네트워크 해킹 공격 대응을 위한 IP Traceback 기술

한신대학교 소프트웨어학과 이형우

차 례

요 약

본 연구에서는 DDoS/DRDoS 공격과 같이 Zombie 및 Reflector 기반의 네트워크 기반 해킹 공격에 대해 스푸핑된 공격 패킷의 근원지 IP를 역추적할 수 있는 기술에 대해 분석하였다. 현재까지 제시된 IP 역추적 기법은 크게 패킷을 중심으로 마킹 방법론을 사용한 기법과 ICMP 프로토콜과 같은 프로토콜 등에 대한 변형을 통해 근원지 패킷의 전달 경로 정보를 관리하는 기법 및 네트워크 망 구조 측면에서의 관리 프로토콜을 응용한 방법 등으로 나눌 수 있다. 각각의 기법은 현재의 인터넷 환경에서 적용하였을 경우 DDoS 공격에 대해 장단점을 보이고 있으며 적용 방법 및 해킹 공격의 특성에 따라서 각기 다른 성능을 보인다. 본 연구에서는 지금까지 연구된 IP 역추적 방법론에 대해 고찰과 함께 각 기법을 비교하고 시뮬레이션 방법 등에 대해 제시하며 앞으로 급속도로 확산될 것으로 예상되는 IPv6 기반의 네트워크 공격에 대응하는 방법 등 새로운 역추적 기법에 대해서도 살펴보았다.

I. 서 론

인터넷을 통해 편리함과 정보 교류 등을 활성화하는 등 순기능과 함께 인터넷을 통해 시스템 해킹 및 정보유출, 불법 침입, 악성 바이러스 유포 등 역기능도 점차 확대되고 있다. 역기능으로 대표적인 것은 서비스 거부 공격(Denial of Service)[1]으로 최근에는 분산 공격을 통해 호스트 및 네트워크 자원을 급격히 소진하여 서비스 성능 저하 및 불가를 유발하게 된다. 이와 같은

공격 형태는 인터넷을 통해 손쉽게 구현할 수 있는 반면, 방지 및 추적 방법은 어려운 실정이다. 이는 TCP/IP 프로토콜의 특성상 DoS 공격 등에 대처할 수 있는 보안 구조가 제공되지 않았기 때문이다. DoS 공격자는 손쉽게 IP 패킷의 송신자 주소를 변경(스푸핑)하여 피해 시스템에게 보낼 수 있다[2]. 이럴 경우 실제 IP 패킷이 보내진 송신자 주소가 아니기 때문에 DoS 패킷에 기록된 송신자 주소만을 가지고는 스푸핑된 패킷의 실제 공격지를 추적할 수 없다.

IP 패킷의 헤더에는 전송 근원지에 해당하는 32비트 IP 주소를 포함하고 있다. 그러나 TCP/IP에서의 보안 취약성에 의해서 전송자 IP는 손쉽게 위조/변경될 수 있다. 현재 사용되는 라우터 역시 성능 측면에 중점을 두고 있어서 스푸핑된 IP 패킷에 대한 필터링, 판별 기능을 제공하지 못하고 있다. 따라서 공격자는 스푸핑된 패킷을 생성하여 DoS 공격을 손쉽게 수행할 수 있다.

IP 역추적(IP Traceback) 기법[4,5,6,7,8,9,10]은 공격 피해 시스템 관리자에게 DoS 공격의 실제적인 공격 근원지 IP 주소를 알려주는 기능을 제공한다. 또한 대부분의 DoS 공격은 Zombie를 통한 간접적인 공격 형태를 보인다. 물론 IP 패킷에 대한 변형을 판별하기 위해 분산 필터링 기법 등도 제시되었으며, 라우터의 성능을 개선하여 IP 주소에 대한 검증 기능을 포함하기도 하였다. 이와 같은 방식은 ingress filtering 기법에 [3]해당하는 것으로, 라우터로 들어오는 패킷에 대한 검증, 판별 기능을 제공하는 구조이다. 하지만 DoS 공격과 같은 대단위 패킷에 대한 효율적 역추적 기능을 제공하지 못하여 한계점을 갖는다. IP Traceback 기법은 기존의 필터링 기법과 달리 능동적인 방식으로 피해 시스템에서 공격 근원지를 판별할 수 있는 기법이다.

DoS 공격에 대한 대응 방법으로 백신, 침입탐지 및 침임감내 기술 등과 같은 수동적인(passive) 대응 방법과 공격 근원지 추적 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. 본 연구에서는 해킹 및 바이러스에 대한 능동적인 대응 방안에 대해 고찰하고 현재까지 제시된 전향적/대응적 역추적 기법의 특성을 비교 분석하고자 한다.

II. IP 근원지 역추적 기술

1. 근원지 역추적 기술 분류

인터넷에서의 패킷 특성상 TCP 계층을 중심으로한 서비스 중심의 역추적 기능 보다는 패킷 자체의 네트워크 전송 과정을 다루는 IP 계층에서의 역추적 기능을 제공하기 위한 연구가 활발히 진행되고 있다. 따라서 IP 계층을 중심으로 현재까지 제시된 역추적 기술을 분류하면 해킹 대응 방식에 따라 크게 전향적 역추적 기술(proactive IP traceback)과 대응적 역추적 기술(reactice IP traceback)로 나눌 수 있으며, 세부 기술로 나누어 본다면 라우터 중심의 역추적 기술, 패킷 정보에 대한 관리 시스템 구현 기술, 특수 네트워크 중심 기술 및 관리 기술 중심 역추적 방식으로 분류할 수 있다. IP 역추적 기술이 갖추어야 하는 요구사항으로는 다음과 같다.

- 기존 네트워크 프로토콜과의 호환성
- 네트워크 부하 최소화
- 구현 가능성
- 기존 라우터 및 네트워크 구조와의 호환성
- DDoS 공격 대응력과 시간/자원 활용의 효율성

2. Proactive 역추적 기술

본 기술은 네트워크상에 패킷이 전송되는 과정에서 사전에 역추적 경로 정보를 생성하여 패킷에 삽입하거나 목적지로 전달하여 주기적으로 관리하면서 만일 해킹 공격이 발생하면 이미 생성, 수집된 정보를 이용하여 해킹 공격 근원지를 판별하는 기법이다. 현재 사용되는 기법으로는 링크 검사법(link testing), 로깅 기법(logging) 등의 초기 대응 기법과 능동적인 IP 역추적 기법으로 패킷에 대한 확률적 마킹(PPM : probabilistic packet marking) 기법과 전통적인 ICMP 메시지를 변형한 iTrace (ICMP traceback) 기법 등이 있다.

가. 링크 검사법(Link testing)

hop-by-hop 추적 방식에 해당하는 것으로 각 라우터에서는 연결된 링크에 대해 검사하면서 트래픽이 DoS 공격으로부터 전송된 패킷인지의 여부를 검사하게 된다. 자동화된 역추적 방법을 제공하지는 못하며 직접적으로 패킷 전송 경로를 조합/판별하는 방법에 해당한다. 따라서 네트워크 관리 측면에서의 오버헤드가 발생하게 된다. 링크 검사법에 대한 구현 결과로 제시된 input debugging 기법에서는 공격 유형(attack signature)을 기반으로 공격 트래픽에 대해 판별하고 실제로 전송된 경로를 판별한다. 그러나, 이 기법인 경우 서로 다른 ISP 관할 네트워크에 대한 검사에 한계가 있으며, 공격 유형에 대한 판별이 쉽지 않다. 링크 검사법의 또 다른 적용 기법으로는 controlled flooding 기법이 있다. 이 기법은 피해 시스템에서 상위 라우터로 패킷을 생성하여 전송하면서 반대로 DDoS 해킹 공격 패킷량의 변화를 측정하고 최종적으로 공격 근원지를 찾아내는 방식이다. 그러나 이 기법 역시 DoS 공격의 일종에 해당할 수 있다는 단점이 있다.

나. 로깅 기법(Logging)

로깅 기법은 라우터에서 전송된 패킷에 대한 특성 등을 기록해 놓은 후에 데이터 마이닝 등의 추론 시스템을 적용하여 공격 근원지를 검출하는 기법이다. 물론 많은 양의 정보를 저장/관리하고 있어야 하며 데이터 처리량 또한 방대하여 효율적인 대응 기법이라고 할 수는 없다.

이에 대한 해결책으로 확률적인 샘플링 기법을 적용하여 처리 데이터를 줄이고, 필터 기법 등을 적용하여 처리/판별 과정을 간략화하는 방법 등이 제시되기도 하였으나 방대한 패킷에 대한 판별 과정에서의 오류 수정 과정 등이 보완되어야 한다.

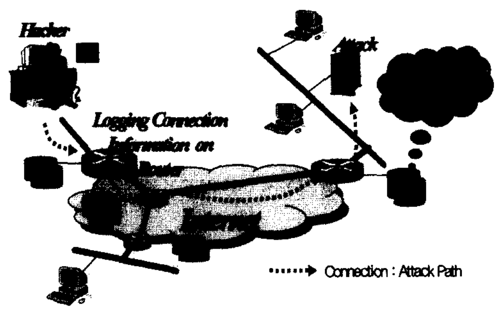


그림 1. 로깅 기법의 작동 구조

다. PPM 기법[4,5]

스푸핑된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해서는 IP 계층을 중심으로 네트워크 상에 전송되는 패킷에 대해 네트워크를 구성하는 주요 요소인 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달되었다는 정보를 삽입하는 방식이다.

즉, 인터넷을 통해 전달되는 패킷에 대해 라우터는 IP 계층을 중심으로 패킷 헤더 정보를 확인하여 라우팅하게 되는데 이때, IP 헤더에서 변형 가능한 필드에 대해서 라우터에 해당하는 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다. 아래 (그림 2)와 같이 IP 헤더에서 16비트 ID 필드에 라우터 자신의 IP 정보를 삽입하게

된다.

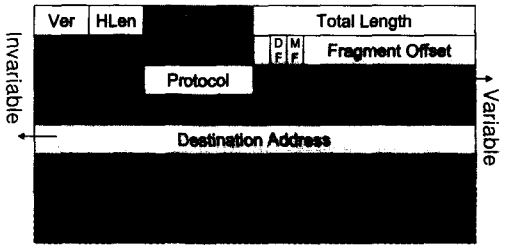


그림 2 IP 헤더 형태

각 라우터에서 삽입된 정보는 다시 다음 라우터로 전달되고 최종적으로 목적지 피해 시스템에 전달된다. 아래 그림과 같이 각 라우터에서 마킹된 정보가 전달되면 추후에 해킹 공격이 발생하였을 경우 해킹 공격에 해당하는 패킷에 기록된 라우터 정보를 재구성(reconstruction)하여 실제적인 패킷의 전달 경로를 재구성하게 된다.

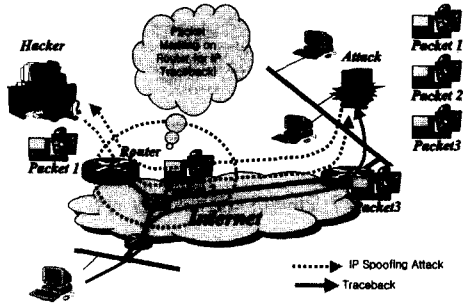


그림 3. PPM 기법 구조

각 라우터에서 전달된 정보를 마킹하는 과정에서 모든 패킷에 마킹하게 되면 전체 네트워크에 대한 지연 현상이 발생하기 때문에 일반적으로 라우터에서는 확률 p로 패킷을 샘플링하여 마킹하게 된다.

이때 라우터에서 마킹하는 정보의 구성에 따라 노드 샘플링(node sampling), 에지 샘플링(edge sampling) 및 개선된 패킷 마킹 기법 등이 제시되었다. 아래 (그림 4)와 같이 노드 샘플링 기법은 패킷이 전송된 경로 정보를 확률 p로 샘플링하여 목적지에 전송하는 과정을 보인다.

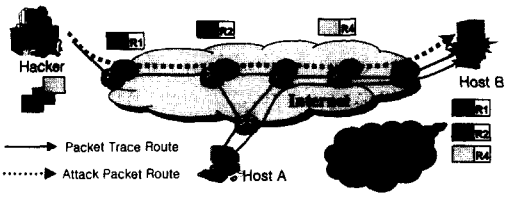


그림 4. 노드 샘플링 기반 PPM 기법

아래 (그림 5)는 에지 샘플링 방법으로 라우터에서 자신의 IP 주소 정보만을 패킷 헤더에 마킹하는 것이 아니라, 패킷이 전달된 앞단의 라우터 IP 주소까지도 같이 마킹하여 전달하는 방식이다. 이와 같은 노드 샘플링 기법은 해킹 공격 경로를 재구성하는 과정이 노드 샘플링 기법보다 뛰어나다.

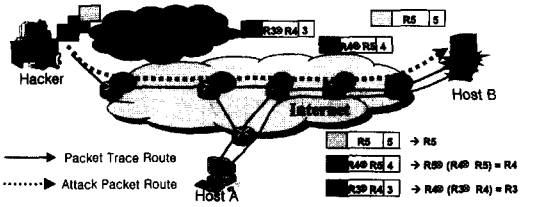


그림 5. 에지 샘플링 기반 PPM 기법

변형된 PPM 기법으로는 라우터에서 마킹하는 패킷에 대한 인증 기능을 제공하여 마킹 과정에서 보안 기능을 제공하는 기법 등이 있다.

라. iTrace(ICMP Traceback) 기법[6]

ICMP 역추적 기법은 PPM 기법과는 다른 접근 방법으로 수행된다. 라우터에서는 일반적으로 $\frac{1}{20,000}$의 확률로 패킷을 샘플링하여 iTrace 메시지를 생성하고 이를 패킷의 목적지 IP로 전송한다. iTrace 메시지는 일반적인 ICMP 메시지와 유사하게 전단계 라우터 정보와 다음 단계 라우

터 정보를 포함하고 있으며 패킷의 payload 정보 등을 포함하여 전달하게 된다. 생성시에 TTL(time of live) 필드 값은 255로 설정되어 전달되며 목적지에서는 TTL 값을 보고 네트워크 위상에서의 홉 거리 정보이기 때문에 공격 경로 재구성에 사용된다. iTraceback 기법에 대한 작동 방식은 아래 (그림 6)과 같으나 일반적으로 PPM 기법과 마찬가지로 DDoS 공격에 대응하기 위해서는 상대적으로 많은 정보가 필요하기 때문에 개선된 기법으로의 연구가 진행되고 있다.

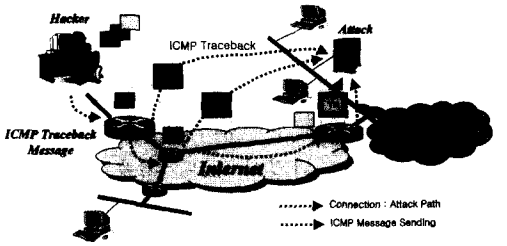


그림 6. iTrace(ICMP Traceback) 기법

3. Reactive 역추적 기술

본 기법은 해킹 공격이 발생하였을 경우 피해 시스템에서 해킹 트래픽 연결에 대한 공격 경로를 홉 단계로 추적해 가는 방식이다. 구체적인 기법은 오버레이(overlay) 네트워크 방식, 해쉬 기반 역추적 기술 및 IPSec 기반의 역추적 기법 등으로 나눌 수 있다.

가. 오버레이 네트워크 기반 역추적[8]

본 기법은 역추적 라우터(TR : tracking router) 모듈을 네트워크에 별도로 설치하고 해킹 공격이 발생하였을 경우, 네트워크 위상에서의 종단 시스템과 연결된 라우터에서 전달된 정보를 TR로 전송한다. 즉, 기존의 ingress 필터링 기법과 유사하게 종단 라우터에서 보내진 트래픽 정보는 터널링 방식으로 TR 라우터에 전달된다. 각 패킷에 대해 20 바이트 정보의 패킷 서명(packet signature) 정보를 생성하여 TR로 전달하게 된다. TR에서 수집된 패킷 관련 정보 등을 재구성하여 실제로 패킷이 전달된 경로를 분석하는 기법이지만, 네트워크 구성상 단일 TR로 전체 네트워크를 관리할 수 없기 때문에 소단위 네트워크에 적합한 기법이다. 또한 단일 ISP 네트워크상에서 구현 가능한 기법이며 이기종의 네트워크 환경에는 적용할 수 없다. 또한 해킹 공격은 짧은 기간 동안에 수행될 수도 있기 때문에 전체 경로를 역추적하는데 어려움이 발생할 수도 있으며, 공격자에 의해서 터널링된 패킷이 위조될 수도 있기 때문에 보안상의 문제가 발생하게 된다.

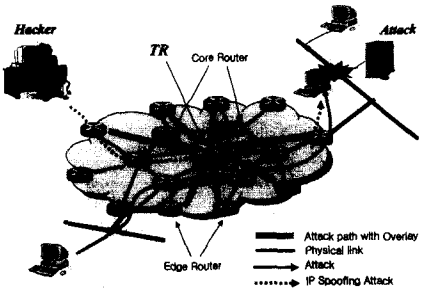


그림 7 오버레이 네트워크 기반 역추적

나. 해쉬 기반 역추적[9]

본 기법은 SPIE(source path isolation engine) 기반 역추적 서버를 구성하고 전체 네트워크를 서브 그룹으로 나누어 각 그룹별로 에이전트를 두어 망을 관리한다. 그리고 각 라우터에는 DGA(data generation agent) 기능을 탑재하여 운영한다. DGA에서는 해당 라우터에 전달된 패킷에 대해 패킷의 메시지 해쉬값에 해당하는 IP 헤더 정보와 8 바이트 정보의 payload 정보를 수집 관리하고 이를 bloom filter 구조로 저장하게 된다. 만일 목적지 시스템에 있는 IDS 시스템에 의해 해킹을 발견하였을 경우 SPIE 시스템에서

는 네트워크 그룹을 관리하는 SCAR 에이전트를 통해 그룹내 DGA 라우터에 저장된 정보와 해킹 패킷 정보를 비교 분석하여 이를 다시 SPIE 시스템에 전달하게 되면 해킹 관련 패킷의 전송 경로를 재구성하게 된다.

본 기법을 적용하기 위해서는 SPIE, SCAR 및 DGA 기능을 구축하여야 하며 추가적인 모듈로 제공되기 때문에 이기종 환경의 ISP간 적용도 가능하다. 실험 결과 0.5% 정도의 추가적인 해쉬 정보가 생성되어 전달되고 SCAR에서는 주기적으로 패킷에 대한 해쉬값을 관리하기 위한 메모리가 필요하다.

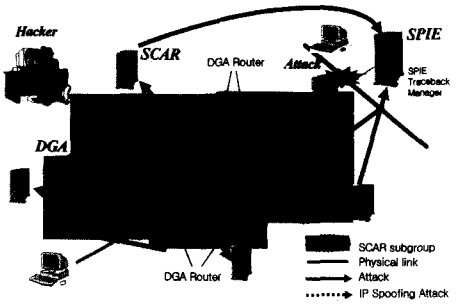


그림 8. 해쉬 기반 역추적 기법

다. IPSec 기반 역추적[10]

본 기법은 오버레이 네트워크 기반 역추적 기법에서 발생하는 터널링 과정에서의 보안상 취약점을 보완하기 위해 제시된 기법이다. 전체 네트워크에 대한 위상을 각 라우터가 알고 있다는 가정하에 해킹 공격이 발생하게 되면 네트워크상의 라우터와 피해 시스템간에 IPSec 연결이 구성되어 공격자에 의한 공격 패킷이 해당 라우터를 통해 전송될 경우 IPSec 터널을 통해 경로 정보를 피해 시스템에 전달하게 된다. 다시 네트워크 위상에서의 주변 라우터를 선정하여 IPSec 터널을 구성하고 패킷에 대한 전송 여부를 판별하여 이를 피해 시스템에 전달하는 과정을 반복한다. 이와 같은 과정을 통해 해킹 공격 발생시 실제적으로 패킷이 전송된 경로상의 라우터를 판별할 수 있게 된다.

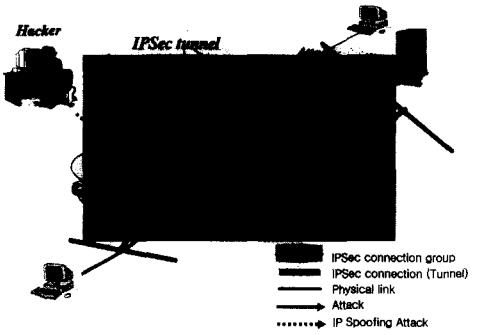


그림 9. IPSec 기반 역추적 기법

물론 IPSec을 이용한 역추적 방식은 피해 시스템과 라우터간에 IPSec 터널 연결을 구성한 경우에는 공격 경로를 파악할 수 있으나, IPSec 연결을 취하지 않는 네트워크에서는 경로 재구성에 어려움이 있게 된다.

III. Reflector 공격 기반 IP 근원지 역추적 기술

서비스 거부 공격은 Zombie 기반의 분산 공격 형태로 발전하면서 더욱 강력한 공격 형태를 보이게 되고, 한단계 더 진보된 reflector 기반의 DRDoS 공격 형태로 발전하였다. 다단계 공격 형태를 보이면서 실제 DoS 공격 근원지에 대해 역추적이 더욱 어려워지고 있다. reflector 기반의 DRDoS 공격으로 인해 공격 근원지에 대한 역추적은 더욱 어려워지고 있다.

Reflector 기반의 공격에 대한 대응 기법으로 제시된 것은 Reverse iTrace 기법이 있다. 이 기법은 iTrace 기법이 ICMP 패킷을 피해 시스템으로 전송하는 것을 다시 역으로 적용하여 중간 라우터에서는 ICMP 패킷을 패킷의 근원지 주소로 보내는 방식을 사용한다.

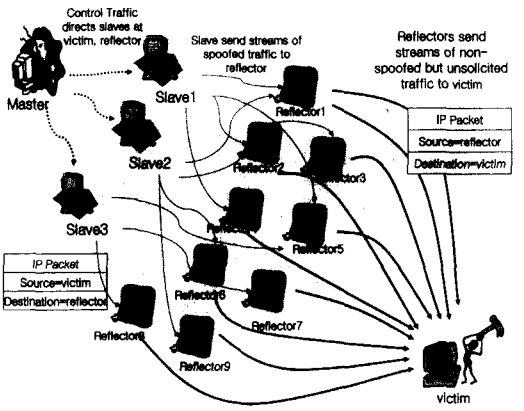


그림 10 Reflector 기반 DDoS 공격 기법

물론 개선된 기법도 제시되고 있다. 기존의 Pushback 기법을 적용하여 Reflector 공격에 대응하는 방식이 제시되었다. 기존의 Pushback 기법은 라우터에서 패킷 폭주가 발생하였을 경우 ACC 기반의 모듈을 적용하여 해킹 패킷의 형태와 비교하고 만일 해킹으로 판단될 경우 라우터에서는 패킷이 전송된 앞단의 라우터에게 Puashback 메시지를 전송하여 라우터로 하여금 패킷 필터링 모듈을 작동시키도록 한다. 따라서 일반적인 Pushback 기법은 해킹 등의 DoS 공격이 발생할 경우 다량의 패킷이 전송되게 되므로 이를 라우터에서 제어할 수 있는 기능을 제공한다.

하지만 기존의 Pushback 기법은 DoS 공격 등에 대한 제어/판단 기능은 제공하지만, 피해 시스템에게 공격 근원지에 대한 역추적 기능을 제공하지는 못한다. 따라서 개선된 역추적 기법으로는 패킷에 대한 제어/판별 기능을 제공하는 Pushback 기법을 IP 역추적 모듈과 접목하는 방법이 제시되었다.

제시된 기법을 활용할 경우 기존의 IP 역추적 기법과 같이 공격 근원지에 대한 IP 역추적 기능을 제공할 뿐만아니라, 전체적인 DDoS 패킷에 대한 감소/제어 기능까지도 제공하기 때문에 효율적인 것으로 나타났다.

또한 앞에서 제시한 iTrace 기법을 적용할 경우 Reflector 등에 기반한 다단계 DRDoS 공격에서의 근원지 역추적 기능도 제공할 수 있는 장점을 제공한다.

IV. IP 근원지 역추적 기술 비교 평가

현재 발표된 기존의 IP 역추적 관련 기술들의 성능을 비교 분석하면 다음 [표 1]과 같다. IP 역추적과 관련하여 기존의 기법들을 관리 시스템 부하, 네트워크 부하, 피해 시스템의 부하, 메모리 요구, 적용 가능성, 역추적 기능, 대역폭 부하, 보안 기능, DDoS 대응, 확장성 및 경로 재구성 시 필요한 패킷 수 등을 기준으로 비교해 보았다.

라우터에서의 접근 제어 기능을 제공하는 필터링 기법은 SYN flooding 기법과 유사하게 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 보이고 있다.

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 조금 취약한 특성을 보이고 있다.

오버레이 네트워크와 해쉬 기반, IPSec 기반

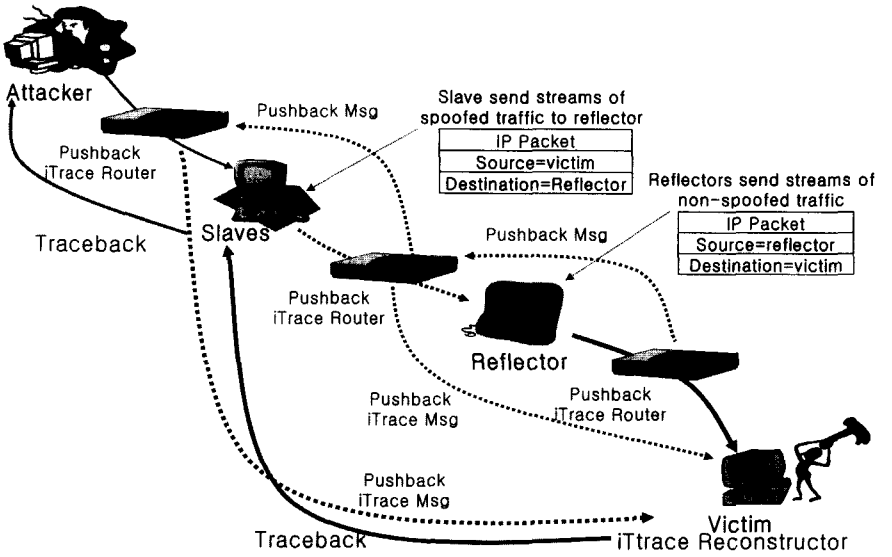


그림 11. Reflector 기반의 DDoS 공격에 대한 대응 기법

역추적 기법인 경우 기존의 라우터에 대한 관리 시스템을 추가하거나 특정 모듈을 부가하여 역추적 기능을 제공하는 방식이기 때문에 전체적으로 관리 시스템의 부하가 크다고 할 수 있으나, 역추적 기능이 뛰어나고 보안 기능 및 DDoS 대응 측면에서 우수한 성능을 보이고 있다. 특히 기존의 네트워크를 구성하는 라우터에 추가적인 기능을 제공하는 방식으로 많은 변화 없이도 기존의 ISP와 연계하여 이기종의 네트워크 환경에도 적용 가능하다는 장점을 제공한다. 그러나, 이와 같은 기법은 특정한 환경을 구축하여 역추적을 수행하는 것으로 일반적인 인터넷 환경에 적용하고자 할 경우 일부 적용 불가능한 경우도 발생할 수 있다.

전체적으로 현재까지 제시된 IP 역추적 기법을 검토하였을 경우 대부분 기존 라우터에 대한

표 1. IP 역추적 기법 성능 비교 평가

특성 / 기법	관리 시스템 부하	네트워크 부하	피해 시스템 부하	메모리 요구	대역폭 부하	역추적 기능	적용 가능성	보안 기능	DDoS 대응	확장성	경로 재구성 패킷수
Ingress filtering	×	×	×	×	×	×	▽	×	×	△	×
SYN flooding	×	×	↓	×	↓	×	▽	×	×	△	×
Logging	↑	×	×	↑	×	▽	▽	◇	▽	◇	1
PPM	↓	↓	↑	↑	×	△	△	◇	▽	△	↑
iTrace	↓	↓	↑	↑	↓	△	△	◇	▽	△	↑
Overlay Network	↑	↓	↓	↓	↑	△	△	◇	◇	▽	1
Hash based TB	↑	↓	↓	↓	↓	△	△	△	◇	▽	1
IPSec based TB	↑	↓	↑	×	↑	△	△	△	▽	▽	↔
Controlled flooding	×	×	×	↓	↑	×	△	×	×	×	1

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

변형 및 추가적인 네트워크 / 시스템 부하가 발생하며, reactive 기법에서는 추가적인 대역폭에 부하가 발생한다는 것을 알 수 있다. 따라서 라우터에서의 부하를 비롯하여 전체적인 관리 시스템의 부하와 대역폭 부하를 줄이면서 확장성을 제공하고 DDoS 대응 성능을 향상시킬 수 있는 기법에 대한 연구가 필요하다.

2. 개선된 역추적 기법 고찰

인터넷 프로토콜은 TCP/IP 프로토콜의 중심이다. IP는 OSI 참조 모델의 네트워크 계층에 해당하고, 비연결 서비스와 최선의 전달 서비스를 전송 계층에 제공한다. 특히 IP 패킷에서의 헤더는 20 바이트의 고정 길이 구성 요소와 최대 40 바이트의 가변 길이의 선택적인 구성 요소를 갖는다.

인터넷을 구성하는 물리적인 네트워크 장비인 경우 다양한 형태의 프로토콜을 사용하여 연결되어 있으며 작동 방식 역시 매우 다양하다. 따라서 인터넷을 통한 해킹 공격 역시 매우 다양한 형태로 발생하게 된다.

해킹 공격에 대한 대응 기술을 고찰할 때 우선 고려해야 하는 것은 인터넷 프로토콜 구조상 어느 계층을 중심으로 고찰할 것인가를 우선 결정해야 한다. 일반적으로 IP 계층에서의 역추적 기능을 제공하는 것이 일반적이며 TCP 계층인 경우 서비스 종류에 의존적이기 때문에 일반화하기에 어려움이 많이 있다. IP 계층에서의 역추적 기능을 제공하는 과정에서도 피해 시스템이 직접 모든 네트워크를 관리할 수 없기 때문에 결국에는 라우터에 의존하여 역추적 기능을 수행하게 된다.

이때 기존의 라우터에서 부가적인 기능을 어느 정도 추가할 것이며 어떠한 기능을 제공해야 하는 지에 따라서 여러 가지 기법으로 분류할 수 있다.

가. 전향적 기법에 대한 재고찰

전향적인 기법인 경우 패킷을 중심으로 IP 헤더 정보에 정보를 마킹하는 방식으로 기존의 마킹 구조에서 유발하는 문제점을 해결할 수 있는 방안이 제시되어야 한다. 즉, 기존의 기법에서는 확률 p로 패킷을 선정하게 되는데 경로 재구성을 위해서는 상당히 많은 개수의 마킹된 패킷이 필요하다. 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 있으며, 최소한 하나의 노드 또는 에지 정보를 마킹하는데 알고리즘에서는 최소한 8개의 패킷을 선정하여 마킹해야 하기 때문에 전체적인 효율 면에서도 비효율적이다.

iTrace 기법인 경우 기존의 패킷 정보에 대해 PPM과 마찬가지로 확률 p로 샘플링하여 메시지에 대한 iTrace 메시지를 생성하고 이를 목적지 IP로 전송하는 방식이다. 그러나 현재 DDoS 공격 기법 중의 하나로 ICMP 기법을 이용한 방식이 발견되고 있어서 결국에는 iTrace 기법 역시 목적지 피해 시스템 측면에서 보았을 경우에는 또다른 하나의 DDoS 공격으로도 보일 수 있기 때문에 이를 해결할 수 있는 방안이 제시되어야 한다.

이와 같이 전향적 기법인 경우 패킷에 대해 일정 확률 p를 만족할 경우 샘플링하여 전송하는 기법을 사용하고 있는데, 이에 대한 구체적인 방안도 여러 가지를 생각할 수 있을 것이다. 만일 PPM 또는 iTrace 메시지를 발생하는 라우터에서 고정적인 형태의 확률 p에 의존하여 샘플링하지 않고 전체 네트워크의 트래픽 특성에 따라 능동적으로 확률 p를 조정할 수 있다면 기존 기법에 비해 네트워크 부하, 메모리 및 역추적 기능 등에서 보다 향상된 기법을 제공할 수 있을 것이다. 또한 해커에 의한 오류 경로 재구성을

방지하기 위해서는 전통적인 보안 구조를 역추적 모듈과 접목하여 제공한다면 더욱 개선된 기법을 제공할 수 있을 것이다.

나. 대응적 기법에 대한 재고찰

오버레이 네트워크를 이용한 역추적 기법인 경우 특정 네트워크 위상에만 적용가능하며 라우터의 구조가 동적으로 변화하는 일반적인 네트워크 환경에는 적용하기 어렵다. 또한 종단 라우터가 아닌 망 내부 라우터에 연결된 라우터를 거쳐서 전달되는 패킷인 경우 쉽게 추적할 수 없다는 문제점이 발생한다.

해쉬 기반 역추적 기법인 경우 패킷에 대한 해쉬 값을 일정한 주기로 관리 전송하는 방식이지만 네트워크가 규모가 방대한 경우 전체 성능에 많은 문제점이 발생하게 된다. 또한 IDS 시스템 등을 통해 해킹 등이 발견된 경우 역추적 과정을 수행하는 방식이므로 우선 네트워크 자체에 대한 공격이 수행된다면 본 기법 역시 작동하지 않는다는 문제점이 발생한다.

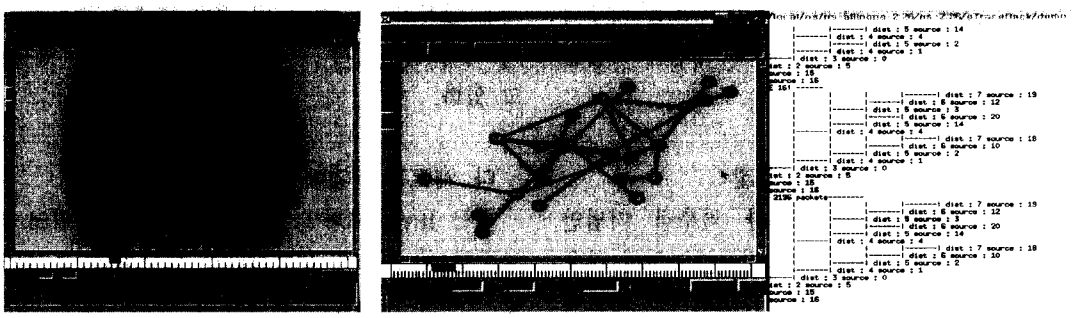
IPSec에 기반한 역추적 기법인 경우 우선 공격자는 IPSec이 가지고 있는 보안 및 인증 특성에 의해서 DDoS 공격을 수행하지는 않을 것이며 일반 네트워크 환경에서 해킹 공격을 수행할 것이다. 따라서 IPSec 기법을 적용한다는 것은 결국 목적지 시스템과 라우터간에 IPSec으로 채널을 구성하고 트래픽에 대한 확인 과정을 수행한다는 것이다. 결국 역추적 과정에서 IPSec으로 채널이 구성된 네트워크 그룹과 공격자가 포함되어 있는 비 IPSec 기반 일반 네트워크 간의 연계 기능을 제공해야 한다.

결국 현재까지 제시된 기법을 종합적으로 비교하였을 경우 전향적 기법인 경우 라우터를 통해 패킷에 HMAC 등의 기능을 제공하고 확률 p를 다양한 기준으로 선정하여 iTrace 패킷을 생성하는 방식이 필요하며, 대응적 기법인 경우 해쉬 방식에 기반한 단일 패킷 역추적 방식이 여러 가지 측면에서 우수한 역추적 성능을 제시하고 있다.

다. 새로운 환경에 대한 고찰

최근 IPv6, 모바일 환경, Ad-hoc 네트워크 및 능동형 네트워크, 유비쿼터스 네트워크 등 다양한 형태의 네트워크 환경이 구축되고 있다. 특히 유선과 무선으로 대별되는 두가지 환경과 IPv4와 IPv6로 대별되는 프로토콜 표준에 대해 각각 역추적 기능을 어떻게 제공할 것인지에 대한 연구가 필요하다. 또한 IP 계층에서의 보안 프로토콜이 제공되는 환경인 IPSec 기반 환경과 일반 IP 계층에서의 역추적 기능도 고려해 보아야 한다. 또한 기존의 방화벽 및 IDS가 담당하던 기능을 라우터가 포함하여 전체 네트워크의 안전성을 확보하면서도 패킷에 대해 개선된 역추적 기능을 제공하는 기법에 대해서도 연구가 되어야 할 것이다.

특히 IPv6 환경으로 급격히 변화하면서 역시 IPv6 환경에서의 DDoS 공격 등에 대한 대응 기술에 대해 연구가 수행되고 있다. IPv6는 기존의 IPv4보다도 성능, 보안 및 안전성이 개선된 구조를 제공하고 있다. 단순히 네트워크 주소 공간의 확대 뿐만 아니라, IPv6에서는 기본적으로 AH 및 ESP 기반의 IPSec 모듈을 통해 패킷을 전송하게 된다. 따라서 IPv6 기반의 패킷은 기존의 IPv4 기반 네트워크 환경보다 안전성이 향상되었다. 하지만 IPv6 구조의 복잡성 및 난해성으로 인해 마찬가지로 기존 IPv4 환경과 유사한 방식의 DDoS 공격이 가능하다. 특히 IPv6에서는 이동성을 지원하는 과정에서 보안 취약점이 발견되는 등 더욱 더 심각한 문제를 유발할 수도 있다. 따라서 앞으로는 IPv6 환경에 기반한 DDoS 대응 기술에 대해 심도있는 연구가 수행되어야 할 것이다.



(그림 12) NS-2 기반의 IP 역추적 시뮬레이션

3. IP 역추적 시뮬레이션

네트워크 공격 등에 대한 대응 기술로 제시된 IP Traceback 기술의 성능을 실험하기 위해서는 일반적으로 네트워크 공격 형태를 모의적으로 구성하고 현재의 DDoS 공격과 유사한 형태를 시뮬레이션하여 대응 기법의 성능을 비교 분석할 수 있다.

현재 IP 역추적에 대한 시뮬레이션 기법으로 가장 많이 사용되는 것은 NS-2 기반의 시뮬레이터를 기반으로 실험하는 것이다. 유선 네트워크 형태를 랜덤하게 구성하여 DDoS 공격 네트워크 형태를 구축하고 이를 통해 패킷을 전송하여 피해 노드에서의 경로 역추적 과정을 모의 실험할 수 있다.

NS-2 시뮬레이터는 Southern California 대학의 Information Sciences Institutes 에서 개발한 것으로서 대부분의 인터넷 프로토콜을 시뮬레이션 할 수 있고 연구자들이 제안하는 새로운 프로토콜들을 시나리오에 맞게 시뮬레이션하여 기존의 프로토콜과 비교해 수 있어서 많은 연구 결과를 검증하기 위해 사용하고 있다. NS-2 시뮬레이션을 기반으로 실험할 경우 제시한 알고리즘에 대한 성능을 효율적으로 실험할 수 있으며 제시한 알고리즘과 기존 알고리즘을 효율적으로 비교/분석할 수 있는 특징을 제공한다.

(그림 12)와 같이 DDoS 공격 네트워크를 구성하고 이를 기반으로 현재까지 제시된 IP 역추적 기법들에 대해 시뮬레이션하여 전체적인 트래픽량을 비교 분석할 수 있다. 임의의 형태의 네트워크를 시뮬레이터상에서 구성할 수 있으며 이를 통해 다양한 형태의 네트워크 토폴로지를 구성할 수 있다. 본 연구에서는 (그림 12)와 같은 공격 구조를 설계하고 실제적으로 IP 패킷에 대한 역추적 성능을 실험할 수 있다.

V. 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 기술에 대해 살펴보았다. 역추적 기술의 구조와 현황, 문제점 및 성능 비교 평가를 중심으로 기술하였으며, 현재까지 제시된 IP 역추적 기술에 대한 개선 방향 등에 대해 고찰하였다. 본 연구 분야는 앞으로도 네트워크를 대상으로한 해킹 공격 등에 능동적으로 대처하기 위해서는 다양한 분야에 대한 연구가 필요하다.

참 고 문 헌

[1] L. Garber. "Denial-of-service attacks trip the Internet". Computer, pages 12, Apr. 2000.

[2] Computer Emergency Response Team, "TCP SYN flooding and IP Spoofing attackts," CERT Advisory CA-1996-21, Sept, 1996.

[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, Department of 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.

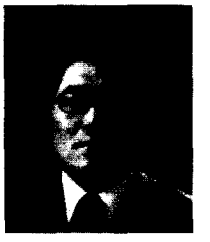
[10] H. Y. Chang et al., "Deciduous : Decentralized Source Identification for Network-based Intrusions," Proc, 6th IFIP/IEEE Int'l Symp., Integrated Net., Mmgt., 1999.

[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.

[14] W. Lee and K. Park, "On the Effectiveness of Route Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," Proc. SIGCOMM, ACM Press, pp. 15-26., 2001.



이 형 우

1994년 2월 : 고려대학교 컴퓨터학과 졸업(이학사)

1996년 2월 : 고려대학교 컴퓨터학과 졸업(이학석사)

1999년 2월 : 고려대학교 컴퓨터학과 졸업(이학박사)

1996년 ~ 현재 : 컴퓨터과학기술연구소 연구원

1999년 ~ 2003년 : 천안대학교 정보통신학부 조교수

2003년 ~ 현재 : 한신대학교 소프트웨어학과 조교수

<관심분야> 정보보호, 네트워크 보안, 해킹·바이러스, 스테가노그래피, 침해대응/스팸대응기술, 컴퓨터 포렌식스 기술 등