TTL 기반 개선된 패킷 마킹 기법을 이용한 공격 근원지 역추적 기법

김길한° 이형우
한신대학교 소프트웨어학과

gillty@empal.com°, hwlee@hanshin.ac.kr

Attack Origin Traceback with Advanced Packet Making Mechanism

Gill-Han Kim°, Hyung-Woo Lee
Department of Software, Hanshin University

요 약

인터넷을 통한 보안 위협 중 대표적 방법으로는 분산 서비스 거부 공격(DDoS)이 있다. DDoS은 해킹 공격자가 공격 근원지 IP 주소를 스푸핑하여 공격목표로 하는 시스템의 가용자원을 고갈시키거나 과도한 부하를 유발시켜 서비스를 중단시킨다. 이에 대한 대응 기술로 제시된 IP 역추적 기술은 DDoS 공격의 근원지를 판별하고 공격 패킷이 네트워크 상에서 전달된 경로를 재구성하는 기법이다. 본 연구에서는 기존의 역추적 기술인 패킷 마킹 기법에서 DDoS 공격에 대한 판별 과정 없이 임의의 패킷에 대해 역추적 정보를 생성 즉 DDoS 공격에 능동적으로 대응하고 있지 못하는 단점에 착안하여 DDoS 공격 패킷에 대해 개선된 패킷 마킹 기법을 제시하고, 또한 TTL을 통하여 스푸핑된 IP 근원지를 효율적으로 역추적하는 방안을 제시하였으며. 실험 결과 네트워크 부하를 줄이면서도 역추적 성능을 향상시킬 수 있었다.[1)]

1. 서 론

현재 TCP SYN flooding[1] 공격과 같은 서비스 거부 공격(Dos: Denial of service)[2]을 통해 TCP/IP 체계의 취약점이 노출되어 있기 때문에 네트워크 및 인터넷에서의 해킹 공격에 대응할 수 있는 방안에 대해 연구가 진행되고 있으며, DDoS 공격과 같은 해킹 공격에 대한 대응하는 방법은 크게 백신, 침입탐지 및 침임감내 기술 등과 같은 수동적인(passive) 대응 방법과 공격 근원지 역추적(Traceback) 기법과 같은 능동적인(active) 대응 방법이 있다.

역추적 방식은 네트워크상에 패킷이 전송되는 과정에서 사전에 라우터는 역추적 경로 정보를 생성하여 패킷에 삽입하거나 패킷의 목적지 IP 주소로 전달하여 주기적으로 관리하는 방식이다. 만일 피해 시스템에서 해킹 공격이 발생하면 이미 생성, 수집된 역추적 경로 정보를 이용하여 스푸핑된 해킹 공격 근원지를 판별하는 기법이다. 패킷에 대한 확률적 마킹(PPM : probabilistic packet marking)[3,4] 기법과 ICMP 메시지를 변형한 iTrace (ICMP traceback)[5] 기법 등이 이에 해당한다. 또한 최근 제시된 pushback[6] 기법은 DDoS 공격이 발생하였을 경우 패킷에 대한 판단 기능을 제공하며 패킷 전달 경로를 따라서 패킷에 대한 전송 제어 기능을 제공한다. 이 기법은 DDoS 공격 트래픽에 대한 제어 기능을 제공하지만 DDoS 해킹 공격 근원지를 역추적하는 기능은 제공하지 못하고 다만 패킷 전달 경로를 따라 패킷에 대한 전송 제어 기능을 제공하여 전체적인 네트워크 성능을 높여주고 있다.

따라서, 본 연구에서는 기존의 DDoS 공격에 대한 제어 기능을 제공하는 pushback 기법을 역추적 기능과 접목하여 스푸핑된 DDoS 패킷에 대한 IP 근원지를 역추적하는 기술을 제안하고자 한다. 라우터에서는 pushback 기법을 적용하여 트래픽에 대한 판별/제어 기능을 수행하며 만일 DDoS 공격이 발생하였을 경우 상위 라우터로 pushback 메시지를 전송하고 역추적 정보를 해당 패킷의 헤더에 마킹하여 전달한다. 제시된 기법을 통해 기존의 역추적 기법보다 관리시스템 부하, 네트워크 부하 및 역추적 기능 등을 향상시킬 수 있었다.

1) 본 연구는 대학IT연구센터육성지원사업의 연구결과로 수행되었음

2. 개선된 패킷 마킹 기반 역추적

2.1 ACC 기반 역추적 구조

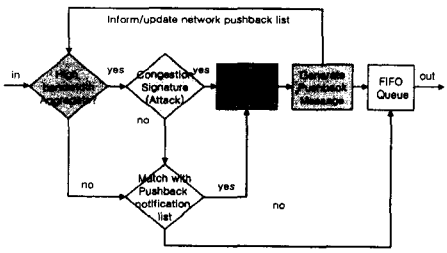
네트워크는 노드 집합 V와 에지 집합 E로 구성된 그래프 $G=(V,E)$로 정의할 수 있다. 다시 네트워크 노드 집합 V는 종단 시스템과 내부 노드에 해당하는 라우터로 나눌 수 있다. 에지는 V 집합 내에 있는 노드들에 대한 물리적인 연결에 해당한다. $S \subset V$를 공격자라고 정의하고 $t \in V/S$를 피해 시스템이라고 정의한다. 만일 $|S| = 1$일 경우 단일 공격자에 의한 해킹 공격을 의미하고 공격 경로 정보 $P = (s, v_1, v_2, ..., v_d, t)$인 경우 공격 시스템 s에서 피해 시스템 t로 d개의 라우터를 통해 전달된 공격 경로를 의미한다. 이때 전달된 패킷의 수를 N이라고 하자. 만일 패킷내에 라우터에 대한 링크 정보 $(v, v') \in E$를 마킹할 수 있는 필드가 있다면 이를 확률 p로 샘플링하여 전달하게 된다. 패킷에 대해서 라우터에서는 일정한 확률로 패킷을 선택하여 에지에 대한 정보와 라우터에 대한 거리 정보를 패킷내에 포함시켜 전달할 수 있다. 기존의 기법에서는 임의의 확률 p로 패킷을 선택하여 여기에 라우터에 대한 링크 정보를 마킹하여 전달하게 된다. 만일 네트워크 상에서 노드 v_i에서 마킹하였을 경우 다른 라우터에 의해서는 재마킹되지 않고 전달될 확률 α_i을 계산하면 다음과 같다.

$$\alpha_i = Pr(x_d = (v_{i-1}, v_i)) = p(1-p)^{d-1} \ (i = 1, 2, ..., d)$$

따라서 확률 α_i는 공격자에 해당하는 패킷 정보가 다른 라우터에 의해서는 재마킹되지 않고 피해 시스템에 전달될 확률을 의미한다. 결국 피해 시스템에서 α_i 값을 높이기 위해서는 p 값을 크게 해야 하는데, 이는 라우터에서 빈번하게 마킹 과정을 수행해야 한다는 것을 의미하므로 기존의 기법에서는 결

과적으로 네트워크 성능을 저하시키게 된다.

본 연구에서 제시하는 기법은 라우터에서 임의의 확률 p로 패킷을 샘플링하여 마킹하지 않고 pushback 기반 ACC 모듈에 의해서 이상 트래픽이 발견되었을 경우 패킷에 대한 마킹 과정을 수행하게 된다. 물론 기존의 ACC 기법에서 사용하는 방법과는 달리 이상 트래픽이 발견되었을 경우 단순히 pushback 메시지를 상위 라우터에 재귀적으로 전달하는 것이 아니라, 상위 라우터에 pushback 메시지를 전달하면서 해당 패킷에 마킹 과정을 수행하는 것이다. 본 연구에서 제안한 구조는 아래 <그림 1>과 같다.



<그림 1> 제안한 라우터 기반 DDoS 근원지 역추적 구조

제안한 구조에서는 라우터에 들어온 패킷에 대해 트래픽의 대역폭을 검사하고 일정 이상으로 도착하게 되면 공격 형태에 해당하는 혼잡 시그너쳐인지를 판단하게 된다. 만일 공격 형태 트래픽에 해당한다면 패킷에 마킹과정을 수행하고 동시에 해당 패킷에 대한 pushback 메시지를 생성하여 이를 라우터의 출력 큐로 하여금 앞단위 라우터에게 전송토록 한다. 만일 대역폭 조건을 만족하지 않을 경우에는 이전에 pushback 메시지를 통해 주변 라우터로부터 전달된 정보가 있는지를 확인하고 만일 해당된다면 마찬가지로 패킷에 대한 마킹 과정을 수행한다. 위 조건을 만족하지 않을 경우 일반적인 트래픽으로 간주하여 다음 라우터로 전달한다.

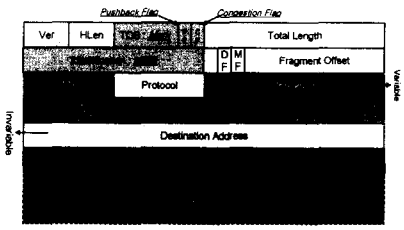
2.2 ACC 기반 개선된 마킹 기법

2.2.1 패킷 마킹 필드

라우터 R_x의 IP 주소를 A_x라고 하자. 그리고 R_x에 도착한 IP 패킷을 P_x라고 할 때, P_x에서의 헤더에서 마킹 정보를 저장할 수 있는 24 비트를 M_x라고 하자.

패킷 P_x에서 M_x는 아래 <그림 2>와 같이 TOS(type of service) 필드 8비트와 ID 필드 16비트로 구성된다. TOS 필드인 경우 현재 필드에 대한 정의만 되어 있을 뿐 실제적으로 사용하고 있지 않다. 따라서 TOS 필드 값을 사용한다고 하더라도 전체 네트워크에 영향을 미치지 않는다. 현재의 TOS 필드는 상위 3비트가 우선순위 비트로 설정되어 있고, 다음 3비트는 최소지연, 최대 성능 및 신뢰성 필드로 정의되어 있으나 현재는 사용하고 있지 않다. 다만 최근에 RFC2474에 의하면 Differenciated Service 필드(DS field)로 재정의하였으며 TOS 8비트 중에서 상위 6비트만을 사용하고 하위 2 비트는 사용하지 않고 있다.

따라서 본 연구에서는 TOS 필드 중에서 현재 사용하고 있지 않은 2비트에 대해서 PF(pushback flag)와 CF(congestion flag)로 정의한다. 특히 CF인 경우 RFC2474에서도 네트워크상에서 혼잡 현상이 발생하였을 경우 1로 설정하도록 정의되어 있다.



<그림 2> 제안한 기법에서의 패킷 마킹 필드

2.2.2 TTL 이용하여 거리정보 계산

24비트 M_x 정보에 대해서 라우터 R_x에 대한 IP 주소 A_x 값을 패킷 헤더에 마킹하는 과정은 다음과 같다.

패킷에서 마킹이 가능한 24비트 정보에 대해서 pushback 과정을 통해 이상 트래픽이 발생하였을 경우 이에 대한 마킹을 위해 라우터 R_x 자신의 IP 주소 A_x와 pushback에 의한 전단계 라우터 R_y의 IP 주소 A_y를 패킷에 마킹한다. 24비트 내에 두개의 라우터 주소값을 마킹해야 하기 위해서 라우터에 대한 해쉬 값을 적용하여 인증 기능도 제공하는 주소값을 마킹하게 된다. 모든 패킷의 TTL(time to live) 필드는 8비트 정보로 구성되며 패킷 전송시 일반적으로 255로 설정되어 전송된다. 라우터에 의해 전송되는 과정에서 TTL 값은 1씩 감소되어 최종적으로 목적지에 전달된다. 현재 TTL 값은 네트워크상에 패킷 전송시 대역폭을 확보하고 목적지에 도착하지 않는 패킷을 제어하기 위한 목적으로 사용된다. 기존의 연구에서는 TTL 값을 사용하지 않고 다만 별도의 hop 카운터 필드를 두어 패킷이 전달된 거리 정보를 계산하도록 하고 있다. 그러나, 본 연구에서는 라우터 R_x에 도착한 패킷의 TTL 값에서 일부 정보를 사용하여 패킷 마킹 과정에 사용한다.

구체적으로 TTL 필드 8비트에서 일반적으로 네트워크 홉 거리는 최대 32 정도로 되어 있기 때문에 라우터 R_x에 도착한 패킷 P_x의 TTL 필드 하위 6 비트 정보만으로도 패킷이 전달된 거리 정보를 계산할 수 있다. 즉, 패킷 P_x에서 TTL 필드에서 하위 6비트 정보에 추출하여 이를 T_x라고 하고 패킷의 TOS 6비트 필드 P_x^{TF}에 저장한다.

$$T_x = TTL\,of P_x \wedge 00111111$$

T_x 값은 현재 패킷이 공격지 시스템으로부터 전달된 거리 정보를 나타내며, 만일 이를 패킷에 포함시킨다면 목적지 시스템 V에 패킷이 도달하였을 경우 V에서 마찬가지로 계산된 T_x 값을 비교하여 패킷이 라우터 R_x로부터 전달된 거리 정보도 계산할 수 있다.

2.2.3 제안된 패킷 마킹 기법

앞에서 제시한 ACC 기반 pushback 모듈을 통해 이상 트래픽이 발생하였다는 것을 통보받게 되면 이제 라우터 R_x에서는 pushback 메시지 내에 포함된 혼잡 시그너쳐에 해당하는 패킷 P_x에 대해서 마킹 과정을 수행한다.

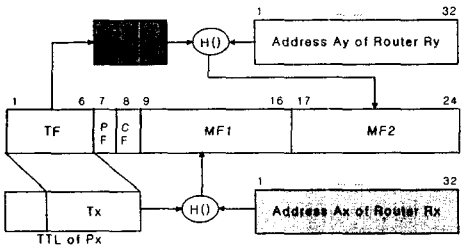
우선 pushback 메시지를 받았기 때문에 TOS 필드에서의 PF 필드를 1로 설정한다. 그리고 현재 패킷 P_x에서의 TTL 필드 8 비트에 대해 T_x값을 계산하고 이를 TOS 필드 6비트에 저장한다. 그리고 라우터 R_x의 주소 A_x와 앞에서 계산된 T_x 값에 대해 해쉬 함수 $H(\cdot)$를 사용하여 8비트 해쉬 값을 계산하고 이를 ID 필드 처음 8비트인 P_x^{MF1}에 마킹한다. 마킹된 패킷은 패킷의 목적지 주소에 해당하는 라우팅 경로의 다음

라우터 R_y에게 전달된다.

이제 라우터 R_y는 패킷의 PF 필드값 P_x^{PF}을 보고 1로 설정되어 있는 경우 패킷에서의 TOS 필드 6비트에 해당하는 P_x^{PF}에서 1을 뺀 값과 라우터 IP 주소 A_y에 대해 마찬가지로 해쉬 함수를 적용하여 P_x^{MF2} 에 마킹한다.

$$P_x^{MF1} = H(T_x \mid A_x),\ P_x^{MF2} = H(P_x^{TF} - 1 \mid A_y)$$

마킹과정을 수행한 후에는 CF 필드 값을 1로 설정하여 다음 라우터로 전송하게 되며 다음 라우터는 PF 필드 값과 CF 필드 값이 1로 설정되어 있는 경우에는 이전 라우터에 의해 마킹된 패킷이므로 더 이상 마킹 과정을 수행하지 않는다.

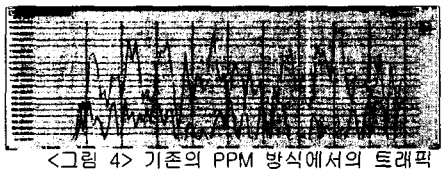


<그림 3> 제안한 기법에서의 패킷 마킹 구조

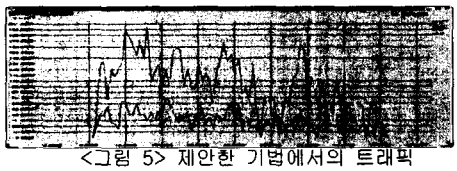
3. 성능 분석

본 연구에서 제시한 기법에 대한 성능을 평가하기 위해서 Linux 환경에서 ns-2 시뮬레이터를 이용하여 성능을 분석하였다. 네트워크를 구성하고 0 노드, 1번 및 2번 노드에서 DDoS 공격을 수행하도록 시뮬레이션 하였다.

실험 결과 기존의 패킷 마킹 기법은 DDoS 공격에 대해 각 라우터에서 확률 p로 샘플링하여 마킹하는 방식이므로 전체 마킹된 패킷(파란선:v1.tr)의 수가 DDoS 트래픽(붉은선:r0.tr)에 비례하여 생성되는 것을 볼 수 있다. 본 연구에서 제시하는 기법인 경우 pushback 기법을 적용하여 DDoS 트래픽에 대한 마킹 과정을 수행하기 때문에 마킹된 패킷의 수가 25% 정도 감소하는 것을 확인할 수 있었다.



<그림 4> 기존의 PPM 방식에서의 트래픽



<그림 5> 제안한 기법에서의 트래픽

제안한 기법과 기존의 IP 역추적 관련 기술들의 성능을 비교 분석하면 다음과 같다. 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 보인다.

기존의 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 취약한 특성을 보인다. 전체적으로 현재까지 제시된 IP 역추적 기법을 검토하였을 경우 대부분 기존 라우터에 대한 변형 및 추가적인 네트워크/시스템 부하가 발생한다는 것을 알 수 있다.

본 연구에서 제시한 기법은 기존의 PPM 기법과 유사한 방식으로 작동하기 때문에 관리 부하가 적으며, 라우터에서 패킷에 대한 판별 및 제어 기능을 적용하였기 때문에 DDoS와 같은 해킹 공격이 발생하였을 경우 전체 네트워크의 부하를 줄일 수 있다는 장점을 제공한다. 또한 기존의 PPM 기법에서는 임의의 확률 p로 패킷을 선정하여 마킹 과정을 수행하였으나 본 연구에서 제시한 기법은 ACC 기반 혼잡 제어 기능을 사용하고 TTL 필드 값을 이용하여 경로 정보를 마킹하기 때문에 피해 시스템에 도달하는 역추적 경로 재구성에 필요한 패킷의 수를 줄일 수 있었다.

따라서 전체 네트워크 상의 대역폭을 향상시킬 수 있고, 적은 개수의 마킹 패킷만을 가지고도 DDoS 공격 근원지에 대한 경로를 재구성할 수 있다. 경로 재구성을 위해서는 네트워크에서 n개의 라우터를 거치는 경우 단지 n개의 역추적 메시지만으로 근원지 경로를 재구성할 수 있다는 장점을 제공한다. 물론 라우터에 ACC 기반 pushback 모듈에서의 DDoS 관련 판별 기능을 추가로 수행하기 때문에 메모리 요구는 증가한다는 단점이 있다.

4. 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 기술을 제시하였다. 기존 역추적 기술의 구조와 현황, 문제점 등을 고찰하여 네트워크상에서 DDoS 해킹 공격에 대한 판단/제어 기능도 제공하면서도 피해 시스템에서는 스푸핑된 해킹 공격 근원지를 효율적으로 역추적할 수 있는 새로운 패킷 마킹 기법을 제시하였다. 제시한 기법은 기존의 기법보다 부하, 성능, 안전성 및 역추적 기능에서 개선된 특징을 보인다.

참 고 문 헌

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

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

[3] 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.

[4] D. X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback," Proc, Infocom, vol. 2, pp. 878-886, 2001.

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

[6] S. Floyd, S. Bellovin, J. Ioannidis, K. Kompella, R. Mahajan, V. Paxson, "Pushback Message for Controlling Aggregates in the Network," Internet Draft,2001