인터넷 백본망상에서 네트워크 공격 고립을 위한 전역 트래픽 제어 구조

종신회원 노 병 희*

A Global Traffic Control Architecture For Isolating Network Attacks In Highspeed Internet Backbone Networks

Byeong-hee Roh* *A Life Member*

요 약

본 논문에서는, 인터넷 백본 네트워크상에서 악성의 네트워크 공격 트래픽을 고립시킴으로서 네트워크 인프라를 보호하기 위한 트래픽 제어 방법을 제안한다. 제안된 방법은 개별 플로우 또는 개별 패킷들에 기반을 둔 기존의 방법들과 달리, 제안된 공격 탐지 및 제어 방법은 집합된 트래픽 수준에서 운영되므로 계산의 복잡성을 현저히 줄일 수 있으므로, 네트워크 공격에 대한 전역 인프라 구축에 활용 가능하다. 실험 결과는 제안된 방법에 의한 트래픽 제어가 네트워크 공격이 이루어질시 정상 트래픽과 네트워크 자원들을 적절히 보호할 수 있음을 보여준다.

Keyword: 네트워크 공격, 트래픽 제어, 자원 관리

ABSTRACT

In this paper, we propose a novel global traffic control architecture to isolate malicious network attacks and protect network infrastructure in Internet backbone networks. Unlike existing methods based on individual packets or flows, since the proposed detection and control methods are operated on the aggregate traffic level, the computational complexity can be significantly reduced, and they are applicable to develop a global defense architecture against network attacks. Experimental results show that the proposed scheme can detect the network attack symptoms very exactly and quickly and protect the network resources as well as the normal traffic flows very efficiently.

Ⅰ. 서 론

최근 들어, 다양한 네트워크 인프라 공격에 의한 인터넷 서비스의 장애를 여러 번 경험하였다. 이러한 네트워크 인프라 공격에 대응하기 위한 많은 연구들이 수행되었으나[1][3][4][12], 이들은 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 효과적일 수가 있다. 백본 링크에서 실시간으로 네트워크 공격들을 찾아내기 위한 방법들이, 예를 들어 [2], 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 다양

* 아주대학교 정보통신전문대학원 (bhroh@ajou.ac.kr)
논문번호 : 040164-0421, 접수일자 : 2004년 4월 21일
※본 연구는 과학기술부 목적기초연구(R05-2004-000-10824-0) 지원으로 수행되었음.

하게 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]. 그러나, 이러한 인프라 구조에 대한 연구는 구조에 대한 제시 단계로서 현재까지 가시화된 결과를 제공하지는 못하고 있다.

기존의 방법들은 개별 패킷 또는 플로우 단위로 공격 징후 감지를 수행하므로 매우 큰 계산상의 복잡성을 요구하고, 개별 장치 단위에서의 제어는 전역 방어 인프라 구축을 위하여 많은 데이터 교환이 요구되므로 고속의 백본망에서 적용하는 데에는 한계를 갖는다. 이러한 문제를 극복하기 위하여, 집합 트래픽 (aggregate traffic) 레벨에서 네트워크 공격 징후 감지를 위한 방법론이 제안되었다[11]. 이 논문에서는 기존의 네트워크 공격에 대응하기 위한 방법들이 개별 패킷 또는 플로우 단위로 수행되는 관점에서와 달리 트래픽 흐름의 관점에서 다루기 위한 방법론을 제시하고 있다. 본 논문에서는 이를 확장하여 네트워크 공격의 흐름을 고립시켜 정상 트래픽 흐름을 보호하고 전역 방어 인프라 구축에 적용하기 위한 트래픽 제어 방법을 제안한다

본 논문의 구성은 다음과 같다. 제2장에서는 [11]에서 제안하는 집합 트래픽 수준에서의 공격 트래픽 징후 감지 방법에 대한 개략적인 설명을 한다. 제3장에서는 제안하는 공격 트래픽 제어 방법을 설명하고, 제4장에서는 이에 대한 실험 결과를 보인다. 마지막으로, 제6장에서는 결론을 맺는다

Ⅱ. 집합 트래픽 레벨에서의 네트워크 공격 징후 감지 방법

Houle과 Weaver[1]들이 정리한 바에 의하면 대부분의 공격 도구들은 다양한 목적에 따라 발신지 및 수신지 IP 주소와 포트 번호들과 같은 IP 패킷들의 주요 속성들을 변조하고 있다. 이러한 변조 특징에 맞추어 공격 트래픽을 분류해 내는 효율적인 방법들이 제안되었고[2][6], [11]에서는 이러한 방법들을 사용하여 실제 인터넷 백본망상에서 수집한 트래픽을 분류하여, 이로부터 네트워크 공격 트래픽은 정상적인 트래픽과 매우 상이한 트래픽 특성을 갖으며, 정상 트래픽 흐름에 영향을 주어 트래픽 패턴에 변화를 주는 양상을 분석하였다. 이러한 분석 결과를 통하여, 집합 트래픽 레벨에서 네트워크 공격에 대한 징후를 감지하기 위한 척도로서 입력 트래픽의 평균 파워 스펙트럼과 패킷수-대-트래픽양에 대한 비율이 사용 가능함을 보였다. 그리고, 이들 척도들을 사용하여 백본 링크상에서 네트워크 공격의 징후를 감지하기 위한 방법을 제안하였다.

분류 척도로 사용되는 평균 파워 스펙트럼은 시간을 일정한 크기인 △로 구분하고, L△ 을 L 개의 중첩되지 않는 연속한 △들로 이루어지는 감지 구간으로 정의한다. c_n 과 v_n (n=0,1,2,…) 을 각각 n-번째 △구간에서 측정된 패킷 개수와 트래픽 양이라고 정의하고, m-번째 감지 구간 동안의 패킷 수 벡터인 $\vec{c}_m = [c_{mL}, \cdots, c_{(m+1)L-1}]$ 와 트래픽양 벡터인 $\vec{v}_m = [v_{mL}, \cdots, v_{(m+1)L-1}]$ (m=0,1,2,…) 를 각각 정의하기로 할 때, $\vec{c}_m$ 에 대한 평균 파워 스펙트럼은 다음과 같이 정의된다[7].

$$\bar{P}(m) = \sum_{k=0}^{L-1} \psi_{mk} \qquad (1)$$

여기에서 $\Psi_m = [\phi_{m0}, \phi_{m1}, \cdots, \phi_{m(L-1)}]$ 는 $\vec{c}_m$에 대한 DFT(discrete-time Fourier transform)를 통하여 구해진다. 즉, $\Psi_m = L^{-2}\left| DFT(\vec{c}) \right|^2$. 평균 파워 스펙트럼은 네트워크 공격에 의한 자기유사성[5]의 영향을 반영한 척도이다.

또 다른 분류 척도로서, m-번째 감지 구간에서의 패킷수-대-트래픽양의 비율은 다음과 같이 정의된다.

$$\bar{R}(m) = \frac{\vec{c}_m \cdot \vec{e}}{\vec{v}_m \cdot \vec{e}} \qquad (2)$$

여기에서 $\vec{e} = [1, 1, \cdots, 1]^T$이고, $[\cdot]^T$는 전치 행렬(transpose matrix)을 의미한다. 이것은 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 되는 상황에 대한 관찰을 통하여 도출되었다.

$x_p(m)$과 $x_r(m)$을 각각 m-번째 감지 구간에서 측정된 평균 파워 스펙트럼과 패킷수-대-트래픽

양 비율에 대한 가중치 평균들이라고 할때, 이들은 다음과 같이 나타내어 진다.

$$x_p(m+1) = \alpha_p x_p(m) + (1-\alpha_p)\overline{P}(m) \quad (3)$$

$$x_r(m+1) = \alpha_r x_r(m) + (1-\alpha_r)\overline{R}(m) \quad (4)$$

여기에서 α_p 와 α_r 은 가중치 상수로서 0과 1사이의 값을 갖는다.

$\overline{P}(m)$ 과 $\overline{R}(m)$에 대한 최대 허용치를 각각 δ_p와 δ_r 라 할 때, $x_p(m)$ 과/또는 $x_r(m)$이 각각 허용치 δ_p 와 δ_r 를 초과하는 경우를 네트워크 공격 징후의 가능성이 있는 것으로서 가정할 수 있다. 이러한 네트워크 공격 징후를 감지해내기 위하여 공격의 징후가 전혀 없는 상태인 정상 상태 (NORMA), 공격 징후의 가능성은 있으나 완전한 공격 징후 결정이 이루어지기 이전의 경계 상태 (ALERT), 그리고 공격이 이루어지는 것으로 판단되는 상태인 공격 상태 (ATTACK)의 세가지 상태를 정의하기로 하고, 이들 상태들간의 천이를 그림 1에 나타내었다.

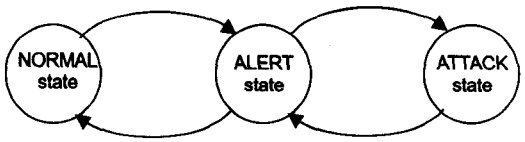


그림 1. 공격 징후 감지를 위한 상태들간의 천이도

이들 상태들을 고려한 네트워크 공격 징후 감지를 위한 알고리즘은 다음과 같다.

<variables>

attack_count : 공격의 정도를 나타내는 계수

Alert_Threshold : ALERT와 ATTACK 상태들간의 천이를 결정하기 위한 임계값

Attack_Threshold : attack_count의 최대값

state : 알고리즘의 현재 상태

<main algorithm>

매 감지 구간의 끝에서 식 (3)과 (4)를 사용하여 x_p 과 x_r을 산출하고, 산출된 이들 값들을 고려하여 이 감지 주기에서의 상태를 다음과 같은 절차에 의하여 결정한다.

```
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
```

Ⅲ. 네트워크 공격 제어를 위한 전역 트래픽 제어 구조

앞 절에서의 공격 트래픽 징후 감지 방법을 적용하여 공격 트래픽을 고립시킴으로써 네트워크 인프라 자원을 보호하기 위한 전역 트래픽 제어 구조를 그림 2에 나타내었다.

인터넷 백본 망은 백본망으로의 패킷 유입과 유출을 담당하는 에지 라우터들과 백본망 내부의 내부 라우터들로 구성된다. 에지 라우터들이 백본망으로의 각 입력 링크에 대하여 작용하는 동작 메커니즘을 그림 3에 나타내었다. 각 에지 라우터는 각 입력 링크별로 패킷 필터부(packet filter unit)와 집합 트래픽 감시부(aggregate traffic monitor)를 채용한다. 링크상에 입력되는 패킷들에 대하여 패킷 필터부는 패킷 필터 테이블에 따라 패킷에 대한 필터를 수행한다. 패킷 필터 테이블에는 필터링할 공격 플로우들에 대한 리스트들을 보유하는데, 이 리스트들은 전역 감지 네트워크(global detection network)의 전역 감지 시스템(global detection system)으로부터 제공된다. 이와 같이 1차적으로 필터된 패킷들의 집합 트래픽을 대상으로 앞 절에서의 방법을 사용한 네트워크 공격 징후 감지가 이루어진다. 초기 상태에는 패킷 필터 테이블에는 아무런 리스트가 없으므로, 필터된 집합 트래픽은 패킷 필터부로 유입되는 트래픽과 동일함에 주의한다. 이때, 공격이 감지된 경우에는 전역 감지 네트워크(global detection network)로 모든 패킷들을 우회 루팅시키고, 정상 트래픽의 경우에는 백본 네트워크로 정상 라우팅 절차에 의하여 포워딩 시킨다.

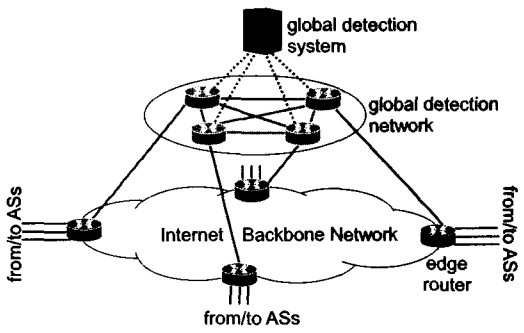


그림 2. 공격 트래픽 제어를 위한 네트워크 구조

전역 탐지 네트워크상에서도 패킷의 목적지 주소에 따른 포워딩이 이루어지나 백본망에서의 패킷 포워딩의 우선 순위가 더 높게 처리된다. 즉, 백본망의 출력 에지 라우터에서는 백본망을 통하여 전달된 패킷들의 포워딩을 우선적으로 처리하고, 여유가 있을 경우에 전역 탐지 네트워크로부터 전달되는 패킷들의 포워딩을 수행한다. 전역 탐지 시스템(global detection system)은 전역 탐지 네트워크로 유입되는 트래픽들을 대상으로 [2] 또는 [6]과 같은 플로우 레벨의 공격 검출 방법을 적용하여 공격 플로우들을 검출해낸다. [2] 와 [6]에서는 플로우를 < 발신지 IP 주소, 목적지 IP 주소, 목적지 포트 번호 >로서 정의하고 있다. 이와 같이 검출된 플로우 정보를 모든 에지 라우터들의 패킷 필터 테이블에 반영하여 공격 플로우들에 대한 패킷 필터링이 이루어지도록 한다.

제안된 공격 트래픽 제어 구조에서는 집합 트래픽 수준에서 한 링크상의 공격 징후의 여부를 감지하고, 공격 징후가 감지된 링크들에 대하여만 전역적인 공격 플로우 검출이 전역 감지 네트워크내에서 이루어진다. 또한, 전역 탐지 시스템에 의하여 검출된 공격 플로우들은 모든 에지 라우터들의 패킷 필터 테이블에 반영되어 해당 공격 플로우에 해당하는 패킷들이 제거된다. 그리고, 이와 같이 1차적으로 필터링된 후의 트래픽을 대상으로 공격 징후 감지가 이루어지므로, 공격 징후 감지를 위하여 적용되는 트래픽양이 줄어드는 효과를 갖는다. 따라서, 시간이 지날수록 각 에지 라우터와 연결된 입력 링크들과 전역 감지 네트워크상에서의 공격 징후 감지를 위한 계산상의 복잡성은 점차 감소하게 될 것이 예상된다. 반면에, 모든 에지 라우터단에서 공격 검출과 필터링을 개별적으로 수행하는 방법들의 경우는 시간에 관계없이 동일한 계산의 복잡성을 보이게 되며, 전역적인 공격 감지 체계 구축을 위하여는 더 많은 데이터 교환과 계산의 복잡성이 요구

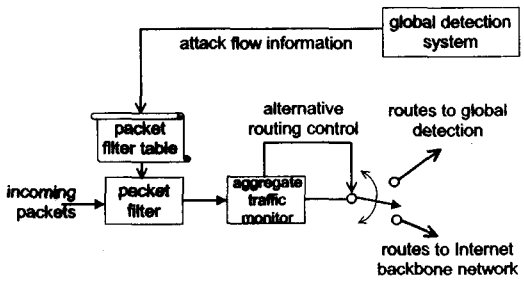


그림 3. 에지 라우터에서의 동작 메커니즘

될 것이다. 이러한 관점에서 볼 때, 제안된 공격 트래픽 제어 구조는 기존의 방법론들에 비하여 네트워크 공격에 더 효율적으로 대처 가능한 방법론을 제공 가능하다.

Ⅳ. 실험 결과

제안된 트래픽 제어 방법의 성능 실험을 위하여 ns-2 (network simulator version 2)[10]를 사용하였으며, 적용된 네트워크 구조를 그림 4에 나타내었다. 백본 네트워크는 에지 라우터들인 ER1, ER2, ER3로 구성되어 있으며, 전역 탐지 네트워크는 라우터 D1, D2로 구성되어 있다. 라우터 R1은 백본 네트워크 외부망의 라우터이다. 단말 N1과 단말 N2는 목적지를 S로 하는 정상 패킷들을 발생시키고 단말 A는 단말 S를 대상으로 하는 공격 패킷들을 생성시키도록 하였다. 정상 트래픽은 Hurst 파라메터값은 0.9, 공격 트래픽은 Hurst 파라메터값이 0.99가 되도록 하여 [9]에서 제안된 방법을 사용하여 발생시켰다. 정상 트래픽의 경우, 발생 패킷수의 평균은 9080.97 패킷/초가 되도록 하였으며, 공격 트래픽의 발생 패킷수의 평균을 달리해 가면서 실험을 수행하였다. 이때, 각 발생된 패킷의 크기 분포는 정상 트래픽과 공격 트래픽 모두 [8]의 결과가 반영되도록 하였다.

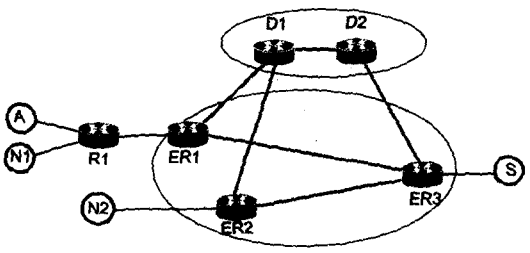


그림 4. 실험 네트워크 구조

제안한 트래픽 제어 구조의 효율성을 보일수 있도록 하기 위하여 다음과 같은 시나리오들을 설정하였다. 모든 시나리오들에서 단말 N2로 부터의 패킷들은 ER2와 ER3를 경유하여 S에 도달한다. ER3에서의 큐잉은 CBQ (class-based queueing) 방식을 사용하도록 하였고 ER1과 ER2로 부터의 링크는 같은 우선 순위를 부여하였고 D2로 부터의 링크보다는 더 높은 우선 순위를 갖도록 하였다.

- 시나리오 1 : 단말 N1과 A의 모든 패킷들은 D1, D2를 경유하지 않고 모두 ER1과 ER3를 통하여 S에 도달한다.
- 시나리오 2 : 단말 A와 단말 N1의 모든 패킷들은 ER1에서 D1으로 우회되어 D2를 거쳐 ER3를 통하여 S에 도달한다.
- 시나리오 3 : 단말 A의 패킷들은 ER1에서 필터링되고, N1은 ER1을 거쳐 ER3를 통하여 S에 도달한다.

시나리오 1은 공격 징후와 트래픽 제어가 적용되지 않은 경우의 패킷 포워딩 결과에 해당하며, 시나리오 2는 링크에서의 공격 징후가 감지되어 우회 루팅되는 경우로서, 전역적인 공격 플로우가 검출되지 않은 경우에 해당한다. 그리고, 시나리오 3은 공격 플로우가 검출되어 에지 라우터에서 필터링이 수행되는 경우에 해당한다.

그림 5는 이러한 세가지 시나리오에 대하여 각 단말들로 부터의 패킷들의 손실율을 보여준다. 실험을 위하여, 각 링크의 대역폭은 100 Mbps, 큐의 길이는 200 패킷 크기로 설정하였다. 또한, 노드 N1과 N2로 부터의 정상 트래픽 양은 고정시켰고, 노드 A로 부터의 공격 트래픽의 양은 변화 시켰다. 그림 5의 수평축은 전체 정상 트래픽의 평균 패킷 발생율의 평균에 대한 공격 트래픽의 평균 패킷 발생율의 비율을 나타낸다. 그림 5에서 볼수 있듯이, 시나리오 1의 경우에, 공격 트래픽이 증가함에 따라 노드 N1과 N2들로 부터의 패킷 손실율은 함께 증가하는 현상을 보여준다. 특히 N2의 패킷 손실율이 N1의 패킷 손실율에 비하여 다소 커지는 결과를 보여주는데, 이것은 모든 노드들 A, N1과 N2로 부터의 패킷들이 ER3로 직접 전달되어 ER3가 FCFS 방식에 의하여 패킷들을 처리하게 되므로, ER2로 부터의 패킷률이 ER1으로 부터의 패킷률에 비하여 작게 될 것이므로, 각 링크에 대하여 동일한 비율로 패킷들이 손실될 때, N2로 부터의 패킷 손실율이 더 커지게 되는 것에서 기인하는 것으로 판단되어진다. 그러나, 시나리오 2의 경우에는, N2 패킷들의 손실율은 시나리오 1의 경우 보다 매우 낮은 수준에서 거의 일정하게 유지되지만, N1 패킷들의 손실율은 크게 증가하고, 시나리오 1의 경우보다 훨씬 더 커지게 됨을 볼 수 있다. 이것은 N1 패킷들이 공격으로 감지되어 D1 라우터로 공격 패킷들과 함께 우회 라우팅되어 ER3에 전달되지만, ER3는 백본망으로 부터의 패킷들에 우선순위를 두어 처리를

하게 되기 때문이다. 즉, N2 패킷들 입장에서는 시나리오 1에 비하여 N1 패킷들이 거의 없는 것과 같은 상태에서 서비스를 받게 되므로, 손실율이 더 낮아지게 되나, N1 패킷들은 우선 순위 처리에서 불이익을 받게되어 이들 성능이 크게 악화되는 결과를 보이게 된다. 시나리오 3의 경우에는 N2 패킷들의 손실율은 공격 트래픽이 없을 때의 시나리오 1의 결과와 매우 유사한 결과를 보여준다.

그림 6에는 그림 5에서 구한 각 노드 N1과 N2에 대한 시나리오별 패킷 손실율의 평균값을 구하여, 시나리오에 따라 패킷 손실율이 어떻게 변화하고 있는지를 나타내었다. 시나리오 1의 경우에는 공격 트래픽이 부가되었으나, 공격에 대한 감지가 이루어지기 전의 상황으로서, N1과 N2의 패킷 손실율은 공격이 없는 경우에 비하여 거의 유사한 비율로 증가하면서 패킷 손실의 영향을 받게 된다. 그러나, 시나리오 2에서 공격에 대한 감지가 이루어진 경우에는 N1의 패킷 손실율이 급격하게 커지고, N2의 패킷 손실율은 급격히 작아진다. 시나리오 3의 전역 감지 네트워크로 부터 공격에 대한 플로우가 감지되어 공격에 대한 필터링이 이루어지는 상태가

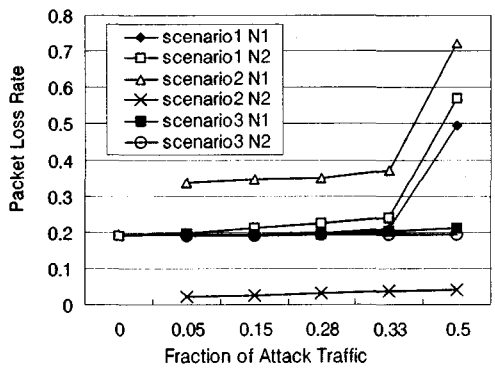


그림 5. 패킷 손실율

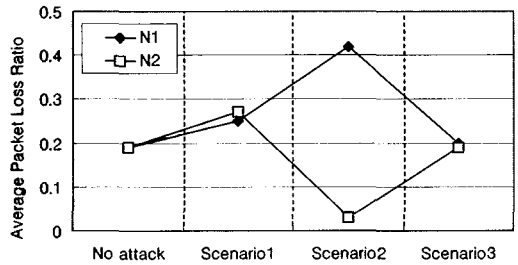


그림 6. 시나리오에 따른 평균 패킷 손실율 변화 추이

되면서 N1과 N2의 패킷 손실율은 공격이 없을때의 수준으로 다시 회복됨을 볼 수 있다. 이와 같이, 패킷 손실 측면에서 볼 때 제안 트래픽 제어 구조는 공격이 감지된 경우, 공격이 이루어지지 않은 링크들로 부터의 트래픽들에 대하여는 공격의 영향을 받지 않도록 보호하면서, 점차적으로 공격을 받은 링크에 대하여도 정상 트래픽들에 대하여는 동일한 수준의 보호를 제공하게 됨을 알 수 있다.

그림 5와 그림 6의 결과들로부터, 제안된 전역 트래픽 제어 구조는 공격 트래픽의 유입시 백본망 상에서 정상 트래픽들을 매우 효율적으로 보호 가능함을 알수 있다. 즉, 공격 트래픽이 링크에 유입될 때, 전역 감지 시스템이 이들 공격들을 분류해 내기 전까지의 짧은 시간동안에는 해당 링크상의 정상 트래픽의 경우 성능 저하가 발생하지만, 공격 트래픽이 없는 링크들로 부터의 정상 트래픽들은 성능 저하없이 패킷 전달이 가능하다. 그러나, 이러한 공격 트래픽이 부가된 링크상의 정상 트래픽들의 일시적인 성능 저하는 전역 감지 시스템과 에지 라우터간의 패킷 필터 테이블 구축에 의하여 신속하게 회복된다. 이와 같이, 제안된 전역 트래픽 제어 구조는 공격 트래픽들을 고립시키는 것 뿐만 아니라, 정상 트래픽을 공격 트래픽으로부터 잘 보호할 수 있음을 알 수 있다.

V. 결 론

본 논문에서는 인터넷 백본 네트워크상에서 악성의 네트워크 공격 트래픽을 고립시킴으로서 네트워크 인프라를 보호하기 위한 트래픽 제어 방법을 제안하였고, 이의 적용시의 효율성을 실험을 통하여 보였다.

네트워크 공격의 징후를 백본망상에서 개별 패킷 또는 플로우 단위로 감지해 내고 제어하는 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. 백본망은 망운영자들에 의하여 글로벌하게 유지, 관리 운영되도록 하기 위하여 다양한 망관리 방법론들이 적용되고 있다. 본 논문의 트래픽 흐름에 기반한 트래픽 제어 방법론과 이러한 망관리 체계와 연동하게 함으로써

전체 인터넷이 공조하는 더 효율적인 전역 방어 인프라 체계를 갖출 수 있을 것이다. 이와 같은 망관리 구조와 연동하기 위한 방법론에 대한 연구는 더 진행되어야 할 것으로 생각된다. 또한, 제안한 방법론의 효율성을 높이기 위하여는 전역 감지 네트워크내에서의 공격 플로우 검출이 매우 정확하고 효율적으로 이루어져야 할 것이다. 본 논문에서는 기존의 링크 단위의 공격 플로우 검출 방법론이 전역 감지 네트워크내에서 전체 트래픽 단위로 이루어지는 것을 가정으로 하였으나, 실제로 이러한 방법을 제공하기 위한 구체적인 방법에 대한 연구도 필요하다.

참 고 문 헌

[1] K. Houle and J. Weaver, "Trends in Denial of Service Attack Technology," CERT Coordination Cen-ter, 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, available at http://net.korea.ac.kr, June 2003.

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

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

[7] S. L. Marple, Digital Spectral Analysis With Applications, Prentice-Hall, Inc., 1987

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

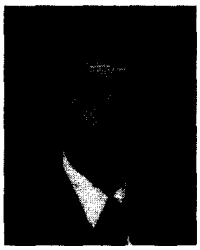
[9] V. Paxon, "Fast, Approximate Synthesis of Fractional Gaussian Noise for Generating Self-Similar Network Traffic," ACM SIGCOMM Computer Communication Review, Vol. 27, Is-sue 5, October 1997

[10] The network simulator version-2, ns-2, http://www.isi.edu/nsnam/ns/

[11] Byeong-hee Roh, "A Novel Detection Methodology Of Network Attack Symptom At Aggregate Traf-fic Level On Highspeed Internet Backbone Links," ICT2004, Brazil, August 2004.

[12] 정유석, 홍만표, 대규모 인프라 공격에 대한 방어 기술의 발전 동향, 정보과학회지, 제21권 제12호 2003년 12월

노 병 희(Byeong-hee Roh) 종신회원



1987년 2월 : 한양대학교 전자공학과 졸업

1989년 2월 : 한국과학기술원 전기및전자공학과 석사

1998년 2월 : 한국과학기술원 전기및전자공학과 박사

1989년 3월~1994년 3월: 한국통신 통신망 연구소

1998년 2월~2000년 3월: 삼성전자

현재 아주대학교 정보통신전문대학원 조교수

<관심분야> 유/무선 인터넷 멀티미디어 통신 및 응용, 트래픽 제어, 유비쿼터스 네트워킹, RFID 네트워킹