것은 결국 목적지 시스템과 라우터 간에 IPSec으로 채널을 구성하고 트래픽에 대한 확인 과정을 수행한다는 것이다. 결국 역추적 과정에서 IPSec으로 채널이 구성된 네트워크 그룹과 공격자가 포함되어 있는 비 IPSec 기반 일반 네트워크 간의 연계 기능을 제공해야 한다.

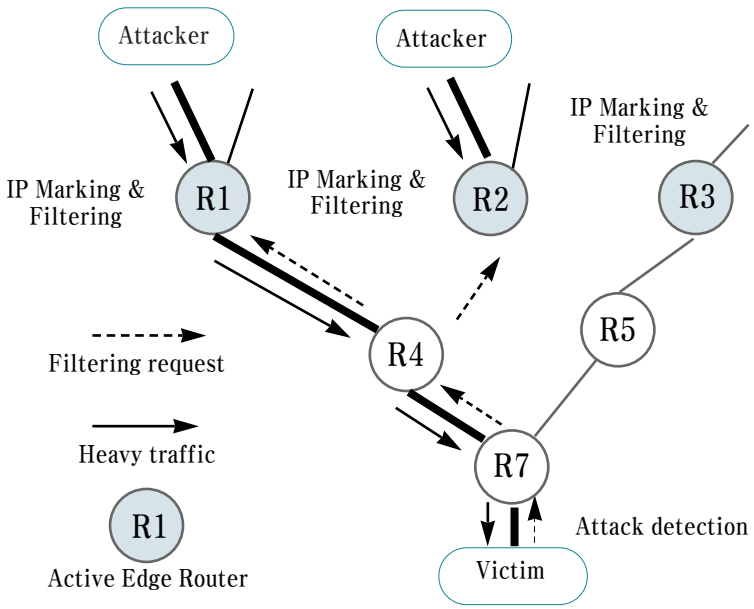
3. Deterministic Pushback 기법을 이용한 역추적 기술

네트워크 및 시스템에 치명적인 DDoS 공격을 탐지하였을 때, 가장 중요한 것은 공격에 대해서 어떻게 대응하느냐 하는 문제이다. 현재까지 제안된 대부분의 방안들의 경우, DDoS 공격 패킷은 공격을 탐지한 네트워크에 위치한 라우터나 방화벽 등에 의해서 필터링을 실시한다. 이와 같이 공격대상 시스템에서 공격 패킷을 제거함으로써, 공격대상 시스템은 공격에 대한 피해를 줄일 수 있다. 하지만 현재 발생하고 있는 DDoS 공격들의 경우 특정 호스트뿐만 아니라 네트워크 자체를 노린다는 특징도 가지고 있다. 따라서, 공격 패킷의 근원지를 파악하고, 공격 근원지에서 공격 패킷에 대하여 필터링을 실시하여 공격 패킷이 외부네트워크로 유입되는 것을 막는 기법이 필요하다. Deterministic Pushback 기법을 이용한 공격자 위치 역추적 및 대응 기술은 공격자가 위치한 네트워크의 에지라우터에서 외부로 나오는 공격 패킷을 필터링 함으로써 전체 네트워크를 대상으로 수행되는 공격에 효과적으로 대응이 가능하다.

가. Deterministic Pushback 기법을 이용한 역추적 기술 구조

[그림 9]는 Deterministic Pushback 기법을 이용한 역추적 및 공격 대응 기술의 구조를 나타내고 있다. 그림에서 굵은 선은 공격 패킷의 흐름을 나타내고 가는 선은 합법적인 패킷을 나타내고 있다. 그리고 화살표는 공격대상 시스템에서 전송하는 Pushback 메시지를 나타내고 있다. 이 기법은 크게 3단계로 DDoS 공격에 추적 및 대응을 실시한다. 첫 번째 단계는 사전 단계로 R1, R2, R3과 같이 호스트와 직접 연결된 모든 에지라우터들은 자신이 담당하고 있는 네트워크에서 발생한 모든 패킷에 자신의 IP주소를 마킹한다. 두 번째 단계는 공격 탐지와 Pushback 메

시지 전송단계로, 공격대상 시스템에서는 DDoS 공격을 탐지한 후, 공격 패킷에 마킹되어 있는 정보를 이용하여 공격자가 위치한 에지라우터의 IP 주소를 확인하고, 공격자가 속한 네트워크의 에지라우터로 Pushback 메시지를 전송한다. 현재까지 제안된 DDoS 공격 탐지의 대부분의 방법은 공격자가 IP 주소를 위장하는 기법을 사용할 경우 공격의 근원지를 알지 못하기 때문에 공격에 적절히 대응하는데 문제점이 있었다. 하지만 이 기법의 경우 공격자가 위치한 네트워크의 에지라우터에서 패킷이 발생한 위치를 정확히 나타내어 주기 때문에 IP 주소 위장으로 인해 발생하는 공격지 판단의 부정확성 문제를 해결할 수 있다. 세 번째 단계는 패킷 필터링 단계로 Pushback 메시지를 전송받은 에지라우터들은 내부 네트워크에서 공격대상 시스템으로 전송되는 패킷을 공격대상 시스템의 요구에 의해 차단한다. Pushback 메시지에는 공격대상 시스템의 주소와 공격대상 시스템이 제한하는 대역폭 정보 그리고 필터링의 기간이 명시되어 있다. 따라서 에지라우터는 이 정보들을 이용하여 내부 네트워크에서 공격대상 시스템으로 전송되는 패킷의 대역폭을 공격대상 시스템이 요구한 기간 동안 제한이 가능해진다.

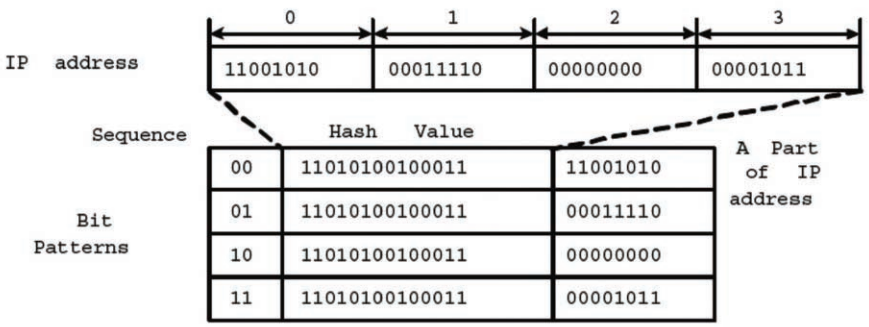


[그림 9] Deterministic Pushback 기법을 이용한 역추적

나. 에지라우터 패킷 마킹 기법

Deterministic Pushback 기법에서 에지라우터의 첫 번째 역할은 자신의 IP 주소를 내부 네트워크에서 발생한 모든 패킷에 표시하는 것이다. 에지라우터가 자신의 IP 주소를 내부 네트워크에서 발생한 모든 패킷에 표시하는 이유는 DDoS 공격의 경우 대부분의 공격자는 자신의 위치를 숨기고 효율적인 공격을 위해 IP 주소 위장을 사용하기 때문이다. 즉, 에지라우터가 자신의 IP 주소를 패킷에 표시해 줌으로써 공격자가 IP 주소 위장을 사용하더라도 공격대상 시스템은 그 패킷이 발생한 위치를 정확히 판단할 수 있다. 하지만 IP 헤더의 경우 에지라우터의 IP를 표시할 수 있는 영역이 없다. 이를 해결하기 위한 방안으로 IP 헤더의 옵션필드에 IP주소를 표시하는 방안을 생각해 볼 수 있으나 이 경우 불필요한 네트워크 자원의 소모와 현재 구축된 네트워크와의 호환성에도 문제가 발생할 수 있다. 따라서 Deterministic Pushback 기법에서는 IP 분할을 이용하여 에지라우터의 IP주소를 표시하는 방안을 제안하였다.

본 기법에서는 마킹으로 인해 패킷 사이즈가 증가하는 것을 피하기 위하여 데이터그램 부분인 IP 및 TCP 옵션 필드를 이용하여 에지라우터의 IP주소를 마킹한다. 특히, TCP/IP 프로토콜 상에서 사용되지 않는 Identification 필드와 Type of Service(TOS) 필드를 이용한다. 이때 이들의 저장 공간이 24비트이므로, 32비트의 IP 주소 정보를 저장하는데 어려움이 있다. 따라서 본 기법에서는 4개 부분으로 IP 주소 정보를 나누어서 저장하는 방법을 사용하였다. [그림 10]은 24 비트의 공간에 32비트의 IP주소 정보를 저장하는 방법을 설명하고 있다. 하나의 비트



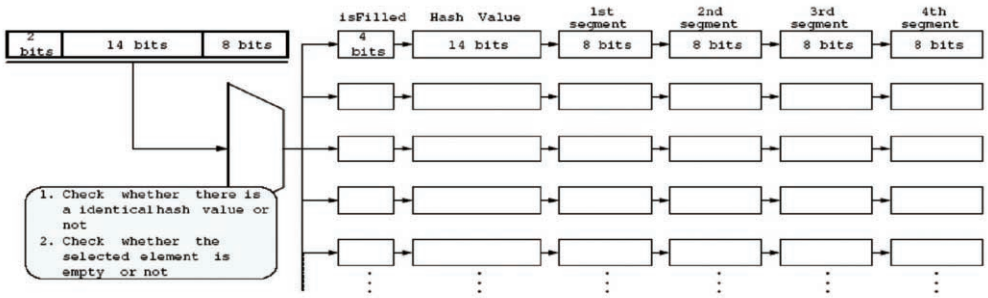
[그림 10] 에지라우터에서 IP 주소정보 마킹 방법

패턴은 3가지 파트(Sequence 정보, Hash Value 및 IP 주소의 일부 8 비트정보)로 구성된다. Sequence 정보는 IP 주소 정보의 해당 부분을 구분하며, Hash Value는 전체 IP 주소에 대한 해쉬 값을 저장하며, 다음의 8 비트 정보는 해당 IP 주소의 일부분을 나타낸다. 이들 정보를 이용하여 공격대상 시스템에서는 해당 패킷에 대한 근원지 에지라우터의 IP 주소 정보를 획득할 수 있다.

다. 에지라우터 IP 주소 확인 방법

공격대상 시스템은 DDoS 공격을 탐지하고 공격과 관련된 정보를 Pushback 메시지를 이용하여 공격 근원지 에지라우터에게 전송한다. 이때, DDoS 공격에 대한 탐지는 IP 헤더의 소스 IP 주소정보를 이용하는 것이 아니라 에지라우터의 IP 주소정보를 이용하여 수행한다. 즉, DDoS 공격의 경우 대부분 IP 주소 위장을 사용하기 때문에 DDoS 공격이 이루어지는 동안 패킷의 소스 IP 주소는 의미를 지니지 못한다. 반면, 앞서 설명하였듯이 에지라우터의 주소는 공격자가 위장하는 것이 불가능하기 때문에 공격의 근원지 탐지를 위해 이 정보를 이용하는 것이 더욱 효과적이다.

본 기법에서는 공격대상 시스템에서 공격을 탐지한 경우 Pushback 메시지를 재구성된 경로를 이용하여 공격자가 위치한 네트워크의 에지라우터로 직접 전송한다. **[그림 11]**은 본 기법에서 분할된 에지라우터의 IP 주소를 재구성하기 위한 해쉬 테이블 형태의 자료구조를 나타내고 있다. 공격대상 시스템은 공격상황을 감지할 경우 IP 헤더의 TOS필드와 Identification 필드에 저장된, 에지라우터의 분할된 IP 주소 정보를 재조합한다. 공격대상 시스템은 공격 패킷에 대한 해쉬 값의 비트 패턴을 관찰한다. 이때 새로운 해쉬 값이 나오면 주소 체인에 새롭게 추가한다. 같은 해쉬 값을 갖는 비트 패턴에 대해서는 Sequence 값을 이용하여 정렬을 실시한다. IP주소 정보의 순서를 나타내는 2bits 정보와 8bits 이전 분할 부분과의 중복 값을 이용하여 분할된 부분이 전체 IP주소에서 차지하는 위치를 찾아낸다. 공격대상 시스템은 먼저 2bits 순서 값을 이용하여 주소 체인에서 입력 받은 주소가 차지하는 위치를 알아낸다. 분할된 주소의 위치를 찾아낸 경우 8bits 중복 값과 이전 분할의 마지막 8bits 값과의 비교를 통해 분할된 값이 어느 주소체인에 포함되어야 하는지를 찾아낸다. 만약 동일한 8bits 값을 찾지 못한 경우 새로운 주소 체인을 형성한다. 이러한 방법을 이용하여 공격 패킷들에 대한 에지라우터 IP 주소정보를 획득할 수 있다.



[그림 11] IP 주소 재조합 기법

라. 에지라우터에서의 공격 패킷 필터링

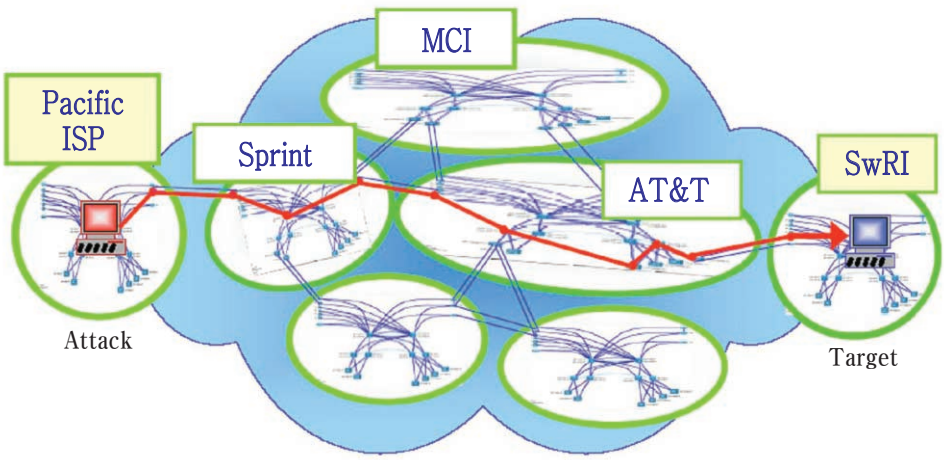
에지라우터의 두 번째 역할은 공격대상 시스템에서 보내온 Pushback 메시지를 기반으로 공격 패킷을 차단하는 것이다. Pushback 메시지는 공격대상 시스템의 IP 주소, 허용하는 대역폭의 크기, 필터링의 기간이 포함되어 있다. 에지라우터는 공격대상 시스템의 IP 주소를 통해 내부 네트워크에서 공격대상 네트워크로 전송되는 패킷은 의심스러운 패킷으로 판단하고, 필터링을 실시한다.

Deterministic Pushback 기법은 소스 주소에 대하여 IP 주소를 위장하여 전송하는 공격에 대해서도 효과적으로 대응이 가능하다는 장점과 기존 PPM 기법처럼 패킷이 경유하는 모든 라우터에서 마킹을 하지 않아도 된다는 장점을 갖는다. 또한 DDoS, 봇넷 및 인터넷 웜 공격에 대하여 공격 근원지에서 공격 패킷을 필터링이 가능하여 전체 네트워크로 공격 패킷의 유입을 근원지에서 빠른 차단이 가능하다는 장점을 갖는다.

4. Automating Packet Traceback 기술

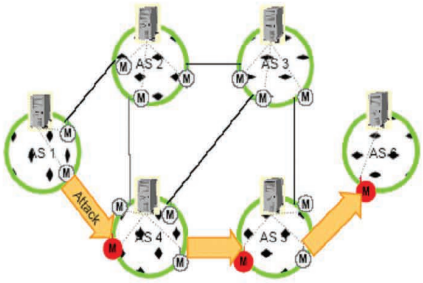
Automating Packet Traceback 기술은 2007년도 CIAS-ISSA Security Symposium에서 발표되었다. 본 문서는 이때 발표된 PPT 자료를 기초로 하여 분석 및 정리한다. Automating Packet Traceback 프로젝트는 Department of Homeland Security의 펀드로 운영되고 있으며, University of Texas at San

Antonio 내의 Southwest Research Institute와 Symantec Research Lab에서 공동으로 연구를 진행하고 있다. 이 접근법은 앞에서 분석한 오버레이 네트워크 기반 역추적 기법 및 해쉬 기반 역추적 기법과 비슷한 기법으로 접근하고 있다. 기존에 연구되었던 역추적 기법들의 실용적 한계를 극복하기 위해서 AS(Autonomous System) 단위에 모니터를 수행하는 하드웨어 장비를 설치하여 공격 패킷의 경로를 찾아내는데 활용한다. AS는 단일 경로제어 정책을 공유하는 네트워크로써, 개개의 ISP나 기업 등이 보유 및 운영하는 네트워크가 된다. **[그림 12]**는 AS로 구성된 전체네트워크를 보이고 있다.

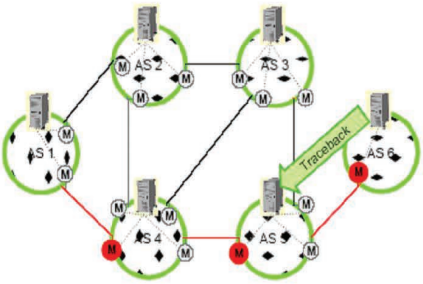


[그림 12] Autonomous System으로 구성된 전체 네트워크

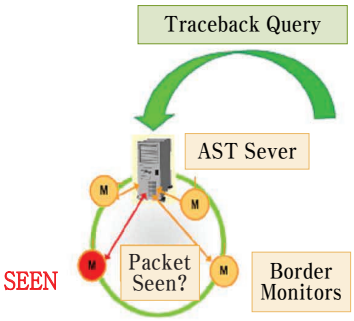
AS Traceback 기법은 IP 주소가 위장되었거나 유효한 소스 주소를 가지는 각각의 싱글 패킷을 대상으로 한다. 또한 하드웨어 기반임으로 실시간 또는 몇일 이내로 공격 패킷에 대한 빠른 추적이 가능하다. 별도의 모듈을 라우터에 추가할 필요가 없으며, 종단 호스트 시스템이나 IP 프로토콜과도 상관없이 동작 가능하다. 한편, 라우터의 성능저하에 전혀 영향을 미치지 않는다는 장점을 갖는다. **[그림 13]**을 보면 각각의 AS 단위에 AST 서버가 위치하고, 여러 개의 모니터들이 동작하고 있다. AST 서버는 해당 AS 내의 전송되는 모든 패킷들에 대한 정보를 일정시간 저장하게 된다. 공격이 탐지되면 **[그림 14]**와 같이 해당 패킷에 대한 AS 단위의 추적이 가능하게 된다.



1. Attack path : Packet signature is recorded by border monitors

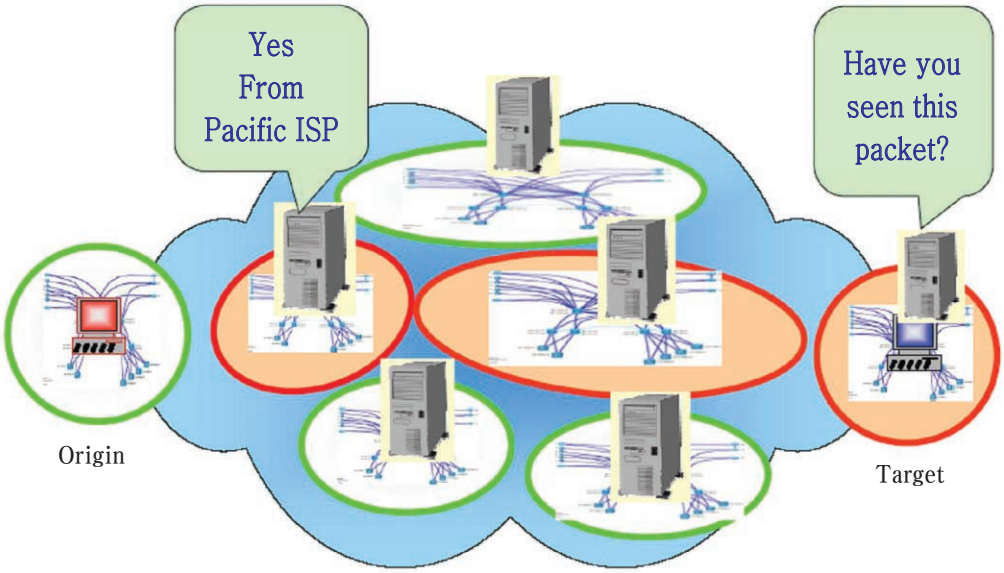


2. Traceback path "SEEN" reply by border monitors



[그림 13] Autonomous System Traceback-1

AS Traceback 기법의 모니터는 하드웨어로 구현되어 Passive tap의 형태로 구동된다. 또한 패킷에 대한 정보는 MD5 해쉬를 이용하여 작은 용량으로 저장하며, 프라이버시 보호도 가능하다. AST 모니터들은 digest tables에 일정 시간동안 저장을 하게 되는데 이때 하드웨어의 메모리 용량에 따라 저장하는 시간을 여유롭게 잡을 수 있다. 이 기법은 기존의 해쉬기반 역추적 기법에 대한 연구에서 AS를 이용하여 확장한 개념이라고 볼 수 있다. 현재 Automating Packet Traceback 기법의 연구 결과는 오버헤드와 추적에 대한 성공확률 등에 대한 시뮬레이션을 마친 상태이며, Symantec 및 IDEA Laboratory에서 시험 중에 있으며, 향후에는 ISP에 설치하여 시험할 예정이다.



[그림 14] Autonomous System Traceback-2

5. 결 론

사이버공격 근원지 역추적 기술은 DDoS, 스캐닝 공격 등에 가장 효과적으로 대응할 수 있는 기술로 연구자 및 기관의 담당자들이 많은 관심을 갖는 분야이다. 하지만 현재까지의 연구결과들은 연구수준에서 머무르고 있으며, 실용화 단계로 진행되는 사례는 찾아보기 힘들다.

본 문서에서는 2003년 말까지의 역추적 기술 동향을 기술하고, 효과적인 역추적 기법 중에 하나인 Deterministic Pushback 기법을 소개하는 한편, 최근에 연구 및 실험이 진행중인 Southwest Research Institute의 Automating Packet Traceback 기법에 대하여 설명하였다. 2003년 말까지의 역추적 기술을 보면 라우터에 별도의 모듈을 심어야 하거나, 네트워크 단위로 서버를 설치하여 로깅을 해야만 했다. 이에 대한 단점을 극복하고자 하는 기법이 Deterministic Pushback 기법이다. 이 기법은 에지라우터에서 나가는 패킷에 대해서만 마킹을 실시하며, 공격 탐지 시 해당 에지라우터에 메시지를 전송하여 근원지 라우터에서 효과적으로 필터

링을 실시하도록 하는 기법이다. 하지만 이 기술 역시 에지라우터에 기능을 추가해야 하는 단점을 갖는다. 최근에 연구가 진행되고 있는 Automating Packet Traceback 기법은 기존의 해쉬 기반 역추적 기법을 확장한 기법으로 AS 단위로 AST 서버를 설치하고, 라우터에 하드웨어로 동작하는 모니터를 설치하여 전송 패킷에 대한 정보를 남기는 기법을 이용하고 있다. AS 단위로 서버를 설치한다는 것과 하드웨어 기반으로 모니터를 동작시켜 성능을 높인다는 것이 특징이라 할 수 있다. 이 기법이 현재 시험 중이며 곧 ISP에 적용 시험을 실시한다고 하므로 결과를 지켜볼 필요가 있을 것이다.

사이버공격 근원지 역추적 기술은 많은 기관에서 필요로 하고, 관심을 갖는 기술임에는 틀림이 없다. 하지만 기술을 연구하고 해당 기술을 상용화하는 데는 많은 어려움이 있다. 제일 큰 문제점은 전 세계의 네트워크에 다 같이 적용하지 않고서는 전체적인 효과를 발휘 할 수가 없다는 점일 것이다. 그러나 정부 기관 네트워크부터라도 최신의 역추적 기술을 적용해 나간다면 단일 해킹공격 등에 대한 대응에 효과적일 수 있을 것으로 생각되며, 향후에는 전체 네트워크로 확장해나가는 노력이 필요하다. 향후 지속적으로 성능 및 실용성이 높은 역추적 기술의 연구 개발에 많은 노력이 절실히 필요하다.

참고 사이트 WWW

[1] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attacks", In Proc. IEEE INFOCOM 2001, 2001.

[2] D. X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback", In Proc. IEEE INFOCOM 2001, 2001.

[3] Steve Bellovin, Tom Taylor, "ICMP Traceback Messages", RFC 2026, Internet Engineering Task Force, February 2003.

[4] A.C. Snoeren, C. Partrideg, 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 2001.

[5] Jung-Taek Seo, Ki-Wook Sohn and Eung-Ki Park, "A Deterministic Pushback Method to Mitigate DDoS Flooding Attack", LNCS 4413. December. 2007.

[6] Sandra Dykes, "Automating Packet Traceback", CIAS-ISSA Security Symposium 2007.

[7] 이형우, “DDoS 해킹공격 근원지 역추적 기술”, 한국정보보호학회 논문지, 제13권 5호, 2003.10.

[8] 김병룡외 3인, “마킹알고리즘기반 IP 역추적에서의 공격근원지 발견기법”, 한국정보보호학회 논문지, 제13권 1호, 2003.2.

[9] 김종민외 2인, “다중 에이전트를 이용한 역추적 시스템 설계 및 구현”, 한국정보보호학회 논문지, 제13권 4호, 2003.8.