MIB 정보와 패킷 분석을 통한 DDoS 공격의 탐지

Detection of DDoS Attacks using MIB Information and Packet Analysis

김미혜
충북대학교 전기전자컴퓨터공학부

원승영
(주) 네오네스

Mi-Hye Kim (mhkim@chungbuk.ac.kr)
School of Electronic & Computer Eng., Chungbuk National University

Seung-Young Won (sywon@neones.co.kr)
Neones Co., Ltd.

중심어 : MIB, 패킷분석, DDoS

Keyword : MIB, Packet Analysis, DDoS

요 약

DDoS 공격은 네트워크 대역폭, 프로세스 처리능력, 기타 시스템 자원을 고갈시킴으로써 정상적인 서비스를 할 수 없도록 하는 공격 형태이다. DDoS 공격의 인지는 시스템이나 네트워크가 느려지거나 접속 불능 상태 등 직관적으로 인지할 수도 있지만 정확하고 효율적인 분석을 통한 DDoS 공격의 탐지가 필요하다. 본 논문에서는 MIB 정보를 이용하여 트래픽 폭주를 탐지하고, 패킷 분석을 통하여 공격 트래픽을 탐지하는 효율적인 DDoS 공격 탐지 시스템을 제안하였다.

Abstract

DDoS is an attack type that interfere with normal service by running out network bandwidth, process throughput, and system resource. It can be recognized intuitively by network slowdown and connection impossibility state, but it is necessary to detect DDoS attack by exact and quantitative analysis. In this paper, the exact and efficient DDoS attack detection system which is able to detect traffic flooding by MIB information, and attack traffic by packet analysis is proposed and realized.

I. 서론

최근 인터넷 보안 체계를 공격하는 경향은 네트워크 및 시스템 자원을 모두 소비해서 실제 자원을 사용해야 하는 사용자가 서비스를 받을 수 없게 하는 DDoS(Distributed Denial of Service) 공격이 주를 이루고 있다[1]. DDoS 공격의 인지는 시스템이나 네트워크가 느려지거나 접속 불능 상태 또는 CPU, 메모리 사용량 등을 통해 직관적으로 인지할 수도 있다. 하지만 보다 정확하고 계량적인 분석을 통한 DDoS 공격의 탐지가 필요하다. DDoS 공격의 탐지에 있어서 가장 중요한 부분은 공격을 정확히 탐지하여야 하며 탐지를 위한 시스템 자원을 효율적으로 사용해야 하는 것이다. 트래픽 폭주가 발생하였다고 하여 모두 공격으로 탐지하고 대응조치를 한다면 인터넷 사용자와 공급자 모두에게 크나큰 손실을 가져오게 될 것이다. 또한 탐지를 위해 많은 시스템 자원을 사용한다면 정상적인 서비스를 제공하지 못하는 문제점이 발생한다. 따라서 본 논문에서는 효율적인 시스템 자원의 사용으로 트래픽 폭주를 탐지하기 위하여 MIB 정보 중에서 이상 트래픽을 탐지할 수 있는 중요 객체들을 선정하여 트래픽 모니터링을 하고 생성된 로그를 분석하여 트래픽 폭주를 탐지하였다. 그리고 정확한 공격 트래픽의 탐지를 위하여 트래픽 폭주를 발생시킨 패킷들을 수집하고 수집된 패킷들의 근원지 IP 주소와 프로토콜별 목적지 포트를 분석하여 정상 트래픽과 공격 트래픽을 판단하는 시스템을 제안하였으며, 제안한 시스템의 검증을 위해 MIB(Management Information Base) 정보를 이용한 탐지, 패킷 캡쳐 응용 프로그램을 이용한 탐지와 제안 시스템과의 탐지 시간 및 시스템 자원 사용률을 비교 분석하였다.

II. DDoS 공격 탐지

1. DDoS 공격 유형

DDoS 공격은 여러 에이전트를 이용하여 동시에 피해 호스

접수번호 : #031115-003
접수일자 : 2003년 11월 15일, 심사완료일 : 2003년 12월 9일

*교신저자 : 김미혜, e-mail : mhkim@chungbuk.ac.kr

트로 DoS 공격을 행함으로써 일반적인 DoS 공격보다 강력한 파괴력을 가진 공격 형태이며, TCP SYN 플러딩, Trin00, TFN, Stacheldraht 공격 등이 있다[2].

1.1. TCP SYN 플러딩 공격

TCP SYN 플러딩 공격은 연결형 프로토콜인 TCP 연결의 결점을 이용한 공격이다. 삼중 핸드쉐이크 절차를 이용하여 연결하는 과정에서 half-open 상태로 계속 머물게 하여 버퍼 오버플로우를 발생시켜 공격하는 방법으로 메모리 고갈로 인해 정상적인 요청 연결을 요구하는 호스트에게 응답을 할 수 없도록 하는 DoS 공격이다.

1.2. Trin00 공격

Trin00 공격은 몇 개의 마스터와 수많은 에이전트로 구성된다. 공격자는 마스터를 TCP 포트 27665번을 이용하여 제어하고 마스터와 에이전트간의 통신은 UDP 포트 27444번과 31335번을 이용하는 것이 Trin00 공격의 특징이다.

1.3. TFN 공격

TFN 공격은 Trin00 공격과 유사한 DDoS 공격으로 많은 근원지에서 하나 혹은 여러 개의 피해 호스트에 대해 서비스 거부 공격을 수행한다. 하지만 TFN 공격의 특징은 공격자가 마스터로 접속하기 위한 별도의 포트가 준비되어 있지는 않다는 것이다. 따라서 공격자가 마스터로 접근하려면 telnet 등의 프로그램을 사용해서 마스터를 제어하여야 한다.

1.4. Stacheldraht 공격

Stacheldraht 공격은 Trin00 공격의 네트워크 구조와 TFN 공격의 다양한 공격 방법과 연결상의 암호화 기능을 포함한 DDoS 공격이다. 네트워크의 제어는 공격자와 마스터사이의 통신에 대칭 키 암호 방식을 사용하는 간단한 프로그램을 통해 이루어진다.

2. 기존의 DDoS 공격 탐지

2.1. TCP SYN 플러딩 공격 탐지

H. Wang와 D. Zhang, K. G. Shin은 TCP 헤더의 SYN, FIN, RST 플랙을 이용하여 TCP SYN 플러딩 공격을 탐지하는 연구를 하였다[3]. DDoS 공격이 없는 경우 TCP 연결과 종료는 재전송의 경우를 제외하면 거의 동일한 비율로 발생할 것이다. 하지만 TCP SYN 플러딩 공격이 발생하면 대량의 SYN 플랙을 가진 TCP 패킷이 급격히 증가하므로 SYN 플랙의 탐지비율이 FIN 플랙의 탐지비율 보다 훨씬 많아지게 된다. 이러한 성질을 이용하여 DDoS 공격 중 TCP SYN 플러딩 공격을 효과적으로 탐지하는 방법을 제시하고 있다. 하지만 이 방법은 TCP 연결 생성의 특성을 이용하는 방법으로 TCP SYN 플러딩 공격의 탐지에는 매우 유용하지만 그 이외의 다른 DDoS 공격 유형에 대해서는 탐지할 수 없는 단점을 가지고 있다. 그림 1은 TCP 패킷 분류 과정을 도시한 것이다.

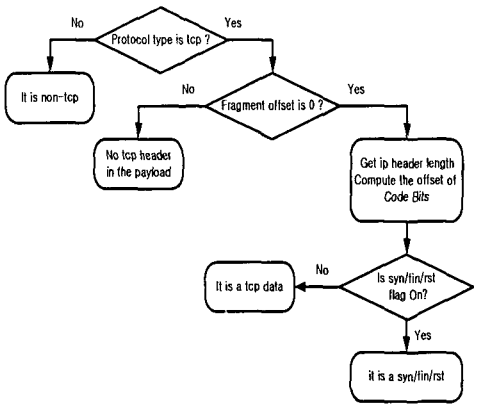

그림 1. TCP 패킷 분류 과정

2.2. 근원지 IP 주소의 무작위성을 이용한 탐지

T. M. Gil과 M. Poletto는 특정 서브 네트워크 내부로 들어가는 패킷 비율과 밖으로 나가는 패킷 비율의 불균형 현상을 이용해서 DDoS 공격을 탐지하는 방법을 연구하였다.[4] 이 탐지 방법은 임의의 서브 네트워크 P에 대해서 R(P)를 들어가는 패킷 비율과 나가는 패킷 비율로 가정한다면 Rmin < R(P) < Rmax 인 경우를 정상적인 상태로 인식하고 그 외의 경우를 DDoS 공격 상태로 인식하는 방식을 사용하였다. DDoS 공격에 사용되는 공격 패킷의 근원지 IP 주소가 속여지는 현상을 이용하며 DDoS 공격 패킷에 대한 피해 호스트의 응답 패킷이 DDoS 공격이 시작된 방향이 아닌 다른 방향으로 빠져나가는 것을 모니터링 함으로써 DDoS 공격을 탐지할 수 있는 탐지 방법이다. 하지만 이런 종류의 탐지 방법은 공격자가 근원지 IP 주소를 속이는 빈도를 줄이게 되면 정확한 DDoS 공격의 검출이 불가능해지는 단점을 가지고 있다.

2.3. 주파수를 이용한 탐지

P. Barford, J. Kline는 변동적인 네트워크 트래픽의 주파수 특성을 구분하여 DDoS 공격이나 포트 스캔 공격을 탐지하는 연구를 하였다[5]. DDoS 공격이 발생했을 경우 고주파와 중

주파에서는 공격을 탐지해 냈지만 저주파에서는 공격의 영향을 미치지 못한 것을 알 수 있다. 하지만 제안한 주파수를 이용한 DDoS 공격 탐지 방법에서는 웨이블릿 변환된 주파수만을 이용하여 DDoS 공격을 판단함으로써 정상 트래픽과 주파수 파형이 비슷한 공격 트래픽에 대한 탐지가 어려운 문제점을 가지고 있다. 그림 2는 고주파와 중주파에서의 DDoS 공격 탐지를 보여주고 있다.

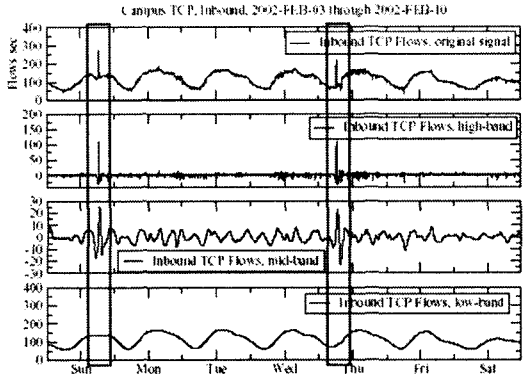

그림 2. 고주파와 중주파에서의 DDoS 공격 탐지

III. 제안한 DDoS 공격 탐지 모델

1. DDoS 공격 탐지 모델

본 논문에서 제안한 DDoS 공격 탐지 모델은 그림 3과 같이 구성된다.

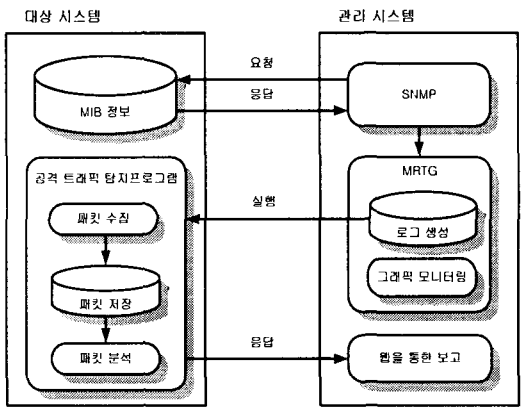

그림 3. DDoS 공격의 탐지 모델

대상 시스템은 관리 정보 베이스인 MIB의 정보와 패킷을 수집하고 분석하기 위한 공격 트래픽 탐지프로그램으로 구성되며 관리 시스템은 대상 시스템의 관리 정보를 요청하고 응답 받기 위한 SNMP(Simple Network Management Protocol)와 수집된 MIB 정보를 이용하여 로그를 생성하고 그래픽화된 모니터링을 하기 위한 MRTG(Multi Router Traffic Grapher)로 구성된다. SNMP를 이용하여 DDoS 공격에 대하여 반응할 수 있는 프로토콜별 특정 MIB 객체의 정보를 수집하고 MRTG를 이용하여 생성된 로그값이 시스템 성능을 고려한 임계값을 넘어서는 수신 트래픽이 발생할 경우에 폭주로 탐지하였다.

2. MIB 정보를 이용한 트래픽 폭주의 탐지

트래픽 폭주를 탐지하기 위하여 표 1과 같은 MIB 정보를 이용하여 트래픽 모니터링과 로그를 생성하여 분석하는 방법을 사용하였다.

표 1. 트래픽 모니터링을 위한 MIB 객체

구분	객체	정의
TCP	tcpInErrs	오류로 수신된 TCP 세그먼트의 총 개수
UDP	udpNoPorts	수신된 UDP 데이터그램 중 목적지 포트에 응용 프로그램이 없는 데이터그램의 총 개수
ICMP	icmpInErrors	수신된 ICMP 메시지 중 오류 (불량 ICMP 검사합, 길이 불량 등)로 판명된 ICMP 메시지들의 개수

트래픽 모니터링을 하기 위하여 네트워크의 트래픽을 측정하는 도구인 MRTG를 이용하여 모니터링과 로그를 생성하였다. 본 논문에서는 MRTG에 의해 생성된 로그를 사용하여 트래픽 폭주를 탐지하는 방법을 이용하였다[6]. 로그 파일은 그림 4와 같다.

```
1066099202 3526286401 1816703875
1066099202 3677 109 3677 109
1066098903 9704 113 9704 113
1066098900 9686 112 9704 113
1066098600 8011 108 22428 128
1066098300 22259 127 22428 128
1066098000 5504 105 5543 113
1066097700 1741 113 2451 113
1066097400 2563 112 19310 113
1066097100 19189 112 19310 192
1066096800 1258 279 1567 8967
```

그림 4. MRTG의 로그 파일

본 논문에서는 트래픽 최대 수신값에 시스템 성능이 허용하는 임계치를 두어 임계치 이상의 트래픽이 발생할 경우 트

래픽 폭주로 판단하고 공격 트래픽 탐지프로그램을 실행하여 공격 트래픽을 탐지하였다. 그림 5는 MIB 정보를 이용한 트래픽 폭주의 탐지 흐름도이다.

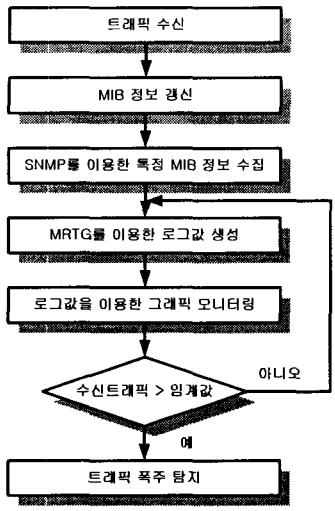

그림 5. MIB 정보를 이용한 트래픽 폭주의 탐지 흐름도

3. 패킷 분석을 통한 공격 트래픽의 탐지

DDoS 공격의 특징은 프로토콜별 플러딩 공격이 가능하며, 근원지 IP 주소를 속이기 위하여 근원지 IP 주소와 목적지 포트 번호를 무작위로 생성하여 공격한다는 것이다. 이러한 DDoS 공격의 트래픽을 탐지하기 위하여 본 논문에서 제안한 공격 트래픽 탐지프로그램을 사용하였으며 프로토콜별 근원지 IP 주소와 목적지 포트 번호를 분석하여 공격 트래픽을 판단하였다. 정상적인 트래픽 폭주가 발생한 경우에는 응용프로그램이 있는 특정 포트를 사용하여 트래픽이 발생한다. 그림 6은 FTP 사용으로 인한 정상 트래픽이 발생했을 때의 패킷 정보를 보여주고 있다.

```
2.418308   coyote.chungbuk.ac.kr sywon.chungbuk.ac.kr  FTP-DAT FTP Data: 1200 bytes
2.418485   coyote.chungbuk.ac.kr sywon.chungbuk.ac.kr  FTP-DAT FTP Data: 1448 bytes
2.418618   coyote.chungbuk.ac.kr sywon.chungbuk.ac.kr  FTP-DAT FTP Data: 1448 bytes
2.418718   coyote.chungbuk.ac.kr sywon.chungbuk.ac.kr  FTP-DAT FTP Data: 1200 bytes
2.418878   coyote.chungbuk.ac.kr sywon.chungbuk.ac.kr  FTP-DAT FTP Data: 1448 bytes
2.419018   coyote.chungbuk.ac.kr sywon.chungbuk.ac.kr  FTP-DAT FTP Data: 1448 bytes
2.419116   coyote.chungbuk.ac.kr sywon.chungbuk.ac.kr  FTP-DAT FTP Data: 1200 bytes
```

그림 6. FTP 사용으로 인한 정상 트래픽

하지만 공격의 경우 포트 번호의 무작위성이 발생되는 특징으로 정상 트래픽과 공격 트래픽을 구분하여 공격을 탐지하였다. 그림 7은 UDP 플러딩 공격으로 인한 공격 트래픽이 발생했을 때의 패킷 정보를 보여주고 있다.

```
0.960342   234.107.71.10      sywon.chungbuk.ac.kr  UDP   Source port: 2084  Destination port: 7916
0.960345   240.42.158.109     sywon.chungbuk.ac.kr  UDP   Source port: 2083  Destination port: 7917
1.000688   27.77.222.119      sywon.chungbuk.ac.kr  UDP   Source port: 2082  Destination port: 7918
1.020365   17.70.4.39         sywon.chungbuk.ac.kr  UDP   Source port: 2081  Destination port: 7919
1.040378   188.222.243.54     sywon.chungbuk.ac.kr  UDP   Source port: 2080  Destination port: 7920
1.060367   133.58.187.60      sywon.chungbuk.ac.kr  UDP   Source port: 2079  Destination port: 7921
1.080379   89.181.29.0        sywon.chungbuk.ac.kr  UDP   Source port: 2078  Destination port: 7922
```

그림 7. UDP 플러딩 공격으로 인한 공격 트래픽

정상 트래픽이 발생했을 경우에는 그림 8에서 보는 바와 같이 근원지 IP 주소가 일정하며 목적지의 응용프로그램이 동작하는 일정한 포트 번호로 트래픽이 수신되는 것을 볼 수 있다. 하지만 공격 트래픽이 발생했을 경우에는 무작위의 근원지 IP 주소와 목적지 포트 번호로 트래픽이 수신되는 것을 알 수 있다. 이러한 공격 트래픽의 특징을 이용하면 공격 트래픽을 정확히 탐지할 수 있다. 공격 트래픽 탐지프로그램은 트래픽 폭주를 발생시킨 패킷을 수집하고 데이터베이스에 저장하며 저장된 패킷 정보들은 정상 트래픽과 공격 트래픽을 구분하는 기준으로 사용된다. 그림 8은 공격 트래픽 탐지프로그램으로 수집된 패킷을 분석하여 정상 트래픽과 공격 트래픽을 판단하는 흐름도이다.

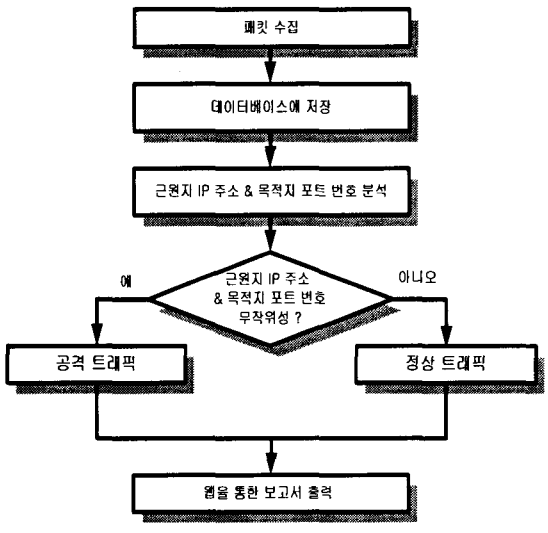

그림 8. 공격 트래픽의 탐지 흐름도

IV. 실험 및 결과 고찰

DDoS 공격을 탐지하기 위하여 공격 시스템과 에이전트에

공격 도구를 설치하였으며, 트래픽 수집과 분석을 통하여 공격 트래픽을 탐지하기 위하여 그림 9와 같이 대상 시스템과 관리 시스템을 구성하였다.

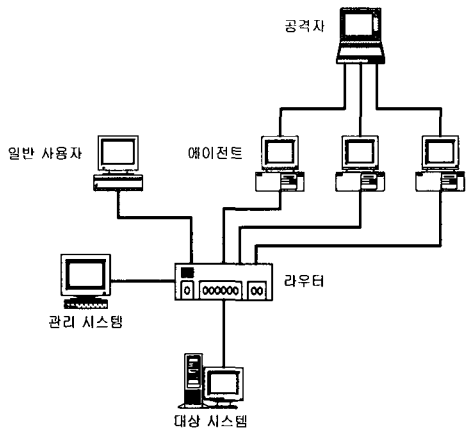

그림 9. 실험 환경 구성도

1. 트래픽 폭주의 탐지 실험

트래픽 폭주를 탐지하기 위하여 대상 시스템에 Trin00을 이용한 UDP 플러딩 공격을 하였다. 그림 10에서와 같이 대상 시스템의 MIB 객체 중 udpNoPorts 객체에서 많은 트래픽이 발생된 것을 알 수 있다.

```
1066912500 1106 43 1108 43
1066912200 1104 43 1110 43
1066911900 1109 43 1110 43
1066911600 1108 43 1111 43
1066911300 1112 43 1116 43
1066911000 505 19 1292 50
1066910700 12 8 15 8
1066910400 12 8 21 10
```

그림 10. UDP 플러딩 공격의 로그

트래픽 공격이 발생할 경우 생성된 로그를 살펴보면 단위 시간당 최대 수신값이 15에서 1292로 급격히 증가하는 것을 알 수 있다. 이와 같이 대상 시스템의 성능을 고려한 임계치 1000을 정하고 단위 시간당 최대 수신 값과 비교하여 임계치 이상의 로그값이 발생할 경우 트래픽 폭주로 탐지하였다. 하지만 DDoS 공격과 달리 정상 트래픽의 순간적인 폭주에서도 트래픽 폭주로 판단되는 경우가 발생하였다. 시간이 경과함에 따라 모니터링 결과와 로그값이 공격 트래픽과 정상 트래픽이 다른 것을 알 수 있으나 트래픽 폭주 공격의 특성상 짧은 시간에 많은 트래픽을 폭주시켜 대상 시스템을 공격함으로써 짧은 시간에 공격을 탐지하는 것이 매우 중요하다. 그림 11은 정상 트래픽의 순간 폭주로 인한 트래픽 폭주로 생성된 로그이다.

```
1066960500 28 10 56 10
1066960200 15 10 15 10
1066959900 18 10 19 10
1066959600 17 10 22 10
1066959300 507 351 507 351
1066959000 1156 864 1284 871
1066958700 102 82 105 87
1066958400 17 5 17 5
```

그림 11. 정상 트래픽의 순간 폭주 로그

DDoS 공격을 탐지함에 있어서 탐지 시간도 중요하지만 효율적인 시스템 자원의 사용률도 중요한 부분을 차지한다. DDoS 공격을 탐지하기 위하여 많은 시스템 자원을 사용한다면 정상적인 서비스를 위하여 사용될 자원이 상대적으로 적어지게 되어 정상적인 서비스를 할 수 없기 때문이다. 그림 12는 MIB 정보를 이용하여 트래픽을 수집하고 트래픽 폭주를 탐지하는데 사용된 CPU 사용률이다.

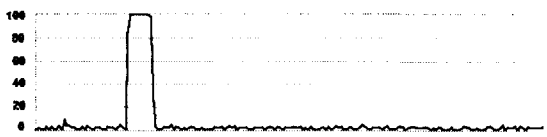

그림 12. MIB 정보를 이용한 트래픽 탐지의 CPU 사용률

트래픽 폭주를 탐지하기 위한 CPU 사용률은 대상 시스템에서 관리 시스템으로 MIB 정보를 가져오는 순간을 제외하면 평균 8.7%의 CPU 사용률을 보이고 있다. 트래픽 폭주 탐지에서는 정상 트래픽과 공격 트래픽을 구분하여 탐지하기 어렵다. 따라서 공격 트래픽을 탐지하기 위해서는 폭주 트래픽의 패킷을 수집하여 분석하는 공격 트래픽 탐지프로그램을 사용하였다.

2. 공격 트래픽의 탐지 실험

공격 트래픽을 판단하기 위하여 공격에 사용되는 패킷의 특징을 이용한 분석이 필요하다. 실험을 위해 TFTP의 사용으로 인해 발생되는 트래픽 폭주와 UDP 플러딩 공격에 의해 발생되는 패킷을 수집하고 패킷의 특징을 분석하여 정상 트래픽과 공격 트래픽을 구분하였다. 그림 13과 14는 각각

TFTP 사용으로 인해 발생된 패킷과 UDP 플러딩 공격에 사용된 패킷을 분석하여 공격 트래픽을 탐지한 결과이다.

210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP
210.115.170.104:3248	210.115.170.110:69	UDP

그림 13. 정상 트래픽의 패킷 분석

127.70.18.48:360	210.115.170.110:9640	UDP
127.57.199.96:5708	210.115.170.110:4292	UDP
127.189.30.42:4539	210.115.170.110:5461	UDP
127.109.156.123:409	210.115.170.110:9591	UDP
127.136.243.54:427	210.115.170.110:9573	UDP
127.92.250.123:4688	210.115.170.110:5312	UDP
127.99.250.50:4845	210.115.170.110:5155	UDP
127.220.224.27:4558	210.115.170.110:5442	UDP
127.229.223.35:5063	210.115.170.110:4937	UDP
127.213.40.30:4691	210.115.170.110:5309	UDP
127.246.104.109:4803	210.115.170.110:5197	UDP
127.145.103.63:4846	210.115.170.110:5154	UDP
127.91.93.3:874	210.115.170.110:9126	UDP
127.209.93.75:5607	210.115.170.110:4393	UDP

그림 14. UDP 플러딩 공격의 패킷 분석

정상 트래픽은 근원지 IP 주소와 포트 번호, 목적지 IP 주소와 포트번호가 일정한 특징을 가지고 있다. 즉 대상 시스템에서 서비스를 제공하는 목적지 포트 번호로 트래픽이 발생한다는 것이다. TFTP의 사용으로 발생되는 트래픽 폭주 패킷을 수집하여 분석한 결과에서 알 수 있듯이 210.115.170.104 시스템에서 3248 포트를 이용하여 대상 시스템이 TFTP를 서비스 해주는 UDP의 69 포트로 트래픽이 폭주한 것을 알 수 있었다. 따라서 트래픽이 폭주되었지만 정상 트래픽으로 판단할 수 있었다. UDP 플러딩 공격에 사용된 패킷을 수집하여 분석한 결과에서 보면 127.70.18.48, ... , 127.209.93.75 등의 근원지 IP 주소와 360, ... , 5607 등의 근원지 포트 번호의 무작위성과 9640, ... , 4393 등의 대상 시스템에서 제공하지 않는 서비스 포트 번호를 무작위로 생성하여 공격 트래픽을 발생시킨 것을 알 수 있다. 이렇게 공격 트래픽의 특징을 이용한 분석으로 공격 트래픽을 정확히 탐지할 수 있었다. 폭주 트래픽의 패킷을 수집하고 수집된 패킷을 데이터베이스에 저장하여 패킷의 특성을 분석하기 위하여 사용된 CPU의 사용률은 평균 52.2%의 높은 사용률을 나타내고 있다. 그림 15는 공격 트래픽 탐지프로그램으로 공격 트래픽을 탐지하기 위한 CPU 사용률이다.

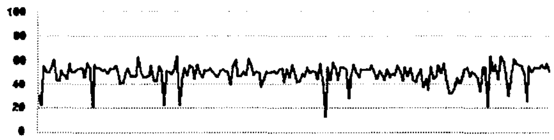

그림 15. 공격 트래픽 탐지프로그램의 CPU 사용률

실험을 통하여 탐지 방법별 DDoS 공격의 탐지 시간, 사용된 시스템 자원을 비교 분석하였다. 그림 16과 17은 각각 탐지 방법별 시간에 따른 탐지율과 CPU 사용률을 비교 분석한 그래프이다.

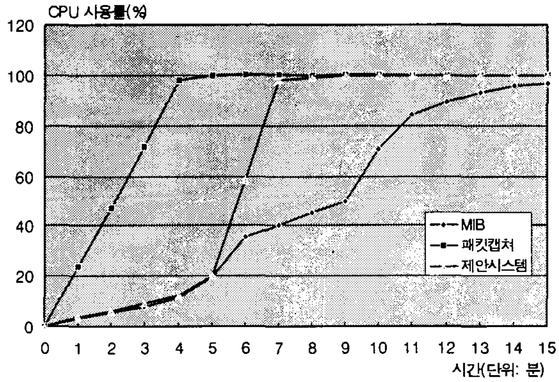

그림 16. 탐지 방법별 시간에 따른 탐지율 그래프

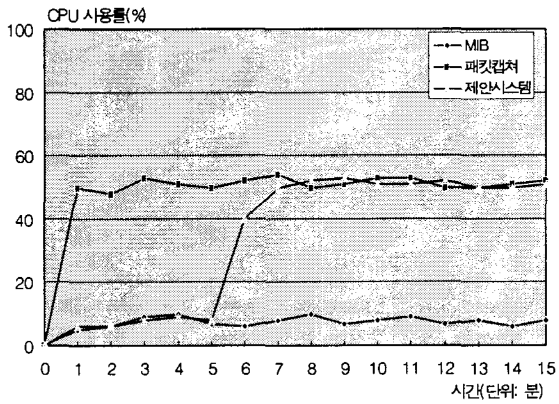

그림 17. 탐지 방법별 시간에 따른 CPU 사용률 그래프

MIB 정보를 이용한 탐지 방법의 탐지 시간은 평균 12분이 지난 후에 공격을 탐지할 수 있으나 공격 탐지를 위하여 평균 8.7%의 효율적인 CPU 사용률을 나타내고 있다. 하지만 공격 트래픽을 정확히 판단하지 못하는 문제가 발생하였다. 패킷 캡쳐 응용 프로그램을 이용한 탐지 방법은 패킷을 수집하고 공격 트래픽을 탐지하는데 걸리는 시간이 평균 3분 22초이며 정확한 공격 트래픽을 탐지할 수 있는 반면 평균 52.2%의 비효율적인 CPU 사용률로 정상 서비스를 제공하는데 있어 시스템 자원의 부족으로 인한 문제점이 발생하였다. 제안한 시스템의 탐지 시간은 평균 7분 24초로 MIB 정보를 이용한 탐지 방법에 비해 공격 트래픽을 탐지하기까지 많은 시간이 필요하나 정확한 공격 트래픽을 탐지할 수 있었으며, 평균 23.4%의 CPU 사용률로 패킷 캡쳐 응용 프로그램을 이용한 탐지 방법에 비해 효율적으로 DDoS 공격을 탐지할 수 있는 것을 확인하였다.

V. 결론

본 논문에서는 DDoS 공격을 탐지 시간과 시스템 자원의 사용률을 고려한 정확하고 효율적인 탐지를 위하여 MIB 정보를 이용한 트래픽 폭주의 탐지와 네트워크 패킷을 수집하고 분석하여 공격 트래픽을 탐지하기 위한 시스템을 제안하였다. MIB 정보를 이용한 공격의 탐지 방법은 효율적인 시스템 자원을 사용하는 이점이 있지만 탐지를 위한 많은 시간이 요구된다. 또한 정확한 공격을 탐지하기 어려운 문제가 발생하였다. 패킷 캡쳐 응용프로그램을 이용한 공격 탐지 방법은 짧은 시간에 공격을 정확히 탐지할 수 있으나 패킷 분석을 위한 패킷 수집 과정에서 시스템 자원을 많이 사용하기 때문에 정상적인 서비스를 제공하는데 있어 문제점이 발생하였다. 제안한 탐지 방법은 MIB 정보를 이용한 탐지 방법에 비해 많은 시스템 자원을 사용했지만 정확한 공격 트래픽의 탐지와 탐지 시간을 단축하였다. 또한 패킷 캡쳐 응용프로그램을 이용한 탐지 방법보다는 탐지하기까지의 시간은 길지만 효율적인 시스템 자원의 사용으로 공격 트래픽을 정확히 탐지한 것으로 분석되었다. 제안한 시스템을 침입 탐지 시스템이나 네트워크 관제 시스템에 적용한다면 효율적인 시스템 자원의 사용으로 인터넷 서비스의 질을 향상시킬 수 있으며 DDoS 공격을 정확하게 탐지하여 네트워크 및 시스템 자원을 보호할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 정현철, 변대용, 트래픽 분석을 통한 서비스거부공격 추적, 한국정보보호진흥원, 2003.

[2] D. Moore, G. M. Voelker, S. Savage, Inferring Internet Denial of Service Activity, Univ. of California, 2001.

[3] H. Wang, D. Zhang, K. G. Shin, Detecting SYN Flooding Attacks, Univ. of Michigan, 2002.

[4] T. M. Gil, M. Poetto, "MULTOPS: a Data-structure for Bandwidth Attack Detection," In Proceedings of the 10 USENIX Security Symposium, 2001

[5] P. Barford, J. kline, D. Plonka, A. Ron, A Signal Analysis of Network Traffic Anomalies, Univ. of Wisconsin, 2002.

[6] http://www.mrtg.org

김 미 혜(Mi-Hye Kim) 종신회원

1992년 2월 : 충북대학교 수학과 (이학사)

1994년 2월 : 충북대학교 수학과 (이학석사)

2001년 2월 : 충북대학교 수학과 (이학박사)

2001년 4월 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 초빙교수

<관심분야> : 퍼지이론, 정보이론, 금융수학

원 승 영(Seung-Young Won) 준회원

2002년 2월 : 충주대학교 컴퓨터공학과 (공학사)

2004년 2월 : 충북대학교 컴퓨터공학과 (공학석사)

2004년 2월 ~ 현재 : (주)네오네스

<관심분야> : 정보보호, 네트워크 보안, 컴퓨터 네트워크