# 트래픽 감지 기법을 통한 라우터에서의 서비스 거부 공격 방지 기법

이호균° 김정녀
한국전자통신연구원 보안운영체제연구팀
{hglee°, jnkim, }@etri.re.kr

# Methods of Defense DoS Attack by Traffic Metering and Controlling Technique in a Router

Ho Gyun Lee° Jeong Nyeo Kim
ETRI Secure OS Research Team

**요 약**

분산 서비스 거부 공격 기법이 점점 더 향상되어감에 따라 이에 대한 대응 기법 또한 여러 가지가 제안되고 있다. 기존의 탐지에 기반을 둔 기법들은 공격을 탐지하기 위한 Rule이 미리 준비 되어야 한다는 점에서 실제 트래픽과 구별이 어려운 DDoS 공격의 경우 효율적인 대응이 될 수 없다. 이를 극복하기 위해서 트래픽 감지와 QoS 기법에 기반을 둔 대응 방안이 활발히 연구 중에 있다. 본 논문에서는 현재까지 나와 있는 트래픽 감지 기반의 대응 기법 연구들을 정리하고 라우터 기반의 보안기능 개발 연구에서 트래픽 감지 기반의 대응 방안 적용 과정을 소개한다.

## 1. 서 론

2003년 1월25일과 1988년11월2일은 컴퓨터 보안 특히 네트워크 보안 담당자들에게는 매우 의미가 깊은 날이다. 전자는 대한민국에서 전문가 뿐 만이 아니라 일반인들까지도 서비스 거부 공격 (DoS) 이 무엇이고 어떤 파괴력을 가진 것인지 인식하게 되는 계기가 된 날이다. 후자는 DoS 공격의 원조 격인 인터넷 웜이 미국에서 처음으로 네트워크에서 확산, 실제 피해를 입힌 날이다[1]. 이것이 계기가 되서 정부 기관과 학계를 중심으로 인터넷 정보전에 대한 연구가 시작되었다. 서비스 거부 공격이란 컴퓨터가 정상적인 작업을 처리하기 위해서 필요한 여러 가지 자원들, 즉 네트워크 대역폭이나 TCP/IP 스택 처리를 위해서 필요한 캐쉬, 메모리, 버퍼들을 향해서 과도한 서비스 요청을 보냄으로써 서비스가 불가능한 상태로 만드는 공격을 지칭한다. 초기의 서비스 거부 공격은 그다지 정교하지 못해 ping 과 같은 ICMP메시지를 단순 반복해서 보냈기 때문에 탐지 기반의 보안 시스템에서도 대응이 가능했지만 서비스 거부 공격이 점점 정교해짐에 따라 결국 공격 패킷들과 일반 패킷들의 구분이 불가능한 상황이 될 것이다. 이를 해결하기 위해 탐지 기반의 대응이 아닌 트래픽 감지 기반의 대응 방법이 각광 받고 있다. 트래픽 감지 기반의 대응 방법은 기존에 공격 패킷들의 패턴을 미리 저장해 두고 이를 네트워크 내부의 모든 패킷들과 일일이 비교해서 공격을 탐지하는 방식과는 달리 기존의 네트워크 기술, 즉 서비스 품질 보장 기법의 요소 기술들을 활용하고 있다. 서비스 품질 보장 기법 즉 QoS 또는 Diffserv 로 지칭되는 기술에는 트래픽 측정과 트래픽 조절이라는 두 가지 핵심 기술이 있다[4][5]. 감지 기반의 대응 방법은 트래픽 측정 기능을 이용해서 Layer 4까지 트래픽의 변화 추이를 감시한다. 이를 통해서 트래픽의 이상 변화를 감지하고 이에 대응하기 위해서 트래픽 조절 기능을 이용하는 것이다. 본 논문에서는 2장에서 현재까지 나온 DDoS 공격의 대응 방안들, 특히 그 중에서 QoS 기법을 이용한 방법에 대해서 기술한다. 3장에서는 네트워크 종합 침해 대응 시스템 개발 연구에 대해서 소개하고, 4장에서는 라우터용 보안 기능 중에서 트래픽 측정과 조절을 이용한 DDoS 공격 완화 기능의 개발 과정에 대해서 설명한다. 마지막으로 5장에서 결론을 맺는다.

## 2. 기존의 대응방법과 감지 기반 대응 방안 정리

### 2.1 공격자 위치 추적 기법

위치 추적 기법은 공격 자체를 막을 수는 없지만 범인 추적에 활용하고 공격에 대한 법률적인 증거 수집에 이용될 수 있다. 위치 추적 기법에는 두 가지 방법이 있다. 첫 번째 방법은 라우터에서 추후에 있을 위치 추적을 위해서 라우터를 지나간 모든 패킷들에 대한 정보를 기록하는 것이다. 두 번째 방법은 라우터가 패킷의 목적지 호스트에게 ICMP와 같은 별도의 정보 패킷을 전송해 주는 방법이 있다[7].

2.2 공격 탐지와 필터링 기법

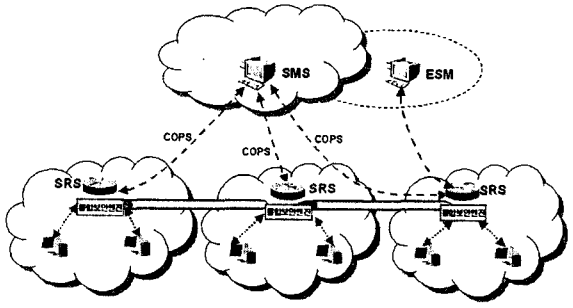
공격 탐지는 공격 패킷과 그 패킷이 속한 플로우를 식별해서 망 관리자에게 보고를 하고 필터링 기능은 망 관리자의 명령 또는 자동 정책에 따라 공격 패킷을 폐기 또는 조절 시킨다. 이때 탐지 기능의 효과성을 측정하기 위해 FNR(False Negative Ratio)와 FPR(False Positive Ratio) 단위를 사용한다. 또한 필터링의 효과 측정을 위해서는 NPSR(Normal Packet Survival Ratio)를 사용한다[2]. NPSR은 뒤에 얘기할 감지 기법을 이용한 DDoS 완화 기법의 단점이 되는 사항으로 이에 대한 개선이 주요 연구 과제 중의 하나이다.

2.3 감지 기반의 대응방법

트래픽 감지 기법은 QoS 기법의 트래픽 측정 기능을 이용해서 트래픽 변화 정보를 보고 공격의 발생을 탐지함과 동시에 트래픽 조절 기능을 이용해서 호스트가 서비스 중단 상태에 빠지는 상태를 미연에 방지한다. 하지만 트래픽을 패턴 정보를 보고 검사하는 것이 아니라 전체양의 변화 상황을 보고 유추하는 것이기 때문에 FNR, FPR 평가 기준으로 보았을 때 높을 성능을 갖고 있다고 말할 수 없다. 또한 트래픽 조절 또한 정확하게 그 패킷이 공격 패킷이란 판단 하에 조절하는 것이 아니므로 NPSR 수치 또한 높다고 할 수 없다. 그럼에도 불구하고 탐지 기법과 비교해서 성능 상의 장점, 그리고 중단 없는 서비스가 가능하단 점에서 매력적인 대응 방안이 되고 있다. 또한 탐지 기법은 기존에 알려져 있지 않은 새로운 공격에 대해서는 전혀 무방비인 반면에 감지 기법은 트래픽 측정 정보로 유추하므로 공격 패턴과 상관없는 대응이 가능하다. 따라서 감지 대응 기법의 가장 주요 연구 과제는 FNR, FPR, NPSR을 높이기 위해서 감지 결과를 판단하고 대응을 가할 패킷을 구분하기 위한 트래픽 분류 기준을 세우는 것이다.

## 3. NGSS와 SRS 소개

NGSS(Next Generation Security System)은 네트워크 종합 침해 대응 시스템의 약자이다. NGSS는 공중망이나 ISP망과 같은 전달망의 엑세스망에 위치하여 전달망을 통과하는 트래픽에 대한 총체적인 보호를 통하여 차세대 네트워크 보안 서비스를 고객 사이트에게 제공하기 위한 시스템이다. NGSS는 보안관리기능을 수행하는 SMS와 보안노드 기능을 수행하는 SGS와 SRS, 그리고 이들 사이의 상호작용을 제공해주는 인터페이스로 구성된다. SMS 시스템은 NGSS 시스템의 관리 대상 네트워크에 대한 보안 서비스의 제공과 효율적인 보안 관리의 제공을 위한 제반 기능을 지원한다. SGS (Security Gateway System)는 대규모 네트워크 환경에서 침입 탐지 및 대응을 위한 보안노드이다. SRS는 보안기능을 추가한 라우터이다. 보안기능으로는 패킷필터링, 침입탐지, 신뢰채널, 사용자인증, 접근제어, 감사추적, 트래픽미터링 및 보안관리 등이 있다. 본 논문에서 NGSS 시스템에서 SRS의 보안 기능, 특히 트래픽미터링을 통한 DDoS 공격 방어에 초점을 맞추고 있다. 그림 1은 NGSS망에서 SMS와 SRS간의 망 구성을 나타내고 있다.




(그림 1) NGSS 시스템 내에서 SMS와 SRS 전개도

SRS는 상용 라우터를 기반으로 하여 그 위에 보안기능을 올려놓은 형태이며 크게 세 가지 엔진으로 분류할 수 있다. 맨 아래쪽은 네트워크 엔진으로서 패킷 단위의 처리를 필요로 하며 성능 향상을 위하여 전용 하드웨어를 사용하는 것을 고려할 수 있는 부분이다. 여기에는 트래픽미터기능, 패킷센서/필터기능, 신뢰채널기능이 있다. 네트워크 엔진 위쪽은 보안 엔진으로서 네트워크 인터페이스나 특정 하드웨어에 종속되지 않는 기능들이 여기에 속한다. 여기에는 사용자인증, 접근제어, 정책적용, 침입탐지 및 감사/로그 기능이 있다. 보안 엔진 위는 서비스 엔진으로서 명령어 및 라이브러리, 인증 인터페이스, 경보관리, 대응관리, 정책관리, 노드관리 및 키 관리 인터페이스 기능이 있다.

## 4. SRS의 감지 기반 대응 메커니즘

SRS 트래픽 감지 기능은 세 가지로 분류된다.

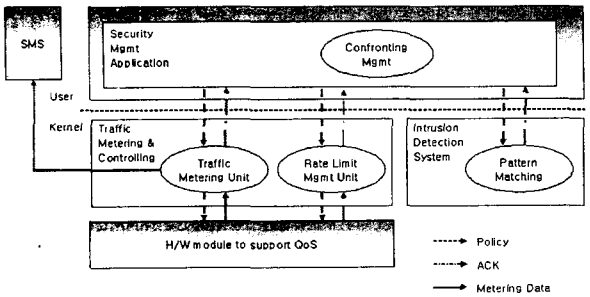
1) 트래픽 통계 정보 보고 기능

상위 SMS가 트래픽 Flow 단위까지 분석이 가능하도록 트래픽 통계 정보를 주기적으로 전송한다. 기존 네트워

크 장비와의 호환을 위해서 전송 프로토콜은 Netflow 포맷을 따른다. SMS를 위한 정보 수집의 정확성을 향상시키는 것과 SRS의 기존 네트워크 기능 서비스에 걸리는 부하를 줄여야 하는 상반된 요구 사항을 적절히 조절할 수 있도록 Timing Control 기능이 지원된다.

2) 트래픽 조절 기능 (대응 기능)

SMS에서 공격이라고 판단한 flow들을 제거 또는 조절하기 위한 기능으로 Diffserv의 Traffic Control 기능을 이용한다. 기존의 Diffserv-Traffic 조절 기능은 IPv4 프로토콜의 TOS 필드 값을 이용해서 트래픽을 분류하고 여러 가지 큐잉 이론을 이용하여 트래픽을 조절하였다. SRS에서는 기존 메커니즘에 트래픽 분류를 TOS 필드가 아니라 5-tuple 기준으로 분류할 수 있도록 수정한다. 여기서 5-tuple은 송신ip, 수신ip, 송신 port, 수신 port, 프로토콜 타입이 된다.




(그림 2) SRS의 트래픽 감지 기반 대응 메커니즘

3) 자동 대응 결정 기능

SRS는 SMS의 대응 정책에 따라서 트래픽 조절 기능을 수행할 뿐만 아니라 SRS 자신 또는 SRS가 관리하는 서브넷 망을 서비스 불능 상태에 빠뜨릴 수 있는 명백한 이상 트래픽이 유입될 경우 자동으로 해당 트래픽의 유입을 막을 수 있도록 한다. 이는 Aman Garg의 Idea와 유사하나 Aman Garg의 아이디어처럼 관리하는 서브넷의 모든 호스트의 자원 소비 추이를 추적하지 않고 각 트래픽들을 분류시켜서 각 트래픽 분류 전체의 Volumn 변화 추이만을 추적한다[3]. 이는 트래픽 감지 기능이 올라가는 라우터의 기존 서비스에 걸리는 부하를 최소화하기 위함이다. 트래픽 분류 방법은 SMS로 보고하는 Netflow 포맷의 5-tuple 까지가 아닌 3-tuple만을 기준으로 한다. 3-tuple에는 protocol type과 송신 port, 수신 port가 포함된다. SRS는 트래픽 분류 테이블을 유지하고 있는데 이는 3-tuple 항목들을 Hash 테이블로 동적으로 관리한다. 또 각 3-tuple 항목은 timer-control 이 정한 시간에 따라 갱신되며 이 시간은 5분을 넘지 않는다. 이는 SRS와 해당 서브넷을 다운시킬 수 있는 시간 이내가 된다.

## 5. 결 론

본 논문에서는 DDoS 공격의 메커니즘과 동향에 대해서 정리하고 지금까지 연구되어온 대응 방안에 대해서 기술하였다. 이를 바탕으로 NGSS, SRS 시스템과 SRS 시스템 기능 중 트래픽 감지를 통한 DDoS 공격 완화 기능에 대해서 소개하였다. NGSS는 DDoS 공격 대응을 위한 3가지 방어 방법인 공격 예방, 추적, 탐지와 대응 기능 모두를 아우르는 종합 침해 대응시스템 구축을 목표로 개발 중에 있다.

## 참 고 목 록

[1] Lars Klander, " Hacker Proof : The Ultimate Guide to Network Security", Delmar Learning, Jan. 1997

[2] Rocky K.C. Chang, "Defending against Flooding-based Distributed Denial-of-Service Attack : A Tutorial", IEEE Communication Magazine, Oct. 2002

[3] Aman Garg, "Mitigating Denial of Service Attack Using QoS Reguration"

[4] Y. Bernet et al., "A Framework for Differentiated Services", IETF Internet Draft, Feb. 1999.

[5] S. Blake et al., "An Architecture for Differentiated Services", RFC 2475, Dec. 1998.

[6] S.Gilson, "The Strange Tale of the Denial of Service Attack Against GRC.COM," http://grc.com/dos/grcdos.htm, Mar. 2002

[7] S. Savage et al., "Practical Network Support for IP Traceback," Proc. ACM SIGCOMM, Aug. 2000, pp. 295308.