우회 DoS 공격을 탐지하기 위한 모델 설계*

김용석° 전준철 유기영
경북대학교 컴퓨터공학과
{shadowguys°, jcjeon33}@infosec.knu.ac.kr yook@knu.ac.kr

Detecting scheme against bypass Denial of Service Attack

Yong-Seok Kim° Jun-Cheol Jeon Kee-Young Yoo
Department of Computer Engineering, Kyungpook National University

요 약

현재 사용 되어지는 컴퓨터 통신 프로토콜(OSI 7 layer reference model)은 구조적인 문제점을 들어내고 있다. 이런 문제점 때문에, 해커들은 수많은 패킷들을 생성시키는 Denial of Service(DoS) 공격과 Distributed Denial of Service(DDoS) 공격을 사용하여 한 호스트나 한 네트워크 자원에 치명적인 악영향을 미친다. 특정한 TCP 포트나 UDP 포트에 공격을 가하는 경우에는 룰 기반의 침입탐지 시스템(IDS)이 탐지 해낼 수 있지만, 다른 임의의 포트에 공격을 가하게 되면 IDS는 이것을 탐지하지 못한다. 따라서 우리는 임의의 포트에 DoS나 DDoS 공격들이 일어났을 때 이 공격들을 탐지할 수 있는 모델을 설계하였다.

1. 서 론

인터넷의 발달은 컴퓨터를 통해 언제 어디에서든 우리가 원하는 정보를 쉽게 얻을 수 있게 되었다. 하지만 1969년도에 생겨난 인터넷은 조금씩 구조적인 문제들을 드러내고, 이러한 구조적인 문제들은 해커들로 하여금 사이버 공간에서의 범죄를 일으키는 데 이용되고 있다. 다른 해킹들보다 최근 몇 년간 그 수위를 높여가고 DDoS 공격은 불특정다수의 인터넷 사용자들에게 네트워크 사용 또는 서비스 사용에 심각한 영향을 미친다는 점에서 그 공격 기법에 대한 대응 방안 모색이 시급한 실정이다. 이러한 공격의 경우 Attacker가 신분을 감추기 위하여 IP Spoofing 기술을 기반으로 공격하므로, 공격 대상 시스템뿐만 아니라 공격 대상의 루트(route)에 있는 시스템들까지 성능저하를 야기한다.

그 중 2002년 2월 Yahoo, Amazon, CNN에 발생하여 각 웹 사이트들에 큰 피해를 입히면서 세계적인 문제로 부상되었으며[1], 국내에서는 2003년 1월 25일에는 MS-SQL 웜으로 발생된 DDoS 공격으로 인해 국가 핵심 인터넷이 마비가 되는 심각한 피해를 초래하였다. 이러한 DDoS 공격은 날로 다양해지고 자주 발견되고 있으며 인터넷 정체의 주 요인이 되고 있다[2].

DDoS 공격을 탐지하는 현재의 방법은 주로 방화벽이나 IDS를 이용한다. 하지만 이들은 룰 기반의 필터링이나 탐지를 하기 때문에 룰에서 벗어난 우회 공격은 탐지할 수 없게 된다. 예를 들어 "Winnuke attack" 응용 프로그램은 TCP 139번 포트인 NETBIOS Session Service에 패킷 flooding 공격을 가한다. 이렇게 된다면 룰 기반의 IDS는 이것을 쉽게 탐지할 수 있을 것이다. 하지만 이 공격 툴을 TCP 139번 포트가 아닌 21번 포트나 다른 특정 포트로 공격을 가한다면, IDS는 FTP command overflow attempt와 같은 잘못된 경고를 나타낸다. 따라서 본 논문은 효율적인 네트워크 자원 사용을 저해하는 DoS나 DDoS 우회 공격을 탐지하는 모델을 제시 하겠다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 DoS, DDoS 공격을 기술하고, 3장에서는 DoS나 DDoS 공격의 예방, 탐지 및 대응에 있어서 문제점을 기술하고, 4장에서는 우리가 제안한 우회 공격을 탐지하는 모델을 제시하고 분석한다. 마지막으로 결론에 대하여 기술할 것이다.

2. 공격의 유형

한 네트워크나 호스트를 마비시키는 DDoS 공격은 DoS 공격의 변형된 형태이다. 본 장에서는 DoS 공격과 DDoS 공격을 소개한다.

2.1 DoS 공격

DoS는 한대의 Attacker가 한대의 Victim에게 시스템의 정상적인 동작을 방해는 공격 수법으로서 대량의 데이터 패킷들을 통신망으로 보내는 방법이다[3][4]. DoS공격에는 2가지 방법이 있는데 그림 1과 같이 Attacker가 Victim에 직접 공격을 가하는 방법과 Attacker가 Victim이 아닌 Reflector에 공격을 가해서 Victim에 악영향을 미치는 Reflection 공격이 있다.

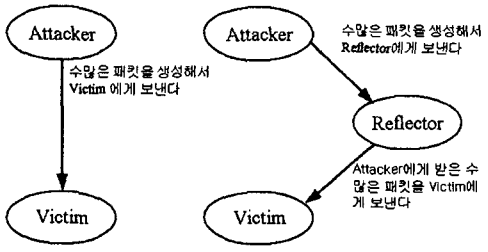

그림 1. DoS(Denial of Service)공격의 2가지 형태

*이 논문은 2003년도 두뇌한국 21사업에 의하여 지원되었음

DoS 공격에 사용되는 응용 프로그램은 SYN Flooding 공격, Ping of Dearth 공격, Tiny Fragmentation 공격, Teardrop, Fragment Overlap 공격 등이 있으며, DoS 공격은 한대의 Attacker가 Victim을 공격하는 방식이므로 큰 타격을 주지 못하며 또한 쉽게 탐지 될 수 있다. 따라서 이에 따른 대응 및 예방이 비교적 쉽다.

2.2 DDoS 공격

DDoS 공격은 인터넷에 연결된 여러 대의 시스템들을 이용해 단일 사이트에 대한 패킷 Flood 공격을 시도하는 것이다[5]. Attacker는 알려진 취약성 조사를 위해 수많은(100,000대 이상) 호스트에 대한 스캔들을 시도해서 취약한 시스템에 대한 권한을 획득하여 그 시스템에 원격에서 실행할 수 있는 응용 프로그램을 설치하고, 원격에서 이를 실행시켜 원격에서 공격을 개시한다.

그림 2와 같이 공격 시에는 Attacker가 이전에 획득한 Slave들에게 IP의 Source 주소는 임의의 주소를 부여 하고 Destination 주소에 Victim을 설정하여 공격을 명령한다.

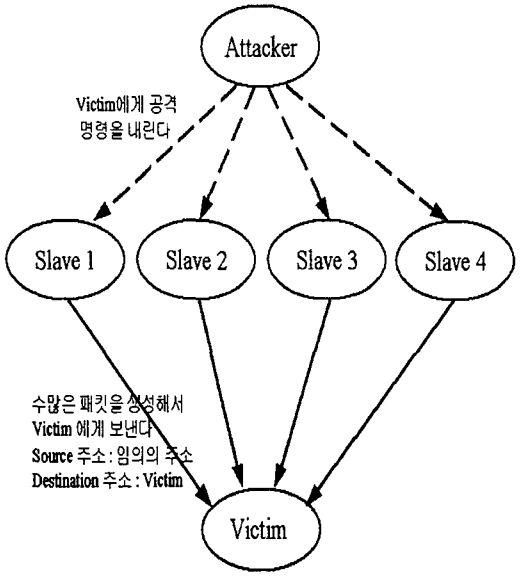

그림 2. DDoS(Distributed Denial of Service)공격의 형태

DDoS 공격에 사용되는 응용 프로그램으로는 TrinOO, TFN, TFN2K, Stacheldraht 등이 있다.

3. 공격의 예방, 탐지 및 대응의 문제점

DoS나 DDoS 공격으로 전송되는 패킷들은 서비스의 합법적인 사용을 위한 패킷과 구분하기 힘들다. 따라서 이런 패킷들을 탐지할 수 있거나 필터링 할 수 있는 일반적인 특성이 없다. 다만 필터링 하기 위해서는 공격 되는 패킷들이 아닌 Attacker가 여러 대의 Slave들로 보내는 공격 명령을 필터링할 수는 있다. 하지만 Attacker가 Slave들과 통신할 때 사용하는 일반적인 포트가 아닌 다른 포트를 사용 시에는 이것도 필터링하지 못할 수도 있다.

인터넷에 광범위하게 퍼져서 공격을 가하는 DDoS공격은 역 추적하기 어렵다. 그리고 분산된 근원지에 대처할 수 있도록 관리 도메인간의 협력이 필요한 반면 관리 도메인간의 협력이 부족하며, DDoS 공격 코드와 자동화된 응용 프로그램은 인터넷으로부터 쉽게 다운 받을 수 있어서 초보 해커도 쉽게 강력한 공격을 실행시킬 수 있고 공격 코드를 변경할 수도 있다. Attacker는 공격 시스템의 신분(identity)을 숨기기 위해 Source 주소에는 임의의 주소를 사용하고, Destination 주소에는 Victim을 사용하기 때문에 공격하는 시스템을 유추하기 어렵다.

4. 우회 공격 탐지 모델

DoS나 DDoS의 패킷들은 일반적인 특징들이 있어서 룰 기반의 IDS나 방화벽은 이것을 쉽게 탐지 하거나 필터링 할 수 있지만, Attacker들의 약간의 변형에 의해 이런 룰 기반의 IDS나 방화벽을 우회할 수 있다. 본 장에서는 우회 하는 공격을 탐지하기위한 모델을 제시한다.

4.1 기초 연구

DoS나 DDoS 공격의 응용 프로그램들은 제작자가 프로그래밍 한대로 특정한 TCP 포트를 공격한다. 이 응용 프로그램의 TCP 포트를 조금만 수정하여도 특정한 TCP 포트가 아닌 다른 TCP 포트를 공격할 수 있다. 이런 우회 공격을 탐지하기 위해 현재 네트워크 환경(10/100 Mbps LAN)에서 1대의 서버에 TCP 포트에 전송 되는 최대 패킷의 양을 1초 동안 측정해 보았다. 예를 들어 TCP 포트 23번인 Telnet 서비스에서 1대의 서버와 1대의 호스트가 1초 동안에 서로 전송하는 패킷의 양은 10 ~ 15 패킷 정도이다. 그래서 표 1과 같은 결과를 얻을 수 있었다.

표 1. 응용 프로그램에 전송되는 패킷의 측정 양

서비스(프로토콜/포트)	패킷 양(단위: 패킷/초)
Telnet (TCP/23)	15
FTP (TCP/21)	10
SSH (TCP/22)	40
HTTP (TCP/80)	25
SMTP (TCP/25)	25
Ping (ICMP)	5
데이터가 6550 일때 Ping (ICMP)	45

표 1의 결과에 의해서, 1초 동안에 전송 되는 패킷의 양 x는 45와 같거나, 보다 적을 것이다. 하지만 1초 동안 측정된 DoS 공격의 패킷의 양은 약 100개 정도이다. 더욱이 DDoS 공격을 했다면 이것보다 훨씬 더 많을 것이다. 그러므로 한 TCP 포트에 정상적으로 1초 동안에 전송 되는 패킷의 양 x는 $x \leq 45$ 이다. 더욱이 1초 동안에 전송 되는 패킷의 양 x가 45보다 초과 할 경우에, 이것은 DoS나 DDoS 공격이다.

4.2 탐지 모델

위에서 측정된 결과를 기반으로 하여 전송 되는 패킷의 양 x는 x > 45 인 것을 찾아내는 알고리즘을 설명하겠다.

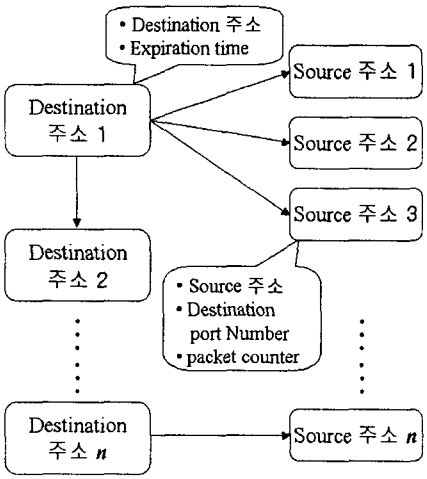

그림 3. 우회 공격 탐지 트리

```
Detect_bypass_attack()
{

    if(새로운 패킷이 들어 왔는가? == true)
        add_to_List(destination address, time);

    else if(현재 destination 시간 –
          리스트에 있는 destination 시간  > 5)
        del_to_List(destination address);

    else
    {
        for (i = 0; i< list_index; i++)
        {
            if(check_to_List(incoming packet) == true)
                add_to_Counts_of_List(i);
        }
    }

    for(i=0;i < List_index; i++)
    {
        if((return_Count_of_List) > 45)
            Alert 하고 버퍼에서 삭제;
    }
}
```

그림 4. 우회 공격 탐지 알고리즘

그림 3과 같이 먼저 패킷의 양을 측정하기 위해 처음 Destination 주소로 들어오는 패킷을 리스트에 각각 노드를 만들고, 이 Destination 주소 노드는 메모리의 활용도를 위해 만기 시간을 5 초로 하여 5초가 지나도 그 주소로 패킷이 들어오지 않으면 그 Destination 주소를 리스트에서 삭제 시킨다.

리스트가 만들어 지면 들어오는 패킷의 Destination 주소 노드와 리스트 안에 들어 있는 Destination 주소를 비교하여, 일치하는 Destination 주소가 있다면 그 Destination 주소에 Source 주소들마다 트리 형태로 노드를 만들어 Destination 주소에 어떤 포트를 사용하고 있는지 저장해 주고, 다음의 패킷이 들어올 때까지 대기한다. 만약 Destination 주소 노드와 Destination 주소가 동일하고 Source 주소 노드와 Source 주소가 동일하면 Source 주소 노드에 패킷 카운터를 1 증가 시킨다. 마지막으로 1초 동안에 만들어진 리스트에 각각의 Destination 주소마다 Source 주소 노드를 모두 다 검사하여 Source 주소 노드 중에서 패킷 counter가 45를 초과한 경우에 DoS나 DDoS 공격과 같은 서비스 거부 공격이 일어났다고 보고 경보 메시지를 출력한다.

4.3 분석

본 탐지기법은 DoS나 DDoS 공격 패킷의 특성을 룰에 적용해서 필터링하거나 탐지하는 기법이 아닌 한 서버의 포트에 전송되는 패킷들을 Source 주소 별로 각각 계산해서 DoS나 DDoS를 탐지하는 방법이므로 DoS나 DDoS 공격의 응용 프로그램이 다른 포트를 공격하더라도 탐지해 낼 수 있다. 하지만 이 공격들을 탐지 하기위해 리스트와 트리를 사용했기 때문에 시스템 오버헤드가 발생될 수 있을 것이다.

5. 결론

방화벽이나 IDS는 일반적으로 룰 기반이기 때문에 일반적인 TCP/UDP 포트에 DoS나 DDoS 공격은 탐지나 필터링할 수 있다. 하지만 일반적인 TCP/UDP 포트 공격이 아닌 다른 포트를 공격 한다면 방화벽이나 IDS 시스템은 이런 공격들을 탐지 하지 못하게 된다. 본 논문에서는 방화벽이나 IDS가 필터링 하거나 탐지 하지 못하는 일반적인 TCP/UDP 포트 공격이 아닌 TCP/UDP 포트 서비스 거부 공격인 우회 공격에 대해 탐지해낼 수 있는 모델을 설계하였다.

[참고문헌]

[1] D. Moore, G Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity." In Proceedings of the 10th USENIX Security Symposium, 2001.

[2] Kevin J. Houle, George M. Weaver, Neil Long, and Rob Thomas. Trends in Denial of service attack technology, October 2001. CERT and CERT Coordination Center.

[3] Computer Emergency Response Team. CERT Advisory CA-1996-21 TCP SYN Flooding Attacks. http://www.cert.org/advisories/CA-1996-21.html, September 1996.

[4] Roger Needham. Denial of Service: An Example. Communications of the ACM, 37(11):42-47, November 1994.

[5] Felix Lau, et al., "Distributed Denial of Service Attacks", Systems, Man, and Cybernetics, 2000 IEEE International.