자동 격리를 감안한 슬래머 웜 전파과정에 대한 모의실험 및 분석

정회원 임 재 명*, 정 한 균, 종신회원 윤 종 호

Simulation and Analysis of Slammer Worm Propagation With Automatic Quarantine

Jae-Myung Lim*, Han-Gyun Jung *Regular Members*,
Chong-Ho Yoon *Lifelong Member*

요 약

본 논문에서는 2003년 전 세계의 인터넷망에서의 심각한 소통 장애를 일으켰던 슬래머 웜 보안공격의 전파 전 과정을 NS-2를 이용한 시뮬레이터로 분석하였다. 기존 연구에서는 Detailed Network-Abstract Network (DN-AN) 모델 기반의 Abstract Network-Abstract Network(AN-AN)모델을 이용한 분석이 수행되었다. 이러한 AN-AN모델은 패킷 레벨까지 정확한 분석이 가능하지만, 초기 300초의 감염구간을 모의실험 하는데 240시간이 소요되는 시간상 문제점이 있었다. 본 논문에서는 이러한 문제점을 해결하기 위한 축소된 모델링 기법을 제시하여 모의실험에 필요한 소요시간을 단축함으로써 소통 장애가 일어난 3.5시간을 107시간에 분석할 수 있었다. 아울러 기존 분석에서는 감염 호스트가 인위적인 치료나 격리 조치가 있을 때까지는 모두 동작하는 것으로 가정하였지만, 슬래머의 과도한 감염 트래픽으로 중계 라우터의 동작이 중지되는 현상에 의해 해당 장비가 감염과정에서 자연적으로 격리되는 격리율 0.00022도 함께 고려하였다. 모의실험 결과, 국제관문국의 국외=>국내방향은 4,787초에 정상 상태로 돌아온 반면, 국내=>국외방향이 3.5시간동안 포화가 되어 소통 장애가 지속됨을 알 수 있었다.

Key Words : Slammer, Worm Model, Worm-propagation, NS-2 Simulation, SIR Model

ABSTRACT

In this paper, we have analyzed a simulation model of Slammer worm propagation process which caused serious disruptions on the Internet in the year of 2003 by using NS-2. Previously we had presented and analyzed Abstract Network to Abstract Network(AN-AN) model being modified from the Detailed Network to Abstract Network(DN-AN) of NS-2. However, packet analysis in AN-AN model had a problem of taking 240 hours to simulate the initial 300 seconds of infection. We have reduced the AN-AN model to save the simulation time and analyzed total 3.5 hours of the network congestions within 107 hours. Moreover, we have derived optimal quarantine rate of 0.0022 considering service outage of network devices caused by the heavy infected traffics, which was not taken into consideration in previous works. As the result of simulation, Although the inbound traffic at the Korean international gateway was back in normal conditions at 4,787 second, due to the revese direction saturation was maintained until 12,600 seconds, the service outage was persisted for 3.5 hours.

※ 본 논문은 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성사업(C1090 0603 0036)지원에 의하여 수행되었습니다.
* 한국항공대학교 정보통신공학과 대학원 (jmlim@kisa.or.kr, jhg798@hau.ac.kr, yoonch@hau.ac.kr)
논문번호 : KICS2007-05-219, 접수일자 : 2007년 5월 1일, 최종논문접수일자 : 2007년 7월 10일

Ⅰ. 서 론

2003년에 발생한 슬래머 웜 공격은 10분 만에 전 세계의 호스트 시스템의 90%이상인 75,000개를 감염시켜 항공권 발권시스템 및 현금자동지급기 등의 인터넷 서비스를 불가능하게 한 역사상 가장 빨리 확산된 컴퓨터 웜 바이러스 공격이었다[1]~[3]. 이러한 슬래머 웜 공격이 시작되면 감염된 호스트의 성능 및 통신망의 환경에 따라 감염 코드가 초당 약 1만~5만개 (30~150Mbps)의 UDP 패킷을 생성하여 임의의 호스트로 발송함으로써 추가 감염을 유발시키면서 감염 호스트 자신은 다른 작업을 하지 못하는 과부하가 발생하여 결과적으로는 서버에 대한 서비스거부(DoS, Denial of Service) 현상이 발생하였다. 또한 슬래머 웜은 취약점이 있는 호스트뿐만이 아니라, 감염 패킷을 임의의 호스트로 무차별 송신함으로써 통신망에 대한 과부하를 유발시켜 다수의 인터넷 사이트 접속지연이 폭증하는 문제를 발생하였다[4].

이러한 웜의 전파과정을 분석하는 모델로 악성 전염병이 전파되는 과정인 Susceptible-Infectious(SI)모델, 패치 등에 의해 내성을 가지거나 회복되는 것을 고려한 Kermack-McKendrick의 Susceptible-Infectious-Removed(SIR)모델, 그리고 SIR모델에 전파과정에 있는 라우터 등에서의 혼잡장애에 의해 확산속도가 포화되는 것을 고려한 모델 등이 있다[5]~[7].

이러한 웜 전파 모델을 활용하여 수행된 기존 연구에서 사용한 시뮬레이터는 감염된 호스트 단위로 구현되었기 때문에 국내 인터넷에 대한 장애가 몇 초만에 어떻게 발생하는지에 대한 과정을 정확하게 분석할 수 없는 문제가 있었다. 최근에는 이러한 문제점을 해결하기 위하여 호스트 단위의 기존 모델링 대신에 감염을 유발시키는 패킷 단위별로 웜 전파과정에 대한 모의실험이 가능한 Detailed Network-Abstract Network (DN-AN)통신망 모델링을 사용한 NS-2 시뮬레이터가 발표되어 보다 정밀한 분석이 가능하게 되었다. 하지만 이 모델은 LAN과 같은 소규모의 망에서만 동작 가능한 제약조건이 있었다[8].

이러한 제약조건을 고려하여, 본 논문에서는 기존 DN-AN 모델을 Abstract network- Abstract network (AN-AN, 이후부터 국내와 국외를 구분하기 위하여 KR-AN으로 표기)모델로 추상화한 새로운 NS-2용 시뮬레이터를 구현하고, 이를 이용하여 최초의 웜 감염 패킷이 국내의 인터넷 국제 관문국(게이트웨이)으로 유입되어 국내 망이 포화되고 정상 상태로 되돌아오는 3.5시간 전 과정을 107시간에 분석하였다.

본 서론에 이어, 제 II 장에서는 웜 전파과정을 다룬 여러 가지의 모의실험용 모델을 분석하였다. 제 III 장에서는 기존 AN-AN모델의 단점인 장시간 소요시간(300초 모의실험에 240시간 소요)를 단축하기 위한 축소형 시뮬레이터를 구현하고, 이 모델이 실제 전파현상을 모의 실험될 수 있는 적절한 축소비율을 도출하였다. 또한 기존 분석에서는 감염 호스트가 인위적인 치료나 격리 조치가 있을 때까지는 모두 동작하는 것으로 가정하였지만, 슬래머의 과도한 감염 트래픽으로 중계 라우터의 동작이 중지되는 현상에 의해 해당 장비가 감염과정에서 통신망에서 격리되는 격리율도 함께 도출하였다. 제 IV 장에서는 이러한 시뮬레이터를 사용하여 당시 국내외 인터넷 환경을 고려한 웜 전파의 총 지속시간인 3.5시간의 전과정에 대한 모의실험 결과를 도출하고 특성을 분석하였으며, 마지막으로 제 V 장에서는 결론을 맺었다.

Ⅱ. 슬래머 웜 전파 모델

2002년 Staniford는 2001년에 맹위를 떨치던 코드레드 및 님다 웜을 분석하면서, 웜의 전파 속도에 따라 다음과 같은 3가지로 구분하였다[13]. 그림 1에서 보듯이 취약한 호스트를 24시간 이내에 감염시키는 보통 웜, 30분 이내에 감염시키는 고속 웜, 그리고 15분 이내에 감염시키는 초고속 웜(Warhol 웜)으로 구분하였다. 특히 초고속 웜의 첫 번째로 기록된 슬래머 웜은 기존 웜과 달리 여러 가지 특징을 갖고 있다.

첫째 기존 코드레드 및 님다 웜들은 TCP/IP기반의 취약한 호스트를 검색 후 감염 코드를 이용하여 감염시킨 반면, 슬래머는 UDP/IP 기반으로 일방향으로 감염을 시도하여 TCP의 응답-대기시간에 의한 전파지연이 없었다. 특히 코드레드나 님다 웜은 스캔 시 호스트의 많은 쓰레드를 이용하여 전파되었는데, 각 쓰레드는 임의의 주소에 대한 개별적인 TCP 세션 연결을 시도하였기 때문에 망의 혼잡상황에 따라 전파속도가 제한되었다. 즉, 각 쓰레드는 초기 연결에 있어서 TCP-SYN 패킷을 보낸 후, 목적 호스트로부터 응답패킷인 SYN-ACK을 받을 때까지 기다려야 했다. 만약에 주어진 시간내 응답을 받지 못하면 time-out으로 처리한다. 이 기간 동안 해당 쓰레드는 정지 상태처럼 다른 호스트를 감염시킬 수가 없었다. 코드레드는 시스템 프로세서의 교환 부하, 커널의 스택 메모리 소진, 쓰레드의 가동 수 제한으

로 인해 곧바로 지연현상이 발생하고 이에 따라 감염 지연 정도가 결정되었다.

이에 반해 슬래머는 감염된 시스템의 인터넷 대역폭에 제한되는 웜이다. 슬래머는 1개의 패킷으로 UDP 1434포트를 통하여 취약한 호스트를 감염시킬 수 있기 때문에 슬래머는 가상적인 피해 시스템으로부터 응답을 기다릴 필요가 없고 감염된 호스트에 의한 다른 호스트에 대한 무차별 스캔을 발생시킬 수 있었다. 슬래머의 감염 발생 프로그램은 매우 간단했고, 감염된 호스트의 인터넷 네트워크의 I/O 처리용량이 초당 10~100M bps이기 때문에 슬래머는 초당 평균 4,000개 이상의 감염 패킷을 발생시키는 폭발적인 감염 전파율에 의해 단기간에 스스로의 감염 증가율이 포화될 정도로 공격적이었다. 하지만, 슬래머는 대부분 자신을 복제하는 처리능력 제한보다는 물리적인 통신링크의 용량에 의해서만 전파과정이 제한되었다. 따라서 슬래머에 감염된 호스트에 의한 2차 감염 시도는 오히려 감염율을 감소시켰다. 왜냐하면 불충분한 대역폭으로 인하여 기존 감염 시도와 2차 감염 시도가 충돌이 일어나서 감염 시도 자체가 통신망의 대역폭을 고갈시켜 감염을 시도하는 패킷조차 전달되지 못하는 상황이 발생하였기 때문이다.

둘째 기존 웜은 TCP 또는 UDP를 막론하고 감염시키는데 여러 번의 패킷 전송이 필요하였다. 그러나 슬래머는 패킷헤더를 포함하여 404바이트의 길이를 가지는 단 1개의 UDP 패킷으로만 취약한 호스트를 감염시킬 수 있어 기존 웜과 달리 매우 효율적인 웜이다. 그전에 맹위를 떨치던 코드레드는 4K바이트, 님다는 60K바이트로 취약한 호스트를 감염시키기 위해서는 최소한 3번 이상의 패킷 전송이 완료될 때까지 연결 상태를 유지하여야 한다. 이러한 특징으로 인해 2001년 가장 많은 호스트를 감염시켰던 코드레드는 초기단계에서는 37분마다 감염 호스트 수를 배가시킨 반면 슬래머는 이보다 20배가량 빠르게 감염시켰다.

마지막으로 슬래머 이후에 블래스터 웜 등에서 취약한 호스트를 탐색하는 과정에서 과도한 ICMP 패킷을 전송하여 네트워크 장애가 발생한 적이 있었지만 슬래머처럼 직접적으로 네트워크 장비에 직접적인 부하를 가중시켜 동작이 중지되도록 하는 웜은 없었다. 슬래머의 스캔은 3가지 방법으로 부하를 가중시켰다. ①매우 큰 트래픽(bps) ②많은 패킷(pps) ③멀티캐스팅 주소를 포함한 매우 큰 새로운 목적주소(Reserved IP, Broadcast IP). 이러한 조합으로 인해 네트워크 장비의 메모리와 CPU 자원의 고갈을 가져와 고장을 유발시켰다[3].

앞으로도, 이러한 슬래머의 동작과 유사한 프로그램을 공격자가 사용하면 특정 국지망에 대한 DoS 공격도 가능하다. 왜냐하면 슬래머 웜의 감염 패킷은 외견상 정상적인 UDP패킷이기 때문에 시스템 관리자의 특정 권한이 필요하지 않기 때문이다. 따라서 주요 기반 통신망에서는 일부 호스트가 통신망 자원을 독점하지 않도록 Commit Access Rate 또는 공정한 큐잉정책 등을 필수적으로 채택하여야 한다.

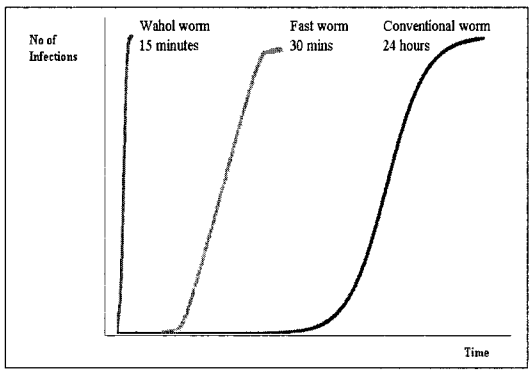


그림 1. 전파속도에 따른 웜의 구분

2.1 웜 전파 모델

웜의 감염 전파에 대하여 여러 가지 모델이 제안되었다. 첫째는 SI모델(Susceptible-Infectious)로 일명 전염병 모델(Epidemic)이라고 한다. 고전적인 단순한 전염병 모델로 고정된 호스트의 총 대수 N에 대하여 감염가능성이 높은 취약한 호스트의 수 $S(t)$는 감염된 호스트의 수 $I(t)$에 대하여 $S(t)=N-I(t)$로 기술된다. 이러한 단순 전염병 모델에서 한정된 호스트 수에 대하여 감염속도 β를 고려하면 감염 호스트 수의 증분은 다음과 같이 기술될 수 있다.

$$\frac{dI(t)}{dt} = \beta I(t) S(t) \qquad (1)$$

둘째는 Kermack-McKendrick의 SIR모델로 SI모델을 확장하여 감염된 호스트에 대한 보안패치 작업에 의해 복구되는 호스트의 수 $R(t)$와 복구비율 γ를 추가로 고려하면 다음과 같이 감염 호스트 수의 증가는 SI모델에 비하여 복구되는 호스트의 증가만큼 감소된다. 고정된 호스트의 총 대수 N에 대하여 취약한 호스트의 수 $S(t)$, 감염된 호스트의 수 $I(t)$, 복구된 호스트의 수 $R(t)$는 $S(t)+I(t)+R(t)=N$로 기술된다.

$$\frac{dI(t)}{dt} = \beta I(t) S(t) - \frac{dR(t)}{dt} \quad (2)$$

$$\frac{dR(t)}{dt} = \gamma I(t) \quad (3)$$

보통 SIR 모델은 슬래머처럼 전파속도가 아주 빨라 인간의 대응작업이 미진한 경우에는 적합하지 않다. 슬래머인 경우 초기 10분 이내에 취약한 호스트의 90%가 전부 감염되었다고 추정하기 때문에 당시 10분 이내에 슬래머의 전파 특성을 파악하여 사람이 대응하기 힘든 시간이기 때문이다.

셋째는 개선된 웜모델로 Improved Worm Mitigation Model(IWMM)모델이 있다. SI 및 SIR모델에 비하여 실제 인터넷 환경에서처럼 사람이 감염되었거나 감염될 위험에 있는 취약한 호스트를 복구 또는 예방한다. 또한 감염비율 β는 대용량 스캔 트래픽으로 인하여 통신망 내부의 라우터나 링크의 용량제한으로 인해 감속된다. 이러한 2가지 요소를 고려하여 제시된 새로운 모델에서는 기존의 고정된 감염비율 β대신에 시간에 따른 변수 값인 $\beta(t)$를 사용할 수 있다. 또한 시간 t에서 인간의 대응에 의하여 감염된 호스트 $I(t)$를 복구한 수 $R(t)$뿐만 아니라 감염될 위험에 있는 취약한 호스트 $S(t)$에 대하여 예방 조치한 호스트 수 $U(t)$와 복구비율 μ를 추가로 고려하면, 고정된 호스트의 총 대수 N에 대하여 $S(t)+I(t)+R(t)+U(t)=N$로 기술된다.

$$\frac{dI(t)}{dt} = \beta(t) I(t) S(t) - \frac{dR(t)}{dt} - \frac{dU(t)}{dt} \quad (4)$$

$$\frac{dR(t)}{dt} = \gamma I(t) \quad (5)$$

$$\frac{dU(t)}{dt} = \mu S(t) \quad (6)$$

그러나 이러한 모델은 코드레드나 님다 웜처럼 장시간에 걸쳐 전파하는 웜인 경우에는 적합하지만 단시간에 확산되었던 슬래머인 경우는 적합하지 않다.

2.2 모의실험을 위한 웜 전파 KR-AN 모델

슬래머 웜처럼 초고속 웜인 경우 적합하지 않다는 점과 패킷 레벨에서의 정확한 분석을 위하여 기존에 제안했던 KR-AN 모델은 다음과 같으며 표기는 표 1과 같이 설정하였다[11].

표 1. KR-AN 모델링 변수

항목	표시(시간 t)
AN/KR 호스트 수	N
AN/KR 취약한 호스트 수	$S(t)$
AN/KR 총 취약한 호스트 수	S_{Max}
AN/KR 감염 호스트 수	$I(t)$
AN/KR 격리수	$R(t)$
AN/KR 감염율	β
AN/KR 격리율	γ
외부망에 의한 감염 호스트 수	$I_O(t)$

감염호스트 수 $I(t)$를 계산하기 위해서 식(7)에서 4개 요소를 고려하였다. 첫 번째 항은 전 시간의 감염 호스트 수 $I(t-1)$이고, 두 번째 항은 취약한 호스트가 감염된 수로 기존 SIR모델을 인용하였다. 세 번째 항은 감염으로부터 격리된 호스트 수로 슬래머 웜인 경우는 과도한 감염 패킷으로 네트워크 장비를 다운시켰기 때문에 제 III 장에서 적정한 값을 구하였다. 네 번째 항은 자체망의 감염 패킷이 아닌 외부 망에서 유입된 감염 패킷으로 감염된 호스트를 표기하였다.

$$I(t) = I(t-1) + \beta I(t-1)\frac{S(t-1)}{S_{Max}} - \gamma I(t-1) + I_O(t-1) \quad (7)$$

$$S(t) = N - I(t-1) - R(t-1) \quad (8)$$

$$R(t) = \gamma I(t-1) \quad (9)$$

식(7) 두 번째 항의 감염율 β는 초당 4,000개의 감염 패킷이 전체 인터넷 대역으로 랜덤하게 퍼졌을 때 각 KR, AN 네트워크의 취약한 호스트에 도달할 확률이다. 즉 $\beta = 4{,}000 \times S_{Max}/2^{32}$로 표시하고 이에 따라 두 번째 항은 다음과 같이 정리할 수 있다.

$$\beta I(t-1)\frac{S(t-1)}{S_{Max}} = 4{,}000 \times \frac{S_{Max}}{2^{32}} \times I(t-1) \times \frac{S(t-1)}{S_{Max}} = 4{,}000 \times \frac{I(t-1) \times S(t-1)}{2^{32}} \quad (10)$$

식(7) 네 번째 항의 외부망에 의한 감염 호스트 수 $I_O(t)$는 외부망에서 들어온 감염패킷수($ProbeRecv$)와 자체망의 남아있는 취약 호스트 수에 비례하며 식(11)과 같이 정리할 수 있다. KR, AN망

으로 유입된 감염 패킷 수($Probe Recv$)는 AN, KR에서 상대망으로 송신된 감염 패킷 수($Probe Out$)와 같으며, 외부망으로 송신된 감염 패킷 수는 식(13)와 같이 표시한다. 식(12),(13)의 아래 첨자 $A or K$는 AN, KR망을 표시한다.

$$I_O(t-1) = Probe Recv \times \frac{S(t-1)}{N} \quad (11)$$

$$Probe Recv_{K or A} = Probe Out_{A or K} \quad (12)$$

$$Probe Out_{A or K} = 4{,}000 \times I_{A or K}(t-1) \times \frac{IP_{K or A}}{2^{32}} \quad (13)$$

외부망에서 유입된 감염 패킷 수($Probe Recv$)는 KR, AN 게이트웨이의 Queue와 통신망 대역폭에 제한을 받기 때문에 다음과 같은 조건을 만족하여야 한다. 식(13)는 상대망으로 송신된 감염 패킷 수(pps)는 상대망 게이트웨이의 Queue 처리용량을 넘을 수 없으며, 식(14)은 KR-AN 링크에 전달되는 패킷 양(bps)는 주어진 대역폭을 넘을 수 없음을 표시한다.

$$Probe Out_{A or K} \le Q_{A or K} \quad (14)$$

$$4{,}000 \times (Probe Out_{A or K} + Probe Recv_{A or K}) \times 8bit \le BW \quad (15)$$

한국인터넷백서에 따르면 당시 한국통신 8.707G, 데이콤 4.2G, 하나로 4.3G, 온세 1.123G, 두루넷 1.55G, EPN 0.355G, SKN 0.455G, 드림라인 0.31G, 에듀넷 0.62G를 포함하여 총 21.21G의 국제구간 대역폭을 확보하고 있었다[12]. 각 ISP의 시간대별 bps와 pps를 합산하여 모의실험을 하여야 하지만, ISP별 대응방법과 또한 감염정도가 각기 틀려서 합산하기보다는 가장 많이 사용하는 한국통신망의 특성을 국내 총량 21.21G로 확대하는 방법을 사용하였다.

또한 정상 트래픽과 감염 트래픽이 혼재되어 있기 때문에 당시 3.5시간 동안은 정상 트랙픽은 반절로 감축되고 나머지가 슬래머에 의한 감염 트래픽으로 추정하였다. 이렇게 추정한 결과 슬래머 웜에 의한 pps와 bps는 각각 다음과 같이 표현하였고 이에 대한 결과 값은 표 [3]와 같다. 이 값은 모의실험시 국제구간의 패킷 전송 제한요소로 사용된다.

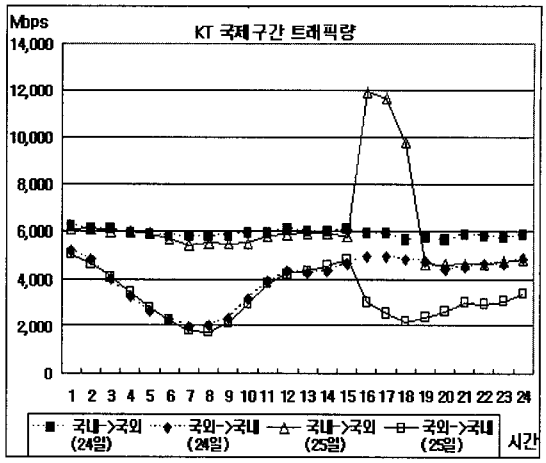


그림 2. 2003년 1월24일 및 25일 KT 국제구간 트래픽(bps)

표 2. 국제구간(21.21G)로 확대한 트래픽 트래픽 양

	국내=>국외(평시)	국외=>국내(평시)
BPS	8.382G	6.960G
PPS	2.121M	1.261M

	국내=>국외(125)	국외=>국내(125)
BPS	16.840G	4.243G
PPS	5.083M	1.700M

$$pps_{슬래머} = pps_{1.25} - \frac{1}{2} pps_{평시} \quad (16)$$

$$bps_{슬래머} = bps_{1.25} - \frac{1}{2} bps_{평시} \quad (17)$$

표 3. 슬래머 웜에 의한 트래픽을 정상 트래픽의 1/2배로 추정한 경우

	국내=>국외(125)	국외=>국내(125)
BPS	12.649G	0.763G
PPS	4.022M	1.070M

그림 2는 정보통신망 침해사고 조사결과[4]에서 당일 14:30분부터 18:00까지 국제망으로 유출(시설용량 : 8.6G)되는 트래픽은 폭증한(5.9G→11.9G) 국내로 유입되는 트래픽은 급감(4.8G→2.1G)라고 표기한 그림이다. 그림 2에서 보듯이 3.5시간 정도 후에는 정상적인 트래픽 상태로 돌아오는데, 본 모의실험에서는 인위적인 포트(1434) 차단보다는 감염 패킷의 폭주로 지역 라우터가 트래픽을 감당하지 못하여 다운되어 해당 라우터 하부에 있는 감염 호스트에서는 더 이상 감염 트래픽을 발생하지 않는 상황만 고려하였다.

Ⅲ. 소요시간 단축을 위한 축소형 시뮬레이터 구현

3.1 KR-AN 모델의 축소화 과정

기존의 KR-AN모델은 패킷 단위의 정확한 모의실험은 가능하지만 이를 처리하는 데 매우 긴 시간이 소요된다는 단점이 있다. 즉 초기 300초 동안 국내외 슬래머 감염수와 국제구간의 트래픽에 대한 모의실험시 무려 240시간이 소요되었다[11]. 이러한 점을 개선하기 위하여 본 논문에서는 기존 KR-AN모델의 특성을 유지시키면서도 모의실험 소요시간을 단축하는 방안을 사용하였다.

우선적으로 가장 많이 시간이 소요되는 국제구간에서 감염 패킷 발송량을 감소시키기 위하여 이를 발생하는 감염수와 취약수, 격리수를 각각 비례적으로 축소시켰다. 아울러 인터넷 주소대역을 2^{32}와 KR 및 AN의 주소대역도 각각 축소비율에 따라 같이 축소하였다. 감염된 호스트에서 발송하는 감염 패킷은 초당 4,000개 동일하게 적용하였다. 축소시 전체 특성이 틀려지지 않는지에 주안점을 두고 빠르게 확인하기 위하여 γ(격리율)을 임의로 1/20으로 고정하고 동일한 초기 300초 구간에서 모의실험을 하였다. 축소 비율은 각 1/4배, 1/8배, 1/16배, 1/64배, 1/256배로 2의 지수승을 택하여 한 결과 다음 <그림 3>과 같은 결과를 얻었다. 축소비율에 따른 AN의 감염수는 각각 비슷한 패턴을 보였으나 다만 축소비율이 커짐에 따라 그래프가 우축으로 일정한 간격을 두고 이동하는 모습을 보였다. 축소비율이 1/16배까지는 원래 패턴과 거의 동일한 모습을 보였으며, 1/64배인 경우 전반적으로 우축으로 10초 정도 이동한 모습을 보였고, 1/256배인 경우는 19초 정도 이동한 모습을 보였다. 적정 축소비율은 1/16 이상이 적당하지만 12,600초까지 분석한다면 모의실험 시간을 감안하여 1/16배보다는 1/64배 정도가 적당하다고 판단하였다.

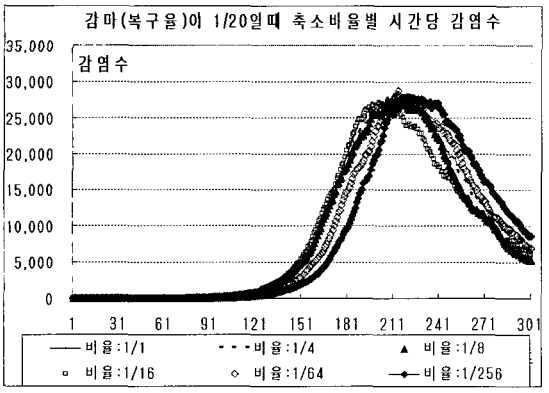


그림 3. 시간대별 축소비율에 따른 감염수 그래프

표 4. 축소비율에 따른 시뮬레이션(시간당 감염수) 시간 차이

축소비율	소요 시간 (300초 측정)	1배와 시간차
1배	64 시간	0초
1/4배	11 시간	0초
1/8배	8 시간	2초
1/16배	3 시간	2~4초
1/64배	41 분	9~11초
1/256배	10 분	19초이내

3.2 12,600초 이후 국제관문국(국내=〉국외방향)이 정상화되기 위한 자동격리율 산정

CAIDA발표[2]에 따라 10분 이내에 취약한 90%의 호스트가 슬매머 웜에 감염되었다고 하였기에 국내 감염수 8,848개보다는 10/9배 많은 9,831개를 취약 호스트로 가정하였다. 감염 호스트가 시간이 지남에 따라 격리(지역 라우터가 부하에 다운되었거나 사람이 포트를 차단을 하여 더 이상 패킷이 발생하지 않는 경우)되어 12,600초에서 남아 있는 감염 호스트 수가 KR인 경우 2,741개이면 국제구간(국내=>국외)이 허용 트래픽 이하로 떨어진다. 이를 근사적으로 확인하기 위하여 12,600초에서 KR의 감염 호스트 수를 측정하였다. 1차 격리율을 10^{-3}에서 10^{-6}까지 변경시키면서 모의실험한 결과 그림 4에서 격리율은 10^{-3}과 10^{-4}사이의 값이 적합한 것으로 판단되었다.

다시 10^{-3}과 10^{-4}사이 구간을 0.0002씩 차등을 두어 모의실험한 결과 그림 5와 같은 결과를 얻었으며, 2,741개에 가장 근사한 값은 0.0002임을 확인하였다. 다시 이를 0.00002씩 차등을 두어 모의실험한 결과 <그림 6>과 같은 결과를 얻었으며 격리율(γ) = 0.00022이 가장 적합한 값임을 도출할 수 있다.

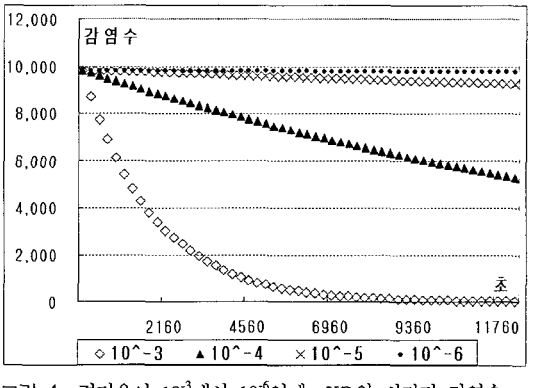


그림 4. 격리율이 10^{-3}에서 10^{-6}일때 KR의 시간당 감염수

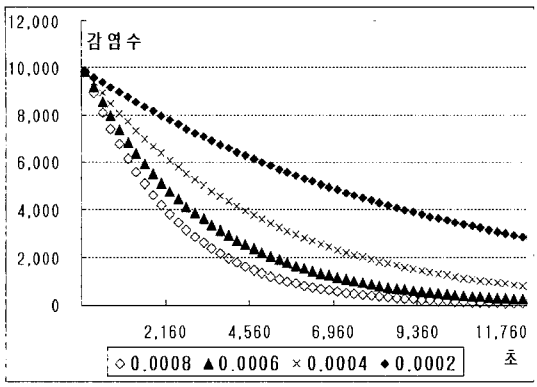


그림 5. 격리율이 0.0008에서 0.002일때 KR의 시간당 감염수

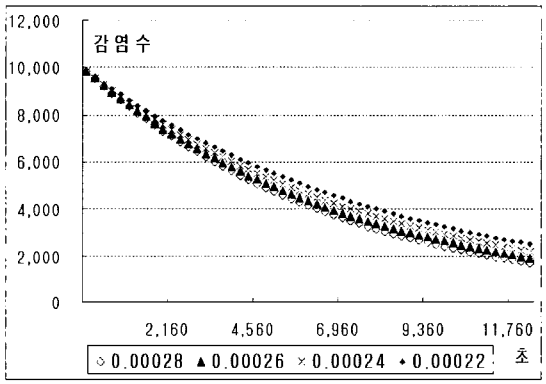


그림 6. 격리율이 0.00028에서 0.00022일때 KR의 시간당 감염수

Ⅳ. NS-2 통신망 시뮬레이션 축소 모델을 통한 국내 슬래머 웜 전파 분석

4.1 모의실험 환경

슬래머 웜 전파과정 분석은 리눅스 PC(CPU 4.7MHz, 메모리 4G)에서 버전 2.30의 NS-2를 이용하였다. 각 변수값은 <표5>과 같으며, CAIDA 자료, 각종 정보화통계와 유무선 통신서비스 가입자 현황을 참조하였다.[9][10]

4.2 분석 결과

2003년 당시 슬래머 웜의 초기 확산단계의 정확한 상태 값이 없기 때문에 당시의 네트워크 트래픽과 네트워크의 구성을 고려하고 상대적인 시간에 따른 감염 호스트의 추이 변화에 주안점을 두고 모의실험을 수행하였다.

최초의 감염은 AN에서 시작되었고, KR은 AN에서 유입된 감염 패킷에 의해서 감염되었다고 가정하였다. 초기 감염부터 국제구간 네트워크가 소통이 원

표 5. 축소비율에 따른 파라메타 값

항목	원래 값	1/64배 축소
인터넷 IP수	4,294,967,296	67,108,864
AN IP수	1,831,970,000	28,624,531
AN 호스트수	717,270,000	11,207,343
AN 취약 호스트 수	73,502	1,148
KR IP수	26,210,000	409,531
KR 호스트수	24,250,000	378,906
KR 취약 호스트수	9,831	153
웜 전파속도	4,000회/초	4,000회/초
웜 패킷크기	404 byte	404 byte
KR=>AN queue	4,042,000	63,156
AN=>KR queue	1,070,000	16,718
국제구간 지연시간	1ms	1ms
국제구간 큐정책	DropTail	DropTail
국제구간 대역폭	13.539 Gbps	0.212 Gbps

활하게 된 3.5시간 동안 전 과정에 대한 모의실험은 PC상에서 총 107시간 소요되었다. 그림 7은 초기 600초 동안 국내외의 감염된 호스트 수의 증가추세를 분석한 결과이다. 감염되는 호스트의 증가추세는 국내와 국외 모두 유사하며 이러한 패턴은 기존 논문에서 보여준 패턴과 일치하는데, 단지 전체 감염소요 시간이 CAIDA는 600초에 전체 취약한 호스트의 90%가 감염되었다고 발표한 반면, 본 논문에서 구현된 시뮬레이터에 의한 모의실험 결과는 376초[1]로 차이가 있었다. 하지만 이러한 감염시간의 차이는 CAIDA에서 사용한 전파모델(RCS, Random Constant Spread)과 본 논문에서 사용한 전파모델인 KR-AN 모델과의 차이에 의한 것일 뿐 전반적인 전파과정을 분석하는 데는 문제가 없다[13]. 모의실험 결과, AN의 최초 감염이 1초에 시작되었다고 가정했을 때 KR의 최초 감염은 36초에 발생하였다. 또한 KR망의 취약한 9,831대 호스트는 249초에 9,670대로 최대 감염되었다. 국외 AN망의 취약한 73,502대 호스트는 224초에 최대 72,688대가 감염되었다. 최대 감염수보다 작은 이유는 AN망과 KR망에서 각각 감염된 호스트 814대, 161대가 슬래머의 과다한 트래픽으로 인해 해당 지역의 망 장비가 다운되면서 인터넷망과 분리가 되어 더 이상 감염 패킷을 발생할 수

1) 여기서의 시간은 절대시간이 아닌 상대적인 시간으로 모델과 파라메타의 값에 따라 변동이 가능하다.

없었기 때문이다. 그림 8은 12,600초 전 구간 동안 국내외의 감염된 호스트 수의 증감추세를 분석한 결과이다. 그림 7에서 224초, 249초에 최대로 감염되었다가, 과다한 감염 패킷 트래픽으로 인한 자동 격리율(0.00022)에 따라 점진적으로 감소하여 국제구간 트래픽이 원활하게 된 3.5시간 이후의 남아 있는 감염 호스트 수는 AN망 총 감염 수 73,502대 중 18,517대, KR망에서는 9831대 중 2,468대가 감염 상태로 남아 있었으나, 그림 9, 그림 10에 보듯이 발생된 감염 패킷이 해당 구간 대역폭 이내여서 소통에는 거의 지장이 없었다.

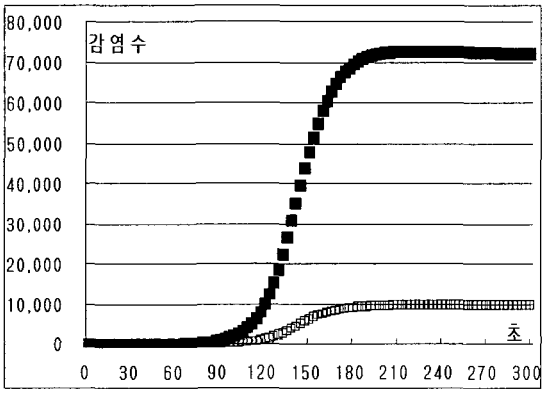


그림 7. 초기 300초 동안 국내외 감염 호스트 수
■ : 국외 감염 호스트 수 (224초, 72,688대 / 73,502대)
□ : 국내 감염 호스트 수 (249초, 9,670대 / 9,831대)

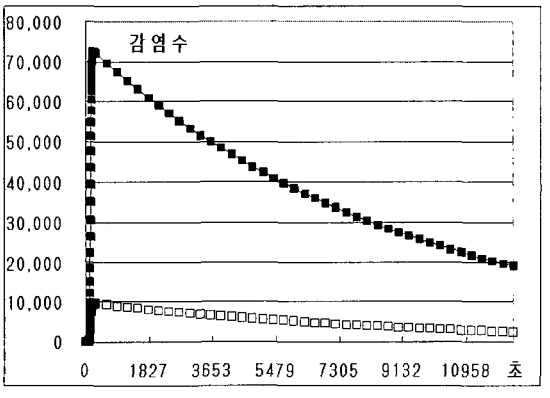


그림 8. 소통 장애 시간대(12,600초) 국내외 감염 호스트 수
■ : 국외 감염 호스트 수 (12,600초, 18,517대 / 73,502대)
□ : 국내 감염 호스트 수 (12,600초, 2,468대 / 9,831대)

그림 9는 국내에서 감염된 호스트에 의해 국외로 송신된 웜 감염 패킷 수를 표시하였다. 133초에 4,041,984개로 포화되었으며, 251초에 최대 16,495,938개가 되었고, 이후 12,600초까지 국제구간 허용치를 넘어서 지속적으로 소통 장애를 일으킨 가장 큰 원인이 되었다. 그림 10은 외국의 감염된 호스트가 국제관문국(게이트웨이)을 통하여 국내로 송신한 웜 감염 패킷 수를 표시하였다. 150초부터 국내방향 감염 패킷은 1,069,952개로 포화되었으며, 225초에 최대 1,774,348개가 되었고, 이후 4,787초까지 지속적으로 포화 상태를 유지하다가 이후부터는 정상 상태로 되돌아 왔다. 그러나 TCP/IP 특성상 3-Way handshaking이 되지 않음으로써 국내방향 대역폭은 여유가 있었지만 국외방향이 소통장애가 있어 12,600초까지는 지속적으로 소통장애 상태가 되었다.

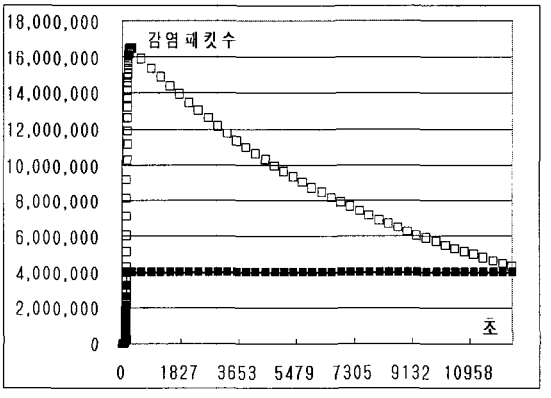


그림 9. 소통장애 시간대 국내에서 국외로 나간 감염 패킷 수
■ : 국내 ➡ 국외로 보낸 감염 패킷 중 국제구간 통과패킷 수
□ : 국내 ➡ 국외로 보낸 총 감염 패킷 수

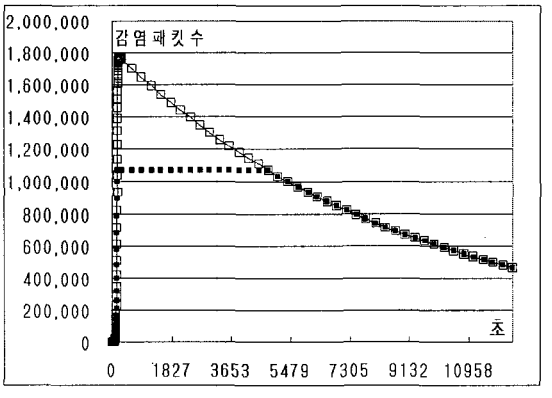


그림 10. 소통장애 시간대 국외에서 국내로 들어온 감염패킷 수
□ : 국외에서 국내로 보낸 총 감염 패킷 수
■ : 국외에서 국내로 보낸 감염 패킷 중 국제구간 통과패킷 수

그림 11은 시간대별 국내 감염 호스트 수를 표시한 것이다. 그림에서 보듯이 국내 감염의 대부분은 국외에서 유입된 감염 패킷에 의하여 감염되었음을 보여주고 있다. 국내 전체 감염수 9,831대중 8,620대

(88%)가 국외에서 들어온 감염 패킷에 의하여 감염되었다. 국외에서 유입된 감염 패킷으로 감염된 호스트 수는 143초에 초당 185대로 최대를 기록하였고, 144초에 국내 및 국외 스캔에 의하여 초당 최대 207대가 감염되었다. 국외에서 유입된 감염 패킷에 감염이 많았던 것은 슬래머 웜 전파 특성상 랜덤하게 스캔하기 때문에 국내 감염된 호스트에서 발생한 감염 패킷은 대부분 국내(KR)의 IP대역보다는 국외(AN)로 나갔기 때문이다[2]. 이 결과를 보면 랜덤하게 전파하는 초고속 웜이 발생했을 때에는 우선적으로 국제관문국에서 전파에 악용되는 포트(예: 슬래머인 경우 1,434포트)를 일시적으로 차단하는 것이 감염을 감속하는 데 가장 좋은 방법으로 판단된다.

그림 12는 시간대별 국외 감염 호스트 수를 표시한 것이다. 국외 감염의 대부분은 국외 자체의 스캔에 의하여 감염되었음을 보여주고 있다. 국외 전체 감염수 73,502대중 11,207대(15%)가 국내 감염호스트에서 나온 감염 패킷에 의하여 감염되었다. 국외 자체 스캔으로 감염된 호스트 수는 142초에 초당 1,466대를 최대를 기록하였고, 국내발 감염 패킷에 의해 감염된 호스트 수는 132초에 293대로 최대를 기록하였다.

표 6, 표 7에 이러한 분석 내용을 모아서 시간대별 국내외 감염 호스트 수 및 국제관문국 트래픽 상태를 정리하였다. 처음 1.3시간 동안은 국내외 감염 호스트 모두가 국제구간의 네트워크 소통 장애의 원인이었지만, 1.3시간 이후부터는 순수하게 국내의 감

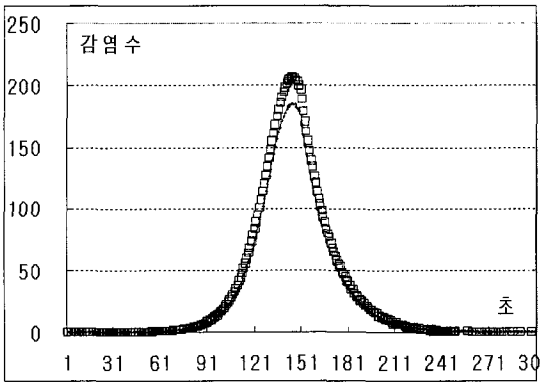


그림 11. 시간대별 국내 감염 호스트 수
■ : 국외에 들어온 감염 패킷에 의해 감염된 국내 호스트 수
□ : 국내 총 감염 호스트 수

2) 2003년 국내 IP대역(KR) 합 : 26,210,000,
국외 IP대역(AN) 합 : 1,831,970,000

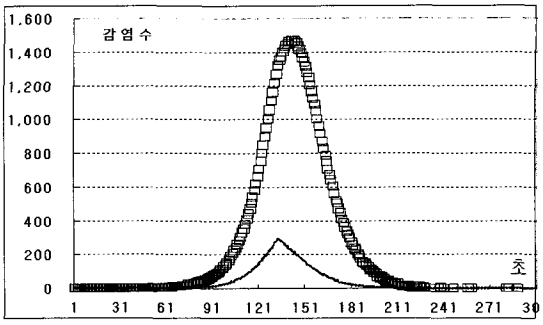


그림 12. 시간대별 국외 감염 호스트 수
■ : 국내에 나간 감염 패킷에 의해 감염된 국외 호스트 수
□ : 국외 총 감염 호스트 수

염 호스트 때문에 3.5시간(12,600초)까지 지속적으로 장애가 발생하였다. 여기에서 시사점은 슬래머 웜처럼 단시간에 대용량의 감염 패킷을 발생시켜 300초 이내에 취약한 호스트가 전부 감염되었다면, 인터넷을 최대한 빠르게 원상회복을 위해서는 최단 시간에 국내 감염 호스트를 자연 격리율(0.00022) 이상으로 인터넷 망에서 분리해야 한다는 점이다.

표 6. 시간대별 KR, AN망 감염 호스트 현황

시간	AN망	KR망
1초	최초 감염	-
36초	-	최초 감염
142초	초당 최대 감염 (1,466대/초)	-
144초	-	초당 최대 감염(207대/초)
224초	최대 감염(72,680대 감염)	-
249초	-	최대 감염(9,670대 감염)
12,600초	18,517대 감염	2,468대 감염

표 7. 시간대별 국제관문국 트래픽 현황

시간	국제관문국 국내=>국외방향	국제관문국 국외=>국내방향
1초	최초 감염	-
36초	-	최초 감염
133초	포화 (4,041,984개 피킷)	-
150초	-	포화 (1,069,952개 패킷)
225초	-	최대 포화 (1,774,348개 패킷)
251초	최대 포화 (16,495,938개 패킷)	-
4,787초	-	정상 상태 (1,069,760개 패킷)
12,600초	준 정상 상태 (4,210,707개 패킷)	정상 상태 (452,085개 패킷)

V. 결 론

본 논문에서는 2003년 전세계의 인터넷망에서 심각한 소통 장애를 일으켰던 슬래머 웜 공격에 대한 분석용 모의실험 모델인 KR-AN모델을 축소화시킨 새로운 모의실험 모델을 제안하고, 기존 모델에서는 생략했던 슬래머 웜에 의한 과도한 감염 패킷으로 인한 망 장비장애의 격리율에 대한 적정 값(0.00022)을 산정하였다. 이를 사용하여 슬래머 웜에 의한 국제관문국 인터넷 소통 장애에 대한 전 시간대(3.5시간, 12,600초) 상황을 분석하여 장애 발생시간 및 원인을 찾았다.

향후에는 이를 활용하여 슬래머 웜같은 비정상 트래픽에 대하여 탐지 후 몇 초 이내에 어떠한 방법으로 대응해야 인터넷 장애를 막을 수 있는지 연구할 계획이다.

참 고 문 헌

〔1〕 "Analysis of the Sapphire Worm." A joint effort of CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego, 2003.

〔2〕 David Moore, et al., "The Spread of the Sapphire/ Slammer Worm." available at http://www.caida.org/ publications/ papers/2003/sapphire/sapphire.html.

〔3〕 David Moore, et al., "Inside the slammer worm," IEEE Magazine of Security and Privacy, pp. 33-39, July/ Aug. 2003.

〔4〕 "정보통신망 침해사고 조사결과," 정보통신망 침해사고 합동조사단, 2003. 2.

〔5〕 C.C.Zou, W.Gong, and D.Towsley, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," WORM'03, Washington, 2003. ACM 1-58113-785-0/03/0010, October 27, 2003.

〔6〕 Stefan Misslinger, "Internet Worm Propagation," Technische University Munchen, 2003.

〔7〕 C.Onwubiko et al., "An Improved Worm Mitigation Model for Evaluating the Spread of Aggressive Network Worms," Serbia & Montenegro, Belagrade, Nov, 2005.

[8] Kevin Fall, Kannan Varadhan, "The ns Manual".

〔9〕 정보통신부, 유·무선 통신서비스 가입자 현황(2003년1월)

〔10〕 주요국내외정보화현황(2004년)

〔11〕 임재명, 윤종호, "슬래머 웜 전파과정 분석을 위한 네트워크 모델링 및 시뮬레이터 구현", 통신공학회지, 2007. Vol.32

〔12〕 2003 한국인터넷백서, 한국전산원.

〔13〕 S. Staniford, V. Paxson, N. Weaver, "How to Own the internetin your spare time," Proceedings of the 11th USENIX Security Symposium (Security '02), 2002.

임 재 명 (Jae-Myung Lim) 정회원

1981년 2월: 한양대학교 전자공학과(공학사)
1983년 9월: 한양대학교 전자공학과(공학석사)
2001년 3월 : 항공대학교 통신정보공학과 박사과정
2000년 11월~현재 : 한국정보보호진흥원 스팸대응팀장

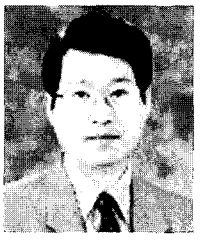
<관심분야> 정보화역기능(해킹, 바이러스, 스팸)

정 한 균 (Han-Gyun Jung) 정회원

2005년 2월 : 한국항공대학교 정보통신공학과(공학사)
2007년 2월 : 한국항공대학교 정보통신공학과(공학석사)
2007년 3월 : 한국항공대학교 정보통신공학과 박사과정

<관심분야> QoS, 무선망 핸드오버

윤 종 호 (Chong-Ho Yoon) 종신회원



1984년 2월 : 한양대학교 전자공학과 졸업(공학사)
1986년 2월 : 한국과학기술원 전기 및 전자공학과 졸업(공학석사)
1990년 8월 : 한국과학기술원 전기 및 전자공학과 졸업(공학박사)
1991년 9월-현재 : 한국항공대학교 항공전자정보 통신공학부 교수

<관심분야> 유무선통신망 설계 및 성능분석