향상된 통계기반 분산 서비스 거부(DDoS) 공격 탐지 시스템

송병학*, 홍충선**
경희대학교 컴퓨터공학과
e-mail : bhsong@networking.khu.ac.kr*, cshong@khu.ac.kr**

An Enhanced Statistical Detection Mechanism against DDoS attacks

Byung Hak Song*, Choong Seon Hong**
Dept. of Computer Engineering, Kyung Hee University

요 약

DDoS(Distributed Denial-of-Service) 공격은 인터넷 침해가운데 가장 위협적인 공격들 중 하나이며 이러한 공격을 실시간으로 탐지하기 위한 연구는 활발히 이루어져 왔다. 하지만 기존의 탐지 메커니즘이 가지고 있는 높은 오탐지율은 여전히 보완해야할 과제로 남아 있다. 따라서 본 논문에서는 DDoS 공격 탐지의 근거로 사용된 기존의 트래픽 볼륨(traffic volume), 엔트로피(entropy), 그리고 카이제곱(chi-square)을 이용한 비정상 행위탐지(Anomaly detection)방식의 침임탐지시스템이 가지는 오탐지율(false alarm rate)을 개선할 수 있는 방안을 제안한다. 또한 공격 탐지 시 프로토콜, TCP 플래그(flag), 그리고 포트 번호를 이용하여 네트워크 관리자에게 보다 자세한 공격 정보를 제공함으로써 효율적으로 공격에 대처할 수 있는 시스템을 설계한다.

1. 서론

초고속 인터넷 인프라가 구축되면서 해킹 및 인터넷 침해에 대한 사고 사례가 매년 증가하고 있다. 특히 DDoS 공격은 단순한 공격기법과 어디서나 구할 수 있는 툴로 인해 초급해커(Script kiddie)도 얼마든지 공격할 수 있다. 2000 년 2 월에 야후, 아마존과 같은 인터넷 포털 사이트가 심각한 피해를 입었으며, 전 세계 인터넷 트래픽을 관장하는 미국 내 13 개의 루트 서버가 DDoS 공격을 받아 그중 9 대가 일시적으로 정상 작동이 불가능 해지는 사례도 있었다[1]. 그리고 이러한 공격으로 인해 우리나라는 2003 년 1.25 인터넷대란을 겪기도 했다. 또한 최근 봇(Bot)[2]의 증가는 이러한 DDoS 공격과 같은 네트워크 자체에 위협을 주는 요소를 증가시키고 있다. 앞으로 유무선 통합 환경에서의 이러한 사고는 더욱 증가할 것으로 예상된다.

현재 IDS(Intrusion Detection System)이 가지고 있는 문제점들 중에 하나는 높은 오탐지율이다. 상용화된 IDS 의 알람(alarm) 평균 90%이상이 오탐지 또는 실패한 침입 시도에 해당할 정도로 오탐지율은 심각하다[3]. 그리고 이러한 문제로 인해 특정 IDS 알람이 오탐임을 판단하기까지 인력과 시간이 낭비될 뿐만 아니라 IDS 알람에 무감해져 실제 공격 발생 시 능동적인 대응력이 낮아지게 된다.

따라서 본 논문에서는 이러한 문제를 해결하기 위해 기존의 탐지 메커니즘의 정확성을 향상시킬 수 있는 방안을 제안한다. 또한 공격 탐지 시 프로토콜, TCP 플래그, 그리고 포트번호를 이용하여 네트워크 관리자에게 보다 자세한 공격 정보를 제공함으로써 효율적으로 공격에 대처할 수 있는 시스템을 설계한다.

본 논문의 구성은 다음과 같다. 2 장에서는 대표적인 DDoS 공격 유형과 기존의 세 가지 비정상 행위 탐지 알고리즘에 대해서 알아보고 3 장에서는 기존의 탐지 메커니즘의 오탐지율을 향상시킬 수 있는 방안을 제안한다. 마지막으로 4 장에서는 본 연구가 가지는 의의와 향후 연구 계획으로 마무리한다.

2. 관련연구

2.1 서비스 거부 공격 유형

This work was supported by MIC and ITRC project.

서비스 거부 공격의 유형에는 대표적으로 SYN 플러딩(SYN Flooding) [4][5], UDP 플러딩(UDP Flooding) [4][5], 그리고 ICMP 플러딩(ICMP flooding) [4][5]이 있다. 이러한 서비스 거부 공격들은 DDoS 공격의 근간이 되어 하나의 마스터(master)가 다수의 슬레이브(slave)를 이용해 희생자(victim)를 공격하게 된다.

먼저 SYN 플러딩은 서버에 접속을 요청하는 패킷을 보낸 후 정보를 보내지 않아 서버가 열린 상태로 기다리고 있는 경우 연결 설정이 초기화되기 전에 위조된 패킷을 플러딩하여 포트의 대기 규에 더 이상 저장할 수 없는 상태로 만드는 공격이다.

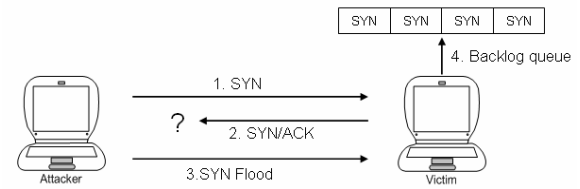

그림 1. SYN 플러딩에 의한 서비스 거부 공격

두 번째로 UDP 플러딩은 UDP 의 비연결성 및 비신뢰성 때문에 공격이 용이한 방법이다. UDP 는 소스 주소와 소스 포트를 스푸핑(spoofing)하기 쉽다. 이러한 약점들을 이용해 그림 2 와 같이 과다한 트래픽을 희생자에게 전송함으로써 희생자간(Victim A, Victim B) 네트워크를 마비시킨다.

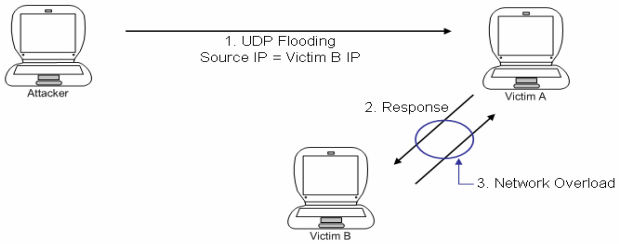

그림 2. UDP 플러딩에 의한 서비스 거부 공격

ICMP 는 호스트간 혹은 호스트와 라우터간의 에러 상태 혹은 상태 변화를 알려주고 요청에 응답을 하는 기능을 담당하는 네트워크 제어 프로토콜이다. 이러한 ICMP 는 활성화된 서비스나 포트가 필요하지 않다. 이러한 ICMP 의 특징을 악용한 ICMP 플러딩은 대량의 ICMP 패킷을 공격자가 직접 희생자에게 전송하는 방법으로 그 변종의 예로 Smurf, Welchia worm 등이 있다.

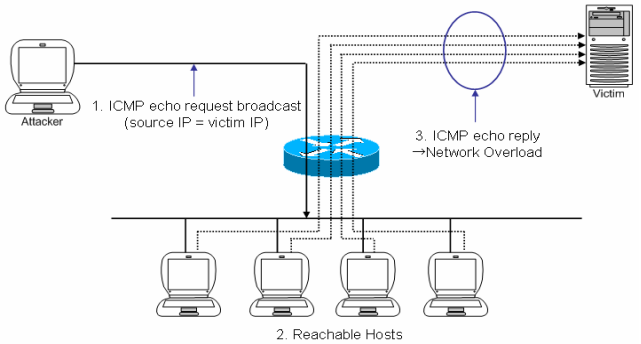

그림 3. ICMP 에 의한 서비스 거부 공격

2.2 통계적 탐지 알고리즘

DDoS 공격은 일반적인 패킷으로 공격이 이루어지므로 합법적인 패킷과 구분하기 어렵고, 각각의 공격 소스에서 보내는 패킷의 양이 적기 때문에 로컬 네트워크 관리자가 쉽게 탐지할 수 없다. 따라서 이를 탐지하기 위해서는 통계적인 방법을 사용하는 것이 가장 효율적이다.

통계적인 탐지 알고리즘에는 트래픽 볼륨(traffic volume), 패킷 속성값의 엔트로피(entropy) [6], 카이 제곱 (Chi-Square) 검증법[6]등이 사용되고 있다.

이 가운데 트래픽 볼륨 측정은 패킷이 이더넷 카드에 도착하는 시간을 계산하는 것이다.

$$T = \sum_{i=1}^{n} (PAT[i-1] - PAT[i])$$

위 공식은 각각의 패킷이 도착하는 시간을 측정하여 그룹단위로 패킷이 도착한 시간을 계산한다. 즉 100 개의 패킷을 한 그룹으로 설정을 했다면 100 개의 패킷이 이더넷 카드에 도착하는 시간을 측정하는 것이다. 트래픽 볼륨 값이 낮을 수록 이더넷 카드에 도착하는 패킷의 수가 증가했다는 것을 의미한다. 이것은 현재의 트래픽이 갑자기 증가했다는 것으로 이상 트래픽 발생 가능성을 암시한다.

다음 엔트로피 연산법은 어떠한 네트워크 속성값에 대한 임의성(randomness)을 계산한 뒤, 그 값의 평균의 변화량을 탐지하는 방법이다.

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

위의 공식은 n 개의 속성 값에 대한 엔트로피 H 를 구하는 공식이다. 여기서 p_i 는 i 번째의 속성값이 선택될 확률을 나타낸다.

카이 제곱 검증법은 속성값에 대한 분산도를 측정하는 방법이다. 여기서는 기대값에 대한 분산도를 계산하여 그 값에 따라 비정상적인 속성값을 탐지할 수 있다. 이 방법의 구체적인 식은 다음과 같다.

$$x_2 = \sum_{i=1}^{B} \frac{(N_i - n_i)^2}{n_i} \quad , n_i = \frac{n}{B} \quad , n = total\ sample\ size$$

여기서 B 는 샘플 패킷들이 가질 수 있는 값들을 묶어놓은 binning 값이다.(ex. 패킷길이는 0-64, 65-128, 129-255 로 binning 될 수 있다) N_i 는 N 개의 샘플 패킷에서 각각의 binning 범위에 속하는 패킷의 개수이고, n_i 는 일반적인 분포에서 binning 에 속하는 기대값이다.

DDoS 공격을 실시간으로 탐지하기 위해서 앞에서 언급한 세 가지 통계적 이론을 바탕으로 설계하였으며 트래픽 볼륨은 임계값보다 작고 소스 주소에 대한 엔트로피, 그리고 케이제곱은 임계값이상을 될 때 DDoS 공격으로 판단한다[7].

3. 제안사항

기존의 세 가지 통계적 이론인 트래픽 볼륨, 소스 주소에 대한 엔트로피, 카이 제곱을 이용한 탐지 알

고리즘이 가지는 오탐지율을 향상시키고 관리자에게 탐지된 공격의 보다 자세한 특징 정보까지 제공할 수 있는 시스템을 구성하고자 한다.

3.1 향상된 통계기반 탐지 메커니즘

학교 망 내에 기존의 세 가지 통계적 이론을 근거로 설계한 IDS 를 시험 운용한 결과 HTTP 와 같은 정상적인 트래픽의 갑작스런 증가에도 알람을 알리는 오동작을 쉽게 경험할 수 있었다.

DDoS 공격 트래픽은 다양하게 분산된 소스 주소를 가지며 소수의 타겟(target) 주소로 집중화되는 특성을 갖는다. 그래서 이러한 트래픽의 성향을 이용하여 그림과 같이 소스 주소에 대한 엔트로피뿐만 아니라 목적지 주소에 대한 엔트로피도 같이 DDoS 공격 탐지의 근거로 사용하고자 한다.

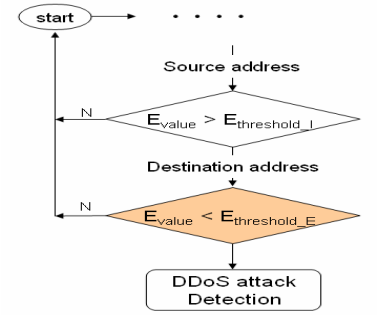

그림 4. 소스 주소와 목적지 주소에 대한 엔트로피

다음은 목적지 주소에 대한 엔트로피 알고리즘을 이용하여 일정그룹의 패킷의 분산된 정도를 계산하는 과정을 나타난 의사코드(pseudocode)이다.

```
FOR constant number of packets DO
    FOR constant number of packets DO
        j = i+1
        IF captured_IP_i(dst_address) EQUAL captured_IP_j(dst_address) THEN
            INCREMENT specific_IP_count_j(dst_address) by 1
        ENDIF
prob_specific_IP_j = specific_IP_count_j(dst_address) / total_packet_num_j
FOR number of IP addresses in constant number of packets DO
    entropy_temp = entropy_temp + prob_specific_IP_j log2 prob_specific_IP_j
```

따라서 기존의 트래픽 볼륨, 소스 주소에 대한 엔트로피, 카이제곱과 목적지 주소에 대한 엔트로피를 같이 사용하면 기존의 IDS 의 오탐지율을 개선할 수 있을 것이라 기대된다.

그림 5 는 비정상 탐지 메커니즘의 전체 흐름도를 나타내고 있다. 기존의 세 가지 통계기반 알고리즘과 목적지 주소에 대한 엔트로피 알고리즘을 통해 탐지된 DDoS 공격은 프로토콜, 포트번호, 그리고 TCP 플래그값 별로 트래픽양이 아닌 비율을 기반으로 탐지된 패킷들을 분석한다. 그래서 DDoS 공격이 발생했을 때 네트워크 관리자에게 DDoS 공격의 유형(TCP SYN 플러딩, UDP 플러딩, 그리고 ICMP 플러딩)뿐만 아니라 해당 공격 트래픽이 어떤 포트로 침입해 왔는지에 대한 통계 정보를 제공한다.

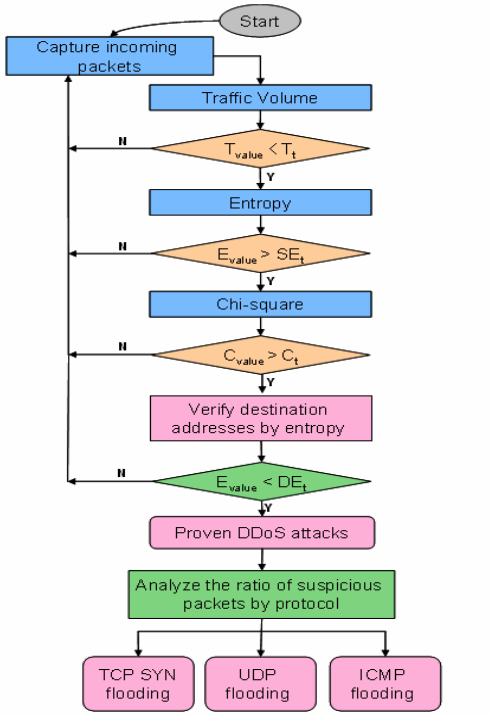

그림 5. DDoS 탐지 메커니즘의 전체 흐름도

아래의 의사코드는 공격이라고 판단되어진 패킷들로부터 공격의 특징 정보를 얻어오는 과정을 나타낸다. Counter 함수의 field 파라미터는 프로토콜 타입, 포트 번호, 그리고 TCP 플래그값이 올 수 있다.

```
Counter(field):
FOR constant number of packets DO
    FOR constant number of packets DO
        j = i+1
        IF suspicious_IP_i(field) EQUAL suspicious_IP_j(field) THEN
            INCREMENT suspicious_IP_count_j(field) by 1
        ENDIF
CALL sort(suspicious_IP_count_j(field))
```

3.2 탐지 임계값(threshold) 계산

그림 6 은 학교 망에 구축한 모의 DDoS 공격 테스트 환경에서 Stacheldraht[8]로 공격 테스트 시 기존의 통계기반 IDS 의 동작을 나타낸 그래프이다. 트래픽의 급격한 증가로 트래픽 볼륨 값은 0 에 가까워지고 엔트로피 값은 증가하며 카이제곱 값은 공격의 시작 시 일시적인 피크를 이루는 모습을 볼 수 있다. 하지만 기존의 탐지 메커니즘은 경험에 의존해 임계값을 산출하기 때문에 공격의 시작시점을 명확하게 파악하기는 쉽지 않다.

그림 7 은 시간을 기준으로 측정된 패킷의 수를 나타낸 그래프이다. 슬라이딩 윈도우 A 는 목적지 주소 엔트로피를 포함한 네 가지 통계적 탐지 알고리즘이 계산하는 패킷의 범위를, 슬라이딩 윈도우 B 는 임계값 계산에 사용되는 패킷을 범위를 나타낸다. 실험 환경에서는 슬라이딩 윈도우 A 를 1000 패킷으로 슬라이딩 윈도우 B 를 5000 패킷으로 설정하여 테스트하였다.

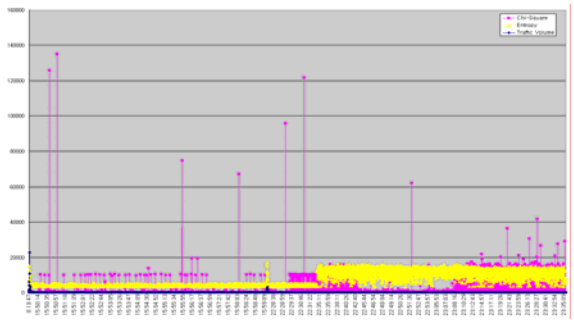

그림 6. DDoS 공격 테스트 시 통계기반 IDS 의 결과

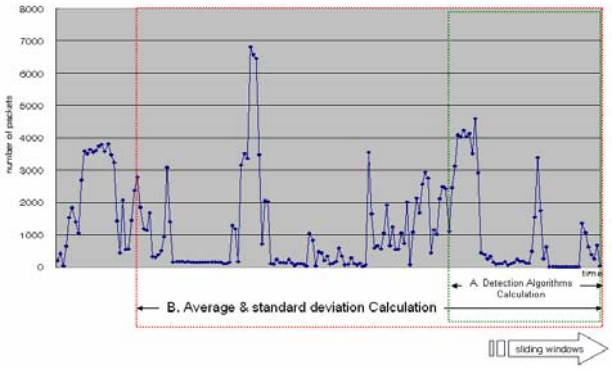

그림 7. 슬라이딩 윈도우를 이용한 임계값 계산

네 가지 탐지 알고리즘의 임계값은 다음의 식을 이용하여 계산한다.

- 트래픽 볼륨

$$T_t = \mu_T - k\sigma_T \quad ,(k = 1,2,3\cdots)$$

μ_T : *average of traffic volume*

σ_T : *standard deviation of traffic volume*

- 소스 주소 엔트로피

$$SE_t = \mu_I + k\sigma_I \quad ,(k = 1,2,3\cdots)$$

μ_I : *average of source address entropy*

σ_I : *standard deviation of source address entropy*

- 카이제곱

$$C_t = \mu_C + k\sigma_C \quad ,(k = 1,2,3\cdots)$$

μ_C : *average of chi – square*

σ_C : *standard deviation of chi – square*

- 목적지 주소 엔트로피

$$DE_t = \mu_E - k\sigma_E \quad ,(k = 1,2,3\cdots)$$

μ_E : *average of destination address entropy*

σ_E : *standard deviation of destination address entropy*

일정한 크기의 패킷 그룹에서 측정된 각각의 통계값이 μ 에 가까운 값일수록 정상적인 패킷을 의미하고 멀어질수록 비정상적인 패킷을 의미한다. k 값이 3 일 때 99.7%의 신뢰성을 가지게 되며 각각의 탐지된 값이 소스 주소 엔트로피, 그리고 카이제곱의 임계값 (T_t, SE_t, C_t)보다 클 때, 그리고 트래픽 볼륨과 목적지 주소 엔트로피의 임계값(DE_t)보다 작을 때 공격으로 판단하게 된다. 그림 5 의 탐지 과정은 이러한 네 개의 임계값 계산과정을 포함하고 있다.

4. 결론

본 논문에서는 기존의 DDoS 탐지 메커니즘이 가지고 있는 문제점을 언급하고, 이에 관한 해결방안을 제시하였다. 트래픽 볼륨, 소스 주소에 대한 엔트로피, 카이제곱, 그리고 목적지 주소에 대한 엔트로피를 같이 사용함으로써 기존 IDS 의 오탐지율을 개선할 수 있다. 또한 신뢰성 있는 임계값 계산을 바탕으로 공격 탐지의 정확성을 향상시킬 수 있을 것으로 기대된다. 마지막으로 공격 탐지 시 의심스러운 패킷을 분석하여 관리자에게 공격에 대응할 수 있는 유용한 정보를 제공할 수 있다.

향후 연구 과제로는 본 논문에서 제안한 탐지 메커니즘을 테스트베드로 구축하여 구현하고 실제적인 성능에 대한 검증을 하는 것이다. 그리고 더 나아가 지능적인 형태로 발전된 DDoS 공격에 대한 탐지 메커니즘에 대한 연구가 필요하다.

참고문헌

[1] R. Power, “2000 CSI/FBI Computer Crime and Security Survey”, Computer Security, vol. 16, no 2, 2000, pp33-49

[2] Bill McCarty, “Botnets: Big and Bigger”, Security & Privacy Magazine, IEEE, Vol. 1 Issue 4, pp.87-90, July-Aug. 2003

[3] Stephen Northcutt, Judy Novak, “Network Intrusion Detection : An Analyst’s Handbook(2nd Edition)”, New Riders Publishing, September 2000

[4] 한국정보보호진흥원, “IPv6 보안 기술 해설서”, Oct. 2005

[5] 이종엽, 윤미선, 이훈, “DoS 공격의 유형 분석 및 탐지 방법”, KNOM Review, Vol. 6, No. 2, pp.21-32, Feb. 2004

[6] Feinstein L., Schnackenberg D, Balupari R., Kindred D., "Statistical Approaches to DDoS Attack Detection and Response", DARPA Information Survivability Conference and Exposition(DISCEX 2003), April 22-24, 2003

[7] Yoohwan Kim, Wing Cheong Lau, "PacketScore : Statistical-based Overload Control against Distributed Denial-of-Service Attack", IEEE INFOCOM, Vol. 4, 2594-2604, March 2004

[8] The "stacheldraht" distributed denial of service attack tool, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis