고속 인터넷 백본망에서의 분산형 서비스 거부 공격 탐지 방법

정회원 김 선 호*, 정회원 윤 명 철**, 종신회원 노 병 희***

Distributed Detection of DDoS Attack Symptoms in Highspeed Backbone Networks

Sun Ho Kim*, Myungchul Yoon** *Regular Members*, Byeong-hee Roh*** *Lifelong Member*

요 약

분산형 서비스 거부 (DDoS) 공격들에 대한 징후 감지는 산상의 복잡성과 컴퓨팅 자원을 요구한다. 본 논문에서는 고속의 백본망에서 DDoS 공격 징후를 효율적으로 감지해 낼수 있는 방법을 제안한다. 본 논문에서 제안하는 방법은 기존의 개별 패킷 또는 플로우 단위의 방법들과 달리 집합 트래픽 흐름의 관점에 기반을 두고 있다. 이럼으로써, 제안된 방법은 매우 낮은 계산량으로 수행될수 있어, 고속의 백본망에서 적용 가능하다.

Keyword : 네트워크 공격, 트래픽 특성, DDoS 탐지

ABSTRACT

It might be more efficient that detections of distributed denial of service (DDoS) attacks are done in backbone domain than in individual local networks or links. However, because existing schemes for detecting DDoS attack symptoms have been focused on individual packets or flows, they require much higher computational complexities. In this paper, we propose an efficient method to detect DDoS attack symptoms in backbone networks. Unlike conventional schemes focused on individual packets or flows, the proposed method is carried at aggregate traffic level. So, our proposed schemes can be operated with very lower computational complexity, and can be run in very high-speed backbone networks.

Ⅰ. 서 론

네트워크 인프라 공격에 대응하기 위한 많은 연구들이 수행되었으나[1][2][3][4], 이들 방법들은 대부분 개별 망 단위에서 의심스러운 패킷들 또는 플로우들을 분류하고 필터링하는 방법론에 초점이 맞추어지고 있으므로, 매우 큰 계산상의 복잡성과 컴퓨팅 자원을 요구한다. 따라서, 이들 방법들을 고속의 인터넷 백본망에 적용하기에는 적합하지 않다. 이들 기존 방법론들의 문제를 해결하기 위하여 Roh등[5]은 개별 패킷 또는 플로우 단위가 아닌 집합된 트래픽 단위에서 네트워크 공격의 징후를 탐지하는 방법을 제안하여 복잡성과 계산량을 현저히 줄임으로써 고속의 백본 링크에 적용가능하도록 하였다. 그러나, 이 방법은 단일 링크단에서만 공격 징후 탐지가 가능하여, 공격의 유형을 전체 백본망 단위에서 찾아내어 이에 대한 대응책을 제공하는데는 한계를 갖는다.

※ 본 연구는 한국학술진흥재단 지역대학우수과학자지원사업(D00640, R05-2004-000-10824-0)의 지원으로 수행되었음.
* 대우일렉 IS연구소 (shkim11@dwe.co.kr) ** 단국대학교 (천안캠퍼스) 전자공학과 (myoon@dankook.ac.kr)
*** 이주대학교 정보통신전문대학원 (교신저자: bhroh@ajou.ac.kr)
논문번호 : KICS2006-09-382, 접수일자 : 2006년 9월 1일, 최종논문접수일자 : 2006년 2월 10일

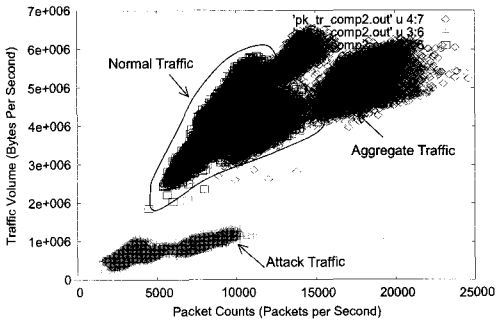
본 논문에서는 Roh등[5]이 제안한 단일 링크단에서의 공격 징후 탐지 방법을 확장하여 고속의 백본망 단위에서 네트워크 공격 징후를 탐지하기 위한 방법을 제안한다. 제안하는 방법은 백본망 단위에서 이루어지므로 네트워크 공격의 징후뿐만이 아니라, 공격의 유형까지도 탐지 가능하다.

본 논문의 구성은 다음과 같다. 제2장에서는 네트워크 공격 트래픽의 특성에 대하여 대하여 기술한다. 제3장에서는 제안하는 방법을 설명하고, 제4장에서는 이에 대한 실험 결과를 보인다. 끝으로, 제5장에서는 본 논문의 결론을 맺는다.

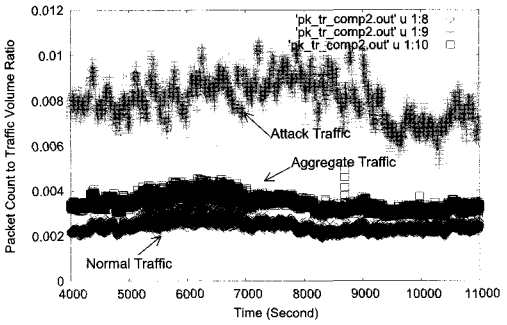
Ⅱ. 네트워크 공격 트래픽 특성[5]

Houle 등[1]이 정리한 바에 의하면 대부분의 공격 도구들은 다양한 목적에 따라 발신지 및 수신지 IP 주소와 포트 번호들과 같은 IP 패킷 들의 주요 속성들을 변조하고 있다. Kim등[2]은 이러한 변조 특징에 맞추어 공격 트래픽을 분류해 내는 효율적인 방법을 제안하였고, 논문 [5]에서는 이 방법을 사용하여 실제 인터넷 백본망상에서 수집한 트래픽에 적용하여 네트워크 공격 트래픽의 패턴을 분석하였다. 캡쳐한 패킷들중에서 공격의 특성을 갖고 있는 패킷들만을 모아 구성한 패킷열을 공격 트래픽(attack traffic), 공격 트래픽이 아닌 패킷들만을 모아 구성한 패킷열을 정상 트래픽 (normal traffic), 그리고 원래의 캡쳐한 패킷열을 집합 트래픽(aggregate traffic)이라고 정의하였다.

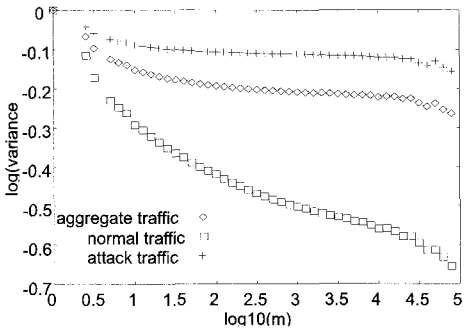
여러 트래픽 특성들중에서 각 유형별 트래픽들의 1초동안 발생된 패킷수와 트래픽양들간의 관계를 그림 1에 나타내었다. 그림 1(a)는 전체적인 관점에서 보인 상관관계를 보여주는데, 정상 트래픽에 공격 트래픽이 부가된 집합 트래픽에서는, 트래픽 양의 변화 비율보다 패킷수의 변화 비율이 더 크게 나타나고 있다. 또한, 그림 1(b)에는 특히 공격 트래픽이 많이 발생한 시간 구간동안을 선택하여 시간에 따른 트래픽양에 대한 패킷 개수의 비율(CVR, count-to-volume ratio)의 변화 특성을 나타내었는데, 전체 트래픽에서의 이 비율이 정상 트래픽에서의 비율에 비하여 매우 크게 변화됨을 볼 수 있다. 일반적으로 공격 트래픽양은 정상 트래픽양에 비하여 작아서 집합 트래픽의 흐름에서 공격의 패턴을 찾아내는 것은 쉽지 않을 수도 있다. 그러나, 그림 1 에서와 같이 패킷의 수를 트래픽의 양과 함께 고려함으로써, 공격에 의한 트래픽의 변화 징후를 감지해내는 것이 가능하게 된다.



(a) 트래픽 유형별 패킷수와 트래픽양간의 관계



(b) CVR 변화 특성



(c) 자기유사성 특성

그림 1. 네트워크 공격 트래픽 특성

공격 트래픽의 자기유사(self-similar) 특성을 그림 1(c)에 나타내었다. 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, Husrt 파라메터가 큰 트래픽은 평균 비트율, 네트워크 부하의 동일한 환경에서 링크 이용율, 소통율, 손실율등과 같은 네트워크 성능에 더 큰 영향을 미치게 된다[11]. 이러한 자기 유사

특성이 네트워크 공격 트래픽에 의하여 어떠한 영향을 미치는지를 보이기 위하여 variance time plot(VTP) 방법[6]을 사용하여 구한 Hurst 파라메터들을 그림 1(c)에 나타내었다. 그림1(c)에 보인 바와 같이, 공격 트래픽이 정상 트래픽 보다 더 큰 자기 유사 성질을 갖음을 알수 있다. 또한, 전체 트래픽의 자기 유사성은 공격 트래픽의 추가에 의하여 증가됨을 알수 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 피해뿐만 아니라, 전체적인 네트워크의 성능에 직접적인 피해를 가중시키게 된다.

Ⅲ. 백본망에서의 DDoS 공격 탐지 방법

본 장에서는 본 논문에서 제안하는 백본망 단위에서 DDoS 공격을 효율적으로 탐지하기 위한 방법에 대하여 설명한다.

3.1 네트워크 시스템 모델

본 논문에서 고려하는 네트워크 모델은 그림 2와 같다. N개의 edge router들 E_0, E_1, …, E_{N-1} 이 백본에 연결되어 있으며, 각 라우터들은 다른 라우터들로 전달되는 트래픽에 대한 정보를 global detection system (GDS)에 제공한다. 라우터들이 제공하는 트래픽 정보와 이를 사용하여 GDS가 공격을 감지해 내는 방법은 다음에서 설명하기로 한다.

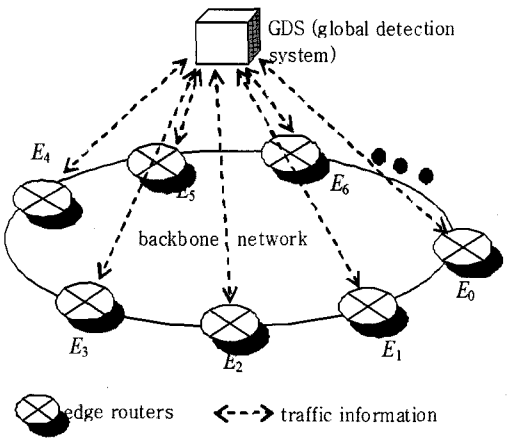


그림 2. 네트워크 모델

3.2 백본망 단위의 확장된 DDoS 징후 탐지 방법

3.2.1 공격 징후 탐지 알고리즘

본 논문에서 제안하는 백본망 단위의 공격 징후 탐지 알고리즘은 [5]에서 제안한 단일 링크 단위의 방법을 확장한 것이다. 제안 하는 방법은 [5]에서와 같이 집합 트래픽에 대한 측정을 기반으로 한다.

트래픽 측정을 위하여 시간을 일정한 크기인 △로 구분하기로 한다. 이로부터, c_n^{ij}와 v_n^{ij} (i,j=0,1, 2,…,N-1)를 각각 n-번째 △ 구간에서 측정된 E_i 에서 E_j로 전달되는 패킷 개수와 트래픽 양이라고 정의하기로 한다. 감지구간을 L개의 중첩되지 않는 연속한 △들로 이루어진 시간 구간으로 정의할 때, m-번째 감지구간에서의 L개의 중첩되지 않는 c_n^{ij}와 v_n^{ij}들로 각각 이루어진 벡터들인 $\vec{c}^{ij}(m)$과 $\vec{v}^{ij}(m)$을 다음과 같이 정의하기로 한다.

$$\vec{c}^{ij}(m)=\left[c_{mL}^{ij},\cdots,c_{(m+1)L-1}^{ij}\right] \quad (1)$$

$$\vec{v}^{ij}(m)=\left[v_{mL}^{ij},\cdots,v_{(m+1)L-1}^{ij}\right] \quad (2)$$

이로부터 평균 파워 스펙트럼 $\overline{P}^{ij}(m)$과 CVR $\overline{R}^{ij}(m)$이 구해진다.

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

$$\overline{R}^{ij}(m)=\frac{\vec{c}^{ij}(m)\cdot\vec{e}}{\vec{v}^{ij}(m)\cdot\vec{e}} \quad (4)$$

여기에서 $\Psi_m^{ij}=\left[\phi_{m0}^{ij},\phi_{m1}^{ij},\cdots,\phi_{m(L-1)}^{ij}\right]$ 는 $\vec{c}^{ij}(m)$에 대한 DFT(discrete-time Fourier transform)를 통하여 구해진다. 즉, $\Psi_m^{ij}=L^{-2}\left|DFT(\vec{c}^{ij}(m))\right|^2$. 또한, $\vec{e}=[1,1,\cdots,1]^T$이고, $[\cdot]^T$는 전치 행렬(transpose matrix)을 의미한다.

$x_P^{ij}(m)$과 $x_R^{ij}(m)$을 각각 m-번째 감지구간에서 측정된 평균 파워 스펙트럼과 CVR에 대한 가중치 평균들이라고 할때, 이들은 다음과 같이 나타내어진다.

$$x_P^{ij}(m)=\alpha_P^{ij}\cdot x_P^{ij}(m-1)+(1-\alpha_P^{ij})\overline{P}^{ij}(m) \quad (5)$$

$$x_R^{ij}(m)=\alpha_R^{ij}\cdot x_R^{ij}(m-1)+(1-\alpha_R^{ij})\overline{R}^{ij}(m) \quad (6)$$

여기에서 α_P^{ij}와 α_R^{ij}은 가중치 상수로서 0과 1사이의 값을 갖는다.

m-번째 감지구간에서의 $\overline{P}^{ij}(m)$과 $\overline{R}^{ij}(m)$에 대한 최대 허용치를 각각 $\delta_P^{ij}(m)$과 $\delta_R^{ij}(m)$이라 하기로 한다. 이때, $x_P^{ij}(m)$과/또는 $x_R^{ij}(m)$이 각각 허용치 $\delta_P^{ij}(m)$과 $\delta_R^{ij}(m)$을 초과하는 경우를 네트워크 공격 징후의 가능성이 있는 것으로서 가정할 수 있으며, 이러한 네트워크 공격 징후를 감지해내기 위하여 공격의 징후가 전혀 없는 상태인 정상 상태 (NORMAL), 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 천이 관계를 그림 3에 나타내었다.

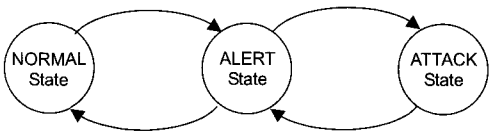


그림 3. 공격 탐지를 위한 상태들간의 천이 관계 다이어그램

$s^{ij}(m)$과 $a^{ij}(m)$을 m-번째 감지구간에서 에지 라우터 E_i 에서 E_j 로 가는 트래픽에 대한 상태값과 공격카운터(attack counter)으로 각각 정의하기로 한다. 상태값은 그림 3에서의 정상상태, 경계상태, 공격상태중의 하나가 될수 있다. 공격카운터값은 이전 감지구간에서의 상태값인 $s^{ij}(m-1)$과 현 감지구간에서의 $x_P^{ij}(m)$과 $x_R^{ij}(m)$에 따라 증가 또는 감소하게 되며, 공격카운터의 크기에 따라 상태가 결정된다. 상태값과 공격카운터를 사용하여 네트워크 공격 징후 감지를 위한 알고리즘을 다음에 나타내었다.

<variables>

$a^{ij}(m)$: m-번째 감지구간에서의 공격카운터

$s^{ij}(m)$: m-번째 감지구간에서의 상태

Alert_Threshold : ALERT와 ATTACK 상태들간의 천이를 결정하기 위한 임계값

Attack_Threshold : 공격카운터의 최대값

<main algorithm>

m-번째 감지구간의 끝에서 식 (5)와 (6)을 사용하여 $x_P^{ij}(m)$과 $x_R^{ij}(m)$을 산출하고, 이 값들을 고려하여 이 감지구간에서의 상태를 다음과 같은 절차에 의하여 결정한다.

```
if (s^ij(m-1)==NORMAL)
  if ((x_P^ij(m)>δ_P^ij(m) AND x_R^ij(m)≤δ_R^ij(m)) OR
      (x_P^ij(m)≤δ_P^ij(m) AND x_R^ij(m)>δ_R^ij(m)) )
        s^ij(m) = ALERT;
        a^ij(m)=a^ij(m-1)+ 1;
  elseif (x_P^ij(m)>δ_P^ij(m) AND x_R^ij(m)>δ_R^ij(m) )
        s^ij(m) = ALERT;
        a^ij(m)=a^ij(m-1)+ 2;
  endif
elseif (s^ij(m-1)==ALERT )
  if ((x_P^ij(m)>δ_P^ij(m) AND x_R^ij(m)≤δ_R^ij(m)) OR
      (x_P^ij(m)≤δ_P^ij(m) AND x_R^ij(m)>δ_R^ij(m)) )
        a^ij(m)=a^ij(m-1)+1;
  elseif (x_P^ij(m)>δ_P^ij(m) AND x_R^ij(m)>δ_R^ij(m) )
        a^ij(m)=a^ij(m-1)+ 2;
  elseif (x_P^ij(m)≤δ_P^ij(m) AND x_R^ij(m)≤δ_R^ij(m))
        a^ij(m)=a^ij(m-1)- 2;
  else
        a^ij(m)=a^ij(m-1)-1;
  endif

  if (a^ij(m)>Alert_Threshold )
        s^ij(m)=ATTACK;
  elseif (a^ij(m) ≤ 0 )
        s^ij(m)=NORMAL;
        a^ij(m)=0;
  endif
elseif (s^ij(m-1)==ATTACK )
  if (x_P^ij(m)>δ_P^ij(m) AND x_R^ij(m)>δ_R^ij(m) )
        a^ij(m)=MIN ( a^ij(m-1)+1,
                      Attack_Threshold );
  elseif (x_P^ij(m)≤δ_P^ij(m) AND x_R^ij(m)≤δ_R^ij(m))
        a^ij(m)=a^ij(m-1)-2;
  else
```

$a^{ij}(m)=a^{ij}(m-1)$-1;

endif

if ($a^{ij}(m) \leq$Alert_Threshold)

$s^{ij}(m)$=ALERT ;

endif

endif

3.2.2 행렬 $A(m)$과 $S(m)$

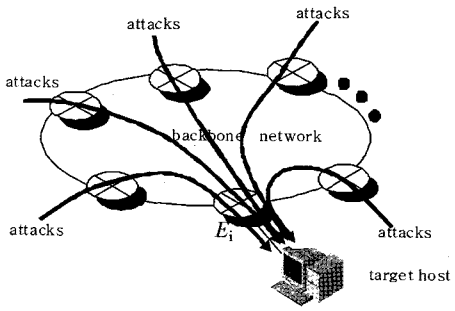
m-번째 감지구간에서의 $a^{ij}(m)$과 $s^{ij}(m)$을 요소로 하는 다음과 같은 NXN 크기의 공격카운터 행렬 $A(m)$과 상태 행렬 $S(m)$을 정의하기로 한다.

$$A(m)=[a^{ij}(m)],\ m=1,2,...,\ i,j=0,1,,..,N-1 \quad (7)$$

$$S(m)=[s^{ij}(m)],\ m=1,2,...,\ i,j=0,1,,..,N-1 \quad (8)$$

행렬 $A(m)$과 상태 행렬 $S(m)$을 통하여 다음과 같은 두가지 유형의 공격 형태의 구별이 가능하다.

■목표집중형 공격 유형의 감지



(a) 트래픽 플로우

$$A(m)=\begin{bmatrix} a^{0,0} & \cdots & a^{0,i-1} & a^{0,i} & a^{0,i+1} & \cdots & a^{0,N-1} \\ a^{1,0} & \cdots & a^{1,i-1} & a^{1,i} & a^{1,i+1} & \cdots & a^{1,N-1} \\ a^{2,0} & \cdots & a^{2,i-1} & a^{2,i} & a^{2,i+1} & \cdots & a^{2,N-1} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a^{N-1,0} & \cdots & a^{N-1,i-1} & a^{N-1,i} & a^{N-1,i+1} & \cdots & a^{N-1,N-1} \end{bmatrix}$$

(b) 행렬 A(m)

$$S(m)=\begin{bmatrix} 0 & \cdots & 0 & s^{0,i}=2 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & s^{1,i}=2 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & s^{2,i}=2 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & s^{N-1,i}=2 & 0 & \cdots & 0 \end{bmatrix}$$

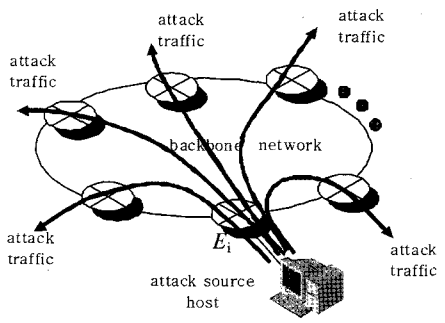
(c) 행렬 S(m) (0:정상상태, 1:경계상태, 2:공격상태)

그림 4. 목표 집중형 공격 유형

목표집중형 공격은 다수의 감염된 호스트가 목표 호스트에 장애를 일으킬 목적으로 해당 목표 호스트로 서비스를 중단 시킬 정도로 매우 많은 패킷들을 전송하는 것이다. 이러한 유형의 공격 상황에 대한 트래픽 플로우를 그림 4(a)에 나타내었다. 그림 4(a)의 경우, 공격의 목표가 되는 호스트가 라우터 E_i 에 연결되어 있으므로, 전 네트워크상의 취약 호스트들에 대한 감염이 이루어진 후에는 이들 감염 호스트들이 발생시키는 패킷들은 다른 라우터들을 통하여 E_i 라우터로 집중된다. 이경우 $A(m)$의 각 요소들 중에서 $a^{ji}(m)$ (j=0,⋯,N-1)의 값들(그림 4(b)에서 박스로 표시된 부분)이 커지게 될 것이고, 공격이 감지된 경우에는 $S(m)$의 요소들중에서 $s^{ji}(m)$ (j=0,⋯,N-1)의 값들(그림 4(c)에서 박스로 표시된 부분)은 공격상태를 나타나게 되고, 나머지 요소들은 정상상태로 나타나게 된다. 이와 같이, 행렬 $A(m)$과 상태 행렬 $S(m)$을 통하여 목표집중형 공격 유형을 감지할 수 있다.

■목표분산형 공격 유형의 감지

목표분산형 공격 유형은 그림 5(a)에서와 같이 한 호스트로부터의 공격 트래픽이 한 곳으로 집중하지 않고 모든 다른 라우터를 통하여 전달되는 상황이다. 이것은 공격 소스 호스트가 네트워크 전체에 연결된 취약 호스트들을 무작위로 찾아서 감염시키고자 할 때, 또는 공격/감염 호스트들이 네트워크를 교란시킬 목적으로 전범위의 IP 주소를 목적지로 하여 패킷들을 생성시키는 경우에 해당한다. 이 경우에는 그림 5(a)에서와 같이 한 라우터를 통하여 공격 패킷이 모든 다른 라우터들로 전달되는 상황이 나타나게 되므로, $A(m)$의 각 요소들 중에서 $a^{ij}(m)$ (^{i}=0,⋯,N-1)의 값들(그림 5(b)에서 박스로 표시된 부분)이 커지게 될 것이고, $S(m)$은 그림 5(c)와 같이 나타나게 된다.



(a) 트래픽 플로우

$$\mathbf{A}(m)=\begin{bmatrix} a^{0,0} & a^{0,1} & a^{0,2} & \cdots & a^{0,N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a^{i-1,0} & a^{i-1,1} & a^{i-1,2} & \cdots & a^{i-1,N-1} \\ a^{i,0} & a^{i,1} & a^{i,2} & \cdots & a^{i,N-1} \\ a^{i+1,0} & a^{i+1,1} & a^{i+1,2} & \cdots & a^{i+1,N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a^{N-1,0} & a^{N-1,1} & a^{N-1,2} & \cdots & a^{N-1,N-1} \end{bmatrix}$$

(b) 행렬 A(m)

$$\mathbf{S}(m)=\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \\ s^{i,0}=2 & s^{i,1}=2 & s^{i,2}=2 & \cdots & s^{i,N-1}=2 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

(c) 행렬 S(m) (0:정상상태, 1:경계상태, 2:공격상태)

그림 5. 목표 분산형 공격 유형

Ⅳ. 실험 결과

4.1 실험 환경

4.1.1 실험 네트워크 구조

실험을 위하여 ns-2 시뮬레이터[8]를 사용하였으며, 사용된 네트워크 구조를 그림 6에 나타내었다. 5개의 에지 라우터 E_0, E_1, …, E_4가 백본망을 통하여 풀-메쉬로 연결되어 있다. 이들 각 에지 라우터는 한 네트워크에서 들어오는 트래픽들을 백본으로 전달하여주는 링크를 제공하는 AS 라우터가 연결되어있으며 이 AS 라우터에는 정상트래픽(N), 목표 집중형 공격 트래픽(AC), 목표 분산형 공격 트래픽(AD) 을 생성하는 세개의 노드들인 N, AC, AD가 연결되어 있다. 그리고 다른 라우터들을 통하여 전달되는 트래픽들을 받아들여 처리하는 싱크 노드(S)가 연결되어 있다.

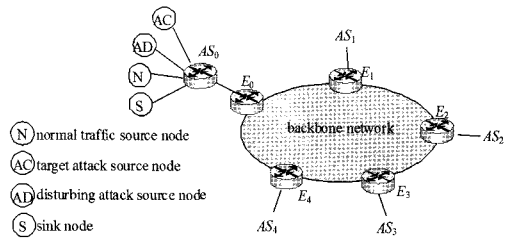


그림 6. 시뮬레이션 네트워크 구조

4.1.2 공격 트래픽 생성 모델

Weaver[10]는 코드레드나 슬래머 웜에 의한 감염 호스트수의 변화에 대한 시뮬레이션 모델을 제시하였고, 그림 7에는 Weaver가 제시한 시뮬레이터를 사용하여 구한 전체 네트워크에서의 감염된 호스트 수의 시간에 따른 변화를 나타내었다.

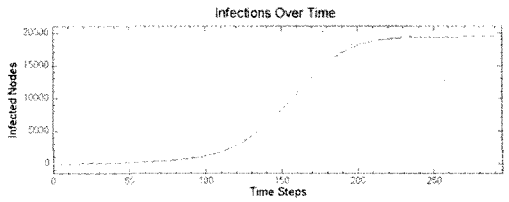


그림 7. 분산 공격에 의한 감염 호스트수의 변화

한 호스트가감염되면 주어진 패턴에 따라 공격 패킷들을 발생 시킬 것이고, 한 네트워크내에서 감염 호스트의 수가 증가하면 이 네트워크로부터 백본망으로 유입되는 집합된 공격 패킷들의 수는 감염 호스트의 수에 따라 비례하여 증가할 것이다. 이러한 상황을 바탕으로, 본 연구에서는 공격 트래픽의 발생을 위한 모델을 구성하기 위하여, 집합된 공격 트래픽의 양은 감염 호스트의 수에 비례한다고 가정한다.

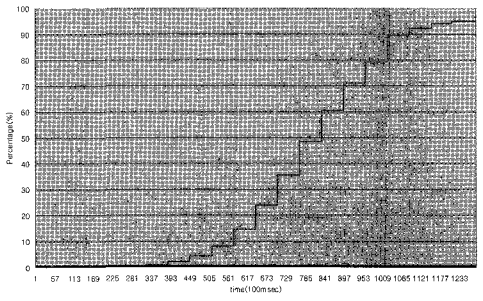


그림 8. 실험에 사용한 감염 호스트수의 변화 모델

그림 8에는 본 연구의 실험에서 사용된 하나의 링크를 통하여 백본망으로 유입되는 집합 공격 트래픽 양(발생 패킷수)의 시간에 따른 변화를 링크 용량에 대한 백분율로 나타내었다. 즉, 그림 7의 Weaver의 시뮬레이터[10]에서 구한 감염 호스트 수 변화 양상 곡선을 6.4초로 구분된 시간구간으로 나누고, 패킷 발생수가 감염 호스트 숫자에 비례하도록 하고 최대로 감염되었을 때(가능 감염 노드 숫자가 더 이상 존재하지 않을 때)의 경우 한 백본 링크 용량의 95%를 점유하도록 하도록 하였다.

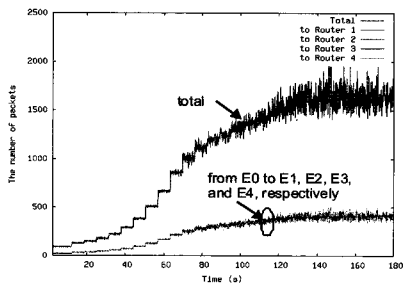
이로부터, 집합된 공격 트래픽의 생성은 다음과 같이 하였다. 즉, 그림 8에 구분된 각 시간대의 발생 패킷수를 평균으로 하고, Hurst 파라메터값은 0.99인 자기 유사 형태로 패킷들을 발생 시켰다[7]. 발생된 공격 패킷의 크기는 64바이트, 240바이트, 404바이트로 생성하였다. 이 값들은 기존 분산 네트워크 공격에서 발생한 패킷 크기들이다[9].

4.2 목표 분산형 공격 형태 탐지 성능 실험 결과

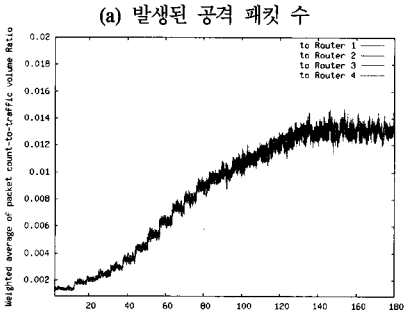
4.2.1 트래픽 생성 방법

목표 분산형 공격에서는 네트워크내의 모든 취약 호스트를 공격의 대상으로 한다. 따라서, 한 입력 백본 라우터로 유입되는 이러한 유형의 공격 패킷들은 백본망내의 모든 다른 라우터를 목적지로 한다.

이러한 상황을 나타내기 위하여, AS0만이 감염되고, 다른 AS들은 감염이 안된 상황을 가정하였다. 특히, AS0는 처음에는 감염이 이루어지지 않은 상태에서 시작하여, 10초부터 감염이 시작되도록 하였다. 감염이 시작된 후에 A0 라우터에 연결된 AD 노드로부터 생성되는 공격 패킷들은 모든 다른 백본 에지 라우터들인 E_1, E_2, E_3, E_4로 균등하게 분산되어 전달되도록 하였으며, 감염이 시작한 후 부터의 AS0에서의 감염 호스트수의 변화는 그림 8을 따른 것으로 하였다.



(a) 발생된 공격 패킷 수



(b) 공격 패킷에 대한 CVR

그림 9. 라우터 E0로부터 생성된 트래픽

그림 9(a)는 그림 8의 모델에 따라 라우터 E_0에서 생성된 총 패킷수와 이들 패킷들중 다른 라우터들인 E_1, E_2, E_3, E_4로 전달된 패킷수들을 나타내었고 이들에 대한 CVR을 그림 9(b)에 나타내었다.

4.2.2 실험 결과

그림 10은 공격이 전혀 이루어지지 않는 경우에 대한 상태행렬 $S(m)$ 값들을 보여준다. 그림 10에서 보는 바와 같이, 공격이 없을 때는 모든 상태가 정상상태(NORMAL)인 0의 값을 나타낸다.

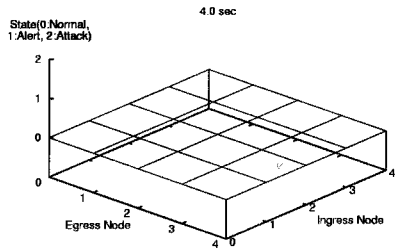
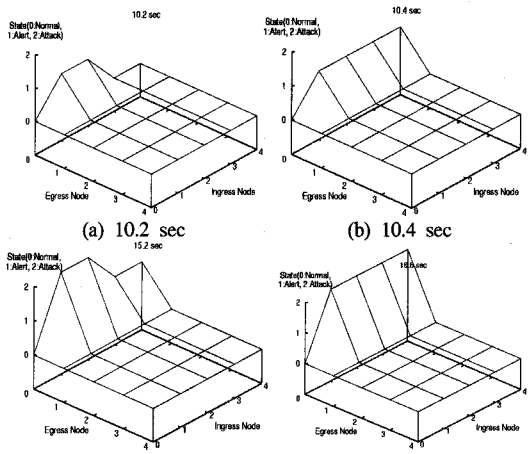


그림 10. E0에서의 초기 S(m) (감염이 없는 경우)

그림 11은 AS0에서 감염이 시작된 후의 $S(m)$의 변화를 보여준다. 그림 5에 나타낸 바와 같이, 목표 분산형 감염 트래픽은 백본망을 통하여 모든 다른 라우터들에게로 전달된다. 따라서, 공격 패킷들이 백본 에지 라우터 E_0로부터 다른 모든 백본 에지 라우터들에게 전달되므로, 그림 12에서와 같이 $S(m)$의 요소들중에서 s^{0j} (j=1,2,3,4) 들만 시간에 따라 경계상태(ALERT)에서 공격상태(ATTACK)로 변화하여, 목표 분산형 공격이 이루어지고 있음을 보여주게 된다.



(a) 10.2 sec (b) 10.4 sec

(c) 15.2 sec d) 15.5 sec

그림 11. 감염 시작후(10초후)의 E0에서의 S(m)의 변화 (AS0에서의 감염이 시작된 이후)

4.3 목표 집중형 공격 형태 탐지 성능 실험 결과

4.3.1 트래픽 생성 방법

목표 집중형 공격은 다수의 감염된 호스트가 목표 호스트에 장애를 일으킬 목적으로 해당 목표 호스트로 서비스를 중단 시킬 정도로 매우 많은 패킷들을 전송한다. 이러한 상황에서 제안 방법이 이러한 공격 유형을 감지해 내는 것을 보이기 위하여, 다음과 같은 방식으로 트래픽을 생성 시켰다.

그림 6의 네트워크 구조에서 공격의 목표가 되는 호스트는 E_2 에 연결되어 있고, AS0, AS1 그리고 AS3 라우터에 연결된 AC 노드로부터 생성되는 공격 패킷들은 모두 E_2 로 향하도록 하였다. 제안방법이 공격의 유형을 정확히 찾아내는 것을 보이기 위하여, AS4는 면역이 잘 되어 공격 패킷의 생성은 전혀 없는 것으로 설정하였다. AC노드는 4.2.절에서의 AD 노드와 동일한 특성을 갖는 공격 트래픽을 생성하지만, 생성된 공격 패킷들은 분산되지 않고, 공격 대상 호스트가 연결되어 있는 라우터 E_2로만 전달된다.

감염이 한 네트워크의 감염된 호스트들로부터 다른 네트워크로 확산되어 가는 것을 보이기 위하여 그림 12와 같은 감염에 대한 시간 프레임을 설정하였다. 즉, 처음 10초간은 감염된 호스트가 하나도 없어서 공격이 이루어지지 않도록 하였다. AS0내의 호스트들의 감염 시작은 10초부터 시작되어 내부 및 다른 네트워크의 호스트들을 감염시키고, 이에 따라 AS1의 호스트들의 감염은 30초부터, AS2는 50초부터, AS3는 70초부터 감염 및 공격이 시작되도록 하였다. 각 AS 내에서의 호스트 감염은 그림 8과 같은 형태를 따르도록 하였다.

그림 12에서, AS4는 공격에 대한 방어가 완벽하여 공격의 영향을 받지 않는 것으로 가정하였으므로, 시간 프레임상에 AS4의 감염은 나타나고 있지 않음에 주의한다. 또한, 공격의 목표가 되는 호스트가 AS2에 연결되어 있으므로, 이 실험에서는 AS2에서의 공격 호스트 수는 고려하지 않는다.

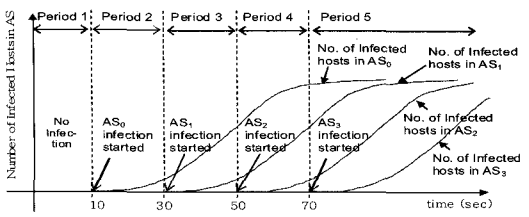


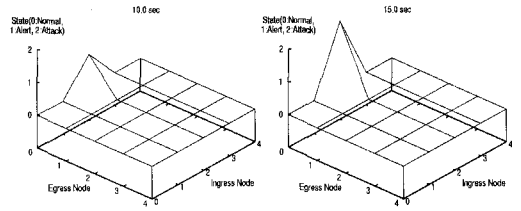
그림 12. 각 AS내의 호스트들의 감염에 대한 시간 프레임 (AS0, AS1, AS2, AS3의 호스트들은 감염되나, AS4는 감염이 이루어지지 않는 것으로 가정함)

4.3.2 실험 결과

Period-1에서의 상태는 그림 10과 같다. Period-2에서 AS0로 부터의 공격이 E_0를 통하여 E_2로 집중됨에 따라, 그림 13에 나타낸 것과 같이 $S(m)$에서의 $s^{0,2}$값만 경계상태에서 공격상태로 바뀌어 이러한 공격이 이루어지고 있음을 감지해 내고 있다.

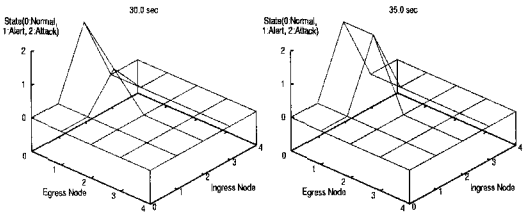
Period-3와 Period-5에서의 상황을 보여주는 그림 14와 그림 15를 통하여도 각각 공격 패킷들이 E_1에서 E_2로, E_3에서 E_2로 향하므로 $S(m)$에서 $s^{1,2}$와 $s^{3,2}$값들이 해당 Period에서 경계상태에서 공격상태로 변화하고 있다.

모든 공격이 활성화된 상태는 그림 15(b)에서 볼 수 있는데, AS4로 부터는 공격이 없으므로, $S(m)$의 $s^{0,2}$, $s^{1,2}$, 그리고 $s^{3,2}$값들만 공격상태를 나타내어 그림 4(b)에서와 같은 형태를 보여줌을 알수 있다. 이로부터, 제안된 방법이 이러한 공격의 상황을 잘 나타내어 줌을 알 수 있다.



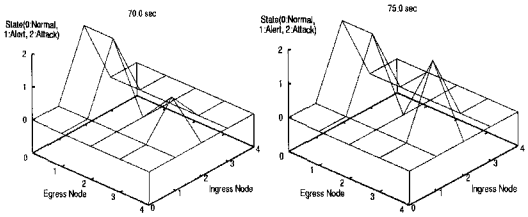
(a) 10 sec (b) 15 sec

그림 13. 목표 집중형 공격 상황에서의 Period-2 동안의 E0에서의 S(m)의 변화 (AS0에서의 감염이 시작된 이후)



(a) 30 sec (b) 35 sec

그림 14. 목표 집중형 공격 상황에서의 Period-3 동안의 E0에서의 S(m)의 변화 (AS1에서의 감염이 시작된 이후)



(a) 70 sec (b) 75 sec

그림 15. 목표 집중형 공격 상황에서의 Period-5 동안의 E0에서의 S(m)의 변화 (AS3에서의 감염이 시작된 이후)

4.4 목표 집중형과 목표 분산형이 혼재된 공격 형태 탐지 성능 실험 결과

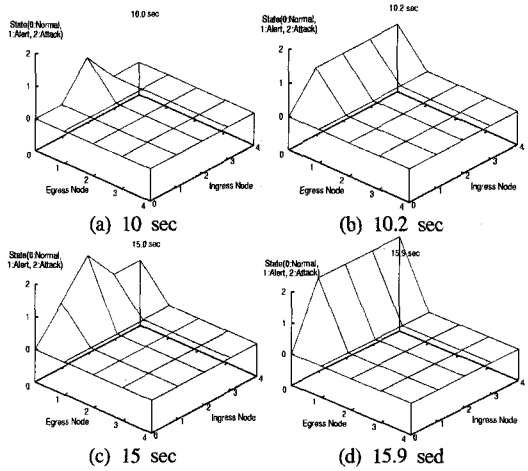
4.4.1 트래픽 생성 방법

4.2와 4.3에서와 동일한 환경으로 목표 분산형 공격과 목표 집중형 공격 트래픽 생성이 동시에 이루어 지도록 하였다. 특히, 목표 분산형 공격의 경우는 4.2와 달리, AS0뿐만이 아니라 다른 AS들에서도 그림 12에서의 감염 시간 프레임에 따라 목표 분산형 공격 트래픽이 발생하도록 하였다.

4.4.2 실험 결과

그림 16은 Period-2동안의 $S(m)$의 변화를 보여준다. 실험에서는 목표 분산형 공격은 AS0의 AD로부터의 공격 패킷들이 다른 모든 라우터들에 균등히 분산되도록 하고, 목표 집중형 공격은 AS0의 AC로 부터의 공격 패킷들이 E_2로 모두 향하도록 하였으므로, $s^{0,2}$가 우선 경계상태에서 공격상태 상태로 변화하고, $s^{0,1}$, $s^{0,3}$, $s^{0,4}$들이 동일한 상태 변화를 보여주고 있다.

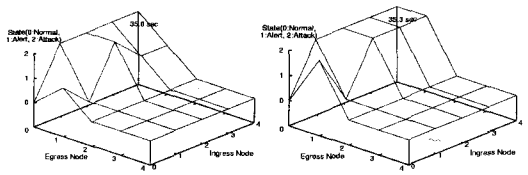
Period-3, Period-4, Period-5에 해당하는 그림 17, 그림 18, 그림 19들에서도 목표 집중형 공격이 이루어지는 노드에 대하여 $S(m)$ 값이 우선 반응하고, 다른 노드들에 대한 값들이 나중에 반응하고 있음을 볼 수 있다. 이와 같이, 목표 집중형 공격은 목표 분산형 공격보다 앞서서 검출되므로, 이러한 특징을 활용한다면 두가지 형태가 혼재하는 경우에도 각 공격의 양상을 구분 가능할 것으로 판단된다. 그러나, 이러한 방안에 대한 연구는 더 진행되어야 한다.



(a) 10 sec (b) 10.2 sec

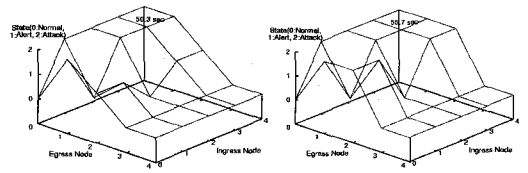
(c) 15 sec (d) 15.9 sed

그림 16. 혼합된 공격 상황에서의 Period-2 동안의 E0에서의 S(m)의 변화 (AS0에서의 감염과 공격이 시작된 이후)



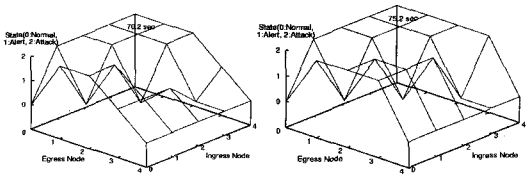
(a) 35 sec (b) 35.3 sec

그림 17. 혼합된 공격 상황에서의 Period-3 동안의 E0에서의 S(m)의 변화 (AS1에서의 감염과 공격이 시작된 이후)



(a) 50.3 sec (b) 55.7 sec

그림 18. 혼합된 공격 상황에서의 Period-4 동안의 E0에서의 S(m)의 변화 (AS2에서의 감염만 시작된 이후)



(a) 70.2 sec (b) 75.2 sec

그림 19. 혼합된 공격 상황에서의 Period-5 동안의 E0에서의 S(m)의 변화 (AS3에서의 감염과 공격이 시작된 이후)

V. 결 론

본 논문에서는 분산 네트워크 공격을 백본망 단위에서 효율적으로 탐지하기 위한 방법을 제안하였고 이의 적용시 분산 네트워크 공격의 위협을 조기에 발견할 수 있음을 실험을 통하여 보였다. 기존의 방법들은 네트워크 공격의 징후를 개별 패킷 또는 플로우 단위로 감지해 냄으로써 매우 큰 계산량과 복잡도를 요구하여 백본망에서의 적용이 불가능하나, 제안한 방법은 집합 트래픽 단위에서 공격 징후를 탐지하므로 기존의 방법들에 비하여 현저히 낮은 계산량과 복잡도를 요구함으로, 초고속의 백본망 단위에서도 네트워크 공격을 신속히 감지하여 낼수 있다.

백본망은 망운영자들에 의하여 글로벌하게 유지, 관리 운영되도록 하기 위하여 다양한 망관리 방법론들이 적용되고 있다. 본 논문에서 제안한 방법은 이러한 망관리 방법들과 연계하여 적용가능하며, 이

렇게 함으로써 효율적인 전역 방어 인프라 체계를 갖출 수 있을 것으로 판단한다.

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] B. Roh, and S.W.Yoo, "A Nobel Detection Methodology Of Network Attack Symptoms At Aggregate Traffic Level On Highspeed Internet Backbone Links," ICT'2004, LNCS, Vol.3124, pp.1226-1235, 2004

[6] 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

[7] 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

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

[9] 안철수연구소 기획실, "SQL_Overflow 웜의 분석 보고서", Technical Report, 안철수 연구소, 2003

[10] Nicholas C. Weaver, Warhol worms: The potential for very fast in plagues. http://www.cs.berkeley.edu/nweaver/warhol.html.

[11] W. Stallings, High-Speed Networks and Internets: Performance and Quality of Service, 2ndEd., Prentice Hall, 2001

김 선 호 (Sun Ho Kim) 정회원

2004 아주대학교 정보및컴퓨터공학부(학사)
2006 아주대학교 정보통신전문대학원(석사)
2006-현재 대우일렉 IS연구소 연구원
<관심분야> 인터넷 통신

윤 명 철 (Myungchul Yoon) 정회원

1986 서울대학교 전자공학과(학사)
1988 서울대학교 전자공학과(석사)
1998 Univ. of Texas at Austin. ECE, (박사)
1988-2000 현대전자(현 하이닉스)
2000-2002 펜택&큐리텔
2005-2006 대구경북과학기술연구원
현재 단국대학교(천안캠퍼스) 전자공학과 조교수
<관심분야> 영상통신, 이동통신, 임베디드씨스템스

노 병 희 (Byeong-hee Roh) 종신회원

1987 한양대학교 전자공학과 (학사)
1989 한국과학기술원 전기및전자공학과 (석사)
1998 한국과학기술원 전기및전자공학과 (박사)
1989-1994 한국통신 통신망 연구소
1998-2000 삼성전자
2000-현재 아주대학교 정보통신전문대학원 부교수
<관심분야> 유/무선 인터넷 멀티미디어 통신 및 응용, BcN 트래픽 엔지니어링, 유비쿼터스 센서 네트워킹, 인터넷 보안