 이에 대하여 마킹확률의 변화와 확보된 정보량의 변화를 통해 경로 재구성이 가능한 홉의 개수를 측정하였다. 〔표 3〕은 시뮬레이션에 사용된 변수와 기본 값을 나타내고 있다.



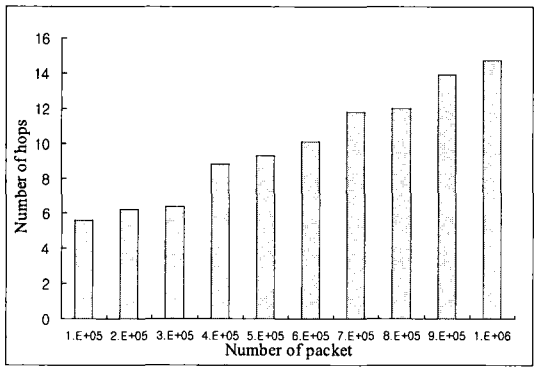
〔그림 11〕 공격자 숫자별 경로 재구성시 필요한 패킷의 수



〔그림 12〕 마킹 확률에 따른 경로 재구성 완성도

〔그림 11〕은 일반적으로 마킹확률과 거리에 따른 계산에 활용되는 $E(N)=\frac{k^*\ln(k^*d)}{p(1-p)^{d-1}}$ 공식을 이용했을 경우 나타난 결과로서, 공격자의 수 k 가 각각 50,100,150,200 일 때 마킹 확률(p)별로 경로 재구성을 하기 위해 필요한 패킷의 수(expected number of packet)를 나타내고 있다. 여기에서 d 는 공격노드로부터 피해노드에 이르는 거리(distance)를 의미한다. 이 결과에서 볼 수 있듯이 공격노드가 많을수록, 다시 말해 DDoS 공격에서 좀비의 숫자가 많아질수록 경로를 역추적 하기 위해 필요한 패킷의 수는 크게 증가됨을 알 수 있다. 또한, 마킹 확률이 감소함에 따라 필요한 패킷의 수가 급격하게 증가하는 것을 볼 수 있다.

〔그림 12〕는 피해 시스템에서 경로 재구성을 담당하는 에이전트(Agent)가 100만개의 패킷을 바탕으로 경로를 재구성할 경우 정확한 역추적이 가능한 홉수를 나



〔그림 13〕 확보한 패킷의 수에 따른 경로 재구성 완성도

타내고 있다. 이 실험에 사용된 전체 홉수는 15이며, 각각의 라우터를 지나는 서로 다른 근원지 주소는 250개이다. 실험 결과에서 알 수 있듯이 마킹 확률이 1/1000과 1/2000인 경우 매우 높은 역추적 성공률을 나타내고 있으나, 1/3000확률에서 그 값이 급격하게 낮아지는 것을 알 수 있다. 이 결과는 두 가지로 예측할 수 있을 것이다. 첫 번째는 이 실험과 같은 조건에서는 1/2000이상의 마킹 확률로 패킷에 마킹을 할 경우 매우 높은 정확도를 가질 수 있다는 것이며, 두 번째로 논문에서 실시한 결과 값이 100번 반복에 의한 평균값임에 비해 마킹 확률이 1/1000-1/10000로 매우 커서 결과의 정확도가 어느 정도 차이를 나타내고 있다고 해석할 수 있을 것이다.

〔그림 13〕은 마킹확률이 1/2000, 전체 홉수 15 그리고 각각의 라우터를 지나는 서로 다른 근원지 주소는 250개인 환경에서 피해 시스템의 에이전트에서 확보된 정보(패킷)를 통해 어느 정도 정확한 역추적이 가능한가를 나타내는 실험 결과이다. 이와 같은 환경에서는 90만에서 100만 사이의 정보를 확보한 경우 15에 근접한 역추적 경로를 찾아낼 수 있음을 나타내고 있다.

V. 결론 및 향후과제

네트워크에서 행하여지는 다양한 공격을 막기 위해서는 지금까지 존재하는 방화벽과 침입탐지 시스템과 같은 수동적인 방어 방법만을 가지고는 근본적인 문제를 해결하기 어렵다. 본 논문에서는 PPM 기법 기반의 IP 역추적 방법을 IPv6 네트워크에 최적화 하는 방안을 제시하였다. 또한, 경로 재구성 실패 시 오류 정정 알고리즘을 제시하였다. 향후 과제로는 제안한 메커니즘의 성능향상과 실제 적용을 위한 요구사항을 도출하여 문제가 있을 경우 개선책을 고려해야 할 것이다. 또한 IP 역추적 기법이 동작하기 위해서 선행되어야할 공격의 탐지 기법과의 연계과정에 관한 부분도 연구되어야한다.

참고문헌

〔1〕 Belenky A. and Ansari N., "On IP Traceback," IEEE Communications Magazine, vol. 41, Issue 7, July 2003.

〔2〕 S. Savage et al., "Network Support for IP Traceback," IEEE/ACM Trans. Net., vol. 9, no. 3, pp. 226-237, June 2001.

〔3〕 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.

〔4〕 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.

〔5〕 Strayer W. T., Jones C. E., Tchakountio F. and Snoeren A. C., "SPIE demonstration: single packet traceback," Architecture DARPA Information Survivability Conference and Exposition2003 Proceedings, vol. 2, pp. 106-107, April 2003.

〔6〕 Minho Sung and Jun Xu, "IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 14, Issue 9, pp. 861-872, September 2003.

〔7〕 Aljifri H., "IP traceback: a new denial-of-service deterrent," IEEE Security & Privacy Magazine, vol. 1, Issue 3, pp. 24-31, June 2003.

〔8〕 W. Stevens and M. Thomas, "Advanced Sockets API for IPv6," RFC 2292, February 1998.

[9] C. Partridge and A. Jackson, "IPv6 Router Alert Option," RFC 2711, October 1999.
[10] 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.
[11] 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.
[12] 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.
[13] Henry C.J. Lee, Miao Ma, Vrizlynn L.L. Thing and Yi 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.
[14] W. Timothy Strayer and Fabrice Tchakountio, "SPIE-IPv6 : Single IPv6 Packet Traceback," Proceedings of the IEEE Internation Conference on Local Computer Networks, pp. 118-125, Nov. 2004.

〈著者紹介〉

허 준 (Joon Heo) 준회원
2002년 2월: 경희대학교 컴퓨터공학과 졸업
2004년 2월: 경희대학교 컴퓨터공학과 석사
2004년 3월~현재: 경희대학교 컴퓨터공학과 박사과정
<관심분야> 유무선 네트워크 보안, 보안 게이트웨이, 암호기술

홍 충 선 (Choong Seon Hong) 정회원
1983년: 경희대학교 전자공학과 졸업 (학사)
1985년: 경희대학교 전자공학과 (공학석사)
1997년: Keio University, Department of Information and Computer Science (공학박사)
1988년~1999년: 한국통신 통신망 연구소 수석연구원/ 네트워킹연구실장
1999년~현재: 경희대학교 전자정보학부 부교수
<관심분야> 네트워크 보안, 인터넷 서비스 및 망관리 구조, 분산 컴포넌트 관리, IP 프로토콜, 센서 네트워크

강 명 수 (Myung Soo Kang) 준회원
2004년 8월: 경희대학교 컴퓨터공학과 졸업
2006년 8월: 경희대학교 컴퓨터공학과 석사
2006년 9월~현재: (주)플랜티넷 교육사업본부 교육서비스 개발팀 연구원
<관심분야> IPv6 보안, 네트워크 보안, 네트워크 프로그래밍