DDoS 공격 방지를 위한 통계적 마킹 방법을 이용한 패킷 필터링 구조

구희정, 홍충선
경희대학교 컴퓨터공학과
e-mail : heejeong@networking.khu.ac.kr

Packet Filtering Architecture Using Statistical Marking against DDoS Attack

Hee Jeong Koo, Choong Seon Hong
Dept. of Computer Science, Kyung Hee University

요 약

인터넷의 급속한 발전은 지난 수년간 데이터 전송 속도의 고속화, 대용량의 데이터 전송 등을 가져오는 긍정적인 효과를 거두었지만 컴퓨터 시스템의 보안 침해 사고와 같은 역기능 또한 날로 증대되어 그 피해 규모가 점점 심각해지고 있다. 본 논문에서는 IDS의 제어 아래 통계적인 탐지 알고리즘을 이용하여 분산 서비스 거부(DDoS) 공격에 대응할 수 있는 패킷 필터링 구조를 제안한다. 이 구조는 탐지 알고리즘에 의해 DDoS 공격으로 인식된 패킷을 IDS가 탐지하여 필터링 모듈에서 효과적으로 공격을 막을 수 있다.

1. 서론

인터넷의 급속한 발전은 지난 수년간 데이터 전송 속도의 고속화, 대용량의 데이터 전송 등을 가져오는 긍정적인 효과를 거두었지만 컴퓨터 시스템의 보안 침해 사고와 같은 역기능 또한 날로 증대되어 피해 규모가 점점 심각해지고 있다. 이 중에서도 분산 서비스 거부(Distributed Denial of Service, DDoS) 공격은 타겟 서버에 다량의 데이터를 보내 갑작스런 트래픽의 범람으로 시스템 성능 저하 및 마비 등의 심각한 문제를 유발시킬 수 있다. 침입 탐지 시스템(Intrusion Detection System, IDS)에서는 유입되는 패킷을 캡쳐해서 탐지 시스템내의 룰셋(rule set)과 패턴 매칭을 통해 공격을 탐지해낸다. 그러나 IDS는 패킷 모두를 캡쳐해서 스트링매칭을 함으로써 탐지하기 때문에 서비스 거부(Denial of Service, DoS) 공격에는 효과적일지 모르나 DDoS 같은 동시다발적인 패킷범람 공격은 탐지하는데 시간이 걸린다는 단점이 있다. 본 논문에서는 IDS의 탐지 알고리즘에 의해 패킷이 DDoS 공격으로 인식되면 IDS에서 룰셋과 매칭하여 공격 패킷을 탐지하고 필터링 모듈에 제어 명령을 내린다. 또한 마킹 모듈(marking module) 을 따로 두어서 IDS가 유입되는 패킷을 캡쳐하여 마킹 정보를 탐지해서 IDS 매니저에게 알리면 IDS내에서 룰셋 매칭하는 시간을 단축시켜 보다 빠르게 패킷 필터링 할 수 있다. 이러한 방법을 사용함으로써 DDoS 공격을 효과적으로 방어할 수 있다.

본 논문은 다음과 같이 구성되었다. 2장에서는 관련 연구로서 분산 서비스 거부 공격과 침입 탐지 시스템의 간략한 구조를 소개하고, 3장에서는 본 논문에서 제안하는 IDS 기반의 패킷 필터링 구조를 설명한다. 4장에서는 결론과 향후과제를 끝으로 논문을 마무리 짓는다.

This was supported by University ITRC project of MIC.

2. 관련연구

2.1. 분산 서비스 거부(Distributed Denial of Service) 공격

분산 서비스 거부 공격은 많은 수의 호스트들에 DDoS 공격용 프로그램을 분산 설치하여 이들이 동

시에 목표 시스템에 다량의 패킷을 범람시켜 성능 저하 및 시스템 마비를 일으키는 공격형태이다.

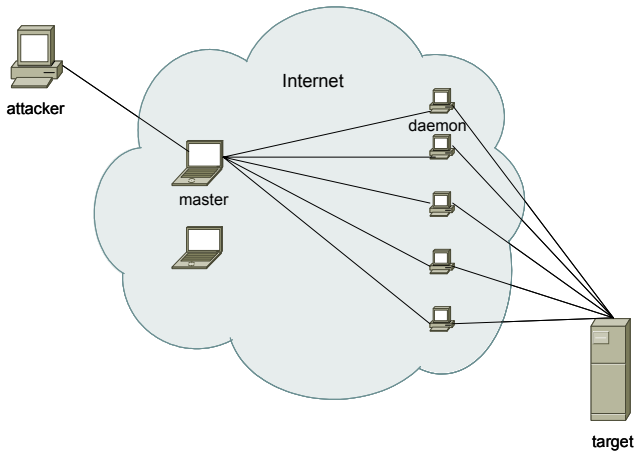

그림1. DDoS 공격 형태

그림1에서 DDoS공격의 공격자(attacker)는 하나 이상의 master를 거느리고, master는 많은 데몬(daemon)을 제어할 수 있어 데몬에 의해 target 시스템을 공격할 수 있다. 공격용 프로그램을 설치한 서버(daemon)에서 직접 공격하는 것이 아니기 때문에, target 시스템에서는 공격을 받아도 공격자가 누구인지 알 수 없어 피해가 더 커진다.

2.2. 침입 탐지 시스템(Intrusion Detection System)

침입 탐지 시스템은 단일 컴퓨터 또는 네트워크로 연결된 여러 컴퓨터를 감독하여 컴퓨터 시스템에 대한 비정상적인 사용, 오용, 남용등을 실시간으로 탐지, 차단, 방어한다.

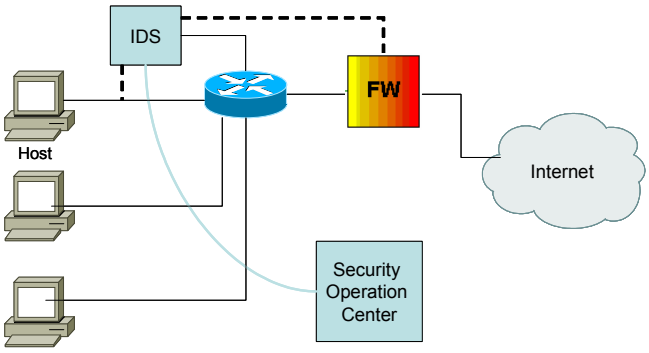

그림2. 침입 탐지 시스템(IDS)의 망 관리

룰(rull)이 있어 이를 임의로 셋팅할 수 있고 네트워크 트래픽을 캡쳐해서 셋팅된 룰과 캡쳐된 패킷을 패턴매칭시켜 조건에 맞으면 IDS 매니저(그림2.에서 Security Operation Center에 해당한다)에게 탐지되었음을 알린다. 매니저는 이 결과를 토대로 웹 상에서 탐지 결과를 그래피컬하게 보여주거나 방화벽, 라우터 또는 인프라 네트워크 내에 있는 다른 IDS들에게 제어명령을 내려 패킷을 차단, 방어할 수도 있다.

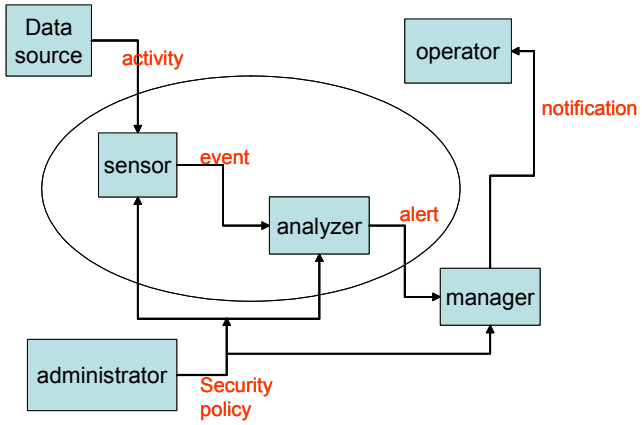

그림3. 침입 탐지 시스템의 구조

그림3은 침입 탐지 시스템의 동작 구조를 나타낸 것이다. 타원의 경계는 IDS를, 화살표는 패킷과 패킷의 정보 이동을 각각 나타내고 있다. Sensor모듈은 Data source로부터 패킷을 실시간으로 캡쳐해서 analyzer로 보낸다. analyzer는 임의의 룰셋으로 캡쳐된 패킷과 매칭을 시켜 이상이 있으면 manager에게 탐지되었음을 알린다. Manager는 특정 operator(방화벽, 라우터 또는 다른 IDS)에게 이 사실을 알려서 DDoS 공격을 방어하거나 웹으로 보여줌으로써 관리자가 알 수 있도록 operator를 제어한다.

기존의 침입 탐지 시스템은 단일 공격자로부터 많은 패킷을 보냄으로써 문제를 일으키는 서비스 거부 공격(DoS)에는 효과적으로 대응하여 탐지할 수 있지만 공격자의 제어 아래 동시다발적으로 많은 수의 데몬들로부터 엄청난 양의 공격을 받는 DDoS 공격을 막는데는 시간이 걸려 공격에 대한 대응시간이 길어진다는 단점이 있다.

3. 제안사항

3.1. 침입 탐지 시스템 기반의 패킷 필터링 설계와 동작 과정

그림4는 본 논문에서 제안한 침입 탐지 시스템 기반의 패킷 필터링 구조를 하나의 인프라 네트워크 망을 보기로 나타낸 것이다. 인프라 네트워크 안에는 몇 개의 서브 네트워크가 있고 서브 네트워크의 에지 라우터와 전체 네트워크의 에지 라우터 간

path에는 IDS와 필터링 모듈이 물려있다. 인프라 네트워크 안에 있는 IDS들은 탐지 공지를 받을 매니저와 연결되어 있다. 전체 네트워크의 에지 라우터에는 마킹 모듈이 있어 에지 라우터로 유입되는 패킷에 특정 값을 마킹한다.

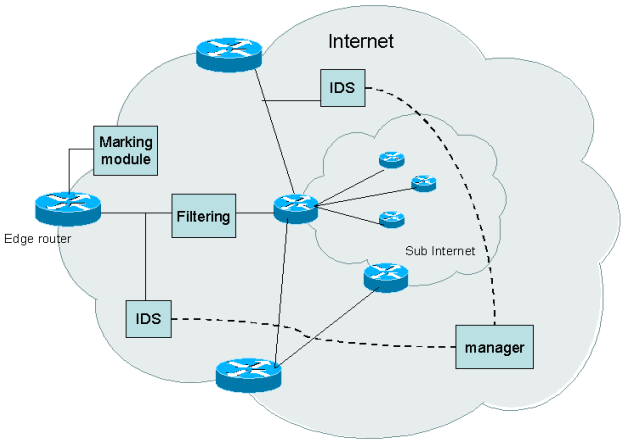

그림4. 침입 탐지 시스템 기반의 패킷 필터링 구조

인프라 네트워크의 에지 라우터로 패킷이 유입되면 그림5와 같은 순서로 패킷 필터링이 이루어진다.

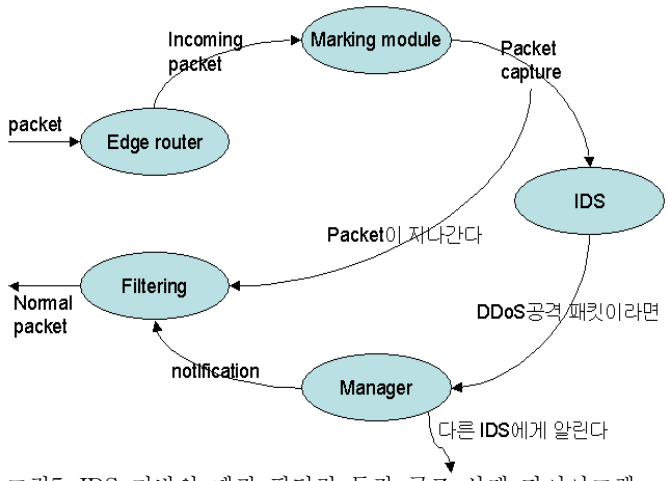

그림5. IDS 기반의 패킷 필터링 동작 구조 상태 다이어그램

에지라우터를 통해 패킷이 유입되면 마킹 모듈이 호출된다. 마킹 모듈에서는 통계적 탐지 알고리즘[1]에 의해 패킷에 마킹을 하고 라우터 밖으로 내보낸다. 통계적 탐지 알고리즘에 대한 자세한 설명은 지면상 본 논문에서는 생략하기로 한다. 패킷이 IDS를 지나가면 IDS에서는 패킷을 캡쳐하고 룰셋과 패킷에 마킹된 정보를 근거로 스트링 매칭을 통한 탐지를 시작한다. 매칭 결과 DDoS 공격 패킷으로 인식되면 IDS는 Manager에게 이상이 탐지되었음을 알리고 Manager는 Filtering 모듈 또는 인프라 네트워크 안에 있는 다른 IDS에게 제어 명령을 내려 DDoS 공격을 방어한다. Filtering 모듈은 우선순위 큐잉에 따라 DDoS공격 패킷을 우선순위가 제일 낮은 큐에 할당하고 정상적인 패킷을 먼저 내보내게 된다. 따라서 인프라 네트워크 안의 서브 네트워크 안까지 DDoS 공격 패킷이 거의 침입할 수 없다. 필터링 모듈은 또한 각 라우터 앞에 놓여 있어야 하는 비효율성을 서브 네트워크의 에지라우터 앞에만 설치함으로써 한 네트워크 안에서 필터링 작업량을 줄일 수 있도록 하였다.

3.2. 통계적 탐지 알고리즘을 이용한 패킷 마킹

에지 라우터에서 패킷이 유입되면 라우터상에 있는 마킹 모듈에서 통계적 탐지 알고리즘을 이용하여 패킷에 특정 값을 마킹한다. 탐지 알고리즘에 의해 계산된 엔트로피(entropy) 값은 DDoS공격 패킷일 경우 정상적인 패킷보다 높은 값을 가진다.[2] 다음 그림6은 1200000개의 패킷이 path를 지나간 경우 엔트로피 값의 분포를 나타낸 그래프이다. 앞에서 말한 것과 같이 탐지 알고리즘에 대한 자세한 기술은 본 논문에서는 생략할 것이다.

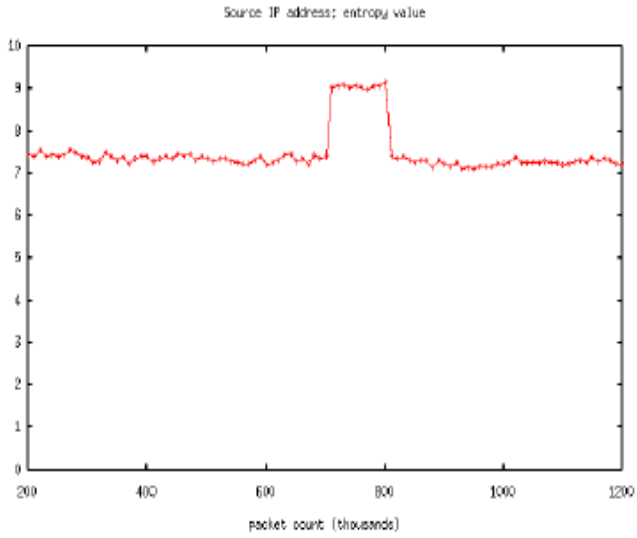

그림6. 통계적 탐지 알고리즘에 의한 DDoS공격에 의한 엔트로피 값

700~800개의 패킷이 유입될 때 엔트로피 값이 9정도까지 올라갔으므로 이 시기의 패킷들을 DDoS공격 패킷으로 보고 마킹 모듈에서 패킷의 옵션 필드 중 8비트 code비트에 마킹해둔다. 그림7은 IP 패킷의 옵션 필드를 나타낸 것이다. 8비트 code비트 중

2비트 class의 예약비트 01과 11 비트를 사용하여 DDoS공격 패킷인지 아닌지를 판별해둘 수 있다.

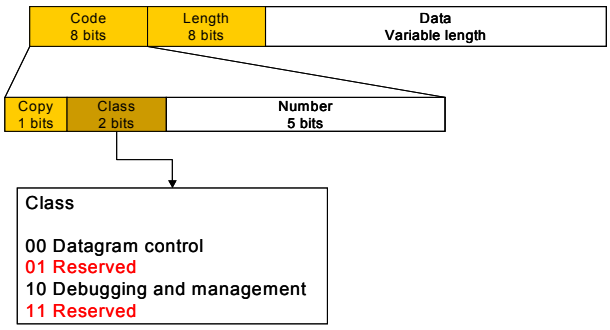

그림7. IP 패킷의 옵션 필드

3.3. 우선순위 큐잉에 기반한 패킷 필터링 구조

DDoS 공격은 특정 시간동안 다량의 트래픽을 유발시킨다. 그러므로 임의의 임계값을 정하여 임계값 이하 또는 이상의 값을 갖는 패킷들에 우선순위를 부여하여 높은 우선순위를 갖는 패킷은 허용하고 임계값 이상 유입되는 패킷은 DDoS 공격 패킷이라고 보고 차단하여 Filtering 하게 된다.[3] 이것을 우선순위 기반의 큐잉기법이라고 하며 큐에 할당되는 버퍼는 카운터나 시간을 임의로 정하여 값을 초과하면 버퍼에서 삭제시켜 버퍼 낭비를 줄인다.

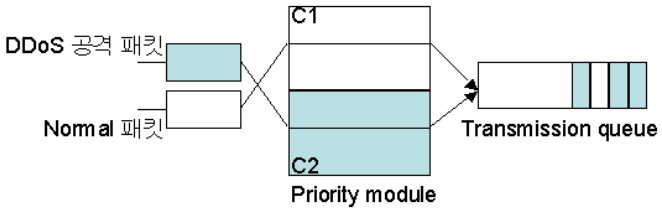

그림8. 우선순위 큐잉 기반의 패킷 필터링 구조

그림8은 DDoS 공격 패킷과 정상적인 패킷이 필터링 모듈로 들어왔을 때 우선순위 큐잉 구조를 나타낸 것이다.[5] priority module에서 윗부분이 우선순위가 높고 아랫부분이 우선순위가 낮다. 정상적인 패킷인 경우 우선순위를 높게 두어 큐에서 빨리 내보내지도록 하였고 DDoS공격 패킷인 경우 우선순위를 낮게 두어 정상적인 패킷의 전송량보다 매우 낮은 량으로 보내거나 큐에서 삭제시킨다. 이러한 방법을 사용함으로써 서브 네트워크 안으로 유입될 수 있는 DDoS공격을 탐지, 차단, 방어할 수 있다.

4. 결론 및 향후과제

본 논문은 침입 탐지 시스템을 기반으로 분산 서비스 거부 공격을 탐지하고 방어할 수 있는 패킷 필터링 구조를 제안하였다. IDS는 패킷을 캡쳐해서 Rull과의 스트링 매치를 통해 이상을 탐지하므로, DDoS와 같은 다량의 패킷 공격을 빠르고 효과적으로 막기 위해서 에지 라우터에서 패킷이 유입되면 통계적 탐지 알고리즘에 의해 계산된 엔트로피 값을 IP 패킷인지의 여부의 기준으로 삼아 명시해둔다. IDS는 DDoS 공격 패킷을 탐지하여 Manager로 탐지 사실을 알리고 필터링을 제어하도록 한다. 필터링 모듈은 우선순위 큐잉에 의해 DDoS 공격 패킷에 낮은 우선순위를 두어서 공격을 효과적으로 차단시킬 수 있다. 향후과제로는 제안된 패킷 필터링 구조의 성능을 입증할 수 있는 시뮬레이션 및 실제적인 구현이 필요하다.

참고문헌

[1] Laura Feintein, DanSchnachenberg, Ravindra Balupari, Darrell Kindred, “Statistical Approaches to DDoS Attack Detection and Response”, Information Survivability Conference and Exposition(DISCEX′03), IEEE 2003

[2] Tiziani Ferrari, Giovanni Pau, Carla Raffaelli, "Measurement Based Analysis of Delay in Priority Queuing", GLOBECOM′01, IEEE 2001

[3] Sapon Tranchaiwiwat, Kai Hwang, "Differential Packet Filtering Against DDoS Flood Attacks", ACMSIGCOMM 2003

[4] Jun Xu, Minho Sung, "IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks", International Conference on Parallel and Distributed Systems, IEEE 2003

[5] R.J. Gibbens and F. P. Kelly, "On Packet Marking at Priorty Queues", International Conference on Automatic Control, IEEE 2002