

논문 2006-43TC-7-8

DDoS 공격에 대응하는 분산 네트워크 보안관리 기법

(A Scheme of Distributed Network Security Management against DDoS Attacks)

김 성 기**, 유 승 환*, 김 문 찬*, 민 병 준***

(Sung Ki Kim, Seung Hwan Yoo, Moon Chan Kim, and Byoung Joon Min)

요 약

웜 확산이나 자동화된 공격 도구에 의한 DDoS(Distributed Denial of Service) 공격은 도메인 경계를 넘어 통신 경로를 공유하는 정당한 사용자의 접근을 방해하기 때문에 지엽적인 도메인 차원의 방어와 대응은 현실적인 해결책이 되지 못한다. 더욱이 발신지 IP 주소를 위조하거나 정당한 발신지 IP 주소를 가지고 bogus 패킷을 과도하게 전송시키는 DDoS 공격은 정당한 사용자의 접근을 식별할 수 없게 한다. 본 논문에서는 이러한 문제점을 해결하기 위해 이웃하는 도메인간에 DDoS 공격 플로우를 식별하고 공격자 추적과 대응을 협업하는 분산 네트워크 보안관리 기법을 제시한다. 본 논문에서는 인터넷이 다수의 도메인으로 이루어져 있고 각 도메인에는 하나의 이상의 도메인 보안 관리자가 있다고 가정한다. 분산된 도메인 보안 관리자는 자신의 도메인 경계 라우터와 물리적 회선을 공유하면서 도메인 안팎으로 유통되는 공격성 패킷들을 식별하고 이웃하는 도메인 보안 관리자와 공격 발원지 추적 및 대응을 위한 메시지 교환을 수행한다. 도메인 보안 관리자를 구현하고 테스트베드를 통해 실험한 결과 지엽적인 도메인 차원의 탐지 및 대응에 비하여 탐지의 정확성(FPR: False Positive Rate, FNR: False Negative Rate)과 대응 효과(NPSR: Normal Packet Survival Rate)가 우수하였다.

Abstract

It is not a practical solution that the DDoS attacks or worm propagations are protected and responded within a domain itself because it clogs access of legitimate users to share communication lines beyond the boundary a domain. Especially, the DDoS attacks with spoofed source address or with bogus packets that the destination addresses are changed randomly but has the valid source address does not allow us to identify access of legitimate users. We propose a scheme of distributed network security management to protect access of legitimate users from the DDoS attacks exploiting randomly spoofed source IP addresses and sending the bogus packets. We assume that Internet is divided into multiple domains and there exists one or more domain security manager in each domain, which is responsible for identifying hosts within the domain. The domain security manager forwards information regarding identified suspicious attack flows to neighboring managers and then verifies the attack upon receiving return messages from the neighboring managers. Through the experiment on a test-bed, the proposed scheme was verified to be able to maintain high detection accuracy and to enhance the normal packet survival rate.

Keywords : DDoS(Distributed Denial of Service) Attacks, Worm, Security Management

I. 서 론

최근의 DDoS 공격은 웜(worm)의 형태로 종합되고 있으며 정상적인 패킷 패턴을 유지하면서 기존 보안 시스템이 공격 탐지의 기준으로 사용하는 규칙이나 임계

치를 교묘히 피하는 스텔스 공격 양상을 보이고 있다^[1].

이러한 DDoS 공격 패킷의 패턴은 크게 두 가지로 구별된다. 하나는 발신지 IP 주소를 랜덤하게 위조하여 패킷을 보내는 경우이고, 다른 하나는 정당한 발신지 IP 주소를 사용하지만 목적지를 랜덤하게 바꾸는 bogus 패킷의 발송이다. 전자의 공격은 공격자가 위치한 네트워크 경계 라우터에서 egress 필터링을 통해 효과적으로 방지할 수 있지만, 인터넷 상의 다른 모든 네트워크에서도 이를 지원하고 수행해야하는 전제조건이 따른다. 그

* 학생회원, ** 정회원, *** 평생회원, 인천대학교 컴퓨터공학과

(Dept. of Computer Science & Eng. Univ. of Incheon)

접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

리고 후자의 공격은 egress 필터링으로는 사전에 방지 할 수 없다는 것과 bogus 패킷의 목적지가 되는 네트워크에서는 경계 라우터가 극심한 패킷 처리 부하를 겪는 문제가 있다. 이 두 가지 공격 모두는 공격자가 의도하는 대로 공격대상을 결정할 수 있다. 그러나 공격을 하는 측이나 공격을 받는 측의 네트워크에서는 보안 시스템 입장에서 이들 공격 패킷의 식별이 쉽지 않다. 즉 현재의 트래픽이 비정상이라고 해서 경보를 발생한다 해도 정당한 사용자들의 접근을 정확하게 식별하기 어려운 문제가 있다. 게다가 공격 발원지를 추적하여 차단하지 않으면 도메인 경계를 넘어 통신 경로를 공유하는 정당한 사용자에게 최소한의 서비스 품질도 보장하기 어렵게 하고 마침내 서비스 거부 현상을 겪게 한다. 따라서 지엽적인 도메인 차원에서 DDoS 공격을 탐지하고 대응한다는 것은 현실적으로 한계가 있다.

본 논문에서는 발신자를 위조하고 목적지를 가변시키는 DDoS 공격으로부터 정당한 사용자의 접근을 보호하는 분산 네트워크 보안관리 기법을 제시한다.

현재의 정보 인프라를 수정하고 취약점을 모두 제거하지 못하는 현실에서 이와 같은 공격을 비용 효과적으로 대응하기 위해서는 접근권한이 미치는 범위, 보안정책, 보안 수행 환경이 서로 다른 네트워크, 즉 이종 도메인들 간에 공격자 식별과 대응을 상호 협력할 수 있는 분산 네트워크 보안관리 구조와 방안이 필요하다.

본 논문에서 제시하는 분산 네트워크 보안관리 구조는 인터넷이 다수의 도메인으로 이루어져 있고 각 도메인에는 하나 이상의 도메인 보안 관리자가 있다고 가정한다. 분산된 도메인 보안 관리자는 자신의 도메인 경계 라우터와 물리적 회선을 공유하면서 도메인 안팎으로 유통되는 공격성 패킷들을 식별하고 이웃하는 도메인 보안 관리자와 공격 발원지 추적 및 대응을 위한 메시지 교환을 수행한다. 교환되는 메시지는 식별된 공격자 정보를 담고 있는 pushback 메시지가 있고 이에 대한 응답 메시지로서 feedback 메시지가 있다.

pushback 메시지는 공격 발원지에서 공격 행위를 차단하는 역할을 하며, feedback 메시지는 공격자로 오인된 정상 이용자의 접근을 회복시킨다.

본 논문의 연구결과는 II장에서 논할 기존의 연구들이 간과하고 해결하지 못한 두 가지 중요한 문제점을 해결한다. 하나는 기존 정보 인프라에 현실적으로 적용하기 쉽고, 네트워크의 고속화에 역행하지 않으면서 보안성 향상을 이룰 수 있다는 것이고, 다른 하나는 정당한 사용자의 접근을 보호할 수 있다는 것이다. 이에 반

해 기존의 연구들은 이미 설치되고 운용중인 정보 인프라 전체에 상당한 수정을 가해야하는 현실적인 문제가 있고, 공격탐지로부터 정당한 사용자의 접근을 보호하지 못하는 단점이 있다.

본 논문의 II장에서는 DDoS 공격의 탐지와 대응에 관련된 기존의 연구결과들을 분석한다. III장에서는 분산 네트워크 보안관리 구조를 제시한다. IV장에서는 트래픽 플로우 정보를 유지할 수 있는 방법을 제시하고, DDoS 공격 유무의 판정과 공격성 플로우의 식별 방안을 제시한다. V장에서는 분산 네트워크 보안관리 방안을 제시하고 VI장에서는 실험방법과 결과를 분석한다. 마지막으로 VII장에서 결론을 맺는다.

II. 관련 연구

본 장에서는 DDoS 공격의 문제를 해결하기 위한 기존의 연구 결과들에 대하여 논한다.

DDoS 공격과 관련된 기존의 연구들은 크게 공격 탐지 방안을 위한 연구^[2]와 대응방안을 위한 연구, 그리고 보안 시스템들 간의 협업을 통해 공격을 탐지하고 대응하기 위한 연구^[3,4,5]들이 있다. 공격 대응을 위한 연구는 다시 IP 역추적 기술을 사용하여 공격 발원지를 추적하고 고립시키기 위한 연구^[6]와 공격의 강도를 완화시키는데 초점을 둔 연구^[7]가 있다.

Stone^[8]등은 네트워크상의 라우터가 "tracking" 라우터라고 하는 특별한 라우터로 패킷을 선택적으로 재지향하는 IP 터널을 사용하여 트래픽 범람 공격 징후를 탐지하고 의심스러운 트래픽을 차단할 수 있는 오버레이 네트워크(일명, CenterTrack)를 제안하였다.

Mahajan^[9] 등은 공격의 강도를 완화시키기 위해 집중형 혼잡을 제어하고 트래픽이 집중되지 않은 업스트림 라우터 쪽에서 공격 플로우들을 억제하는 pushback 기법을 제안하였다.

공격 발원지를 식별하여 대응하는 연구로는 라우터에서 패킷을 마킹하는 방법으로 공격 발원지를 추적하여 고립화하는 IP 역추적 기법^[10]과 ICMP 추적 기법^[11]이 있다. 그러나 참고문헌 [9]의 방안을 포함해서 이러한 기법들을 현실화하기 위해서는 정보 인프라가 이를 지원할 수 있어야 한다는 문제점이 있고, 인터넷 전체에서 공격자를 찾기 위한 패킷 수가 급격히 증가한다는 점과 이를 처리하는 네트워크 장치의 연산 비용이 높아진다는 문제점을 가지고 있다.

보안 시스템들 간의 협업을 통해 공격을 탐지하고 대응

하기 위한 연구로는 DARPA의 IDIP(Intrusion Detection Isolation Protocol)^[3], CITRA(Cooperative Intrusion Traceback and Response)^[4], AN-IDR(Active Network -Intrusion Detection and Response)^[5] 프로젝트가 있다.

IDIP는 기존의 IDS, 방화벽, 호스트 기반 대응 모듈, 기타 보안관리 시스템들 간의 협력을 통해 공격자를 역 추적하고 고립시키기 위한 프로토콜을 포함한 보안 기반 구조이다. 그러나 이 프로토콜 수행에는 몇 가지 문제점이 있다. 첫째, 모든 IDIP 노드가 모든 연결에 대한 감시 기능을 수행해야 하고 라우팅 패킷 정보에 대한 로그를 유지해야 한다는 것이며, 둘째, IDIP의 오탐지 보고에 따라 네트워크 전체에서 과도하게 대응할 수 있는 문제점이 있다. 셋째, 공격자가 고의적으로 IDIP 보고 메시지를 발생 시킬 수 있어 또 하나의 DDoS 공격이 될 수 있다. 마지막으로 IDIP를 프로토콜 스택으로 구현해야하는 부담과 보안 환경 변화에 적응하기 어려운 확장성을 가지고 있다는 문제점이 있다.

CITRA는 IDIP 기반 구조를 그대로 사용하면서 보안 정책 반영이 가능한 구조로 개선되었다.

AN-IDR은 기존의 IDIP 메커니즘과 액티브 네트워크 기술^[12]을 결합하여 IDIP의 기능의 유연성과 확장성을 부여한 시도이다. 액티브 패킷을 이용하여 공격자 추적과 고립화를 달성할 뿐만 아니라 설치된 악성 에이전트의 스캐닝 및 제거와 같은 침해된 시스템 복구 기능도 포함하고 있다. 그러나 이 연구 결과를 수용하기에는 현실적으로 해결해야 할 두 가지 결함들이 있다. 하나는 기술적인 문제로서 모든 IDR 수행 노드가 액티브 노드어야 한다는 점이며, 액티브 네트워크 기술이 내포하고 있는 문제, 즉 액티브 패킷의 인증, 공격자의 액티브 노드 악용 및 오용 방지, 결함 및 취약점에 완전무결한 액티브 노드의 구현이라는 문제점이다. 또 하나의 문제점으로는 법률적인 문제로서 도메인 경계를 넘는 추적과 실행, 사용자 패킷을 감사하는 행위가 법률상 자유롭지 못하다는 점이다.

III. 분산 네트워크 보안관리 구조

가. 네트워크 보안관리 구조

본 절에서는 차치적으로 보안정책을 적용하고 관리할 수 있는 범위의 네트워크, 즉 도메인을 중심으로 네트워크 보안관리 기능을 협업하는 구조를 제시한다.

(그림 1)은 Inter-domain 구조를 보이고 있다. 독립된 각 도메인들이 이웃 도메인들과 연결된 논리적인 구조를

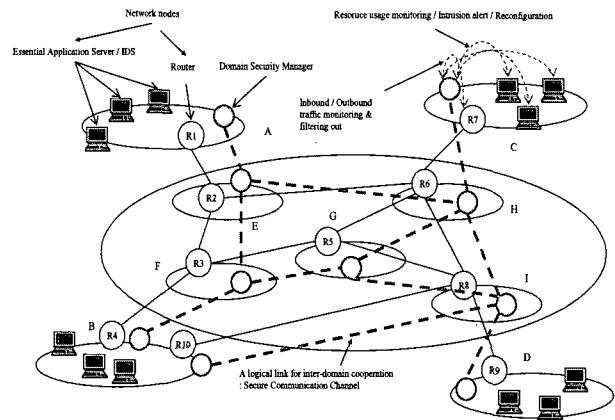


그림 1. 분산 네트워크 보안관리 구조

Fig. 1. Distributed network security management Architecture.

보이고 있다. 각 도메인의 경계에는 각각 하나의 도메인 보안 관리자(DSM : Domain Security Manager)를 두고 있으며 이웃하는 DSM과 point-to-point 연결을 맺는다. 이때 이들 간의 연결은 공격자에 의한 외부 공격을 막기 위해 안전한 통신 채널을 유지한다.

(그림 1)에서 각 도메인은 보안관리 목적으로 선택적으로 분할이 가능하며 내부적으로 보안 권한이 미치는 범위에 따라 sub-domain을 둘 수 있다. 호스트 수가 많은 도메인을 여러 sub-domain으로 분할하게 되면 공격 탐지 대상의 수가 분산되어 탐지 수행에 필요한 컴퓨팅 자원을 덜 수 있다.

나. 도메인 보안 관리자

DDoS 공격 탐지와 대응의 핵심적인 역할을 수행하는 DSM은 라우터나 스위치와 같은 네트워크 장치가 맡아야 할 기능을 대신 함으로써 전체 네트워크에 부하를 주지 않고 효과적인 보안관리를 수행한다. (그림 2)는 DSM

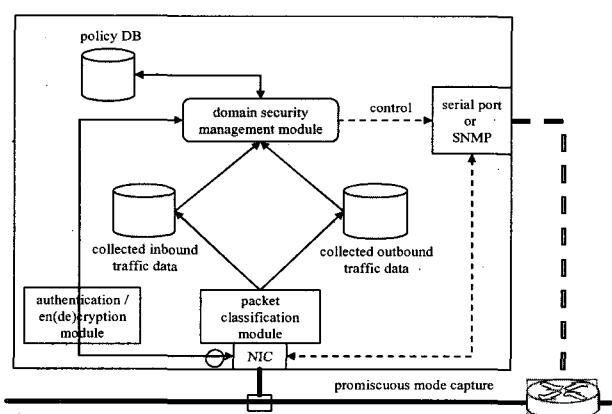


그림 2. 도메인 보안 관리자 시스템 구조

Fig. 2. A System Architecture of DSM.

시스템의 구조를 보이고 있다.

DSM은 (그림 2)와 같이 라우터를 유출입하는 모든 트래픽을 감시하기 위해 물리적 회선을 공유하도록 구성되어 있으며 네트워크 디바이스로부터 수집된 패킷 정보는 패킷분류 엔진을 통해 Inbound 트래픽 데이터 저장소와 Outbound 트래픽 데이터 저장소에 기억된다. 이 두 부분은 4 장에서 소개할 트리 기반 자료구조를 의미하는 메모리 공간이다. 이를 저장소에 기억된 트래픽 정보를 토대로 도메인 보안관리 모듈이 공격 탐지와 공격자 식별을 수행한다.

탐지된 공격에 대해 대응할 수 있도록 DSM과 라우터는 상호 연결되는데 이들 간의 인터페이스는 공격자에게 악용되지 않도록 Out-of-band 네트워크를 사용한다. 별도의 이더넷 인터페이스 모듈을 통한 통신이나 SNMP를 이용할 수 있으며, 기타 시리얼 통신 포트를 이용할 수 있다. 이와 같이하는 이유는 공격 탐지와 대응을 라우터의 기능에서 분리시킴으로서 네트워크 고속화에 역행하지 않고 효과적인 보안관리 수행을 도모하기 위함이다.

공격자의 의도에 악용되지 않고 도메인 상호간에 안전한 보안관리 협력을 수행하려면 각 도메인의 경계 라우터를 중심으로 이웃 도메인과 상호 신뢰하고 인증 가능한 메시지를 교환할 수 있어야 한다. 이러한 도메인 간 메시지 교환은 각 도메인과 이웃 도메인 사이에서만 이루어지며 보안관리 협력을 위해 전체 인터넷을 순회 할 필요는 없다. 보안관리 협력을 위한 메시지 교환은 암호화 및 인증처리에 드는 연산 비용을 부담해야하고, 공격자에게 노출되지 않도록 하기 위해, 분산된 DSM에서 수행한다.

다음 (그림 3)은 이러한 연결 구조를 보이고 있다. DSM에 대한 직접적인 공격은 라우터로부터 보호되며, DSM 간의 연결은 안전한 통신 채널을 통해 보호된다.

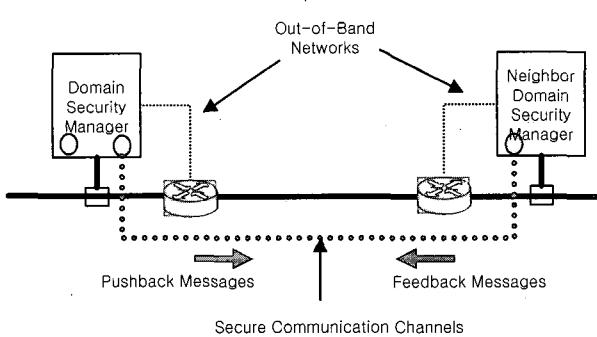


그림 3. DSM 간의 연결

Fig. 3. A form which DSM's are connected each other.

IV. DDoS 공격 탐지와 공격자의 식별

가. 공격자 식별을 위한 트래픽 플로우 정보의 유지
본 논문에서는 트래픽 플로우를 구성하는 최소의 정보로서 송수신자의 IP 주소와 서비스 포트 정보를 중심으로 통신 링크 상의 패킷 헤더 정보를 수집한다. 그리고 이를 토대로 주기적인 공격 플로우를 식별한다.

수집한 패킷 정보를 토대로 트래픽 플로우를 분류하고 공격성 플로우를 주기적으로 식별하기 위해서는 연속적인 패킷 수집 활동으로부터 송수신 IP 주소 및 서비스 포트들 간의 관계를 잘 나타내고 유지할 수 있는 방법이 필요하다.

본 논문에서는 도메인 내부 호스트의 IP 주소를 root로 하는 트리 형태의 자료구조가 되도록 트래픽 플로우 구성정보를 저장하고 유지하는 방법을 제시한다.

(그림 4)는 DSM에서 일정 시간동안 수집한 Inbound 플로우 정보를 예시하고 있다. (그림 4)에서 Home은 인터넷에 연결된 호스트 입장에서 자신을 뜻하며 Foreign은 자신을 제외한 다른 호스트를 의미한다. 도메인 경계에서 트래픽 플로우를 감시하는 탐지 시스템 입장에서 Home은 도메인 내부에 있는 호스트를 뜻하고 Foreign은 도메인 외부에 있는 호스트를 의미한다.

Home IP라고 표시된 root 노드의 숫자 257은 서버의 IP 주소를 10진수로 표현한 것이며 leaf 노드의 일부에 표시한 숫자 역시 같은 방법으로 서버에 접근한 사용자 호스트의 IP 주소(Foreign IP 주소)를 나타낸 것이다. 그리고 leaf 노드에서 각 IP 주소 밑에 표시한 수치는 일정 시간 동안 카운트된 패킷의 수 또는 바이트 수를 나타내는 것이다.

하나의 도메인 내에 있는 호스트들은 제각각 다수의 서비스 포트를 개방하여 서비스를 제공할 수 있기 때문에 하나의 Home IP 노드에는 다수의 Home Port를 자식 노드로 가질 수 있다. 또 각 서비스 포트에는 다수의

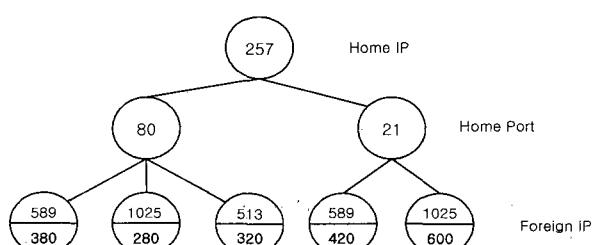


그림 4. 중복 패킷 카운트가 있는 5 개의 Inbound Flow
Fig. 4. 5 inbound flows has a count of packets counted respectively.

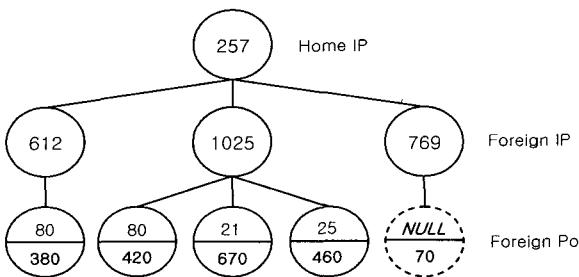


그림 5. 중복 패킷 카운트가 있는 Outbound Flow
Fig. 5. Outbound flows has a count of packets counted respectively.

외부 호스트에서 접근할 수 있기 때문에 그 자식 노드로서 Foreign IP를 가질 수 있다. (그림 4)는 FTP(포트 21)과 HTTP(포트 80) 서비스를 동시에 제공하고 있는 하나의 서버에 원격에서 5 명의 사용자가 각 서비스에 접근했음을 뜻하고 있다.

위 (그림 5)의 트리는 IP 주소가 257 인 도메인 내부 사용자가 일정 시간동안 다른 도메인에 있는 2 곳의 서버와 1 곳의 호스트로 패킷을 송신한 결과를 표현한 것이다. (그림 5)의 leaf 노드 중 NULL을 의미하는 노드는 서비스 포트가 없는 프로토콜, 예를 들어 ICMP 패킷이 70 회 전송된 것을 의미한다.

나. DDoS 공격 판정 방안

본 논문에서는 발신지와 목적지 IP 주소 변화에 주목하는 탐지에 역점을 둔다. 단 방어 차원에서의 Inbound 트래픽만 보는 것이 아니라 outbound 트래픽도 함께 본다. 즉 자신의 도메인 내에서 어느 호스트가 발신지 IP 주소를 위조 했는지를 가려내어 기억하고 있는 것이다. 또한 IP 주소를 위조하지 않더라도 웜 확산과 같이 랜덤하게 목적지 주소를 바꾸는 공격자도 가려내어 기억한다. 기억해둔 정보는 도메인 상호간에 보안관리 협력 수행 시에 이용한다. 예를 들어 피공격자 도메인에서 발신지 위조 여부나 웜 확산 증거를 확인해달라는 요청 메시지가 도착하면 그 진위 여부를 응답해 줄 수 있다. 그러나 어떤 근거로 요청과 응답을 할 수 있는지가 관건이다.

(1) DDoS 공격 판정을 위한 척도

(그림 4)와 (그림 5)에서 Foreign IP 주소에 대한 엔트로피 값은 각 방향에 대한 DDoS 및 웜 확산 트래픽 발생 여부를 판정하는 척도가 되어준다.

다음 식 (1)의 엔트로피 계산 알고리즘은 수집된 패킷 샘플의 임의성(randomness)을 조사할 수 있는 방법

을 제공한다.

$$H = - \sum_{i=1}^n P_i \cdot \log_2 P_i \quad (1)$$

여기서 n 은 수집된 패킷 샘플이 갖는 패킷의 종류의 수를 의미한다. 예를 들어 Inbound 또는 Outbound 트래픽, 어느 한쪽에 대해 2,000 개의 패킷을 수집했다고 가정하고 발신지 IP 주소가 같은 것 끼리 묶었을 때 5 종류가 나왔다면 $n = 5$ 이다. P_i 는 전체 샘플 패킷 중에서 i 번째 종류의 패킷 속성 정보가 나온 빈도수를 의미한다. 예를 들어 발신지 IP 주소가 각각 { 1, 2, 3, 4, 5 }를 갖는 5 개의 묶음이 나왔다고 가정하고 각각의 패킷 수가 {250, 150, 300, 600, 700} 이었다고 하면, P_1 의 값은 250/2000 이다. 이렇게 해서 구한 엔트로피 값 H 는 2,000 개의 패킷 샘플이 어느 정도의 임의성을 갖는지를 알게 해준다.

이러한 엔트로피 계산 알고리즘 수행은 앞에서 제안한 트리 기반의 트래픽 플로우 구성 정보를 이용하면 손쉽고 빠르게 구할 수 있다. 예를 들어 (그림 4)의 트리에서 발신지 IP 주소에 대한 엔트로피 계산 비용은 트리의 leaf 노드를 탐색하는 시간에 비례한다. 즉 leaf 노드의 수가 식 (1)에서 n ($n = 5$) 값이 되며 각 노드에 카운트된 패킷 수를 T 초 동안 수집한 패킷 수로 나눈 값이 확률 P_i 값이 된다.

이러한 계산 수행의 이점은 이용해서 매 T 초마다 도메인 내 특정 호스트를 의미하는 트리의 루트 노드를 중심으로 Foreign IP 주소에 대한 엔트로피 값의 크기를 감시할 수 있다. Foreign IP 주소에 대한 엔트로피 값은 외부에서 들어오는 DDoS 공격이나 내부에서 웜 확산 양상(bogus 패킷의 발송)을 일으키는 공격 판정의 척도가 되어준다.

(2) DDoS 공격 판정의 주기

웜 확산이나 DDoS 공격 상황에서 공격을 판정하는 시간 주기 T 값을 결정하기 어렵다. 왜냐하면 시간 간격 T 에 따라 축적된 샘플 패킷의 수가 달라지고 그에 따른 엔트로피 값의 차이가 생기기 때문이다. 따라서 적정 주기의 T 값을 결정하는 것이 중요하다.

이것이 중요한 이유는 바로 엔트로피 값이 웜 확산이나 DDoS 공격과 유사하게 나타나는 정상 트래픽이 존재하기 때문이다. 대표적인 웜 확산 트래픽과 유사한 예로는 파일을 공유할 수 있도록 지원하는 peer-to-peer" 응용이 있고, DDoS 공격 트래픽과 유사한 예로는 철도

예약서비스에 폭주하는 hot spot 트래픽이 있다.

엔트로피 값을 스냅샷으로 보았을 때 이들 두 응용은 각각 웹 확산이나 DDoS 공격 양상을 보이지만 시간 경과를 지켜보면 엔트로피 값이 감소하는 경향을 보인다. 그것은 공유 peer의 수가 한정되어 있고, 예약 서버에 접근을 시도하는 사용자의 수가 한정되어 있기 때문이다. 따라서 도메인 경계에서 밖으로 나가는 Foreign IP 주소나 피공격자 서버로 들어오는 Foreign IP 주소의 엔트로피 값을 적정 주기 T 까지 지켜보면 그 시간 구간 안에 감소 현상을 보인다. 적정 주기의 T 값을 결정하기는 어렵지만 T 값의 상한치를 결정하는 것은 가능하다. 본 논문에서는 다음과 같은 방법으로 T의 상한치, K를 결정한다.

$$K = \frac{\bigcup_{i=1}^{\alpha} W_i (1 + k \cdot W_i)}{SR}, \quad (0 \leq k \leq 1) \quad (2)$$

여기서 W 값은 하나의 응용이 가질 수 있는 정상적인 연결의 Foreign IP 주소의 수이고 α 는 각 도메인 보안 정책이 접근을 허용하는 응용의 수, k는 여유도 값이다. 즉 W는 하나의 응용이 가질 수 있는 정상 이용자의 모집단의 크기라고 볼 수 있다. 이 경우 응용별 W 값의 합은 각 응용 별로 Foreign IP 주소의 분포가 중복된 것을 고려한 값이다. 예를 들어, 하나의 도메인에서 접근을 허용하는 응용이 5 가지라고 하면, K 값은 5 개의 응용에서 접근하는 Foreign IP 주소의 합집합의 원소 수를 SR(Sampling Rate)로 나눈 값이다. 일반적으로 W의 값은 응용의 특성을 분석하거나 히스토리 기반의 통계치를 이용하여 산정할 수 있다.

(3) DDoS 공격의 판정

본 논문에서는 시계열 분석에서 널리 사용되는 EWMA 알고리즘을 이용하여 엔트로피 크기의 변화를 추적하고 CUSUM 알고리즘을 통해 DDoS 공격 발생 여부를 최종적으로 판정한다. EWMA 알고리즘은 다음과 같다.

$$H_{T+1} = \lambda \cdot H_T + (1 - \lambda) \cdot H'_T, \quad (0 \leq \lambda \leq 1) \quad (3)$$

본 논문에서는 식 (3)에 매 T 초마다 감시한 엔트로피 값을 적용하여 K 초 전후의 엔트로피 변화를 감시한다.

여기서 H_{T+1} 와 H'_T 는 각각 다음 주기 T 초와 현재의 엔트로피 예측 값이고 H_T 는 현재의 관측 값이다.

그리고 λ 는 지수평활계수로서 관측 값 이동에 대한 가중치이다.

매 T 초마다 $H_T > H'_T$ 이면 미래 시점에서도 엔트로피 값이 상승 할 것이라는 것을 의미한다. 이것은 도메인 내 특정 호스트에서 나가거나 들어오는 연결 대상과 그 수가 과다하게 증가할 것이라는 것을 반증하는 것이다. 그러나 엔트로피 값이 상승과 하락을 반복하는 패턴을 보이면 $H_T - H'_T$ 값이 양수 또는 음수를 반복하며 공격 판정을 어렵게 한다.

CUSUM 알고리즘은 매 T 초마다 과거의 $H_T - H'_T$ 값을 현재의 $H_T - H'_T$ 값과 누적해서 합을 구함으로써 상승과 하락을 반복하는 엔트로피 값의 변화를 좀 더 평활 시킨다. 이를 통해 현재 트래픽에 대한 엔트로피 값이 증가하는 패턴인지 감소하는 패턴인지 확인 할 수 있다.

다. DDoS 공격자 식별 방안

일반적으로 통신 트래픽에서 발신지 IP 주소별 패킷 수의 분포는 power-law 분포^[13]를 따른다^[14]. 참고문헌 [15]에서는 IP 주소가 랜덤하게 바뀌는 DDoS 공격이 IP 주소 별 패킷 수의 분포가 이러한 power-law 분포 현상에 어긋나는 대표적인 사례로 보고 공격자를 가려내는 방법을 제시하였다.

본 논문에서는 참고문헌 [15]에서 제시한 방법을 본 논문에서 제안한 트리에 응용하여 공격자를 식별 한다. 본 논문에서는 트리에서 Foreign IP 주소를 담고 있는 노드를 중심으로 chi-square 통계량 분석을 수행한다. 먼저 트리에서 Foreign IP 주소의 패킷수를 카운트 할 때 마다 다음과 같은 지수감소 연산을 적용한다.

$$A(t+1)' = A(t) \cdot e^{-\left\{ \frac{1}{t} \cdot \log \frac{A(t+1)}{A(t)} \right\} \cdot t} \quad (4)$$

여기서 A(t) 와 A(t+1)'의 값은 각각 t 초와 t+1 초에서 실제 카운트된 패킷의 수이며 A(t+1)'은 지수감소를 반영한 패킷 수이다. 이때 업데이트 주기 t 값은 지수감소 연산 수행에 소요되는 시간이 무시할 만큼 작으므로 패킷을 수집할 때 식 (4)의 결과를 얻을 수 있다. 따라서 패킷을 수집할 때마다 패킷수와 함께 트리의 Foreign IP 주소 노드에 기억시킨다.

엔트로피 측정주기인 매 T 초마다 트리에 저장된 데이터를 균형하여 위 (그림 6)과 같은 구조의 데이터를 별도의 테이블 형태의 기억공간(DB 또는 파일)에 저장 한다. 이 테이블에 로깅되는 정보들은 공격판정 시점인

Inbound / Outbound 구분 플래그			
현재 엔트로피 값			
엔트로피 평균			
Foreign IP 주소값(<i>i</i>)	패킷 수	지수감소 적용 패킷 수	바이트 수
Foreign IP 주소값(<i>n</i>)	패킷 수	지수감소 적용 패킷 수	바이트 수

그림 6. 로그 데이터의 구조

Fig. 6. Structure of log data.

표 1. Foreign IP 주소의 패킷 수에 따른 등급화

Table 1. A table of bins are ranked by the # of packets of the Foreign IP address.

bin 번호	패킷 수 Rank	bin 총 패킷 수 (관측도수)	bin 패킷 수 평균 (기대도수)
1	1	N_1	n_1
2	4	N_2	n_2
3	16	N_3	n_3
4	256	N_4	n_4
5	1,024	N_5	n_5
6	4,096	N_6	n_6
7	나머지	N_7	n_7

K 초까지 매 T 초 마다 업데이트 된다.

공격 판정 주기 K 초가 되면 도메인 내 각 호스트의 로그 테이블을 참조하여 아래 (표 1)과 같은 bin 테이블을 생성한다. 생성 방법은 모든 Foreign IP 주소를 지수감소 적용 패킷 수로 정렬한 후에 이를 중심으로 Foreign IP 주소를 (표 1)과 같이 몇 개의 bin 으로 구분한다.

(표 1)에서 각 bin은 지수감소 적용 패킷 수를 기준으로 정렬된 Foreign IP 주소들을 등급별로 묶은 것이다. 여기서 관측도수 N_i 는 각 bin의 총 패킷수이며 기대도수 n_i 는 매 공격 판정 주기마다 업데이트되어 왔던 총 패킷 수의 평균이다.

(표 1)과 같은 정보를 토대로 다음과 같이 chi-square 통계량을 조사한다.

$$\chi^2 = \sum_{i=1}^B \frac{(N_i - n_i)^2}{n_i} \quad (5)$$

식 (5)에서 N_i 값은 현재 트래픽량에 대한 프로파일을 나타내며 n_i 값은 매 공격판정 주기마다 업데이트되는 기준선(baseline)이 되어 준다. 따라서 보안 책임자의 개입 없이 트래픽 상황에 따라 자동적으로 설정되는 기준선을 갖게 되며 현재의 트래픽에서 어떤 bin 이 기준선을 벗어나는지를 구별할 수 있게 해준다.

본 논문에서는 (표 1)에서 N_i 값과 n_i 값의 차이가 큰 bin을 찾아 이 bin 에 해당하는 Foreign IP 주소들을 공격자로 분류한다..

V. 분산 네트워크 보안관리 방안

가. Intra-domain 보안관리

분산 네트워크 보안관리는 다음과 같이 두 가지 작업으로 이루어진다.

Intra-domain 보안관리

Inter-domain 보안관리

Intra-domain 보안관리는 다시 3 단계로 세분화된다.

DDoS 공격 발생 여부의 탐지

공격자 식별

식별한 공격자에 대한 보안 대응

다음은 Intra-domain 차원에서 DSM이 수행하는 보안관리 알고리즘을 C 언어 형식으로 표현한 것이다.

```

void DetectDDoSAttack(float K, float T, float *Entropy_Avg,
                      TREE* tree) {
    float t, CUSUM_Value = 0;
    float Abnormity = 0;
    float C_Entropy = 0; /* Current Entropy value */
    float E_Entropy = C_Entropy + 1.0;
    /* Estimated Entropy value */

    for(T=0; T < K; T++)
    { // T : 엔트로피 측정 주기, K : 공격판정 주기
        for(t=0; t < T; t++) // t : 패킷 샘플링 주기
        {
            패킷 헤더 정보 수집;
            Update(tree); // 트리 업데이트
            발신지 IP 주소 위조여부 검사;
            // MAC-IP 주소 테이블 이용, 트리 root 노드에 표시
            패킷 수 지수감소 연산 적용;
        }

        C_Entropy = Get_Entropy_value(tree);
        // 트리를 참조, current entropy value 계산
        E_Entropy = EWMA(C_Entropy, E_Entropy);
        // estimated entropy value 계산
        Abnormity = C_Entropy - E_Entropy;
        CUSUM_Value += Abnormity;

        *Entropy_Avg = Get_Entropy_Average(C_Entropy);
        // 엔트로피 평균치 계산
    }

    for(i=0; i < domain_host_num; i++)
    // domain_host_num : 매크로 상수, 도메인 호스트 수
    UpdateLogFile(tree->root[i].LogFile);
    // Logfile : 파일 포인터
    // 트리 참조, root 별 Entropy value 로깅
    // root 별 entropy 평균 로깅
    // root 별 foreign IP 노드 정보 로깅
    // (IP 주소, 패킷수, 지수감소 적용 패킷 수 로깅)
}

if(Current_Entropy > *Entropy_Avg && CUSUM_Value > 0)
    ReponseAgainstDDoSAttack(tree);
}

```

```

void ResponseAgainstDDoSAttack(TREE *tree)
{
    int bin_number;
    BINTABLE *BinTable;
    VIOLATOR *ViolatorTBL;
    SUSPECT *SuspectTable;
    BOGUS *BogusPktSenderTBL;

    for(i=0; i < domain_host_num; i++) {
        BinTable = MakeBinTable(tree->root[i].LogFile);
        // 각 호스트 별 로그 파일을 참조,
        // 표 1에서 제시한 테이블을 생성
        ViolatorTBL = FindViolator(tree->root[i].Violation);
        // 트리 root 노드의 Violation 필드 참조,
        // IP Spoofing 시도한 호스트 주소 식별
        BogusPktSenderTBL =
            FindBogusPktSender(tree->root[i].OutEntropy);
        // 트리 root 노드의 Outbound Entropy 필드 참조,
        // bogus 패킷 발송자 식별
    }

    bin_number = ChiSquare(BinTable);
    SuspectTable = SetSuspect(BinTable, bin_number);
    LogIntoDB(ViolatorTBL, SuspectTable, BogusPktSenderTBL);
    // 다음 정보를 DB 에 저장
    /* EntryID, 도메인 ID, 공격자로 분류된 패킷의 IP주소,
       접근한 HomeIP 주소, 접근한 서비스포트, 타임스탬프 */

    IsolateViolator(ViolatorTBL); // 라우터(방화벽)에서 차단
    Degrade_Packet_Priority(SuspectTable); // 대역폭 제한
    SendPushbackMsg();
    // 다음 데이터를 전송
    /* PushbackMsg ID, 도메인 ID, 공격자로 분류된 패킷의 IP주소,
       접근한 HomeIP 주소, 접근한 서비스포트, 타임스탬프 */
}

```

그림 7. Intra-domain 보안관리 알고리즘

Fig. 7. An algorithm for security management within a domain.

(그림 7)에 나타난 바와 같이 DSM에서 공격 판정이 이루어지고 공격자가 식별되었으면 식별된 정보를 타임스탬프와 함께 자신의 local DB에 저장한다. 이때 DSM은 (그림 2, 3)에서 보인 것처럼 별도의 out-of-band 인터페이스를 통해서 IP 주소를 위조한 Outbound 플로우들을 차단하고 비정상이라 의심스러운 플로우들을 라우터에서 트래픽 처리율을 제한되도록 제어한다. 트래픽 처리율을 제한하는 방법은 공격자로 분류되지 않은 정상적인 연결의 Foreign IP 주소에 대해서는 트래픽 성형(traffic shaping)^[16]을 통해 높은 대역폭을 할당하고 나머지에 대해서는 저 대역폭을 할당하는 방법이다. 이와 같은 통신 대역폭 제한 조치와 함께 이들 정보들을 메시지 형태로 DSM에게 전달한다.

나. Inter-domain 보안관리

(1) 보안관리 메시지 교환

Inter-domain 보안관리를 위해서 DSM이 수행하는

메시지의 전달 방식은 다음과 같이 세 가지 형태로 구분한다.

신뢰형 멀티캐스트(Reliable Multicast) 전달 방식

point-to-point 전달 방식

end-to-end 전달방식

신뢰형 멀티캐스트 전달방식은 intra-domain에서 sub-domain 간에 pushback 메시지를 전달할 때 사용하며 point-to-point 연결 형태의 전달은 inter-domain에서 메시지를 전달할 때 사용한다. 그리고 end-to-end 전달방식은 feedback 메시지를 전달할 때 사용한다.

(그림 8)은 이러한 메시지 전달과정을 설명하고 있다. 여기서 pushback 메시지는 피공격자 측 DSM이 공격발원지를 추적하기 위해 발송한 메시지이고 feedback 메시지는 공격 발원자의 DSM이 피공격자 측 DSM에게 응답하는 메시지이다.

pushback 메시지는 다음과 같은 정보들이 포함된다.

pushback 메시지 ID

DSM ID

공격자로 식별된 Foreign IP 주소와 부모 노드 정보(예, 포트 번호, Home IP 주소)

공격 판정 시점의 타임스탬프 값

feedback 메시지에는 다음과 같은 정보들이 포함된다.

feedback 메시지 ID

pushback 메시지 ID

DSM ID

pushback 메시지에 해당하는 공격자 IP 주소

각 DSM들은 pushback 메시지 전달의 신속성을 제공하기 위해 메시지를 수신하자마자 바로 이웃 DSM에게 전달한다. 아울러 불필요한 메시지 응답에 따른 통신 오버헤드를 줄이기 위해서, pushback 메시지에 대한 응답으로 feedback 메시지를 생성할 내용이 없다면 응답하지 않는다. 이렇게 하지 않으면 모든 pushback 메

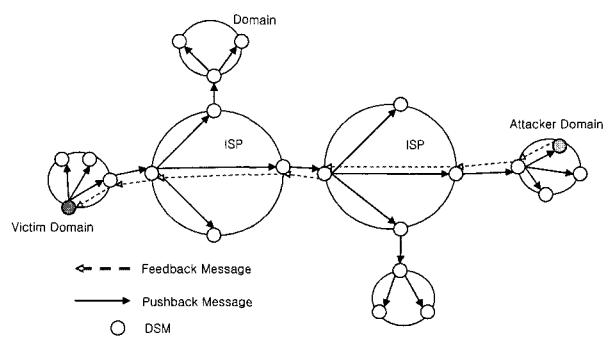


그림 8. 보안관리 협력을 위한 메시지 교환

Fig. 8. Message exchange for security managements among DSM's.

시지에 대한 bogus feedback 메시지를 처리하느라 DSM의 처리부하가 높아진다.

각 메시지에는 메시지 식별을 위한 고유 ID 가 있어 DSM간에 발생할 수 있는 메시지 중복 전달 여부를 가려낼 수 있다.

신뢰형 멀티캐스트 전달방식을 채용하는 것은 DSM이 발송하는 메시지의 전송 횟수를 최소화하기 위함이다. 또 이 전달방식의 사용을 도메인 내부로 국한하는 것은 각 도메인별로 네트워크 환경이나 보안 및 망 관리정책의 차이가 존재하기 때문이다. 실제로 신뢰형 멀티캐스트 메시지를 다중 흡으로 전송하기 위해서는 인터넷에 분산된 라우터들이 도메인의 경계를 넘어서 이를 지원할 수 있어야 한다.

보안관리 협력을 위한 메시지 교환을 이러한 방법으로 수행한다면, 도메인의 수가 d 일 때, 하나의 pushback 메시지를 모든 DSM에게 전달하는 데 필요한 전송 횟수는 대략 $2d-1$ 회로 줄일 수 있다.

(2) pushback 메시지의 인증과 전달

본 논문에서 DSM들은 이웃하는 DSM 간에 상호 인증하는 것을 전제한다. 최초의 DSM이 pushback 메시지를 이웃 DSM에게 보낼 때는 이웃 DSM과 상호 공유하는 비밀 키를 자신들이 공유하는 비밀 키로 암호화하고 암호화된 공유키 데이터를 pushback 메시지에 첨부하여 보낸다. 다음 (그림 9)는 pushback 메시지의 구조를 보이고 있다.

(그림 9)에서 태그 필드를 제외한 나머지 필드는 최초의 pushback 메시지를 발생한 DSM에서 생성하는 것이고, 태그 필드는 이웃하는 DSM이 자신의 또 다른 이웃 DSM에게 전송할 때 첨부하는 공유키 부분이다. pushback 메시지가 DSM들을 거치면서 태그필드 부분만 수정된다. 이러한 전달방식은 DSM들이 상호 신뢰 관계를 갖게 한다.

(3) feedback 메시지의 인증과 전달

pushback 메시지에 응답할 조건을 갖는 DSM은 (그림 9)에 나타낸 피공격자 측 DSM의 IP 주소로 안전한 통신 채널을 생성하기 위해 보안확립(security association)

피공격자 측 DSM IP 주소	pushback msg.	피공격자 측 DSM 의 암호화된 공유키	태그 필드
---------------------	---------------	--------------------------	-------

그림 9. pushback 메시지 구조
Fig. 9. Structure of a pushback message.

을 맺는다. 이 때 공격자 측 DSM은 (그림 9)에 보이는 암호화된 공유키를 원래의 주인에게 제시함으로써 양측 간에 상호 인증을 수행한다.

공격자 측 DSM은 확립된 안전한 통신채널을 통해서 피공격자 측 DSM에게 end-to-end feedback 메시지를 직접 전송한다.

(4) pushback-feedback 메시지의 기능적 역할

DSM의 잘못된 판정으로 트래픽 처리율이 제한되었던 정당한 이용자를 구제해야한다. 피공격자 측 DSM에게 직접 end-to-end로 보고되는 feedback 메시지는 피공격자 측 DSM으로부터 제한받았던 억울한 정상 사용자들의 대역폭을 복원한다. 복원되는데 걸리는 시간은 pushback 메시지 전송과 feedback 메시지 수신에 걸린 시간에 비례한다. feedback 메시지로부터 구제받지 않은 나머지 혐의자 플로우들은 보안 정책에 의해 일정시간 제한된다. pushback 메시지는 공격 발원지에서 공격 행위를 차단하는 역할을 하며, feedback 메시지는 공격자로 잘못 분류된 정상 이용자의 접근을 회복시킨다.

VI. 실험 및 분석

가. 실험 환경 및 도구

실험 환경은 아래 (그림 10)과 같다. 라우팅 테이블 설정에 따라 몇 가지 토폴로지를 구성할 수 있으며 DDoS 공격 효과를 최대화 할 수 있다. 라우터간의 각 링크별 네트워크의 대역폭은 10 Mbps이며 도메인 내 호스트들도 10 Mbps 스위치허브로 연결되어 있다.

DDoS 공격팀지 성능(False Positive Rate, False Negative Rate)과 대응효과(NPSR: Normal Packet Survival Rate)에 대한 실험 결과를 얻기 위해서 두 가지 트래픽을 생성하는 도구를 사용하였다. 하나는 DDoS 공

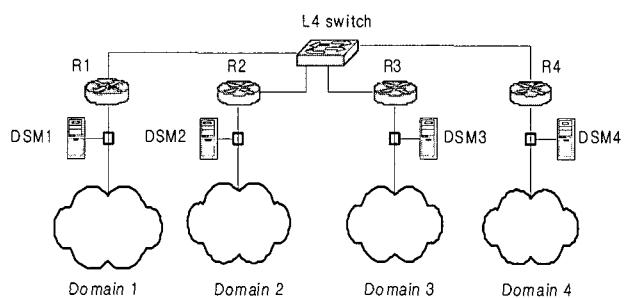


그림 10. 실험 네트워크 환경
Fig. 10. Testbed.

격도구로 잘 알려진 TFN2K이고 다른 하나는 정상 이용자의 HTTP 요구 트래픽을 모사하기 위해 직접 구현한 도구이다. 직접 구현한 도구는 Java 기반의 HTTP 요구 생성 프로그램으로서 랜덤하게 IP 주소를 바꾸거나 패킷 전송 간격을 조절할 수 있으며, 피공격자 서버에 구현된 서비스 URL을 지정된 수만큼 무작위로 변경하여 요청할 수 있다.

본 논문에서는 DSM들 간에는 안전하고 신뢰할 수 있는 멀티캐스트 통신을 지원하기 위해서 Spread^[17]라고 하는 링크 계층 API를 사용하여 DSM의 안전한 그룹 멀티캐스트 통신을 구현하였다.

나. 도메인 차원에서 탐지 및 대응 효과

공격과 정상 트래픽이 혼합된 트래픽에서 공격 플로우들을 식별하는 실험을 수행하였다. 실험에 사용되는 호스트 수가 제한되므로 Java 기반의 HTTP 생성도구의 IP 주소 변경기능을 이용하였다. 본 논문에서는 HTTP 트래픽을 정상 이용자의 접근으로 본다.

이 실험에서 DDoS 공격(TCP-SYN 공격)이 없었던 정상적인 트래픽의 경우에는 매 10초(T: 엔트로피 측정 주기)마다 평균 엔트로피 값이 2.19 이었는데 반해 공격 이후에는 엔트로피 값이 지속 상승하여 60 초(K: 공격 판정주기) 동안 11.67 까지 상승하였다. 따라서 DSM은 본 실험의 트래픽을 공격으로 판정하였다. 다음 (표 2)는 피공격자 측 DSM이 단독으로 대응한 결과이다.

다음 (표 3)은 (표 2)의 결과에 대한 DSM의 공격 탐지 정확도를 구하기 위한 판정표이다.

표 2. 공격자로 분류된 Foreign IP 주소의 수

Table 2. # of foreign IP address classified as Attackers.

공격자로 분류된 Foreign IP 주소의 수	
공격자가 보낸 IP 주소의 수	22,143 / 22,500 개
정상이용자가 보낸 IP 주소의 수	158 / 2,597 개
총들이 발생한 IP 주소의 수	151 개

표 3. DDoS 공격에 대한 DSM의 공격 판정표

Table 3. Decision table of DSM against DDoS Attack.

공격 판정 여부	공격 사실 유무		합계
	True	False	
True	22,143	158	22,301
False	357	2,439	2,796
합계	22,500	2,597	25,097

이 실험에 대한 DSM의 공격탐지의 정확도는 다음 (식 6, 7)을 이용하여 구할 수 있다.

$$\text{False Positive Rate (FPR)} =$$

$$1 - \frac{\text{정상 판정자의 수}}{\text{실제 정상 이용자의 수}} \quad (6)$$

$$\text{False Negative Rate (FNR)} =$$

$$1 - \frac{\text{공격 판정자의 수}}{\text{실제 공격자의 수}} \quad (7)$$

따라서 DSM의 공격 탐지의 정확도는 다음과 같다.

$$\text{FPR} = 1 - (2,439 / 2,597) = 0.061 \quad (6.1\%)$$

$$\text{FNR} = 1 - (22,143 / 22,500) = 0.016 \quad (1.6\%)$$

이 실험에서 라우터를 통해 공격자로 분류된 IP 주소를 갖는 패킷들을 차단하였다면 무고한 피해자가 발생한다. 즉 (표 1)에서 151 개의 정상 이용자의 IP 주소들은 랜덤하게 발신지를 위조한 공격자 때문에 공격자로 오판 받고 서버의 접근이 차단되는 피해를 입는다. 이 실험에서 정상 이용자 2,597 개의 IP 주소가 60초 동안 보낸 총 패킷의 수는 57,212 개이며 이중 151 개의 IP 주소가 보낸 총 패킷의 수는 13,820 개가 나왔다.

도메인 차원에서 공격 대응을 수행한다면 공격 대응 효과(NPSR : Normal Packet Survival Rate)는 다음과 같다. 즉 24 %의 정상 이용자의 트래픽은 보호 받지 못한다.

$$\text{NPSR} = 1 - (13,820 / 57,212) = 0.76 \quad (76\%)$$

특정 도메인을 대상으로 발신지나 목적지를 랜덤하게 변경하여 공격이 반복된다면 본 실험에서 얻은 대응 효과는 의미가 없을 것이다. 왜냐하면 다음 공격 판정 주기에도 무고한 피해가 반복되기 때문이다. 결국 공격 탐지의 높은 정확도에도 불구하고 정상 이용자의 24 %에 해당하는 서비스 접근 트래픽에 대해서는 접근을 보호하지 못하였다. 이러한 문제점이 분산 네트워크 보안 관리의 필요성을 제기한다는 것을 본 실험을 통해 확인한 결과이다.

나. 분산 네트워크 보안관리를 통한 대응효과

다음 실험 결과는 각 도메인에 분산된 DSM들이 보안관리 협력을 통해 탐지한 결과와 대응 효과이다.

발견한 발신지 IP 주소의 수 : 22,496 개

확인된 정상 이용자의 IP 주소의 수 : 158 개

$$FPR = 1 - (2,597 / 2,597) = 0 (0 \%)$$

$$FNR = 1 - (22,496 / 22,500) = 0.02 \%$$

$$NSPR = 1 (100 \%)$$

DSM 간의 pushback 메시지와 feedback 메시지 교환을 통해 위조된 발신지 IP 주소들을 확인하였다. 이를 통해 158 개의 IP 주소에 대한 정상 이용자를 대역 폭 제한에서 해제하였으며 궁극적으로 모든 정상 이용자의 접근을 보호하였다.

VII 결 론

본 논문에서는 발신지를 위조하고 목적지를 변경하는 DDoS 공격을 효과적으로 탐지하고 대응할 수 있는 방안을 제시하였다.

현재의 트래픽량이 비정상적으로 높아서 공격으로 판정한 것은 문제 해결에 도움이 되지 못한다. 정확하게 공격자 플로우를 가려내야하고 정당한 사용자의 접근을 보호 할 수 있어야 한다. 그러나 매번 발신지가 위조되고 목적지가 가변되는 DDoS 공격 트래픽은 피공격자 도메인에서 지연적으로 탐지하고 대응하기에 한계가 있다.

2 장의 관련연구에서 논한 것처럼 이 문제를 해결하기 위한 여러 연구들이 있었지만 모두가 이미 설치되고 운용중인 기존 정보 인프라에 상당한 수정을 가해야 하는 현실적인 문제를 갖고 있다.

본 논문에서는 이러한 문제를 비용 효과적으로 해결 할 수 있는 분산 네트워크 보안관리 구조와 방안을 제시하였다.

분산 네트워크 보안관리의 핵심은 공격성 플로우를 어떻게 탐지하고 식별하는지와 식별된 정보를 분산된 이웃 도메인과 어떤 방법으로 교환하고 대응에 활용하는가에 달려 있다.

본 논문에서는 먼저 트래픽 플로우 정보를 유지할 수 있는 방법을 제시하였고, DDoS 공격 유무의 판정과 공격성 플로우의 식별 방안을 제시하였다. 나아가 이를 식별된 정보를 분산된 이웃 도메인과 안전하고 신뢰할 수 있는 방법으로 공유하여 정당한 사용자의 접근을 보호할 수 있는 분산 네트워크 보안관리 기법을 제시하였다. 그리고 실험을 통해 제시된 방안이 DDoS 공격으로부터 정당한 사용자의 접근을 보호할 수 있음을 확인하였다.

본 논문에서 제시한 기법은 갈수록 공격 수법이 정교

해져 가는 DDoS 공격을 효과적으로 탐지하고 대응할 수 있는 정보 인프라 구축에 큰 도움이 되리라 본다.

참 고 문 헌

- [1] Peter Mell, "An Overview of Issues in Testing Intrusion Detection Systems", NIST Interagency Reprots 7007, 2003.
- [2] Haining Wang, Danlu Zhang, and Kang Shin. "Detecting SYN flooding attacks", In Proceedings of the IEEE Infocom.
- [3] Dan Schenckenberg, Kelly Djahandari, Dan Sterne, "Infrastructure for Intrusion Detection and Response," DARPA Information Survivability Conference and Exposition, DISCEX 2000, Jan., 2000.
- [4] Dan Schenckenberg, Harley Holiday, et al., "Cooperative Intrusion Traceback and Response Architecture (CITRA)", DISCEX 2001, June, 2001.
- [5] Dan Stenrue, et al., "Active Network Based DDoS Defense", Proceedings of the DARPA Active Networks Conference and Exposition (DANCE.02), p. 193, May, 2002.
- [6] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. "Practical network support for IP traceback", In *Proceedings of the ACM SIGCOMM Conference*, pages 295-306, Stockholm, Sweeden, August 2000. ACM.
- [7] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. "Controlling high bandwidth aggregates in the network", In *ACM ComputerCommunication Review*, July 2001.
- [8] Robert Stone, "Centertrack: An IP overlay network for tracking DoS floods", In Proceedings of the USENIX Security Symposium, p. 199 - 212, Denver, CO, USA, July 2000. USENIX.
- [9] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker, "Controlling high bandwidth aggregates in the network", In *ACM Computer Communication Review*, July 2001.
- [10] Stefan Savage, David Wetherall, Anna Karlin, Tom Anderson, "Practical network support for IP traceback", In *Proceedings of the ACM SIGCOMM Conference*, pages
- [11] Steven Bellovin, "ICMP traceback messages", Work in Progress: draft-bellovin-itrace-00.txt.
- [12] David L. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall, G. Minden, "A Survey of Active

- Network Research", In IEEE Communications Magazine, 1997.
- [13] M. E. J. Newman, "Power laws, Pareto distributions and Zipf's law", International Journal of Contemporary Physics 46, p. 323-351, 2005.
- [14] Michalis Faloutsos, Petros Faloutsos, and Christos Faloutsos. "On power-law relationships of the internet topology", In SIGCOMM, p. 251 - 262, 1999.
- [15] Laura Feinstein, Dan Schnackenberg, Ravindra Balupari, Darrell Kindred. "Statistical Approaches to DDoS Attack Detection and Response," DISCEX 2003, p. 303, DARPA Information Survivability Conference and Exposition - Volume I, 2003.
- [16] "Linux Advanced Routing and Traffic Control HOWTO", <http://www.lartc.org/lartc.html>
- [17] Spread Toolkit, "<http://www.spread.org>".

저 자 소 개



김 성 기(정회원)
1996년 인천대학교 전자계산학과
공학사.
1998년 인천대학교 컴퓨터공학과
공학석사.
2006년 인천대학교 컴퓨터공학과
공학박사.
현재 인천대학교 컴퓨터공학과
박사후 연구원

<주관심분야 : 침입감내, 보안관리, 유비쿼터스 컴퓨팅 보안, 분산시스템>



김 문 찬(학생회원)
2006년 인천대학교 컴퓨터공학과
공학사.
현재 인천대학교 컴퓨터공학과
석사과정
<주관심분야 : 유비쿼터스 컴퓨팅
보안, 분산시스템>



유 승 환(학생회원)
2005년 인천대학교 컴퓨터공학과
공학사.
현재 인천대학교 컴퓨터공학과
석사과정
<주관심분야 : 유비쿼터스 컴퓨팅
보안, 컴퓨터 시스템 보안, 분산시
스템>



민 병 준(정회원)
1983년 연세대학교 전자공학과
공학사.
1985년 연세대학교 전자공학과
공학석사.
1991년 미국 캘리포니아대학교
(UCI) 전기 및 컴퓨터
공학과 공학박사.
1984년 ~ 1986년 삼성전자 연구원
1992년 ~ 1994년 한국통신 선임연구원
1995년 ~ 현재 인천대학교 컴퓨터공학과 교수
<주관심분야 : 분산시스템, 보안, 통신망관리>