슬래머 웜 전파과정 분석을 위한 네트워크 모델링 및 시뮬레이터 구현

정회원 임 재 명*, 종신회원 윤 종 호*

Modeling and Network Simulator Implementation for analyzing Slammer Worm Propagation Process

Jae-Myung Lim* ***Regular Member***, Chong-Ho Yoon ***Lifelong Member***

요 약

본 논문에서는 2003년 국내 뿐만 아니라 전세계의 인터넷망에서의 심각한 소통장애를 일으켰던 슬래머 웜 보안공격의 전파과정에 대한 새로운 통신망 모델을 제시하고 NS-2를 이용한 시뮬레이터를 구현하여 웜 보안공격에 의한 전파과정을 분석하였다. 기존 DN-AN모델을 Abstract network-Abstract network (AN-AN)모델로 추상화함으로써 국내 뿐만 아니라 전 세계의 수많은 호스트를 대상으로 한 대규모 인터넷망에 대하여 최초의 웜 패킷이 국내의 인터넷 국제관문국으로 유입된 시점부터 국내의 망이 포화되는 전 과정을 시간대별로 분석할 수 있는 NS-2용 시뮬레이터를 구현하였다. 또한 구현된 시뮬레이터는 감염된 국내의 호스트에 의해 국외의 호스트를 감염시키는 과정도 분석 가능하였다. 시뮬레이션 결과 290초만에 8,848개의 국내 호스트가 감염되었고, 308초만에 66,152개의 국외 호스트가 감염되었다. 또한 공격시 수행되는 웜 감염 전파과정에 의해 국내로 유입되거나 국외로 유출되는 웜 감염패킷들은 국제관문국에서 각각 154초와 135초내에 포화됨을 알 수 있었다.

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

ABSTRACT

In this paper, we present a simulation model of Slammer worm propagation process which caused serious disruptions on Internet in the year of 2003 and analyze the process of Slammer by using NS-2. Recently introduced NS-2 modeling called "Detailed Network-Abstract Network Model" had enabled packet level analysis. However, it had deficiency of accommodating only small sized network. By extending the NS-2 DN-AN model to AN-AN model (Abstract Network-Abstract Network model), it is effectively simulated that the whole process from the initial infection to the total network congestion on hourly basis not only for the Korean network but also for the rest of the world networks. Furthermore, the progress of the propagation from Korean network to the other country was also simulated through the AN-AN model. 8,848 hosts in Korean network were infected in 290 second and 66,152 overseas hosts were infected in 308 second. Moreover, the scanning traffics of the worm at the Korean international gateway saturated the total bandwidth in 154 seconds for the inbound traffic and in 135 seconds for the outbound one.

※ 본 논문은 산업자원부 한국산업기술평가원 지정 한국항공대학교 부설 인터넷정보검색 연구센터의 지원에 의함에 의하여 수행되었습니다.
* 한국항공대학교 정보통신공학과 대학원 (jmlim@kisa.or.kr, yoonch@hau.ac.kr)
논문번호 : KICS2007-03-148, 접수일자 : 2007년 3월 26일, 최종논문접수일자 : 2007년 5월 15일

Ⅰ. 서 론

2003년에 발생한 슬래머 웜 공격은 <그림 1>과 같이 인터넷을 통하여 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 웜공격이 시작되면 감염된 서버의 성능 및 통신망의 환경에 따라 웜 바이러스가 수납된 UDP패킷을 초당 약 1만~5만개 (30~150Mbps)을 생성하여 임의의 호스트로 발송함으로써 추가 감염을 유발시키면서 감염 호스트 자신은 다른 작업을 하지 못하는 과부하가 발생하여 결과적으로는 서버에 대한 서비스거부(DoS, Denial of Service) 공격을 받은 결과를 초래하였다. 또한 슬래머 웜은 취약점이 있는 서버뿐만이 아니라, 감염패킷을 임의의 호스트로 무차별 송신함으로써 통신망에 대한 과부하를 유발시켜 다수의 인터넷 사이트 접속 지연이 폭증하는 문제를 발생하였다.[4]

웜 전파과정은 악성 전염병이 전파되는 과정인 Susceptible-Infectious(SI)모델, 패치파일 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] 슬래머 웜인 경우는 단기간에 급속히 확산되었기 때문에 복구를 고려하지 않는 SI모델에 적합하다고 할 수 있다.

하지만 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 패킷단위별로 웜 전파과정에 대한 시뮬레이션이 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]

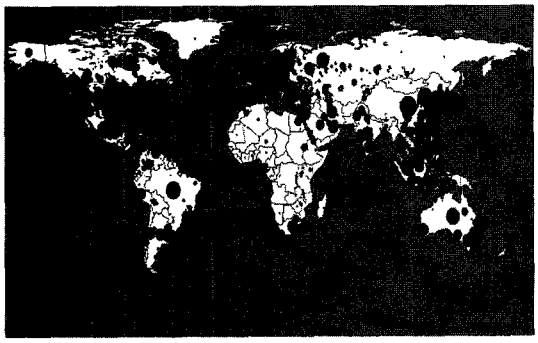


그림 1. CAIDA의 슬래머 웜 확산 시뮬레이션 결과[1]

본 논문에서는 국내 뿐만 아니라 전 세계의 수많은 호스트를 대상으로 한 대규모 인터넷망에 대한 웜 공격과정을 분석할 수 있도록 기존 DN-AN 통신망모델을 Abstract network-Abstract network (AN-AN)통신망 모델로 추상화한 새로운 NS-2용 시뮬레이터를 구현하고, 최초의 웜 감염패킷이 국내의 인터넷 국제관문국(게이트웨이)으로 유입된 시점부터 국내의 망이 포화되는 전 과정을 시간대별로 분석하였다.

제 2 장에서는 웜 전파과정에 따른 SI, SIR, 개선된 SIR모델 3가지를 분석하였다. 제 3 장에서는 패킷레벨의 시뮬레이션이 가능한 DN-AN 모델의 문제점을 분석하고, 제 4 장에서는 이를 개선하여 대규모 망에 대한 시뮬레이션이 가능한 AN-AN모델을 제시하고 NS-2 기반의 시뮬레이터를 구현하였다. 제 5 장에서는 시뮬레이션 결과를 분석하였으며 마지막 제 6 장에서는 결론을 맺었다.

Ⅱ. 웜 전파 모델

웜 바이러스는 자기 복제 및 전파능력을 갖고 있다. 특히 슬래머와 같은 악성 웜 바이러스인 경우, 통신망을 통하여 전파되며, 취약한 호스트를 탐지하고 감염시키기 위해서 지속적으로 스캔닝을 하고, 확산 초기에 전파 최대치에 도달할 뿐만 아니라, 감염 호스트 수에 비례하여 감염비율도 증가하는 특징이 있다.[6] 이러한 웜 바이러스는 자기복제와 전파과정이 생물학적인 바이러스와 매우 유사하기 때문에 다음과 같은 기존의 전염병 모델을 적용할 수 있다.

2.1 Susceptible-Infectious(SI)모델 (Epidemic Model, 전염병 모델)

고전적으로 사용하던 단순한 전염병 모델에 의거, 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. 여기서 감염된 호스트는 복구되지 않거나 폐기되는 것으로 가정한다. 이러한 고전적인 단순 전염병 모델에서 한정된 호스트 수에 대하여 감염속도 β를 고려하면 감

염 호스트 수의 증분은 다음과 같이 기술될 수 있다.

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

즉, 식 (1)은 시간에 따라 감염 호스트의 증분은 감염율 β, 시간 t에서 감염 호스트 수 $I(t)$와 남아 있는 감염 가능한 호스트 수 $S(t)$에 비례하는 것을 의미한다.

2.2 Susceptible-Infectious-Removed (SIR)모델

Kermack-McKendrick의 Susceptible-Infectious-Removed(SIR)모델은 일반적인 SI모델을 확장하여 감염된 호스트에 대한 보안패치 작업에 의해 복구되는 호스트의 수를 고려한 것이다. 즉, 감염 가능성이 높은 취약한 호스트의 수 $S(t)$, 감염된 호스트의 수 $I(t)$, 여기에 복구된 호스트의 수 $R(t)$와 복구비율 γ를 추가로 고려하면 다음과 같이 감염호스트 수의 증분은 SI모델에 비하여 복구되는 호스트의 증분만큼 감소된다. 고정된 호스트의 총 대수 N에 대하여 감염가능성이 높은 호스트의 수 $S(t)$, 감염된 호스트의 수 $I(t)$, 복구된 호스트의 수 $R(t)$는 $S(t)+I(t)+R(t)=N$로 기술된다.

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

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

하지만 이러한 SIR 모델도 전파속도가 아주 빨라 인간의 대응작업이 미진한 경우에는 적합하지 않다. 더욱이 상수 값인 감염비율은 고속으로 전파되는 최근의 웜 바이러스의 특성에 부적합한 단점이 있다.

2.3 Improved Worm Mitigation Model (IWMM)모델

SI 및 SIR모델에 비하여 실제 인터넷 환경에서는 추가적으로 다음 사항이 고려되어야 한다.

- 인간의 대응에 의하여 감염되었거나 감염될 위험에 있는 취약한 호스트를 동시에 복구 또는 예방한다.
- 감염비율 β는 대용량 스캔 트래픽으로 인하여 통신망 내부의 라우터나 링크의 용량제한으로 인해 감속된다.

이러한 2가지 요소를 고려하여 제시된 새로운 모델에서는 기존의 고정된 감염비율 β 대신에 시간에 따른 변수값인 $\beta(t)$를 사용한다. 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.

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

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

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

감염이 확산함에 따라 사람들은 점진적으로 웜을 인식하여 어떻게 대응할지를 습득해서 실지로 대응을 한다. 따라서 시간이 지나갈수록 일반적으로 면역이 된 수가 증가하여 감염가능한 취약한 호스트 수가 줄어들면서 감염속도는 감소한다. 그래서 β_0가 초기 감염비율이라면 $\beta(t)$는 다음과 같이 쓸 수 있다.

$$\beta(t) = \beta_0 [1 - \frac{I(t)}{N}]^{\eta} \quad (7)$$

여기에서 지수 η는 감염된 호스트 수$I(t)$에 대한 감염속도 민감도를 조정하는데 사용한다. 2001년 코드레드의 실지 감염 속도와 2가지 요소를 고려한 웜 모델의 시뮬레이션 결과를 비교하면, 감염예상 집단의 50%가 감염되면 감염비율이 감속됨을 볼 수 있다.[7] 만약 전파모델을 고전적인 SI모델이나 SIR모델을 사용한다면, 대용량의 감염 트래픽으로 인한 네트워크 장비 부하 등 장애에 따른 감염비율의 감속되는 것을 고려하지 않음에 따라 웜의 전파나 피해를 과대평가할 수 있다.

이러한 3가지의 웜 전파 모델은 전체 인터넷에서 시간에 따른 감염 수를 파악하는데 유용하나, 취약한 호스트 비율, 인터넷 네트워크 환경이 각기 틀린 집단에 일률적으로 적용하는 것은 문제가 있다. 2003년 1월 25일 슬래머 웜인 경우, 전 세계적으로 인터넷 소통장애는 있었지만 한국이 특히 인터넷 소통이 심하였던 것은 한국에만 국한된 여러 가지 요소가 다른 나라와 차이가 있었기 때문이다. 따라서 전세계 웜전파 모델을 시뮬레이션하여 국내 상태를 유추해서 해석할 수 있지만, 실지 국내에서 어떤 현상이 벌어졌는지 기존 모델로는 정확하게 해석할 수 없는 한계가 있다.

Ⅲ. 웜 공격과정에 대한 NS-2 통신망 시뮬레이션 모델

3.1 Detailed Network-Abstract Network (DN-AN) 모델

웜 전파과정을 패킷단위로 시뮬레이션하기 위하여 NS-2로 작성된 통신망 모델을 DN-AN 모델이라고 부른다.[8] 이것은 <그림2>와 같이 LAN 외부의 인터넷을 AN(Abstract Network)이라고 추상화시키고, LAN과 같은 소규모 망을 DN(Detailed Network)으로 표기하여, LAN과 인터넷간의 슬래머 웜의 확산과정을 패킷단위로 정밀하게 시뮬레이션 할 수 있도록 하였다. 시뮬레이터에는 DN, AN 네트워크 게이트웨이와 DN 각 호스트에는 웜 감염패킷을 받으면 해당 패킷을 목적지 호스트로 전송하는 Message Passing 에이전트를 붙였다. <그림2>에서는 Message Passing 에이전트를 MP 에이전트로 표시하였다. DN은 취약한 호스트를 DnhWormApp 클래스, 면역된 호스트를 WormApp 클래스로 구분하였고, <그림2>에서는 웜 어플리케이션으로 표시하였다.

이러한 DN-AN 네트워크 모델상에서 실제 슬래머 웜과 동일한 404바이트길이의 패킷, 초당 4000개의 감염 패킷발생율, 감염대상 UDP포트번호로 1434번을 사용하여 UDP기반의 웜 공격과정을 시뮬레이션 할 수 있다. DN의 취약한 호스트는 슬래머 웜의 감염 패킷을 받으면 감염 상태로 변하면서, 감염 1초 후에는 초당 4,000개의 감염 패킷을 랜덤하게 생성하여 DN 및 AN에 할당된 주소영역에 따라 내부망 및 외부망으로 감염 패킷을 송신한다. AN은 감염 호스트 수에 따라 매 초당 감염 패킷을 계산하여 DN 네트워크의 IP주소 대역폭에 해당하는 만큼 DN 네트워크로 전송한다. 감염율, 복구율, DN의 내부 감염율, DN의 취약한 호스트 비율은 각각 시뮬레이션 동작변수로 설정할 수 있어 패킷단위의 웜 공격과정을 정밀하게 시뮬레이션 할 수 있다.

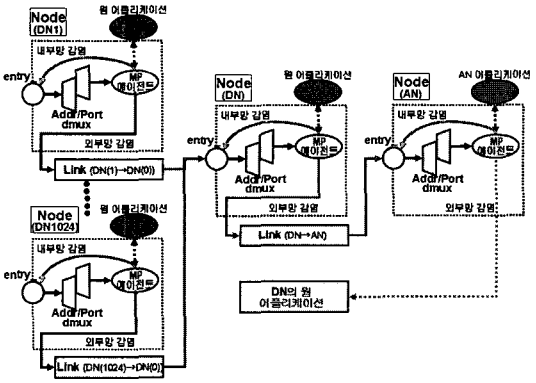


그림 2. DN-AN에 대한 NS2 시뮬레이션 모델

3.2 DN-AN 통신망 모델의 문제점

기존의 DN-AN 모델을 사용한 NS-2 시뮬레이터는 슬래머 웜공격에 대하여 라우터의 Queue 크기 및 전용선 대역폭에 따라 초당 변화를 모니터링 할 수 있는 매우 정밀한 것이다. 그러나 DN에 해당하는 LAN내부에 많은 수의 호스트를 생성하기 때문에 호스트의 개수가 증가하면 엄청난 개수의 패킷에 대한 linked list에 의한 메모리 부족 및 segmentation fault가 발생하는 등의 시스템 및 시뮬레이터의 처리능력 한계로 System Halt 또는 Segmentation Fault 등의 동작오류가 발생하는 문제점이 있었다. <표 1>에서 보듯이 DN의 노드수가 4,096개를 초과하면 시뮬레이션을 위해 사용한 4G바이트의 메모리가 장착된 리눅스 시스템에서 호스트생성 과정 중에 "Segmentation Fault (core dumped)" 오류가 발생하였다. 이러한 문제점을 회피하기 위하여 시뮬레이션이 가능한 범위로 국내 통신망에 해당하는 DN의 호스트의 댓수를 1024개인 소규모 통신망으로 축소하고 이들 중 취약한 호스트 수도 3개로 설정하여 시뮬레이션을 수행한 결과 <표 2>와 같이 334초내에 국외망에 해당되는 AN내의 취약한 74,999개의 호스트를 모두 감염시킬 수 있었지만, DN에 해당하는 국내의 호스트에 대한 감염현상은 파악할 수 없는 문제가 여전히 발생하였다.

표 1. DN-AN 시뮬레이션 결과
(AN 전체 호스트수 = 1,831,970,000, 취약 호스트수 = 74,999)

DN 호스트수	DN내 취약 호스트수	결과
16,777,216	5,634	노드 생성중 Halt
65,536	222	노드 생성중 Halt
32,768	111	Segmentation Fault (core dumped)
4,096	1	시뮬레이션은 가능

표 2. DN-AN 시뮬레이션 결과
(AN 전체 호스트수 = 1,831,970,000, 취약 호스트수 = 74,999)

DN내의 호스트수	DN내 취약 호스트 수	AN의 감염시간
1,024	100	323초
1,024	3	334초

Ⅳ. 웜 공격과정에 대한 개선된 NS-2 통신망 시뮬레이션 모델 : AN-AN 모델

제 3 장에서 다루었던 DN-AN 모델은 패킷단위의 정교한 통신망 모델인 반면에 DN내의 호스트 수가 4,096개를 초과하면 시스템에서 처리하지 못하는 문제가 있었다. 이러한 문제점을 해결하기 위하여 본 논문에서는 <그림 3>과 같이 국내망을 Detailed Network으로 모델링하는 대신에 국외망과 유사하게 추상화시켜 Abstract Network으로 모델링함으로써 국외 및 국내망 모두 Abstract Network인 AN-AN통신망으로 모델링하고, SIR감염모델을 반영하여, DN-AN 모델에서 구현된 Message-Passing 에이전트와 Worm.tcl 프로그램을 수정한 시뮬레이터를 구현하였다. 참고로, 국내망용 AN과 국외망용 AN을 구분하기 위하여, AN-AN을 KR-AN이라고 부르도록 한다.

4.1 감염모델 설정

이러한 KR-AN 시뮬레이션 모델을 구현하기 위하여 각 통신망의 감염된 호스트의 수는 기존 SIR모델을 이용하여 <표 3>와 같이 설정하였다.

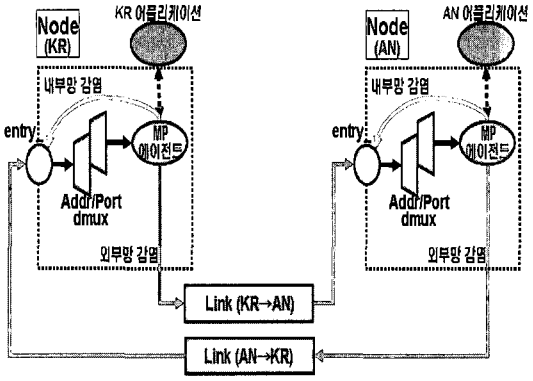


그림 3. KR-AN을 위한 NS2 시뮬레이션 모델

표 3. KR-AN 시뮬레이션 표기

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

감염호스트 수 $I(t)$를 계산하기 위해서 식 (8)에서 4개 요소를 고려하였다. 첫 번째 항은 전시간의 감염 호스트 수 $I(t-1)$이고, 두 번째 항은 취약한 호스트가 감염된 수로 기존 SIR모델을 인용하였다. 세 번째 항은 감염으로부터 복구된 호스트 수로 슬래머 웜인 경우는 초기에 대응을 못했기 때문에 γ를 0으로 처리하였다. 네 번째 항은 자체망의 감염패킷이 아닌 외부 망에서 유입된 감염패킷으로 감염된 호스트를 표기하였다.

$$I(t) = I(t-1) + \beta I(t-1)\frac{S(t-1)}{S_{Max}} - \gamma I(t-1) + I_O(t-1) \quad (8)$$

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

$$R(t) = \gamma I(t-1) \quad (10)$$

식 (8) 두 번째 항의 감염율 β는 초당 4,000개의 감염패킷이 전체 인터넷 대역으로 랜덤하게 퍼졌을 때 KR, AN 네트워크의 취약한 호스트에 도달할 확률이다. 즉 $\beta = 4{,}000 \times \frac{S_{Max}}{2^{32}}$로 표시하고 이에 따라 두 번째 항은 다음과 같이 정리할 수 있다.

$$\eta I(t-1)\frac{S(t-1)}{S_{Max}} = 4{,}000 \times \frac{S_{Max}}{2^{32}} \times I(t-1) \times \frac{S(t-1)}{S_{Max}} = 4{,}000 \times \frac{I(t-1) \times S(t-1)}{2^{32}} \quad (11)$$

식 (8) 네 번째 항의 외부망에 의한 감염 호스트 수 $I_O(t)$는 외부망에서 들어온 감염패킷 수($ProbeRecv$)와 자체망의 취약수에 비례하며 식 (12)과 같이 정리할 수 있다. KR, AN망으로 들어온 감염패킷 수($ProbeRecv$)는 AN, KR에서 상대망으로 나간 감염패킷 수($ProbeOut$)와 같으며, 외부망으로 나간 감염패킷 수는 식 (14)와 같이 표시한다. 식 (13),(14)의 아래 첨자 A or K는 AN, KR망을 표시한다.

$$I_O(t-1) = ProbeRecv \times \frac{S(t-1)}{N} \quad (12)$$

$$ProbeRecv_{K\,or\,A} = ProbeOut_{A\,or\,K} \quad (13)$$

$$ProbeOut_{A\,or\,K} = 4{,}000 \times I_{A\,or\,K}(t-1) \times \frac{IP_{K\,or\,A}}{2^{32}} \quad (14)$$

외부망에서 들어온 감염패킷 수($ProbeRecv$)는 KR, AN 네트워크 게이트웨이의 Queue와 네트워크 대역

폭에 제한을 받기 때문에 다음과 같은 조건을 만족하여야 한다. 식 (15)는 상대망으로 나간 감염패킷 수는 상대망 게이트웨이의 Queue처리용량을 넘을 수 없으며, 식 (16)은 KR-AN 링크에 흐르는 패킷양(bps)는 주어진 대역폭을 넘을 수 없음을 표시한다.

$$ProbeOut_{AorK} \le Q_{AorK} \quad (15)$$

$$4{,}000 \times (ProbeOut_{AorK} + ProbeRecv_{AorK}) \times 8bit \le BW \quad (16)$$

4.2 개선된 KR-AN모델에 따른 시뮬레이션 프로그램의 재구성

첫째 기존 DN 네트워크의 각 호스트들을 추상화한 KR-어플리케이션 모듈을 만들었다. 기존 DN 네트워크의 호스트 노드 수가 최대 4,096개 이상 확장하지 못하기 때문에 DN 네트워크 게이트웨이와 여기에 연결되어 있는 각 DN 호스트들의 웜 어플리케이션에 해당하는 부분을 AN 네트워크처럼 Abstract Network로 추상화하여 KR-어플리케이션으로 만들었다. KR-어플리케이션 모듈은 기존 DN 네트워크의 각각의 웜 어플리케이션을 대신하여 감염패킷 수신에 따라 감염 여부 결정, 감염에 따른 감염패킷 발생 등을 대신하게 하였다.

둘째 AN 네트워크에서 KR 노드의 entry로 감염패킷을 직접 보낼 수 있도록 Link를 변경하였다. 기존 DN-AN 모델에서는 AN-어플리케이션에서 감염된 호스트들이 발생한 감염패킷은 기존 DN 네트워크 내에 있는 각 호스트의 Message Passing 에이전트를 거쳐 웜 어플리케이션 모듈에 전달하였다. 그러나 KR-AN 모델에서는 각 DN 네트워크 내 호스트로 감염패킷을 전달하는 대신 <그림 3>처럼 Link(AN->KR)를 거쳐 KR 노드의 entry로 보낼 수 있게 수정하였다.

V. NS-2 기반 KR-AN 시뮬레이션 결과 분석

5.1 시뮬레이션 환경

구현한 시뮬레이터를 이용한 슬래머 웜 전파과정 분석을 위하여 리눅스 PC(CPU 4.7MHz, 메모리 4G)에 버전 2.30의 NS-2를 설치하였다. 슬래머 웜으로 감염된 호스트가 생성하는 감염패킷의 전송율은 CAIDA자료에 의거 초당 4천개로 설정하였다. 이외의 각 파라메타 값은 <표 4>과 같다. 각 파레메타는 정보화통계와 유무선 통신서비스 가입자 현황을 참조하였다.[9][10]

표 4. 시뮬레이션 값

항목	값
인터넷 IP수	4,294,967,296
AN IP수	1,831,970,000
AN 호스트수	693,020,000
AN 취약한 호스트 수	66,152
KR IP수	26,210,000
KR 호스트수	21,145,268
KR 취약한 호스트 수	8,848
KR=>AN queue	5,083,000
AN=>KR queue	1,113,000
KR<=>AN 지연시간	1ms
KR<=>AN Queue정책	DropTail
KR<=>AN 대역폭	21.21Gbps

5.2 분석 결과

2003년 당시 슬래머 웜의 초기 확산단계의 정확한 상태 값이 없기 때문에 당시의 네트워크 트래픽과 네트워크의 구성을 고려하고 상대적인 시간에 따른 감염호스트의 추이 변화에 주안점을 두고 시뮬레이션을 수행하였다. 최초의 감염은 AN에서 시작되었고, KR은 AN에서 유입된 감염패킷에 의해서 감염되었다 가정하였다. 전 과정에 대한 시뮬레이션은 PC상에서 총 240시간 소요되었으며 결과는 다음과 같다. <그림 4>는 시간대별 국내 및 국외의 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 반면에 본 논문 시뮬레이션 결과는 308초로 차이가 있었다.[1] 감염 시간의 차이는 당시에는 슬래머 웜 공격으로 인한 일부 네트워크 구간은 포화 상태가 되어 더 이상의 감염패킷을 전달하지 못했고, 일부 네트워크 라우터는 과도한 감염패킷으로 인해 정지 상태로 빠져서 시뮬레이션보다 감염패킷이 덜 전달되어 감염시간도 자연히 늦어졌기 때문으로 판단된다. AN의 최초 감염이 1초에 시작되었다고 가정했을 때 KR의 최초 감염은 24초에 발생하였다. 또한 KR망의 취약한 8,848대 호스트와 국외 AN망의 취약한 66,152대 호스트는 각각 290초와 308초에 모두 감염되었다.1) 국내(KR)의 감염시간이 짧고 빠른

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

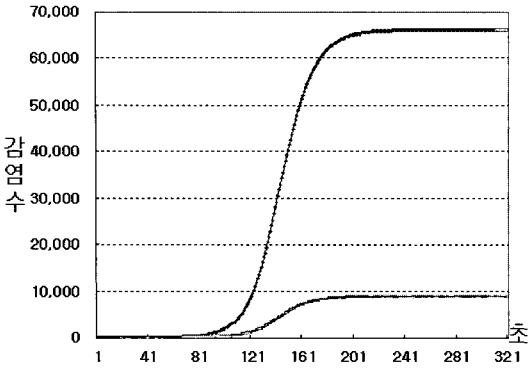


그림 4. 시간대별 국내외 슬래머 웜 감염 호스트 수
청색 : AN의 감염호스트 수 누계
주황 : KR의 감염호스트 수 누계

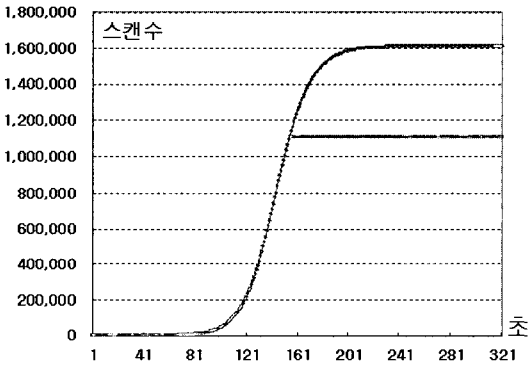


그림 5. 시간대별 국외에서 국내로 유입된 감염패킷 수
청색 : AN에서 KR로 보낸 감염패킷 수
주황 : AN에서 KR로 보낸 감염패킷 중 KR이 받은 수

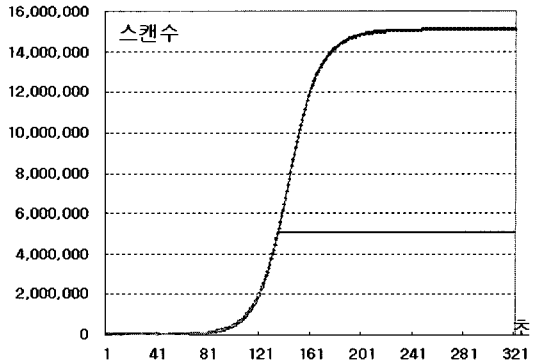


그림 6. 시간대별 국내에서 국외로 나간 감염패킷 수
청색 : KR에서 AN으로 보낸 감염패킷 수
주황 : KR에서 AN으로 보낸 감염패킷 중 AN이 받은 수

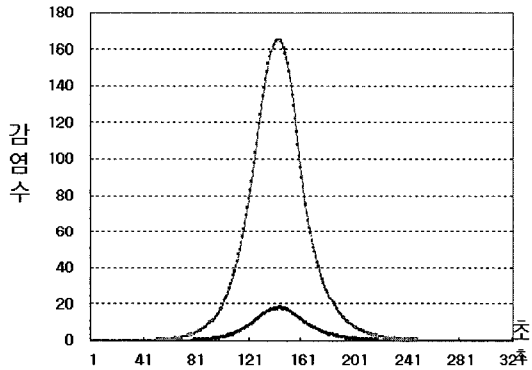


그림 7. 시간대별 국내 감염 호스트 수
청색 : KR에서 KR로 보낸 감염패킷에 의해 감염된 호스트 수
주황 : AN에서 KR로 보낸 감염패킷에 의해 감염된 호스트 수

것은 상대적으로 국외(AN)에 비해 취약한 호스트 비율이 4.4배[2] 높았던 것이 주요 원인으로 추정된다.

<그림 5>은 외국의 감염된 호스트가 국제관문국(게이트웨이)을 통하여 국내로 송신한 웜 감염패킷 수를 표시하였다. 국외에서 국내로 유입되는 감염패킷은 다른 서비스 트래픽이 없고 슬래머 웜 트래픽만 있다고 가정할 때 국내 유입된 감염패킷 수는 154초에 1,113,000개로 Queue를 채웠고, 그 이후부터는 초과된 패킷은 국제관문국에서 통과하지 못하고 버려졌음을 확인할 수 있다. <그림 6>은 국내에서 감염된 호스트가 국외로 송신한 웜 감염패킷 수를 표시하였다. 국외로 나간 감염패킷 수는 135초에 5,083,000개로 포화되어 그 이후부터는 초과된 패킷은 국제관문국에서 버려졌음을 확인할 수 있다. 이로 인해 각각 해당 시간 이후부터는 국제관문국에서 감염패킷 수는 더 이상 증가하지 않고 통신망의 용량 한계로 감속하는 단계로 접어들었음을 알 수 있다.

<그림 7>은 시간대별 국내 감염 호스트 수를 표시한 것이다. 그림에서 보듯이 국내 감염의 대부분은 국외에서 유입된 감염패킷에 의하여 감염되었음을 보여주고 있다. 국외에서 유입된 감염패킷으로 감염된 호스트 수는 142초에 초당 165대로 최대를 기록하였고, 국내 전파에 의해 감염 호스트 수는 같은 142초에 18대로 최대를 기록하였다. 국외에서 유입된 감염패킷에 감염이 많았던 것은 슬래머 웜 전파 특성상 랜덤하게 스캔하기 때문에 국내 감염된 호스트에서 발생한 감염패킷은 대부분 국내(KR)의 IP대역보다는 국외(AN)로 나갔기 때문이다[3]. 이 결과를 보면 랜덤하게 전파하는 초고속 웜이 발생했을 때에는

2) 국내 감염 호스트 수(8,848대)/호스트 수(2114만대) 대비 국외 감염 호스트 수(66,152대)/호스트 수(6억9302만대)

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

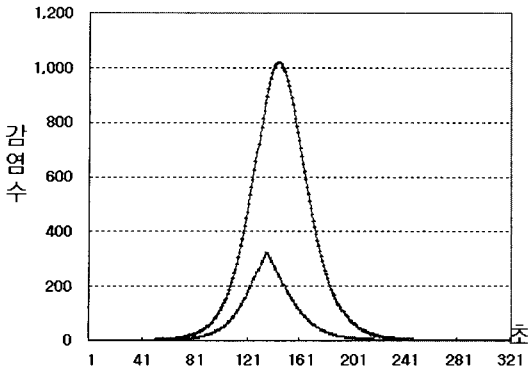


그림 8. 시간대별 국외 감염 호스트 수
청색 : AN에서 AN으로 보낸 감염패킷에 의해 감염된 호스트 수
주황 : KR에서 AN으로 보낸 감염패킷에 의해 감염된 호스트 수

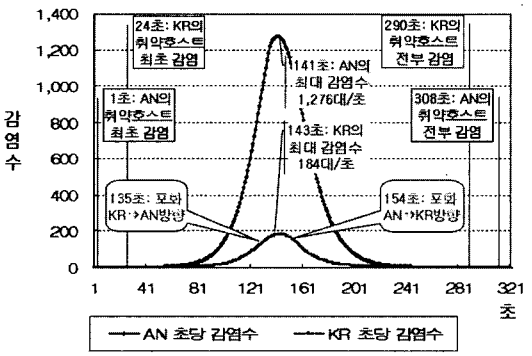


그림 9. 시간대별 슬래머 웜 이벤트

우선적으로 국제관문국에서 전파에 악용되는 포트(예: 슬래머인 경우 1,434포트)를 일시적으로 차단하는 것이 감염을 감속하는데 가장 좋은 방법으로 판단된다.

<그림 8>은 시간대별 국외 감염 호스트 수를 표시한 것이다. 그림에서 보듯이 국외 감염의 대부분은 국외 자체의 스캔에 의하여 감염되었음을 보여주고 있다. 국외 자체 스캔으로 감염된 호스트 수는 143초에 초당 1,019대를 최대를 기록하였고, 국내발 감염패킷에 의해 감염된 호스트 수는 134초에 321대로 최대를 기록하였다.

<그림 9>은 시간대별 국내외 감염 호스트 수 및 국제관문국 상태를 정리하였다. 1초에 국외에서 최초로 슬래머 웜에 의해 감염된 호스트 1대가 발생하였고, 24초에 국외에서 유입된 감염패킷에 의해 국내 취약한 호스트가 감염되었으며, 135초에 국제관문국의 국내에서 국외방향으로 초당 5,083,000개 감염패킷이 발생하여 포화상태가 되었으며, 154초에는 국제관문국의 국외에서 국내방향으로 초당 1,113,000개 감염패킷이 유입되어 포화상태가 되었다. 감염호스트 수의 최대치는 국외인 경우 141초에 초당 1,276대 감염되었으며, 국내인 경우 143초에 초당 184대 감염되었다. 290초에는 국내의 취약한 8,848대 호스트 전부가 슬래머 웜에 감염되었고 308초에는 국외 66,152대의 호스트 전부가 감염되었음을 알 수 있다.

Ⅵ. 결 론

본 논문에서는 2003년 전세계의 인터넷망에서 심각한 소통장애를 일으켰던 슬래머 웜 공격의 전파과정에 대한 새로운 통신망 모델을 제시하고 NS-2를 이용한 시뮬레이터를 구현하여 웜 공격에 의한 전파과정을 분석하였다.

실제 슬래머 웜 전파시에는 아무런 대비가 없었기 때문에 관련된 자료가 불충분하여 제한된 자료를 바탕으로 시뮬레이션 하기에는 부족하였지만 본 논문에서 구현한 시뮬레이터의 유용성을 검증할 수 있었다. 시뮬레이션 결과, 국내의 취약한 호스트 비율이 국외에 비해 4.4배 높았던 것이 주 원인이 되어, 국외보다 국내 전체 감염시간이 13초 빠르게 290초에 나타났다. 또한 국제 관문국에서는 국내발 감염패킷으로 인하여 135초만에 통신망이 포화됨으로써 네트워크에서는 소통의 지장이 발생하고 있었다고 추정된다. 다시 말해서 전체가 감염되기도 전에 이미 네트워크 장비의 처리능력을 초과하였기 때문이라고 추정할 수 있다.

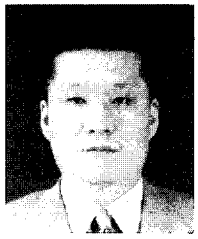
마지막으로, 본 논문에서 구현한 시뮬레이터는 대규모의 통신망에서의 웜 확산과정을 엄청난 수로 발생하는 패킷을 일일이 시뮬레이션하는 것이어서 결과를 얻기에 너무 시간(240시간)이 소요되기 때문에 향후에는 시간을 단축할 수 있는 새로운 시뮬레이션 방법으로 개선할 필요가 있다. 시뮬레이션에 많은 시간을 소요하는 가장 큰 요인인 KR과 AN의 호스트 수 및 취약한 호스트를 각각 동률로 축소하여 시험한 결과와 이번 결과를 비교하여 유사한 결과가 나도록 하는 개선된 시뮬레이터를 구현할 계획이다.

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.

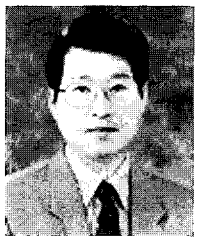
〔2〕 David Moore, et al., "The Spread of the Sapphire /Slammer Worm." available at http://www.caida.org/publications/ papers/2003/sapphire/sapphire.html.
〔3〕 David Moore, et al., "Inside the slammer worm," IEEE Magazine of Security and Privacy, pp. 33-39, July/Aug. 2003.
〔4〕 "정보통신망 침해사고 조사결과," 정보통신망 침해사고 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)

임 재 명 (Jae-Myung Lim) 정회원



1981년 2월 : 한양대학교 전자공학과 공학사
1983년 9월 : 한양대학교 전자공학과 공학석사
2001년 3월 : 항공대학교 통신정보공학과 박사과정
2000년 11월~재 : 한국정보보호진흥원 스팸대응팀장
<관심분야> 정보화역기능 (해킹, 바이러스, 스팸)

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