2005 한국경영과학회/대한산업공학회 춘계공동학술대회
2005 5 월 13 일~14 일, 충북대학교

다중 엔트로피를 이용한 네트워크 공격 탐지 기법
Network Attack Detection Scheme with Multiple Entropy

권기훈*, 김민택**, 김세헌*
*한국과학기술원 산업공학과, (kihoon, shkim)@kaist.ac.kr
**LG CNS Entrue Consulting, mintkim@lgcns.com

Abstract

인터넷의 사용이 증가하면서, DDoS와 같은 네트워크 공격 역시 빠르게 증가하고 있다. 최근 발생하는 네트워크 상의 공격은 특정 호스트에 대한 피해뿐만 아니라, 전체 네트워크의 성능 저하를 유발한다. 이러한 피해를 막기 위해서 효율적인 탐지 기법이 필요하다. 본 논문에서는, 다중 엔트로피를 이용하여 고속의 네트워크 상황에 적합한 탐지 기법을 제시하였다. 제시한 기법은 공격의 발생에 따른 출발지 주소, 목적지 주소, 목적지 포트의 엔트로피를 관찰하여 공격을 탐지한다. 공격이 발생하였을 경우, 각각의 엔트로피는 정상 상태와 다른 값을 가진다. 또한 공격의 특성에 따라 엔트로피 값들은 서로 다르게 변한다. 이를 이용하여 공격의 종류를 파악할 수 있다.

Ⅰ. 서론

인터넷의 사용이 급증함에 따라 국가 경제와 산업에 막대한 가치가 새롭게 창출되었으며, 기존 경제활동 또한 활력과 효율성이 제고되었다. 그러나 정보화가 급속히 진행됨에 따라 해킹, 바이러스, 웜 등의 사이버 공격이 급속히 증가하고 있으며, 그 피해의 정도 역시 커지고 있다[1].

본 연구는 대학 IT연구센터 육성지원사업의 결과로 수행되었음

2003년 1월 25일에 발생한 인터넷 대란의 경우 국가 전체의 인터넷이 마비되는 피해를 입혔다. 이때 전파된 MS-SQL Slammer 웜은 웜 발생 후 10분만에 전세계 취약 호스트의 90% 이상을 감염시킨 것으로 나타났다[2,3]. Code Red 웜은 14시간 이내에 359000 호스트 이상을 감염시켰다[4]. 이러한 최근의 인터넷 상의 공격들은 매우 빠르게 전파되고 있으며, 막대한 경제적 손실도 유발하였다.

과거의 인터넷 상의 공격은 특정 호스트를 대상으로 하는 해킹, 컴퓨터 바이러스, 트로이 목마 등이 주를 이루었으나, 최근에는 인터넷 웜, Bot과 같이 특정 호스트에 대한 피해뿐만 아니라 네트워크를 통해 급속히 전파되어 네트워크 시스템 전체에 피해를 입히는 공격이 주를 이루고 있다.

인터넷 상의 공격을 효과적으로 탐지하기 위해서 침입탐지 시스템에 대한 연구가 널리 수행되었다. 침입탐지 시스템은 정보시스템 또는 네트워크로부터 보안 관련 정보를 수집, 분석하여 침입 또는 오용을 탐지할 뿐 아니라 침입에 대한 적절한 대응기능을 포함하는 시스템이다[5]. 이와 관련하여, 웹 서비스 관리의 측면에서 웹 서버의 초당 http 명령 횟수에 대한 분석이 수행되었다. 이 연구에서는 분산분석을 통하여, 월별요인, 요일요인, 시간요인을 파악하여 자료를 정류화한 후, 자기회귀모형에 적용하였다[6]. Kalman Filter를 사용하면 분산분석에 필요한 방대한 훈련데이터를 줄일 수 있다. 또한 우도비(Likelihood Ratio)를 활용하여 장기간에 걸쳐 발생하는 네트워크 상황의 변화를 탐지할 수 있다[7]. 통계적 품질관리 기법의 하나인 지수가중이동평균(EWMA: Exponentially Weighted Moving Average) 기법을 MIT-LL 데이터에 적용한 연구도 수행되었다[8].

그러나 기존의 연구는 특정 호스트나 네트워크를

대상으로 침입을 탐지하기 때문에 네트워크 전반을 통해 급속히 전파되는 공격을 효율적으로 탐지하기 어렵다. 또한 네트워크의 전송 속도가 증가하고 어플리케이션이 요구하는 대역폭이 커짐에 따라 네트워크 상의 정보를 효율적으로 수집하고 신속히 네트워크 상의 공격 발생을 탐지하는 기법이 필요하다[9].

본 연구에서는 특정 시간 동안 얻어진 패킷의 정보를 바탕으로 엔트로피를 계산하여 이를 공격 탐지에 활용한다. 제안하는 방법은 인터넷 공격의 유형에 따른 근원지 주소, 목적지 주소, 목적지 포트의 엔트로피 변화를 관찰하여 공격을 탐지한다. 위의 정보는 패킷의 헤더만을 관찰하여 얻을 수 있으므로 고속 네트워크 상황에서 적용하기 용이하다.

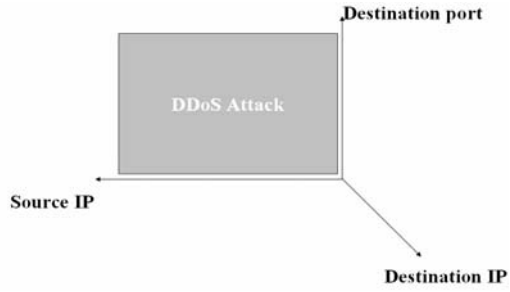
Ⅱ. 네트워크 공격 유형

1. 분산 서비스 거부 공격

서비스 거부(DoS: Denial-of-Service) 공격은 피해 호스트가 인터넷에 정상적인 서비스를 제공하거나 서비스를 받는 것을 방해하는 공격이다. DoS 공격의 방법으로 시스템의 취약성을 공격하는 방법이 있다. 다른 방법으로 복잡한 계산을 요구하여 시스템의 처리 능력을 저하시킨다[10].

분산 서비스 거부(DDoS: Distributed DoS) 공격은 새로운 형태의 DoS 공격이다. 일반적인 DoS 공격과 달리 DDoS 공격은 특정 네트워크 프로토콜이나 시스템의 취약성을 이용하지 않는다. DDoS 공격은 다수의 감염된 호스트가 피해 호스트에게 다량의 무의미한 패킷을 전송하여, 피해 호스트와 인터넷 사이의 자원 불균형을 초래한다. 감염된 호스트로부터 전송되는 막대한 트래픽은 피해 호스트의 연결을 방해한다.

DDoS 공격이 발생했을 경우, 네트워크에서 전달되는 패킷을 살펴보면 다음과 같은 특성을 가진다. 근원지 주소의 경우 매우 폭넓게 분포하게 된다. 그러나 많은 양의 패킷이 특정한 피해 호스트를 향하게 되어, 목적지 주소의 분포는 집중된다. 목적지 포트는 DDoS 공격 도구가 사용하는 방법에 따라 차이를 가지게 된다. 이러한 DDoS 공격의 특징을 3차원으로 나타내면 [그림 1]과 같다.



[그림 1] DDoS 공격

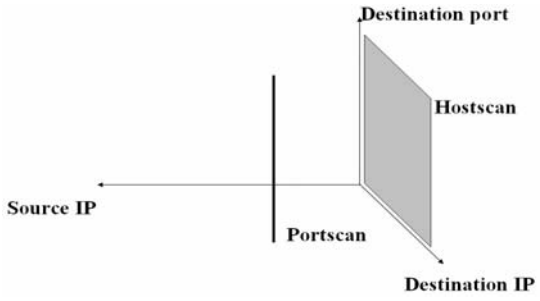
2. Hostscan과 Portscan 공격

Hostscan과 Portscan은 몇몇 네트워크 공격의 준비과정으로 사용된다. 공격을 시행하기 앞서 공격자는 취약성을 가진 서비스를 제공하는 공격 대상 호스트에 대한 정보를 가질 필요가 있다.

Hostscan은 작동 중인 호스트를 찾는 과정이다. 공격자는 hostscan을 이용하여 어떤 호스트가 네트워크 공격에 취약한지 확인한다. 이 경과에 따라 공격자는 공격의 목표를 결정한다.

공격 목표가 결정되면 공격자는 목표 호스트의 열려있는 port를 찾기 위해서 Portscan을 수행한다. 공격자는 선택된 호스트의 port들을 검사하여 어떤 port가 공격에 대해 열려있는지 알 수 있다. 이후 공격자는 선택된 호스트의 열려있는 port를 이용하여 네트워크 공격을 수행한다.

위에서 살펴본 hostscan과 portscan의 특성은 다음과 같다. Hostscan은 특정한 근원지 주소로부터 다양한 목적지 주소로 패킷이 전송된다. 또는 portscan과 동시에 수행되어 일정 근원지에서 다양한 목적지 주소, 목적지 포트로 패킷이 전송된다. Portscan의 경우, 특정한 근원지에서 특정한 목적지를 향하여 다양한 목적지 port로 패킷이 전송된다. 이를 그림으로 나타내면 [그림 2]와 같다.



[그림 2] hostscan, portscan 공격

Ⅲ. 제안하는 탐지 기법

각각의 선택 확률이 P_i 인 n개의 독립적인 심볼이 있을 경우 엔트로피는 다음과 같이 정의된다[11].

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

그러므로 엔트로피는 연속적으로 수집된 패킷으로부터 계산될 수 있다. 특정 시점에 계산된 엔트로피 값을 다른 시점의 엔트로피 값과 비교하여 무작위성(randomness)의 변화를 탐지할 수 있다[12]. 즉 공격이 발생하지 않은 정상 상태와 공격이 발생한 이상 상태의 차이를 탐지할 수 있다.

엔트로피는 특정 샘플의 빈도를 나타낸다. 엔트로피가 낮은 값을 가지면, 소수의 샘플이 자주 발생하게 된다. 엔트로피가 높은 값을 가지면 다양한 샘플들이 낮은 빈도로 발생한다.

앞서 살펴본 공격의 특성을 엔트로피의 변화로 표현할 수 있다. DDoS 공격이 발생하면, 근원지 주소의 엔트로피는 증가하지만, 목적지 주소의 엔트로피는 감소하게 된다. Hostscan의 경우, 근원지 주소의 엔트로피는 감소하지만 목적지 주소의 엔트로피는 증가하게 된다. Portscan이 발생하면 근원지 주소와 목적지 주소의 엔트로피가 감소하고, 목적지 port의 엔트로피가 증가한다. 이를 표로 나타내면 표1과 같다.

[표 1] 공격의 유형에 따른 엔트로피 변화

	근원지	목적지	목적지
	주소	주소	포트
DDoS	↑	↓	↑↓
Hostscan	↓	↑	↑↓
Portscan	↓	↓	↑

네트워크 공격의 유형이 따라 엔트로피가 변화하기 때문에, 네트워크 공격의 종류를 알아내기 위해서 각각의 엔트로피를 독립적으로 관찰하는 것보다 근원지 주소, 목적지 주소, 목적지 포트의 엔트로피 값들을 서로 비교하는 것이 바람직하다. 예를 들어, 근원지 주소의 엔트로피가 급격히 증가하고, 목적지 주소의 엔트로피가 갑자기 감소하면, DDoS 공격이 발생했다고 판단할 수 있다. 그러므로 우리는 간단한 연산을 통하여 이들 엔트로피 상호간의 변화를 파악하는 척도를 제시한다. 제시한 연산은 [표 2]와 같다.

[표 2] 제안하는 공격탐지 척도

DDoS	근원지 주소의 엔트로피 - 목적지 주소의 엔트로피
Hostscan	근원지 주소의 엔트로피 - 목적지 주소의 엔트로피
Portscan	목적지 포트의 엔트로피 - 근원지 주소의 엔트로피 - 목적지 주소의 엔트로피

Ⅳ. 성능 평가

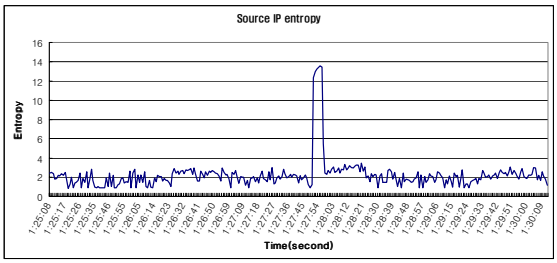
제안하는 기법의 성능을 평가하기 위해서, 우리는 2000 DARPA Intrusion Detection Scenario Specific Data Sets를 사용하였다. DARPA 2000 Data sets는 DDoS 공격과 hostscan 공격이 포함되어 있다.

DDoS 공격은 5단계로 수행되었다. 1단계에서는 어떤 호스트가 작동 중인지 탐색한다. 2단계에서는 취약점을 가진 서비스를 제공하고 있는 호스트를 탐색한다. 3단계에서는 앞서 발견된 호스트에서 취약점을 이용하여 권한을 획득한다. 4단계는 획득된 권한으로 DDoS 프로그램을 설치한다. 5단계에서는 감염된 호스트에게 명령을 내려 DDoS 공격을 수행한다.

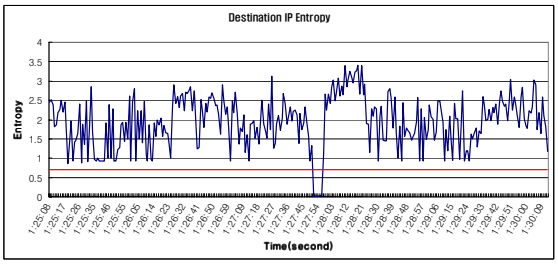
Hostscan 공격은 IPsweep이라는 프로그램

을 활용하여 수행되었다.

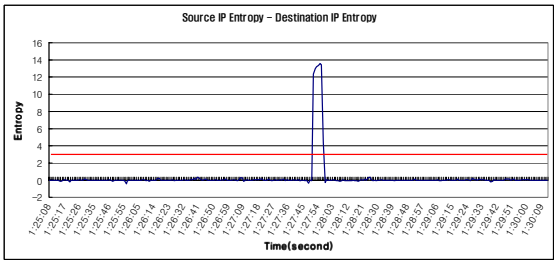
실험에서 상용된 DDoS 공격에 관한 Data Set은 23:21:36에서 02:35:48 사이에 수집되었다. 실제 DDoS 공격은 1:27:51에서 1:27:56 사이의 6초간 발생하였다. [그림 3,4,5]는 각각의 엔트로피의 변화를 보여준다.



[그림 3] 근원지 주소의 엔트로피 (DDoS)



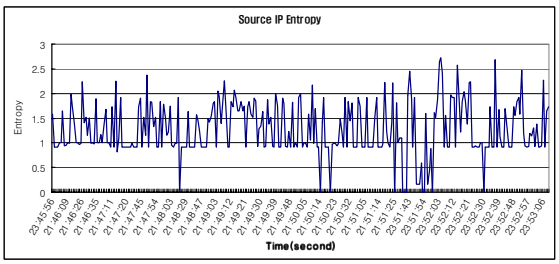
[그림 4] 목적지 주소의 엔트로피 (DDoS)



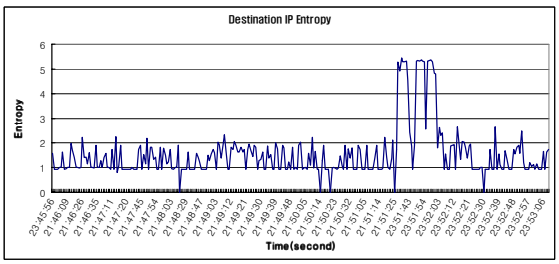
[그림 5] 근원지 주소의 엔트로피 - 목적지 주소의 엔트로피 (DDoS)

DDoS 공격이 발생하면 근원지 주소의 엔트로피가 급격히 증가하고, 목적지 주소의 엔트로피가 급격히 감소하여, 제시한 척도를 활용하여 공격의 발생을 쉽게 탐지할 수 있다.

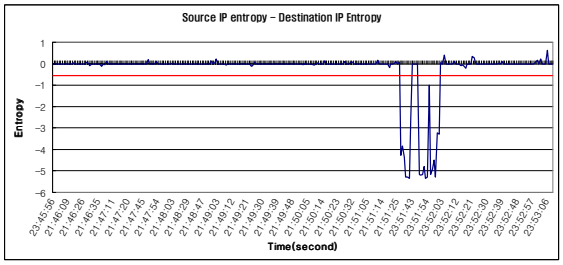
Hostscan 공격은 23:20:45에서 02:36:44 사이의 시간 동안 데이터가 수집되었다. 실제 hostscan은 23:51:36에서 23:51:42, 23:51:49에서 23:51:01 동안 수행되었다. [그림 6,7,8]은 hostscan이 발생하는 동안의 엔트로피 변화를 보여준다.



[그림 6] 근원지 주소의 엔트로피 (hostscan)



[그림 7] 목적지 주소의 엔트로피 (hostscan)



[그림 8] 근원지 주소의 엔트로피 - 목적지 주소의 엔트로피 (hostscan)

위의 그림에서 Hostcan이 발생한 경우, 각각의 엔트로피를 독립적으로 고려하는 것 보다 정확히 공격을 탐지할 수 있음을 알 수 있다.

Ⅴ. 결론

본 논문에서는 고속 네트워크 상의 네트워크 공격에 대해서 실시간으로 적용가능한 통계적 탐지 방법을 제시하였다. 네트워크 공격의 특성을 바탕으로 근원지 주소, 목적지 주소, 목적지 포트의 엔트로피를 기반으로 하는 탐지 기법을 제안하였다. 네트워크에 공격이 발생하면, 각각의 엔트로피는 정상 상태에서

급격히 변화하게 된다. 이를 더욱 명확하게 발견하기 위하여, 간단한 공격 탐지 척도를 제안하였다. 이를 통하여 각각의 공격의 발생과 공격의 유형 역시 파악할 수 있다.

2000 DARPA data sets를 통한 실험에서 공격의 발생에 따른 엔트로피 값의 급격한 변화를 관찰할 수 있었다. 우리가 제안한 기법은 각각의 엔트로피를 독립적으로 관리하는 것보다 더욱 명확히 공격의 발생을 탐지할 수 있다. 즉 공격 탐지에서의 오탐율을 감소시킬 수 있다.

참고문헌

[1] 권기훈, 한영구, 정석봉, 김세헌, 이수형, 나중찬,
[2] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "The Spread of the Sapphire/Slammer worm", http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html
[3] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, "Inside the Slammer worm", IEEE Security & Privacy Magazine, v.1 , i.4, pp. 33-39, July-Aug. 2003
[4] Hood, C., and Ji, c., “Proactive network fault detection ”, Proceeding of IEEE INFOCOM ’97,Kobe, Japan, April 1997,1147-1155
[5] Dorothy E. Denning, "An intrusion detection model", IEEE Transactions on Software Engineering, v.13 n.2, pp. 222-232, Feb. 1987
[6] J. L. Hellerstein, F. Zhang, P. Shahabuddin, "A statistical approach to predictive detection", Computer Networks, vol 35, pp.77-95, 2001
[7] F. Zhang, J. L. Hellerstein, "An Approach to On-line Predictive Detection", In Proceedings of 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, Aug. 29 -Sep. 2000
[8] N. Ye, S. Vilbert and Q. Chen, "Computer Intrusion Detection Through EWMA for Autocorrelated and Uncorrelated Data", IEEE Transactions on Reliability, v.52, n.1, March 2003
[9] X. Gang, Z. Hui, "Advanced methods for detecting unusual behaviors on networks in real-time", In Proceedings of International Conference on Communication Technology Proceedings, v.1, pp.291-295, Aug. 2000
[10] Rocky K. C. Chang, “ Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial ”, IEEE Communications Magazine, Oct 2002
[11] C.E. Shannon, and W. Weaver, The Mathematical Theory of Communication, University of Illinois Press, 1963
[12] Laura Feinstein and Ravindra Balupari, “Statistical Approaches to DDoS attack Detection and Response ”, Proceeding of the DARPA Information Survivability Conference and Exposition