고속 인터넷 백본 링크상에서의 트래픽 측정에 의한 네트워크 공격 징후 탐지 방법☆

Detection of Network Attack Symptoms Based on the Traffic Measurement on Highspeed Internet Backbone Links

노 병 희
Byeong-hee Roh

요 약

본 논문에서는, 고속의 인터넷 백본 링크상에서 네트워크 공격의 징후를 트래픽 측정에 의하여 탐지해 내기 위한 방법을 제안한다. 이를 위하여, 인터넷 백본상에서 나타나는 정상 및 공격 트래픽의 패턴을 분석하였고, 이러한 트래픽 특성을 활용하여 네트워크 공격 감지를 위한 두가지 트래픽 척도를 도출하였다. 이들은 평균 파워 스펙트럼과 패킷수 대 트래픽양 비율이다. 그리고, 이들 트래픽 척도들을 집합된 트래픽 수준에서 측정함으로써 네트워크 공격 징후 감지를 위한 방법론을 제안한다. 실험 결과는 제안된 방법이 네트워크 공격 징후를 매우 잘 감지해내고 있음을 보여준다. 제안된 방법은 개별 플로우 또는 개별 패킷들에 기반을 둔 기존의 방법들과 달리, 집합된 트래픽 수준에서 운영되므로 계산의 복잡성을 현저히 줄일수 있다.

Abstract

In this paper, we propose a novel traffic measurement based detection of network attack symptoms on high speed Internet backbone links. In order to do so, we characterize the traffic patterns from the normal and the network attacks appeared on Internet backbone links, and we derive two efficient measures for representing the network attack symptoms at aggregate traffic level. The two measures are the power spectrum and the ratio of packet counts to traffic volume of the aggregate traffic. And, we propose a new methodology to detect networks attack symptoms by measuring those traffic measures. Experimental results show that the proposed scheme can detect the network attack symptoms very exactly and quickly. Unlike existing methods based on individual packets or flows, since the proposed method is operated on the aggregate traffic level, the computational complexity can be significantly reduced and applicable to high speed Internet backbone links.

Keyword : Network Security, Attack Detection, Attack Traffic Modeling

1. 서 론

최근 들어, 다양한 네트워크 공격에 의한 인터넷 서비스의 장애를 여러 번 경험하였다. 인터넷은 최대한의 연결 제공을 위하여 인터넷을 구성하는 다양한 요소들 상호간의 개방성을 요구하므로, 인터넷 기반 구조에 대한 공격은 매우 큰 영향을 미치게 된다. Houle과 Weaver는 다양한 서비스 거부 (denial of service, DoS) 공격 도구의 개발 및 사용, 그리고 이러한 DoS 공격의 영향에 대한 동향을 정리하였다[1]. 이들의 조사에 의하면, 대부분의 공격 도구들은 다양한 목적에 따라 발신지 및 수신지 IP 주소와 포트 번호들과 같은 IP 패킷 들의 주요 속성들을 변조하고 있다. 표 1에는 플로우내 속성들의 변조에 따른 대표적인 DoS 공격의 형태와 특징을 나타내었다[1,2]. 표 1에서 vspoof와 fspoof 는 타겟 호스트에 대한 공격을 위하여, 발신자를 숨기기 위하여 발신 IP 주소를 변조시키는 전형적인 IP 변조 DoS 공격들로서, vspoof

* 정회원 : 아주대학교 정보통신전문대학원 부교수
bhroh@ajou.ac.kr(제 1저자)
☆ 본 논문은 과학기술부 목적기초연구(R05-2004-000-10824-0) 지원으로 수행되었음.

의 경우에는 수신 포트 번호도 함께 변화하는 경우이고, fspoof는 수신 포트 번호가 고정된 경우이다. 그리고, hostscan과 portscan은 공격대상인 호스트와 취약 포트 번호를 찾기 위한 DoS 공격형태로서 표 1과 같은 속성 변화 특징을 갖는다.

〈표 1〉 DoS 공격 형태의 분류 및 특징

속성 / 공격 형태	발신 IP 주소	수신 IP 주소	수신 포트 번호
vspoof	변화함	고정	변화함
fspoof	변화함	고정	고정
hostscan	고정	변화함	고정
portscan	고정	고정	변화함

네트워크 공격에 대응하기 위한 많은 연구들은 개별 망 단위에서 자신들의 안전을 위하여 의심스러운 패킷들을 분류하고 필터링하는 방법론에 초점이 맞추어 지고 있다. 그러나, 분산형의 글로벌한 네트워크 공격들은 이 공격이 목표물에 도달하여 퍼지기 전에 백본망에서 우선적으로 형태가 드러나게 될 것이므로, 개별 망 단위에서 대응하는 것보다는 백본망 단위에서 대응하는 것이 더 효과적일수가 있다. 백본 링크에서 실시간으로 네트워크 공격들을 찾아내기 위한 방법들, 예를 들어[2], 이 제안되고 있으나, 이들은 개별 패킷들 또는 개별 플로우에 초점을 맞추고 있으므로, 매우 큰 계산상의 복잡성과 컴퓨팅 자원을 요구한다. 공격의 패턴을 찾아내는 방법들에 대한 연구와 함께, 공격 메커니즘이나 도구들도 계속적으로 진화 발전해 나가고 있다. 이와 같이 다양하게 등장 가능한 네트워크 공격에 맞추어 대응하기 위한 방법의 개발은 한계를 보일 수도 있다. 이를 극복하기 위한 유망한 방법론은 전체 인터넷이 공조하는 전역 방어 인프라 구조(global defense infrastructure)를 구축하는 것이다[4,11]. 그러나, 이러한 인프라 구조에 대한 연구는 구조에 대한 제시 단계로서 현재까지 가시화된 결과를 제공하지는 못하고 있다.

본 논문에서는 기존의 네트워크 공격에 대응하기 위한 방법들이 개별 패킷 또는 플로우 단위로 수행되는 관점에서와 달리 트래픽 흐름의 관점에서 다루기 위한 방법론을 제시한다. 이를 위하여, 네트워크 공격 트래픽들이 인터넷 백본 링크상에서 나타나게 되는 특징을 분석하고, 이들 네트워크 공격 트래픽이 정상적인 트래픽 흐름에 어떠한 영향을 미치는지를 분석한다. 이러한 분석을 통하여 공격 징후 감지를 위한 두가지 트래픽 척도인 평균 파워 스펙트럼과 패킷수-대-트래픽양 비율을 도출해 내어 이들을 집합된 트래픽 수준에서 측정함으로써 공격 징후를 감지해 낼 수 있는 방법론을 제안한다. 제안된 방법은 집합된 트래픽 수준에서 동작하므로, 기존의 개별 패킷 또는 플로우 단위로 수행되는 방법들에 비하여 현저히 계산량을 줄일수 있으며, 인터넷 망관리 구조와의 연동이 용이하여 전역 방어 인프라 구조 구축에 적용 가능하다.

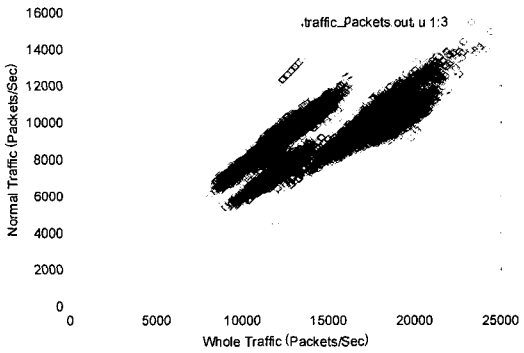
본 논문의 구성은 다음과 같다. 제2장에서는 네트워크 공격 트래픽의 특성과 이들이 정상 트래픽 흐름에 어떠한 영향을 주는지를 분석한 결과를 보이고, 제3장에서는 네트워크 공격 징후를 집합된 트래픽 흐름 차원에서 감지하기 위한 방법을 설명한다. 제4장에서는 제안 방법에 대한 실험 결과를 보이고, 제5장에서는 결론을 맺는다.

2. 네트워크 공격 트래픽 특성

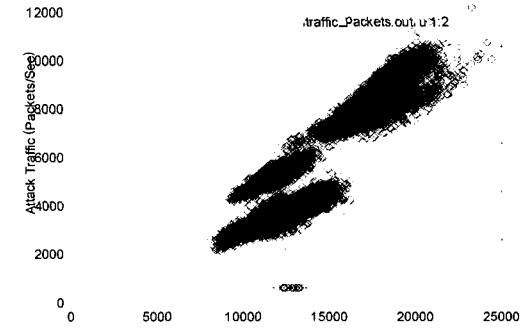
네트워크 공격 트래픽 특성 분석을 위하여, 한국전산원에서 운용하는 해외 인터넷 연결을 위한 T-3 인터넷 백본 링크상에서 캡쳐한 트래픽을 사용하였다[5]. 네트워크 공격 트래픽의 분류는 Kim등이 제안한 방법[2]과 Bloom Filter를 적용한 방법[8]을 함께 적용하여 캡쳐한 트래픽에서 표 1에 보인 각 네트워크 공격 플로우들을 정확하게 구분이 가능하도록 하였다. 네트워크 공격 패킷들의 트래픽 특성을 분석하기 위하여, 캡쳐한 트래픽에서 표 1에 보인 네트워크 공격 패킷들만을 분류하여 구성된 공격 트래픽(attack traffic), 이들 공격 패킷들이 아닌 정상적인 패킷들로만 이루어진 정상 트래픽(normal traffic), 그리고 이들이 모두 합쳐진 전체 트래픽인 집합 트래픽

(aggregate traffic)의 유형으로 구분하여, 이들 트래픽 유형들간의 특징을 분석하였다.

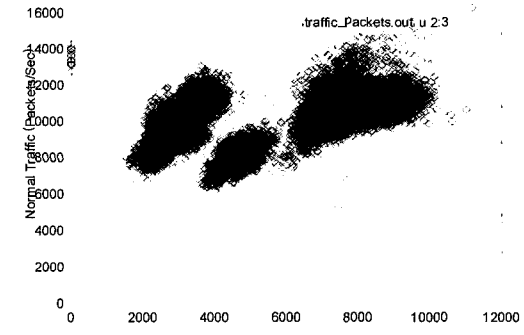
그림 1은 같은 시간(1 초)동안 발생한 패킷수를 트래픽 유형별로 비교하여 나타내었다. 그림 1 (a)와 (b)에서 볼 수 있듯이 전체 트래픽의 발생 패킷수는 정상 트래픽의 발생 패킷수 뿐만 아니라, 공격 트래픽



(a) 집합 트래픽과 정상 트래픽



(b) 집합 트래픽과 공격 트래픽



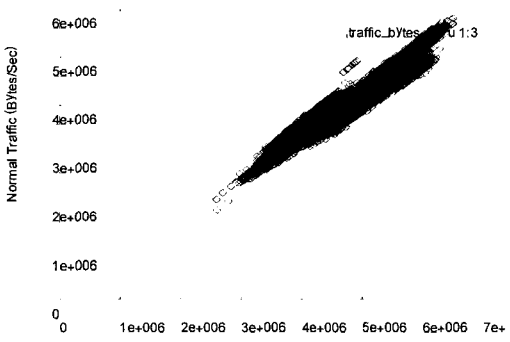
(c) 공격 트래픽과 정상 트래픽

〈그림 1〉 발생 패킷수 비교

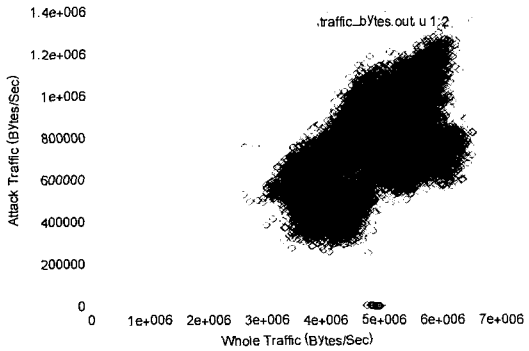
의 발생 패킷수와 비례 관계를 갖는다. 즉, 정상 트래픽과 공격 트래픽에 의한 발생 패킷의 증가는 전체 트래픽의 발생 패킷의 증가에 가시적으로 반영되어 나타난다. 반면에, 그림 1 (c)에서 보듯이 정상 트래픽의 발생 패킷수와 공격 트래픽의 발생 패킷수는 연관 관계가 없다.

그림 2는 같은 시간(1초)동안 발생한 트래픽 크기(바이트수)를 트래픽 유형별로 비교한 것이다. 그림 2 (a)에서 보듯이 집합 트래픽 크기는 정상 트래픽의 크기와 비례 관계를 갖는다. 반면에 공격 트래픽의 크기는 집합 트래픽 크기와 정상 트래픽의 크기와 특별한 상관 관계를 갖지 않음을 알 수 있다. 그림 1과 그림 2에서 볼 수 있듯이, 공격 트래픽의 발생 패킷수는 집합 트래픽에서 가시적으로 보일 정도로 나타나지만, 트래픽 크기 측면에서는 정상 트래픽에 비하여 상대적으로 매우 작은 크기를 보이게 되어 가시적인 영향을 미치지는 않는 것으로 보인다.

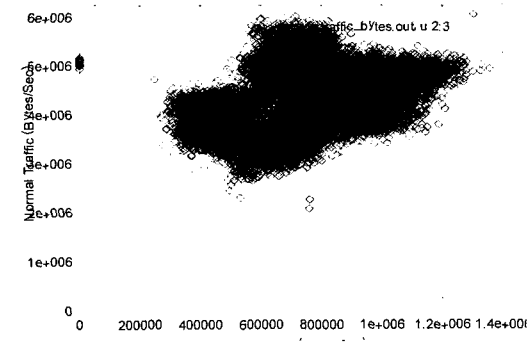
그림 1과 그림 2에서 트래픽 양 보다는 발생 패킷 개수가 더 네트워크 공격의 현상을 잘 관찰할 수 있음을 보았다. 이러한 네트워크 공격 플로우들로부터 발생되는 패킷들의 특성을 보기 위하여 그림 3에 보인 바와 같은 트래픽 유형별 패킷 크기에 대한 누적 확률 분포를 구하였다. 공격 트래픽 패킷들은 정상 트래픽 패킷들에 비하여 매우 작은 크기의 패킷들을 사용하고 있음을 볼 수 있다. 실제로, 90%이상의 공격 트래픽 패킷들은 80 바이트 이하의 크기를 갖는 것으로 분석되었다. 이에 반하여 정상 트래픽 패킷들



(a) 집합 트래픽과 정상 트래픽



(b) 집합 트래픽과 공격 트래픽

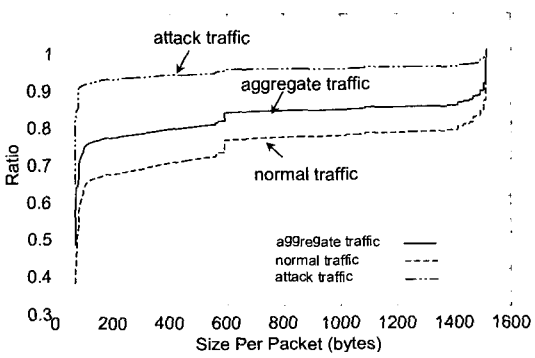


(c) 공격 트래픽과 정상 트래픽

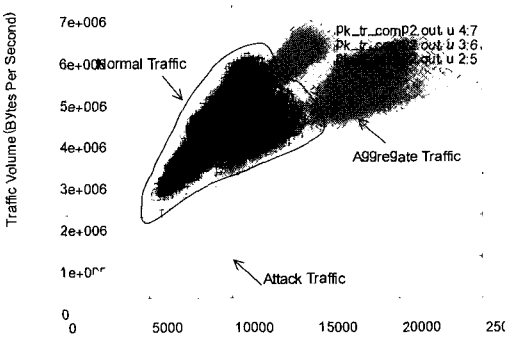
〈그림 2〉 발생 트래픽양(바이트수) 비교

은 70바이트 이하, 590 바이트 근처, 그리고 1450 바이트 이상에서 많은 비율을 차지하며 나머지 크기에는 일정한 수준을 유지하며 산재 되어 있다.

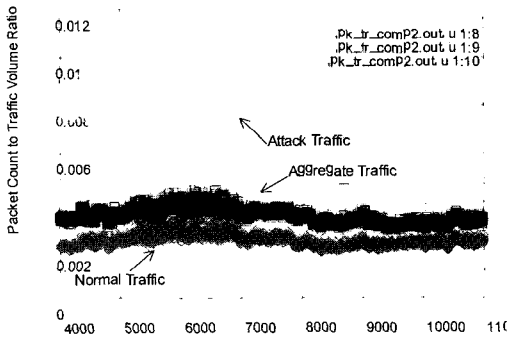
그림 3의 통계 특성이 트래픽 흐름에 영향을 주는 것을 그림 1과 그림 2와 다른 각도에서 보기 위하여 1초동안 발생된 패킷 개수와 트래픽양간의 상관 관계를 그림 4에 나타내었다. 그림 4(a)는 전체적인 관점에서 보인 상관관계를 보여주는데, 정상 트래픽에 공격 트래픽이 부가된 집합 트래픽에 있어서 트래픽 양이 변화하는 비율보다 패킷 개수가 변화되는 비율이 더 크게 나타남을 볼 수 있다. 또한, 그림 4 (b)에는 특히 공격 트래픽이 많이 발생한 시간 구간동안을 선택하여 시간에 따른 트래픽양에 대한 패킷 개수의 비율의 변화 특성을 나타내었는데, 전체 트래픽에서의 이 비율이 정상 트래픽에서의 비율에 비하여 매우 크게 변화됨을 볼 수 있다. 그림 2에서 보인 바와 같이, 공격 트래픽양은 정상 트래픽양에 비하여 작아서 집합 트래픽의 흐름에서 공격의 패턴을 찾아 내는 것은 쉽지 않을 것이다. 그러나, 그림 1과 그림 4에서와 같이 패킷의 수를 트래픽의 양과 함께 고려할 경우, 공격



〈그림 3〉 패킷 크기에 대한 누적확률 분포



(a) 유형별 패킷수와 트래픽양간의 상관관계



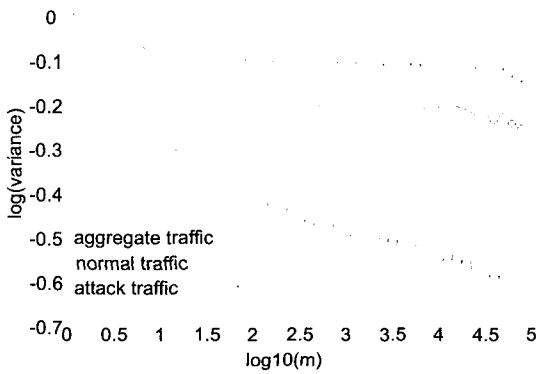
(b) 패킷수와 트래픽양의 변화

〈그림 4〉 패킷수와 트래픽양간의 상관 관계

에 의한 트래픽의 변화 징후를 감지해내는 것이 가능할 것으로 판단된다.

이더넷 트래픽은 자기유사(self-similar) 성질을 갖고 있음이 알려져 있다[6]. 자기 유사 성질은 소스 트래픽 모델링 뿐만 아니라 네트워크 혼잡 제어 방식의 개발에 큰 영향을 준다. 자기 유사 성질은 Hurst 파라메터로서 표현되며, Hurst 파라메터가 클수록 자기 유사 성질이 더 커진다. 일반적으로, Hurst 파라메터가 큰 트래픽은 평균 비트율, 네트워크 부하의 동일한 환경에서 링크 이용율, 소통율, 손실율등과 같은 네트워크 성능에 더 큰 영향을 미치게 된다[7]. 이러한 자기 유사 특성이 네트워크 공격 트래픽에 의하여 어떠한 영향을 미치는지를 보이기 위하여 variance-time-plot (VTP) 방법[6]을 사용하여 Hurst 파라메터를 계산하였다.

그림 5 에는 Hurst 파라메터를 구하기 위한 각 트래픽 유형별 VTP 그래프를 나타내었다. 여기에서 보듯이 공격 트래픽의 Hurst 파라메터값은 정상적인 트래픽들에 비하여 매우 크게 됨을 알 수 있다. 그리고, 정상 트래픽에 공격 트래픽이 더해짐으로써 집합 트래픽의 Hurst 파라메터 값이 함께 증가되는 현상을 볼 수 있다. 이들로부터, 공격 트래픽이 정상 트래픽보다 더 큰 자기 유사 성질을 갖음을 알 수 있다. 또한, 집합 트래픽의 자기 유사성은 공격 트래픽의 추가에 의하여 증가됨을 알 수 있다. 이것은 공격 트래픽의 증가는 단순히 네트워크에 흐르는 트래픽의 양만을 증가시키는 것이 아니라, 자기 유사성을 크게 만들어 동일한 수준의 네트워크 부하에 대하여도 네트워크에 더 심각하게 영향을 미칠 수 있음을 의미한다. 따라서, 공격 트래픽의 증가는 해당 목표에 대한 피해 뿐만 아니라, 전체적인 네트워크의 성능에 직접적인 피해를 가중시키게 된다.



〈그림 5〉 Variance Time Plot (VTP)

3. 트래픽 측정에 의한 네트워크 공격 징후 감지 방법

앞 절에서 네트워크 공격 트래픽은 정상적인 공격 트래픽과 매우 상이한 트래픽 특성을 갖으며, 정상 트래픽 흐름에 영향을 주어 트래픽 패턴에 변화를 주게 됨을 살펴보았다. 본 절에서는 이러한 변화되는 트래픽의 특성을 고려하여, 본 논문에서 제안하는 집합 트래픽 흐름 차원에서 공격 트래픽의 징후를 감지해내기 위한 방법에 대하여 설명한다.

앞 절에서 네트워크 공격 트래픽의 특성은 기존의 정상적인 트래픽 형태와는 매우 다르고, 더 큰 자기 유사성을 갖고 있으며, 공격 트래픽은 전체 트래픽의 자기 유사성을 증가 시키게 됨을 보았다. 일반적으로, 자기 유사성이 커지면 트래픽의 버스트한 특성도 함께 커지게 된다[6]. 앞 절에서는 Hurst 파라메터를 구하는데 VTP 방법을 사용하였으나, Hurst 파라메터를 구하는 방법은 이외에도 주기도(periodogram) 에 의한 방법이 사용될 수 있다[7]. l개의 표본을 갖는 이산시간 시계열 시퀀스 $X_0, X_1, \cdots, X_{l-1}$에 대한 주기도는 다음과 같은 식으로 표현된다.

$$S(w) = \frac{1}{2\pi N}\left|\sum_{k=0}^{l-1} X_k e^{jkw}\right|^2 \quad (1)$$

이때, $S(w)$와 w 간의 관계는 다음식으로 나타낼 수 있다.

$$\lim_{w\to 0} \log S(w) = a_0 \log|w| + a_1 \quad (2)$$

이것은 log-log 그래프상에서 기울기가 a_0인 직선

이 나오는데, 이때 Hurst 파라메터는 $H=(l-a_0)/2$가 된다. 식 (1)의 주기도 계산을 위한 식은 이산 시간 퓨리에 변환 (discrete-time Fourier transform, DFT)에 기초하고 있음을 알 수 있다. Li 등[9]과 Roh 등[10]은 입력 트래픽에 대한 DFT를 통하여 구하여지는 파워 스펙트럼이 통신 시스템의 성능에 주 영향을 미침을 보이고 있다. 본 논문에서는 이러한 기존의 연구들과 앞 절에서의 분석 결과를 기반으로 하여 공격 트래픽의 징후를 판단하기 위한 척도중의 하나로서 평균 파워 스펙트럼 (average power spectrum)을 사용하기로 한다.

평균 파워 스펙트럼을 정의하기 위하여, 시간을 일정한 크기인 Δ로 구분되어 있다고 가정하면, 이 Δ 구간이 트래픽을 측정하는 기본 측정 구간이 된다. c_n과 v_n (n=0,1,2,...) 을 각각 n-번째 Δ 구간에서 측정된 패킷 개수와 트래픽 양이라고 정의하고, L Δ을 L 개의 중첩되지 않는 연속한 Δ들로 이루어지는 감지 주기 시간으로 정의하기로 한다. 이 감지 주기 시간 단위로 공격 징후 감지를 위한 알고리즘이 적용된다. 또한, m 번째 감지 주기 시간 동안의 패킷수와 트래픽양에 대한 벡터인 $\vec{c}=[c_{mL}, c_{mL+1}, \cdots, c_{(m+1)L-1}]$와 $\vec{v}=[v_{mL}, v_{mL+1}, \cdots, v_{(m+1)L-1}]$($m$=0,1,2,...) 를 각각 정의하기로 한다. 이때, $\rightharpoonup$에 대한 평균 파워 스펙트럼은 다음과 같이 정의된다.

$$\overline{P}(m)=\sum_{k=0}^{L-1}\phi_{mk} \tag{3}$$

여기에서 $\Psi_m=[\phi_{m0}, \phi_{m1}, \cdots, \phi_{m(L-)}]$는 $\vec{c}_m$ 대한 DFT를 통하여 구해진다. 즉, $\Psi_m=L^{-2}|\mathrm{DFT}(\vec{c}_m)|^2$.

평균 파워 스펙트럼은 네트워크 공격에 의한 자기 유사성의 영향을 반영한 척도임에 주목한다. 또한, 앞 절의 분석에서 공격 트래픽은 특성이 정상적인 트래픽과 다른 특성을 갖는데, 패킷 개수측면에서의 특성이 더 그러하며, 이에 따라 공격 트래픽이 부가되는 시간 구간에서 트래픽양에 대한 패킷 개수의 비율에 심각한 변화가 나타나게 됨을 보았다. 본 논문에서는 이러한 비율을 또 다른 공격 징후를 감지하기 위한 척도로서 사용할 것이며, m-번째 감지 주기 시간에서의 패킷수-대-트래픽양의 비율은 다음과 같이 나타낼 수 있다.

$$\overline{R}(m)=\frac{\vec{c}_m\cdot\vec{e}}{\vec{v}_m\cdot\vec{e}} \tag{4}$$

여기에서 $\vec{e}=[1,1,\cdots 1]^T$이고, $[\cdot]^T$는 전치 행렬(transpose matrix)을 의미한다.

식 (3)과 식 (4)의 척도들을 사용하여 네트워크 공격 징후를 감지해내기 위하여 본 논문에서 제안하는 방법은 다음과 같다. $x_P(m)$과 $x_r(m)$을 각각 m-번째 감지 주기 시간에서 측정된 평균 파워 스펙트럼과 패킷수-대-트래픽양 비율에 대한 가중치 평균들로서 정의하기로 하며, 이를 다음과 같이 산출한다.

$$x_p(m+1)=\alpha_P x_P(m)+(1-\alpha_p)\overline{P}(m)$$
$$,m=0,1,2,\cdots \tag{5}$$

$$x_r(m+1)=\alpha_r x_r(m)+(1-\alpha_r)\overline{R}(m)$$
$$,m=0,1,2,\cdots \tag{6}$$

여기에서 α_P와 α_r은 가중치 상수로서 0과 1사이의 값을 갖는다. 식(5)와 식(6)과 같이 가중치 평균을 계산하는 이유는 짧은 기간동안의 순간적인 변화보다는 어느 정도 기간동안의 일관된 변화를 추출해내기 위함이다.

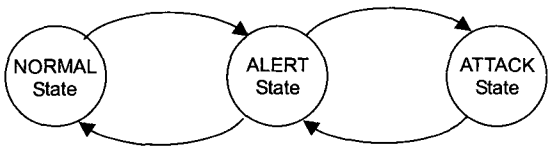
일반적으로 정상 상태 (stationary state)에서의 트래픽 흐름은 사용 시간대에 따른 사용량의 차이만 존재할 뿐, 급격한 변화없이 예측 가능한 범위에서 변화하게 된다. 이와 같은 특정한 정상 상태의 시간 구간 T 동안에 정상 트래픽을 대상으로 하여 식 (5)를 사용하여 측정된 평균 파워 스펙트럼에 대한 평균과

이에 대한 최대 허용치를 각각 m_P와 δ_P로서 정의하기로 한다. m_P는 일반적인 평균 계산식에 의하여 구해지며, δ_P는 트래픽 특성등을 고려하여 정책적으로 정의된다. δ_P를 결정하기 위하여 백그라운드 데이터와 측정 데이터간의 통계적인 차이를 찾아내기 위한 다양한 방법들[12]이 존재하나, 본 논문에서는 트래픽 측정에 의한 방법론으로서의 가능성을 보이기 위하여 다음과 같은 단순한 비교 방법을 적용한다. 즉, 해당 시간 구간 T 동안의 측정된 값 중 최대값에 가중치 K_P를 곱한 값으로 δ_P를 정의하도록 한다. 마찬가지로, 시간 구간 T 동안에 측정된 $\overline{R}(m)$에 대한 평균과 이에 대한 최대 허용치를 각각 m_r와 δ_r로서 정의하기로 한다. δ_r을 구하기 위한 가중치로서는 K_r을 사용한다.

$x_P(m)$과/또는 $x_r(m)$이 각각 허용치 δ_P와 δ_r를 초과하는 경우를 네트워크 공격 징후의 가능성이 있는 것으로서 가정할 수 있으며, 이러한 네트워크 공격 징후를 감지해내기 위하여 다음과 같은 정상 상태, 경계 상태, 공격 상태의 세 개의 상태를 정의한다.

- □ 정상 상태 (NORMAL state): 공격의 징후가 전혀 없는 상태
- □ 경계 상태 (ALERT state) : 공격 징후의 가능성 있으나 완전한 공격 징후 결정이 이루어지기 이전의 예비 공격 상태
- □ 공격 상태 (ATTACK state) : 공격이 이루어지는 것으로 판단되는 상태

이들 상태간의 천이 관계를 그림 6에 나타내었으며, 이들 상태들을 고려한 네트워크 공격 징후 감지



〈그림 6〉 공격 징후 탐지를 위한 상태들간의 천이 관계 다이어그램

를 위한 알고리즘을 그림 7에 나타내었다.

<variables>

attack_count : counter for representing the degree of attack

Alert_Threshold : threshold value for changing between ALERT and ATTACK states

Attack_Threshold : maximum value of attack_count state

: current state of the algorithm

<main algorithm>

At the end of every detection period, update $x_P(\cdot)$ and $x_r(\cdot)$ by using (5) and (6).

Considering $x_P(\cdot)$ and $x_r(\cdot)$, the state at the detection period is determined by the following sequence.

```
if (state == NORMAL )
    if ( ( x_P( · )> δ_P AND x_r( · ) ≤ δ_r) OR
    ( x_P( · ) ≤ δ_P AND x_r( · )> δ_r) )
            state = ALERT;
            attack _count += 1;
    elseif ( x_P( · )> δ_P AND x_r( · )> δ_r )
            state = ALERT;
            attack _count += 2;
    endif

elseif ( state == ALERT )
    if ( ( x_P( · )> δ_P AND x_r( · )> δ_r) OR
    ( x_P( · ) ≤ δ_P AND x_r( · )> δ_r) )
            attack _count += 1;
    elseif ( x_P( · )> δ_P AND x_r( · )> δ_r )
            attack _count += 2;
    elseif ( x_P( · ) ≤ δ_P AND x_r( · ) ≤ δ_r)
            attack_count -= 2;
    else
```

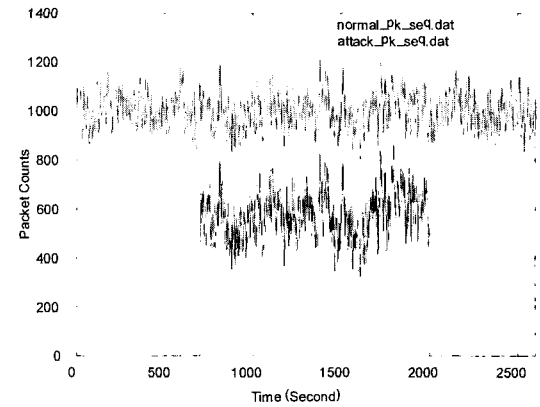
```
                attack _count -= 1;
        endif
        if ( attack_count > Alert_Threshold )
                state = ATTACK;
        elseif ( attack_count ≤ 0 )
                state = NORMAL;
                attack_count = 0;
        endif

  elseif ( state == ATTACK )
        if ( x_P( · )> δ_P AND x_r( · )> δ_r )
                attack_count = MIN ( attack_
                count+1, Attack_Threshold );
        elseif ( x_P( · ) ≤ δ_P AND x_r( · ) ≤ δ_r)
                attack_count -= 2;
        else
                attack_count -= 1;
        endif
        if ( attack_count > Alert_Threshold )
                state = ALERT ;
        endif
endif
```

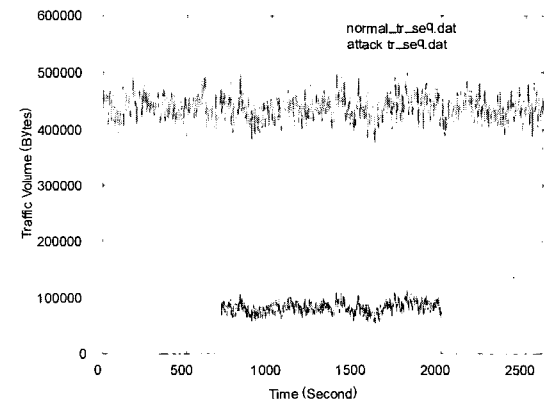
〈그림 7〉 네트워크 공격 징후 탐지 알고리즘

4. 실험 결과

실험을 위한 자기 유사 트래픽 발생을 위하여 [13]에서 제안된 방법을 사용하였으며, 정상 트래픽의 경우, 발생 패킷수에 대한 Hurst 파라메터값은 0.9가 되도록 하였고, 공격 트래픽은 [11]에서의 결과를 반영하여 Hurst 파라메터 값을 0.99가 되도록 하였다. 그리고, 발생 패킷의 수는 2장의 설명에서 사용된 캡쳐한 데이터로부터 구한 값인 정상 트래픽의 경우 9080.97 패킷/초, 공격 트래픽의 경우 5292.8 패킷/초가 되도록 하였으며, 발생 패킷의 크기는 그림 3의 분포를 따르도록 하였다. 공격 트래픽은 일정 시간만 유지되도록 하였다. 이와 같이 하여, 발생된 트래픽 값들을 10 msec 단위로 하여 그림 8에 나타내었다.



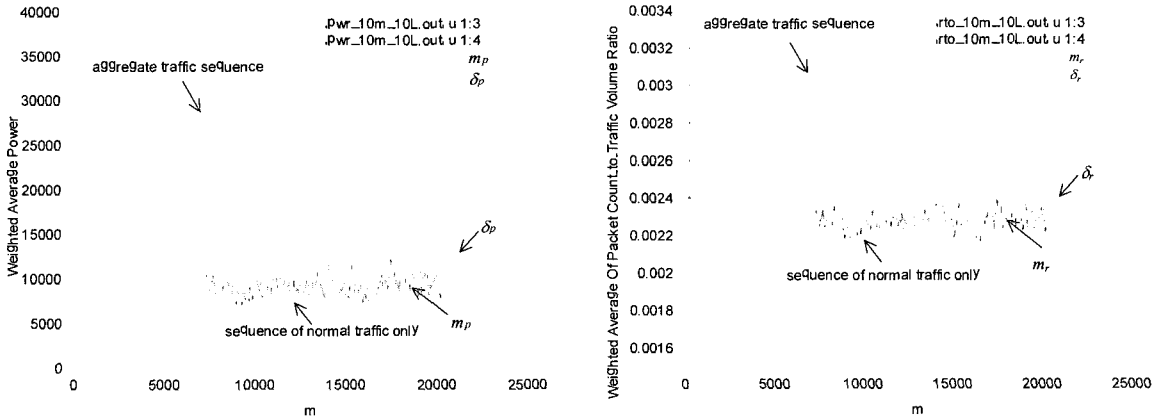
(a) 발생 패킷수



(b) 트래픽 양

〈그림 8〉 발생 트래픽

그림 9는 Δ=10msec, L=10인 경우에 대한 가중치 평균값들인 $x_P(m)$과 $x_r(m)$의 변화를 보여준다. 그림 9를 통하여 제안하는 방법에서 사용되는 척도들이 집합된 트래픽 레벨에서 네트워크 공격 트래픽의 징후를 감지해 내는데 매우 적절히 적용될 수 있음을 보여준다. 즉, 정상 트래픽의 경우는 이러한 가중치 평균값이 정상 상태 시간 구간에서는 예측 가능한 범위에서 움직이나, 이와 같이 비정상적인 네트워크 공격 트래픽들이 들어올 때는 이러한 패턴에



(a) 평균 파워에 대한 가중치 평균값의 변화

(b) 트래픽양에 대한 패킷수 비율에 대한 가중치 평균값의 변화

〈그림 9〉 가중치 평균값들 (Δ=10msec, L=10의 경우)

서 많이 벗어나게 되는데, 본 논문에서 사용한 두개의 척도들이 이러한 현상을 잘 반영해 줄 수 있음을 보여준다.

제안 방법의 효율성을 나타내기 위하여 다음과 같은 성능 척도들을 사용하였다.

$$Exactness = \frac{T_{\text{detdcted}}}{T_{\text{actual}}} \times 100(\%) \quad (7)$$

$$ErrorRatio = \frac{T_{\text{enor}}}{T_{\text{actual}}} \times 100(\%) \quad (8)$$

$$DetectDelay = t_{\text{detected}} - t_{\text{actual}} \quad (9)$$

여기에서, T_{actual}과 T_{detected}는 각각 실제 공격이 이루어진 시간 구간의 길이와 이 시간 구간 내에서 공격으로 감지된 시간 구간의 길이를 의미한다. T_{error}는 실제 공격 구간이 아님에도 공격 구간으로 감지된 시간 길이와 실제 공격 구간임에도 공격으로 분류되지 않은 시간 길이를 나타낸다. 또한, t_{actual}과 t_{detected}은 각각 실험으로 사용된 시퀀스에서 실제 공격이 이루어진 시간과 제안된 방법으로 공격이 이루어짐을 판단하게 된 시간을 나타낸다.

단위 시간 Δ와 측정 구간 L의 변화에 따른 실험 결과를 표 2에 나타내었다. 표 2의 각 셀내의 A/B/C 값은 성능 척도인 Exactness / ErrorRatio / DetectDelay 값들을 각각 나타낸다. 표 2를 구하기 위하여 실험에 사용된 변수들은 다음과 같다. 즉, $\alpha_P = \alpha_r$=0.9, Alert_Threshold=5, Attack_Threshold=Alert_Threshold +5. 그리고, δ_P와 δ_r은 정상적인 트래픽 시퀀스에 대하여 식 (5)와 (6)을 적용하여 구한 최대값을 적용하였다. 즉, $K_P = K_P$=1.

〈표 2〉 실험 결과

L \ Δ	10 msec	100 msec	1sec
10	99.98% / 0.001 / 300msec	99.77% / 0.016 / 3sec	97.71% / 0.275 / 30sec
100	99.77% / 0.016 / 3sec	97.71% / 0.274 / 30sec	N/A
1000	97.71% / 0.274 / 30sec	N/A	N/A

직관적으로도 짐작할 수 있는 바와 같이, Δ 값이 작을수록 Exactness와 ErrorRatio 성능은 더 나아지게 된다. 가능한 측정 구간과 주기 시간에 대하여 구해진 제안된 방법의 정확도는 97%가 넘고 있다. 반면에, L 값이 커질수록 DetectDelay와 ErrorRatio 값들은 커지

게 된다. 더 나은 정확도와 감지 시간 성능을 구하기 위하여는 Δ과 L값이 작도록 하여야 하는데, 이들 측정 구간 관련 변수의 크기는 알고리즘의 계산의 복잡성에 영향을 줄 수 있다. 즉, Δ값이 작을수록 더 정밀한 측정을 수행하여야 하고, 더 많은 계산을 수행하여야 하므로, 시스템에 더 많은 부하를 주게 된다.

5. 결 론

본 논문에서는 집합 트래픽 흐름의 관점에서 고속의 인터넷 백본상에서 네트워크 공격의 징후를 감지하기 위한 방법을 제안하였다. 이를 위하여 네트워크 공격의 형태를 정의하고, 고속의 인터넷 백본 라우터에서 직접 수집한 패킷들에서 이들 네트워크 공격 패킷들을 분류하여 내고, 이로부터 네트워크 공격 트래픽의 특성과 이들 공격 트래픽이 정상 트래픽에 어떠한 영향을 주는지를 분석하였다. 이러한 분석 결과를 통하여 네트워크 공격에 대한 징후를 감지하기 위한 척도로서 입력 트래픽의 평균 파워 스펙트럼과 패킷수-대-트래픽양에 대한 비율이 사용 가능함을 보였다. 또한, 이들 척도들을 사용하여 백본 링크상에서 네트워크 공격의 징후를 감지하기 위한 방법을 제안하였으며, 이의 적용 가능성을 실험을 통하여 보였다.

네트워크 공격의 징후를 백본망상에서 개별 패킷 또는 플로우 단위로 감지해 내는 것은 매우 큰 복잡도를 요구하며, 더욱이 계속적으로 다양하게 진화 발전해 나가고 있는 공격 메커니즘이나 도구들에 맞추어 대응하기 위한 방법론을 찾아내는 것은 한계가 있다. 그러나, 집합 트래픽 흐름을 대상으로 한 방법은 개별 패킷 또는 플로우 단위의 방법론들에 비하여 현저히 낮은 복잡도를 갖고 네트워크 공격에 대응할 수 있다. 특히, 백본망은 망운영자들에 의하여 글로벌하게 유지, 관리 운영되도록 하기 위하여 다양한 망관리 방법론들이 적용되고 있다. 트래픽 흐름에 기반한 방법론은 이러한 망관리 체계와 연동하는 것이 가능하며, 이를 통하여 전체 인터넷이 공조하는 전역 방어 인프라 체계를 갖출 수 있을 것으로 판단된다. 본 논문은 하나의 백본 링크를 대상으로 한 연구에 초점을 맞추었으나, 이를 전체적인 망 구조 차원에서 처리하고 제어하기 위한 방법론의 도출을 위한 방안으로 확장 가능할 것으로 생각하며, 이에 대한 연구는 계속 더 진행되어야 할 것으로 생각된다. 또한, 본 논문에서는 공격 징후 감지를 위한 척도들을 캡처한 데이터에서 경험적으로 추출하였다. 그러나, 다양한 네트워크 공격 형태를 반영할 수 있는 수학적인 트래픽 생성 모델을 도출해 내고 이로부터 더욱더 현실성 있는 제어 방법을 도출하는 것에 대하여도 더 연구가 되어야 할 것으로 생각된다.

참 고 문 헌

[1] K. Houle and J. Weaver, "Trends in Denial of Service Attack Technology," CERT Coordination Center, Oct. 2001

[2] H. Kim, J. Kim, S. Bahk, and I. Kang, "Fast Classification, Calibration, and Visualization of Network Attacks on Backbone Links," Technical Report, June 2003, http://net.korea.ac.kr

[3] A. Chakrabarti and G. Manimaran, "Internet Infrastructure Security: A Taxonomy," IEEE Networks, Vol. 16, No. 6, November/December 2002, pp.13~21

[4] R. Chang, "Defending Against Flooding-Based Distributed Denial of Service Attacks : A tutorial," IEEE Communications Magazine, October 2002, pp. 42~51

[5] 유승화, 노병희 외, 차세대 인터넷으로의 전환에 대비한 데이터/음성/영상 트래픽 측정 및 분석에 관한 연구, 최종보고서, 한국전산원, 2001년 11월

[6] W.E.Leland, M.S.Taqqu, W.Willinger,, and D.V.Wilson, "On the Self Similar Nature of Ethernet Traffic (extended version)", IEEE/ACM Tr. on Networking, Volume 2, No. 1, February 1994, pp.1~15

[7] J. Beran, R. Sherman, M. S. Taqqu, and W. Willinger, "Long Range Dependence in Variable Bit Rate Video Traffic," IEEE Tr. Communications, Vol. 43, No. 2/3/4, Feb/Mar/ Apr 1995

[8] 정은선, 블룸필터를 이용한 인터넷 백본에서의 서비스 거부 공격과 스캐닝 탐지, 석사학위 논문, 아주대학교 정보통신전문대학원, 2004년 2월

[9] S.Li and C.L.Hwang, "Queue Response to Input Correlation Functions: Discrete Spectral Analysis", IEEE/ACM Tr. on Networking, Vol.1, No.5, October, 1993, pp.522~533

[10] Byeong hee Roh, Jae kyoon Kim, "Starting Time Selection and Scheduling Methods for Minimum Cell Loss Ratio of Superposed VBR MPEG Video Traffic," IEEE Tr. on Circuit and Syst. For Video Technology, Vol. 9, No. 6, September 1999

[11] 노병희, 유승화, "백본링크상에서의 네트워크 공격 트래픽 특성 분석," 한국정보과학회지 제21권 제12호, 2003년 12월

[12] R. Jain, The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling, John Wiley & Sons, Inc. 1991

[13] V. Paxon, "Fast, Approximate Synthesis of Fractional Gaussian Noise for Generating Self-Similar Network Traffic," ACM SIGCOMM Computer Communication Review, Vol. 27, Issue 5, October 1997

◐ 저 자 소 개 ◑

노 병 희

1987년 2월 : 한양대학교 전자공학과 졸업 (공학사)
1989년 2월 : 한국과학기술원 전기및전자공학과 (공학석사)
1998년 2월 : 한국과학기술원 전기및전자공학과 (공학박사)
1989년 3월~1994년 3월 : 한국통신 통신망 연구소
1998년 2월~2000년 3월 : 삼성전자
2000년 3월 : 아주대학교 정보통신전문대학원 부교수
관심분야 : 유/무선 인터넷 멀티미디어 통신 및 응용, 트래픽 제어, 유비쿼터스 네트워킹, RFID 네트워킹, 인터넷 보안
E-mail : bhroh@ajou.ac.kr