情報保護學會論文誌
第16卷 第1號, 2006. 2

다중 엔트로피를 이용한 네트워크 공격 탐지*

김 민 택,[1†] 최 영 우,[2‡] 권 기 훈,[2] 김 세 헌[2]
[1]LG CNS Entrue Consulting, [2]한국과학기술원

Network Attack Detection based on Multiple Entropies*

Min-Taek Kim,[1†] Young-Woo Choi,[2‡] Ki Hoon Kwon,[2] Sehun Kim[2]
[1]LG CNS Entrue Consulting, [2]KAIST

요 약

인터넷의 사용이 증가하면서, DDoS (분산 서비스 공격)를 비롯한 여러 가지 네트워크 공격들이 오늘날 인터넷의 안정성에 커다란 위협을 가하고 있다. 인터넷과 같은 대규모 망을 대상으로 한 이러한 네트워크 공격들은 특정 호스트에 대한 피해뿐만 아니라, 전체 네트워크의 성능 저하를 유발한다. 이러한 피해를 막기 위해서 대규모 기간망에서 적용 가능한 효율적이고 간단한 공격 탐지 기법이 필요하다. 이를 위해 빈도의 분포에 대한 간단한 통계치인 엔트로피를 이용하고자 한다. 네트워크 공격에 따라서 특정 근원지 주소, 특정 목적지 주소 그리고 특정 목적지 포트의 비정상적인 빈도가 관찰되기 때문에 위 세가지 항목에 대한 엔트로피의 변화를 이용하여 네트워크 공격을 탐지한다. 세 가지 엔트로피의 변화하는 형태를 분석하여 네트워크 공격의 종류 또한 파악할 수 있다.

ABSTRACT

Several network attacks, such as distributed denial of service (DDoS) attack, present a very serious threat to the stability of the internet. The threat posed by network attacks on large networks, such as the internet, demands effective detection method. Therefore, a simple intrusion detection system on large-scale backbone network is needed for the sake of real-time detection, preemption and detection efficiency. In this paper, in order to discriminate attack traffic from legitimate traffic on backbone links, we suggest a relatively simple statistical measure, entropy, which can track value frequency. There is conspicuous distinction of entropy values between attack traffic and legitimate traffic. Therefore, we can identify what kind of attack it is as well as detecting the attack traffic using entropy value.

Keywords : *DDoS, Entropy, Network attack detection*

Ⅰ. 서 론

인터넷의 사용이 급증함에 따라 국가 경제와 산업에 막대한 가치가 새롭게 창출되었으며, 기존 경제 활동 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]

2003년 1월 25일에 발생한 인터넷 대란의 경우 국가 전체의 인터넷이 마비되는 피해가 발생하였다. 이때 전파된 MS-SQL Slammer 웜은 발생 후 10분만에 전세계 취약 호스트의 90% 이상을 감염시킨 것으로 나타났다.[2,3] Code Red 웜은 14시간 이내

접수일 : 2005년 10월 11일 ; 채택일 : 2006년 1월 25일
* 본 연구는 정보통신부 대학 IT 연구센터 육성·지원사업의 연구결과로 수행되었습니다.
† 주저자 : mintkim@lgcns.com
‡ 교신저자 : ywchoi@tmlab.kaist.ac.kr

에 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.

최근 수년 동안 인터넷 상의 공격을 효과적으로 탐지하기 위해서 탐지 시스템에 대한 연구가 널리 수행되었다. 탐지 시스템은 정보 시스템 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 분산분석을 통하여, 월별요인, 요일요인, 시간요인을 파악하여 자료를 정류화한 후, 자기회귀모형에 적용한 연구가 있었다.[6] 이때, Kalman Filter를 사용하면 분산분석에 필요한 방대한 훈련데이터를 줄일 수 있다. 한편, 우도비(Likelihood Ratio) 를 활용하여 장기간에 걸쳐 발생하는 네트워크 상황의 변화를 탐지할 수 있다.[7] 통계적 품질관리 기법의 하나인 지수가중 이동평균 (EWMA: Exponentially Weighted Moving Average) 기법을 MIT-LL 데이터에 적용한 연구도 수행되었다.[8] 한편, 암호 이론에 근간한 네트워크 보안에 관련한 연구들도 활발히 수행되었다.[13-17] 그러나 기존의 연구는 특정 호스트나 네트워크를 대상으로 침입을 탐지하기 때문에 네트워크 전반을 통해 급속히 전파되는 공격을 효율적으로 탐지하기 어렵다. 이에 기간망 상의 정보를 효율적으로 수집하고 신속히 네트워크에 대한 공격 발생을 탐지하는 기법의 필요성이 증대되고 있다.[9] 그러나 기간망에서는 패킷이 고속으로 처리되어야 하는데, 이는 인터넷 기간망에서의 공격 탐지 알고리즘에 패킷당 메모리 탐색이나 계산에 대한 상당한 제약을 가한다. 따라서 인터넷 기간망에서의 공격탐지를 위한 알고리즘은 빠른 속도와 민감도의 두 가지를 동시에 만족시켜야 한다. 이 두 가지는 서로 교환적인 성격이 있으나 적절한 타협점을 찾는 다면, 특정 호스트나 네트워크에 대한 공격을 기간망에서 사전에 탐지해내는 큰 효과를 볼 수 있을 것이다.

최근 DDoS 공격의 대상은 TCP를 기반으로 한 서비스에 집중되고 있고, DDoS공격의 90% 이상이 SYN Flooding 공격이며, 이러한 SYN Flooding 공격은 TCP에 기반한 서비스에 치명적인 타격을 가할 수 있다. 그러므로 이 논문은 TCP/UDP 하에서의 네트워크 공격을 그 탐지 대상으로 한다.[1-4] 본 연구에서는 여러 개체들의 빈도에 대한 분포와 관련하여 간단한 통계량인 엔트로피를 사용하고자 한다. 인터넷 공격의 유형에 따라서 근원지 주소, 목적지 주소, 목적지 포트에 관한 엔트로피 값들이 매우 민감하게 변화하는 것을 알 수 있었다. 따라서 고속 네트워크 상황에서도 적용 가능하면서도 공격에 민감한 탐지기법을 제안하고자 한다.

본 논문은 다음과 같이 구성된다. 먼저 다음 장에서는 네트워크의 공격 유형에 따른 근원지 주소, 목적지 주소 그리고 목적지 포트의 빈도 분포가 어떻게 달라지는지에 관하여 분석할 것이다. 3장에서는 2장의 분석에 근거하여 효과적으로 공격을 탐지해내기 위한 탐지 기법을 제안할 것이다. 4장에서는 실험을 통하여 제안한 탐지 기법의 성능을 보이고, 마지막으로 5장에서 본 논문의 결론을 내릴 것이다.

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 향하

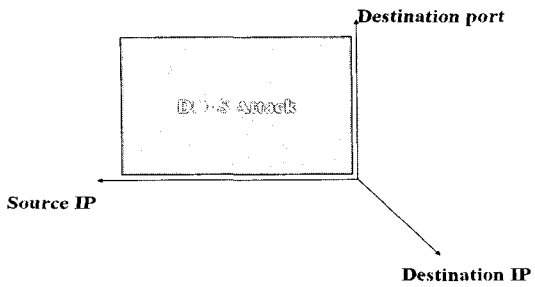


그림 1. DDoS 공격의 차원 특성

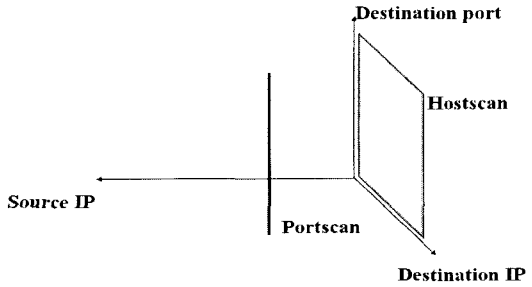


그림 2. Hostscan과 Portscan의 차원 특성

게 되어, 목적지 주소의 분포는 집중된다. 목적지 포트는 DDoS 공격 도구가 사용하는 방법에 따라 차이를 가지게 된다. 이러한 DDoS 공격의 특징을 3차원으로 나타내면 그림 1과 같다. DDoS 공격 패킷의 경우 일반적으로 Source IP Address는 랜덤하게 조작되므로 그 가짓수가 무한히 늘어나는 반면, Destination IP Address는 공격대상으로 집중하게 되므로 하나로 수렴하는 특성을 보인다. 이 경우 Destination Port의 가짓수는 DDoS 공격을 탐지해내는 중요한 변수가 아니다. 왜냐하면 공격 패킷의 Destination Port 고정여부와 관계없이 공격대상을 서비스 불능으로 만들 정도로 충분한 양의 공격 패킷만 있다면 DDoS공격이 될 수 있기 때문이다. 다시 말해, DDoS공격에서는 네트워크상에 패킷의 Destination Address는 하나로 집중되는 반면, Source IP Address는 그 가짓수가 무한히 늘어나고, Destination Port는 고정되거나 변하는 특성을 보인다.

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 2와 같다. 호스트스캔 공격은 어떤 호스트가 공격가능한지 알아내는 네트워크 공격이다. 그러므로 공격패킷의 source IP address는 고정된 반면, 어떤 host가 공격가능한지 알기 위해 destination IP Address와 destination port의 가짓수는 증가하는 특성을 보인다. 포트스캔 공격은 특정 호스트의 어느 포트가 열려있는지 알아내는 네트워크 공격이다. 특정 호스트의 여러 가지 포트에 대한 공격가능성을 알아내는 공격이므로 공격패킷의 source IP Address와 Destination IP Address는 고정된 반면, Destination port의 가짓수는 증가하는 특성을 나타낸다.

Ⅲ. 네트워크 공격 탐지

각각의 선택 확률이 p_i인 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. [12]에서는

Source IP Address의 Entropy만을 고려하였으나, 본 논문에서는 Source IP Address 뿐만 아니라 Destination IP Address와 Destination Port의 entropy를 함께 고려함으로써 DDoS 공격 탐지의 정확성을 제고하고, 이와 더불어 Hostscan 및 Portscan의 탐지도 가능케 하고자 한다.

엔트로피는 특정 샘플의 빈도의 분포를 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 표 1과 같다.

네트워크공격의 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. 근원지 주소, 목적지 주소 그리고 목적지 포트에 관한 엔트로피 값을 각각 H_{s_ip}, H_{d_ip}, 그리고 H_{d_port}으로 표현하기로 하자. 우리는 표 2와 같이 엔트로피 상호간의 변화를 파악하는 간단한 척도를 제시한다.

위의 척도들을 통해 네트워크의 공격을 탐지하기 위해서는 비공격 데이터 셋으로부터 위 척도들의 정상상태 분포를 조사할 필요가 있다. 그러나 이는 본 논문의 초점이 아니기 때문에 일례로 다음과 같은 수식으로 정상상태를 위한 범위를 구하기로 한다. 초기 비공격 기간에서 일정주기마다 위의 척도를 계산한 표본들로부터 평균과 표준편차를 얻을 수 있다. 이를 μ_{T_1}, μ_{T_2}, σ_{T_1}, σ_{T_2} 라 표기하자. 만일, 특정 주기에서 T_1의 값이 $\mu_{T_1}+3\cdot\sigma_{T_1}$보다 크다면 이는 네트워크에 DDoS 공격이 있음을 의미한다. 만일, T_1의 값이 $\mu_{T_1}-3\cdot\sigma_{T_1}$보다 작다면 이는 Hostscan 공격이 있음을 의미한다. 마찬가지로 T_2의 값이 $\mu_{T_2}+3\cdot\sigma_{T_2}$ 보다 크다면 이는 Portscan 공격이 진행되고 있다는 것을 나타내게 된다.

Ⅳ. 성능평가

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 IPsweep 이라는 프로그램을 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, 5는 각각의 엔트로피의 변화를 보여준다.

DDoS 공격이 발생하면 근원지 주소의 엔트로피가 급격히 증가하고, 목적지 주소의 엔트로피가 급격히 감소하기 때문에, 그림 5에서 공격이 일어난 시간대의 $T_1 = H_{s\_ip} - H_{d\_ip}$ 값이 주어진 상한을 크게 상회하여 공격의 발생을 쉽게 탐지할 수 있다. 물론 이 경우에서 그림 3의 H_{s_ip}의 값도 공격 시간

표 1. 공격의 유형에 따른 엔트로피 변화

	근원지 주소	목적지 주소	목적지 포트
DDoS	증가	감소	-
Hostscan	감소	증가	-
Portscan	감소	감소	증가

표 2. 제안하는 네트워크 공격 탐지 척도

DDoS	$T_1 = H_{s\_ip} - H_{d\_ip}$
Hostscan	$T_1 = H_{s\_ip} - H_{d\_ip}$
Portscan	$T_2 = H_{d\_port} - H_{s\_ip} - H_{d\_ip}$

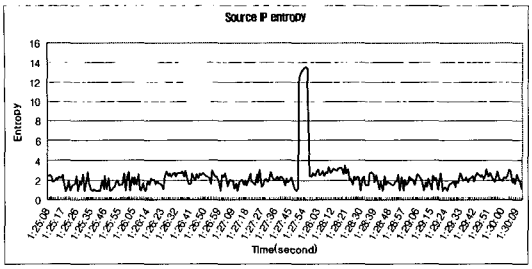


그림 3. H_{s_ip}의 변화 (DDoS의 경우)

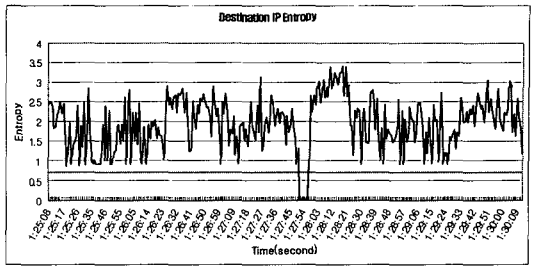


그림 4. H_{d_ip}의 변화 (DDoS의 경우)

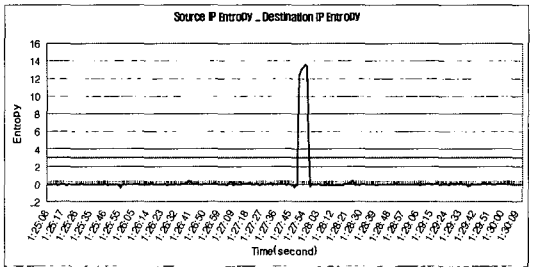


그림 5. $T_1 = H_{s_ip} - H_{d_ip}$의 변화 (DDoS의 경우)

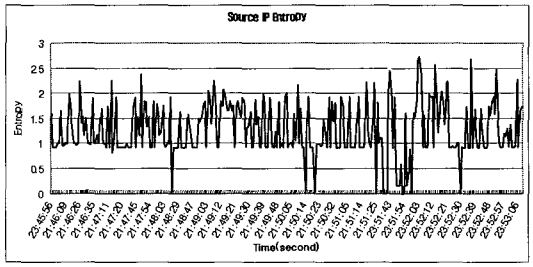


그림 6. H_{s_ip}의 변화 (Hostscan의 경우)

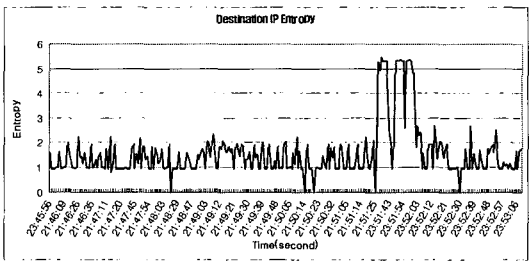


그림 7. H_{d_ip}의 변화 (Hostscan의 경우)

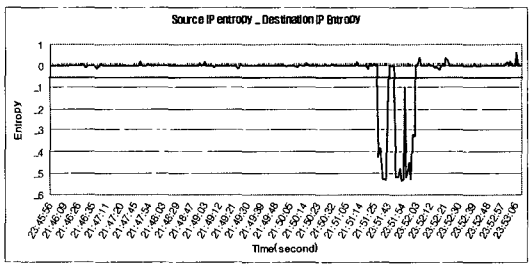


그림 8. $T_1 = H_{s_ip} - H_{d_ip}$의 변화 (Hostscan의 경우)

대에 크게 증가하여 공격 탐지에 이용될 수 있겠으나, 상황에 따라서 H_{s_ip}, H_{d_ip}, 의 값은 눈에 띄는 변화를 보이지 않을 수도 있다. 예로 같은 경우에 그림 4의 H_{d_ip}의 변화를 보면 정상 트래픽들의 엔트로피 분포에서 한눈에 공격임을 알아보기가 쉽지 않다. 그러나 $T_1 = H_{s_ip} - H_{d_ip}$은 비공격 기간의 정상 트래픽에서는 값이 0근처의 매우 작은 범위에서 변화하다가 공격 기간의 이상 트래픽에 대해서는 그 절대값이 수십 배에서 수백 배에 이르기까지 커진다. 다음의 Hostscan 공격의 경우에는 이러한 차이를 더욱 극명하게 보여준다.

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

위의 그림에서 Hostcan이 발생한 경우, 각각의 엔트로피를 독립적으로 고려하는 그림 6과 그림 7의 경우에는 비공격 기간의 정상 트래픽의 것과 비교하여 잘 구분되지 않는다. 그러나 H_{s_ip}와 H_{d_ip}을 동시에 고려한 $T_1 = H_{s_ip} - H_{d_ip}$의 그림 8에서 보면 비공격 기간의 정상 트래픽에서는 절대값이 0근처에서 거의 변화가 없다가 공격기간의 비정상 트래픽에 대해 절대값이 역시 수십 배 이상 증가하여 탐지 하한선보다 훨씬 작아지는 것을 확연히 보여주고 있으며, 따라서 보다 정확히 공격을 탐지할 수 있음을 알 수 있다.

한편, 이 논문에서 시뮬레이션 데이터로 활용하고 있는 2000 Darpa data set의 경우 port scan 공격에 해당하는 데이터를 포함하고 있지 않고, 다른 곳에서도 실제 수행된 Portscan에 대한 data-

set을 구할 수 없는 상황이므로 실제 데이터를 이용한 portscan 탐지법 검증은 어렵다. 하지만 portscan의 일반적인 공격 방법을 검토하였을 때 hostscan과 마찬가지로 본 논문에서 제안된 탐지 기법으로 탐지 가능할 것으로 추정된다.

V. 결 론

인터넷의 사용이 증가하면서, DDoS (분산 서비스 공격)를 비롯한 여러 가지 네트워크 공격들이 오늘날 인터넷의 안정성에 커다란 위협을 가하고 있다. 인터넷과 같은 대규모 망을 대상으로 한 이러한 네트워크 공격들은 특정 호스트에 대한 피해뿐만 아니라, 전체 네트워크의 성능 저하를 유발한다. 이에 본 논문에서는 고속의 인터넷 기간망에서 실시간으로 적용하여 여러 네트워크 공격에 대해서 민감하게 반응할 수 있는 통계적 탐지 방법을 고려하고자 하였다. 먼저 네트워크에 공격에 대한 분석을 통해 공격이 발생하면, 근원지 주소, 목적지 주소, 목적지 포트의 엔트로피들은 각각 정상 상태에서 급격히 변화할 것임을 알게 되었다. 이를 더욱 명확하게 탐지하기 위하여, 세가지 엔트로피를 이용한 간단한 공격 탐지 척도를 제안하였다. 이를 통하여 각각의 공격의 발생과 공격의 유형 역시 파악할 수 있다. 2000 DARPA data sets를 통한 실험에서 우리가 제안한 기법은 각각의 엔트로피를 독립적으로 관리하는 것보다 더욱 명확히 공격의 발생을 탐지할 수 있으며, 따라서 공격 탐지에서의 오탐률을 감소시킬 수 있음을 보여주었다

참 고 문 헌

[1] 권기훈 등 "트래픽 분석에 의한 광대역 네트워크 조기 경보 기법", *정보보호학회논문지*, 제 14권 4호, 8월, 111-121쪽, 2004.

[2] D. Moore et al, "The Spread of the Sapphire/Slammer worm", *http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html*

[3] D. Moore et al, "Inside the Slammer worm", *IEEE Security & Privacy Magazine*, vol.1 , no.4, pp. 33-39, July-Aug. 2003

[4] Hood, C., and Ji, c., "Proactive network fault detection", *In Proceeding of IEEE INFOCOM'97*, pp. 1147-1155, 1997.

[5] Dorothy E. Denning, "An intrusion detection model", *IEEE Transactions on Software Engineering*, vol.13 n0.2, pp. 222-232, 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., 2000.

[8] N. Ye, S. Vilbert and Q. Chen, "Computer Intrusion Detection Through EWMA for Autocorrelated and Uncorrelated Data", *IEEE Transactions on Reliability*, vol.52, no.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*, vol.1, pp.291-295, Aug., 2000

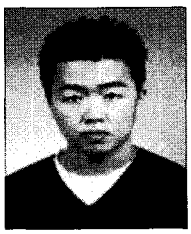
[10] Rocky K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial", *IEEE Communications Magazine*, Oct., 2002

[11] C.E. Shannon, and W. Weaver, The Mathematical Theory of Communication, University of Illinois Press, 1963

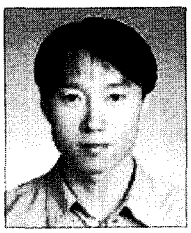
[12] Laura Feinstein and Ravindra Balupari, "Statistical Approaches to DDoS attack Detection and Response", *In Proceeding of the DARPA Information Survivability Conference and Exposition*, 2003.

[13] 조태남 등, "(2,4)-트리를 이용한 그룹키 관리," 정보보호학회논문지, 2001.
[14] 박영호 등, "이동네트워크 환경에서 그룹키 관리구조," 정보보호학회논문지, 2002.
[15] 권정옥 등, "일방향 함수와 XOR을 이용한 효율적인 그룹키 관리 프로토콜: ELKH," 정보보호학회논문지, 2002.
[16] 이상원 등, "Pairing을 이용한 트리 기반 그룹키 합의 프로토콜," 정보보호학회논문지, 2003.
[17] 박영희 등, "Diffie-Hallman 키 교환을 이용한 확장성을 가진 계층적 그룹키 설정 프로토콜," 정보보호학회논문지, 2003.

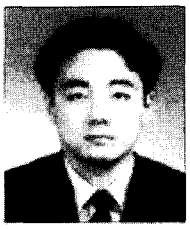
〈著者紹介〉



김 민 택 (Min-Taek Kim) 정회원
2003년 2월: 연세대학교 산업공학과 졸업
2005년 2월: 한국과학기술원 산업공학과 석사
2005년 3월~현재: LG CNS Entrue Consulting
〈관심분야〉 정보보호, 네트워크 보안, 침입 탐지



최 영 우 (Young-Woo Choi) 학생회원
1999년 8월: 한국과학기술원 산업공학과 졸업
2001년 8월: 한국과학기술원 산업공학과 석사
2001년 9월~현재: 한국과학기술원 산업공학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 침입 탐지



권 기 훈 (Ki Hoon Kwon) 학생회원
2001년 2월: 한국과학기술원 산업공학과 졸업
2003년 2월: 한국과학기술원 산업공학과 석사
2003년 3월~현재: 한국과학기술원 산업공학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 침입 탐지

김 세 헌 (Sehun Kim) 정회원
1972년: 서울대학교 물리학과 학사
1977년: 스탠포드 대학교 물리학과 석사
1981년: 스탠포드 대학교 OR 박사
1982년~현재: 한국과학기술원 산업공학과 교수
2003년: 정보통신부 정보보호실태 조사단 단장
2003년~현재: 한국 PKI 포럼 이사
2004년~현재: 국가정보원 국가정보보안협의회 산학연 회장
〈관심분야〉 OR, 이동통신, 정보보호, 네트워크 보안