고성능 네트워크에서 인터넷 웜 확산 모델링

신 원†

요 약

최근 정보기술의 발달로 통신, 방송, 인터넷 등의 모든 서비스들이 하나의 네트워크로 통합되는 광대역 통합망이 등장하게 되었다. 그러나 이에 대한 역기능으로 다양한 위협이 등장하고 있으며, 그 중 인터넷 웜과 같은 악성 코드는 국가 기간망을 뒤흔드는 혼란을 초래할 수 있다. 본 논문은 고성능 네트워크 환경에서 웜 확산에 대한 정확한 예측을 그 목표로 한다. 이를 위해 인터넷 웜에 적용 가능한 확산 모델을 살펴보고, 여러 인터넷 웜을 적용하여 인터넷 환경에서 동작 방식을 분석한다. 제안 모델은 웜 확산 단계와 대응 단계에 따른 영향을 분석하여 인터넷 웜의 확산 규모와 속도를 보다 정확하게 예측할 수 있다. 본 논문의 결과는 광대역 통합 네트워크와 같은 고성능 네트워크에도 적용할 수 있다.

키워드 : 웜 확산, 인터넷 웜, 광대역 통합망

Modeling the Spread of Internet Worms on High-speed Networks

Shin, Weon†

ABSTRACT

Recently broadband convergence network technology is emerging as an integrated network of telecommunication, broadcasting and Internet. But there are various threats as side effects against the growth of information technology, and malicious codes such as Internet worms may bring about confusions to upset a national backbone network. In this paper, we survey the traditional spreading models and propose a new worm spreading model on Internet environment. We also analyze the spreading effects due to the spread period and the response period of Internet worms. The proposed model leads to a better prediction of the scale and speed of worm spreading. It can be applied to high-speed network such as broadband convergence network.

Key Words : Worm Epidemics, Internet Worm, Broadband Convergence Network

1. 서 론

정보기술의 발달로 누구나 네트워크를 통하여 텍스트, 이미지, 사운드, 동영상 등의 멀티미디어 데이터를 접할 수 있게 되었으며, 이를 통한 원격 회의, 가상 학습, 원격 진료 등이 가상세계에서도 가능하게 되었다. 또한, 최근에는 방송, 인터넷, 통신을 융합하여 언제 어디서나 양질의 멀티미디어 서비스를 받을 수 있는 광대역 통합망인 BcN(Broadband convergence Network)이 등장하고 있다. 그러나, 다양한 네트워크 기술과 어플리케이션이 등장함에 따른 역기능들도 함께 증가하고 있다. 인터넷 서비스를 제공하는 다양한 서버에 대한 해킹 시도, 바이러스 및 웜을 통한 공격을 받고 있으며 취약성이 노출되어 정상적인 서비스가 어려운 경우도 발생하고 있다. 그 중 서비스 거부 공격의 형태로 가용성에 피해를 가하기 위해 가장 많이 이루어지는 것이 인터넷 웜을 통한 공격이다.

일반적으로 인터넷 웜은 호스트 운영체제의 구현 버그, 설계 결함 등의 취약성을 이용한 후 비인가된 소프트웨어 코드를 실행하는 악성 소프트웨어(Malicious Software)이다. 뿐만 아니라 인터넷 웜은 같은 취약성을 가진 다른 호스트로 인터넷 망을 이용하여 자기 자신을 복제하도록 구현되어 있는데, 이 과정 중에 수행되는 무한 루프와 발생되는 패킷은 시스템 및 네트워크 환경에 오버헤드를 초래할 뿐만 아니라 인터넷을 통한 정상적인 서비스가 불가능하도록 만든다. 실제 인터넷 웜의 확산은 지수적인 증가를 하고 있으며, 네트워크 성능과 속도에 비례하여 확산되는 것으로 조사되고 있다. 따라서, 고성능 네트워크 환경에서 웜의 확산은 단순한 악성 소프트웨어 확산의 의미뿐만 아니라 웜의 희생자가 곧 또 다른 공격자가 되어 네트워크 전체를 사용불능으로 만드는 분산 서비스 거부 공격의 의미를 가진다.

본 논문에서는 인터넷 웜 확산에 대한 모델링을 통하여 광

† 정 회 원 : 동명정보대학교 정보보호학과 전임강사
논문접수 : 2005년 7월 20일, 심사완료 : 2005년 8월 18일

대역 통합망과 같은 고성능 네트워크 환경에서 그 영향을 분석하고자 한다. 먼저 2장에서는 관련 연구에 대하여 살펴보고, 3장에서는 웜 확산 모델을 제안한다. 4장에서는 웜 확산 모델을 분석한 후 실제 환경을 고려한 시뮬레이션을 수행하고, 마지막 5장에서 결론을 맺는다.

2. 관련 연구

인터넷 웜에 대한 확산은 과거 질병 역학에서 연구한 전염병 확산에 대한 모델을 적용할 수 있다. 이미 많은 학자들에 의해 여러 가지 모델이 제안되어 있으나 실제 컴퓨터 네트워크 상에서 동작하는 인터넷 웜에 적용하기에는 여러 전제 조건과 수정 사항이 필요하다. 본 장에서는 가장 대표적인 모델인 SI 모델[1], SIR 모델[2]과 기타 연구들을 설명한다. 다음 <표 1>은 본 논문에서 사용하는 표기에 대한 설명이다.

〈표 1〉 본 논문의 표기법

표 기	정 의
N	감염 가능한 전체 호스트 수
$S(t)$	시각 t에 취약한 호스트 수
$I(t)$	시각 t에 감염 호스트 수
$R(t)$	시각 t에 제거 또는 복구된 호스트 수
$s(t)$	시각 t에 취약한 호스트 비율
$i(t)$	시각 t에 감염 호스트 비율
$r(t)$	시각 t에 제거 또는 복구된 호스트 비율
β	단위 시간 당 확산율
γ	감염 호스트에 대한 제거율 또는 복구율
δ	취약한 호스트에 대한 복구율

SI 모델은 각 호스트가 S(Susceptible), I(Infectious)의 2가지 상태를 가진다[1]. 호스트가 S 상태를 가지는 경우 β의 비율로 웜에 감염되어 I 상태로 변경된다. 이에 대한 미분 방정식은 다음과 같이 나타낼 수 있다.

$$\frac{dS}{dt} = -\beta SI/N$$
$$\frac{dI}{dt} = \beta SI/N$$

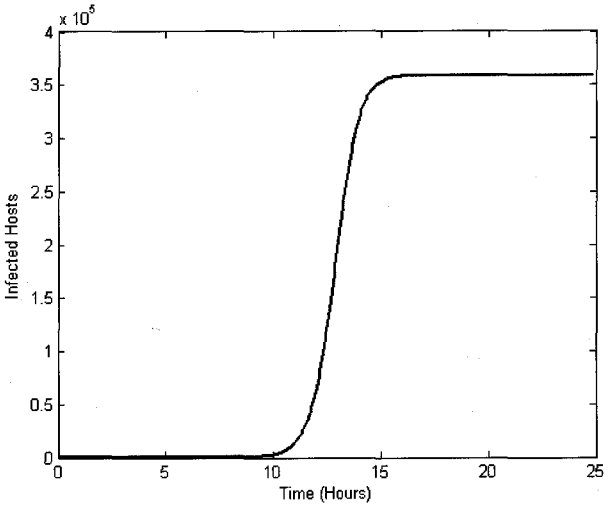
위 식에서 감염된 호스트의 비율은 아래와 같이 나타낼 수 있다.

$$\frac{di}{dt} = \beta i(1-i)$$

위 미분 방정식은 $t \geq 0$인 모든 t에 대하여 $S(t)+I(t)=N$, $s(t)+i(t)=1$, $\frac{di}{dt}+\frac{ds}{dt}=0$을 만족하며, 해를 구하면 다음과 같다.

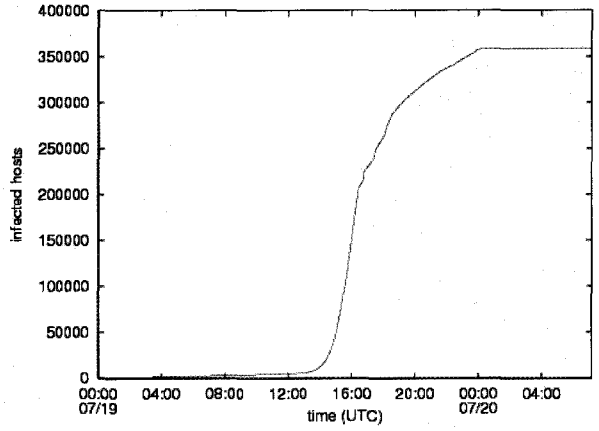
$$i(t) = \frac{1}{1+e^{-\beta(t-T)}}$$ (여기서, T는 적분 상수)

즉, t시점에서 감염된 호스트 비율을 나타낸다. 이를 이용하여 2001년 7월 359,000대를 감염시켰던 Code Red 웜의 확산을 그래프로 그리면 다음 (그림 1)과 같다. 여기서, 감염 가능한 전체 수 $N=359,000$, 확산율 $\beta=1.8$, 초기값 $T=11.9$이다 [3].



(그림 1) Code Red 웜 확산 모델링

다음 (그림 2)는 CAIDA[3]에 의한 Code Red 웜의 실제 측정치이다.



(그림 2) Code Red 웜 확산(2001년 7월)

SIR 모델은 각 호스트가 S(Susceptible), I(Infectious), R(Removed)의 3가지 상태를 가진다[2]. 호스트가 S 상태를 가지는 경우 β의 비율로 웜에 감염되어 I 상태로 변경되고, 감염되어 I 상태인 호스트는 γ의 비율로 제거된다. 이에 대한 미분 방정식은 다음과 같이 나타낼 수 있다.

$$\frac{dS}{dt} = -\beta SI/N$$
$$\frac{dI}{dt} = \beta SI/N - \gamma I$$

$$\frac{dR}{dt} = \gamma I$$

위 미분 방정식은 $t \geq 0$인 모든 t에 대해 $S(t)+I(t)+R(t) = N$, $\frac{dI}{dt}+\frac{dS}{dt}+\frac{dR}{dt}=0$을 만족한다. 그 중 감염된 호스트의 비율은 아래와 같이 나타낼 수 있다.

$$\frac{di}{dt} = \beta si - \gamma i$$

위 식에 따르면 웜이 확산하기 위한 조건을 계속 유지하기 위해서는 S상태에서 비율 β로 확산되는 값이 R상태로 비율 γ로 제거되는 값보다 항상 커야만 한다. 즉, 항상 $\beta si > \gamma i$를 만족해야만 웜이 계속 확산할 수 있다. 또한, SIR 모델에서 R 상태는 반드시 감염 상태인 I 상태에서만 갈 수 있고, 그 경우는 감염 후 웜을 치료하거나 호스트가 중지된 경우에 해당한다.

2001년 7월 Code Red의 확산 이후 인터넷 웜 확산에 대한 관심이 고조되어 이를 분석하기 위한 목적으로 다양한 학자들에 의한 여러 방안들이 시도되었다. S. Staniford 등[3]은 Code Red 웜의 확산을 모델링하기 위하여 고전적 모델인 SI 모델을 적용하고, 웜의 동작 방식을 분석하고 확산 속도에 따라 웜을 분류하였다. 또한, J. Kim 등[4]은 SI 모델을 개선한 SIS 모델과 SIR 모델을 확장하여 웜 전파에 대한 모델을 제안하고 인터넷 토폴로지에 따른 결과를 분석하였다. C. C. Zou 등[5]은 인터넷 웜 확산에서 사람의 대응이 확산을 둔화시킨다는 사실과 감염이 진행될수록 확산율이 감소된다는 동적인 측면을 고려하여 보다 실제적인 모델을 제안하였다.

3. 인터넷 웜 확산 모델의 제안

컴퓨터 바이러스가 특정 파일에 기생하여 그 파일이 실행되는 순간 바이러스가 동작하는 기생형 악성 코드인데 반하여, 인터넷 웜은 독립적인 악성 코드로 일반 프로그램과 같이 그 자체만으로도 실행이 가능하며 다양한 시스템 자원을 활용하여 정의된 동작을 수행한 후 네트워크를 통하여 자기 자신을 복제하여 전파한다. 최근 등장하는 인터넷 웜의 특징을 살펴보면 다음과 같다.

- 메모리 상주형 : 과거 파일 형태의 웜에서 메모리 상주형으로 전환하여 기존의 파일 기반의 백신으로는 치료가 어렵도록 제작되는 추세
- 크기의 감소 : Nimda가 60KB, Code Red가 4KB, Slammer Worm이 404B로 그 크기도 작아지고 있음
- 네트워크 자원의 고갈 : 시스템을 직접 공격하는 것은 물론 다량의 패킷을 발생하여 네트워크 대역폭을 고갈, 결국 DoS(Denial of Service) 또는 DDoS(Distributed DoS)의 효과를 유발
- 비연결 방식을 이용한 무작위 배포 : TCP(Transmission Control Protocol) 패킷을 이용한 연결 전송 방식에서 UDP 패킷을 통한 비연결 전송 방식을 사용
- 스캐닝 속도의 증가 : 감염 대상을 찾는 속도를 증가시키기 위해 랜덤 스캐닝을 사용하고 있으며 갈수록 고속화되고 있음

본 장에서는 앞에서 설명한 SI 모델과 SIR 모델의 특징을 취하여 인터넷 웜 확산에 적합한 새로운 모델을 제안한다.

3.1 제안 확산 모델

제안 확산 모델은 기존 모델과는 달리 특정 시점 λ를 기준으로 확산 단계(Spread Period), 대응 단계(Response Period)로 나뉘어 동작한다.

확산 단계(Spread Period)

$$S \xrightarrow{\beta} I$$

SI 모델과 마찬가지로 각 호스트가 S(Susceptible), I(Infectious)의 2가지 상태를 가진다. 해당되는 미분 방정식은 앞에서 설명한 SI 모델과 같다.

$$\frac{ds}{dt} = -\beta si, \quad \frac{di}{dt} = \beta si$$

여기서, 초기 조건은 $s(0) = s_0 \simeq 1$, $i(0) = i_0 \simeq 0$이고, $0 \leq t < \lambda$인 모든 t에 대해 $s(t)+i(t)=1$, $\frac{di}{dt}+\frac{ds}{dt}=0$을 만족하며, 해는 SI 모델의 해와 역시 동일하다. 단, SI 모델에서 t가 0에서 무한대의 범위를 가지는데 반해, 제안 모델의 확산 단계에서는 t가 인터넷 웜이 확산하기 시작하는 0부터 대응을 시작하는 λ까지만 지속된다.

대응 단계(Response Period)

$$S \xrightarrow{\beta} I \xrightarrow{\gamma} R, \quad S \xrightarrow{\delta} R$$

SIR 모델과 마찬가지로 각 호스트가 S(Susceptible), I(Infectious), R(Recovery)의 3가지 상태를 가진다. 그러나, SIR 모델과는 달리 웜에 대한 대응을 시작하면서 S 상태에서 R 상태로 직접 변경되는 호스트가 존재한다. 각 상태에서의 비율에 대한 미분 방정식은 다음과 같이 나타낼 수 있다.

$$\frac{ds}{dt} = -\beta si - \delta s$$

$$\frac{di}{dt} = \beta si - \gamma i$$

$$\frac{dr}{dt} = \gamma i + \delta s$$

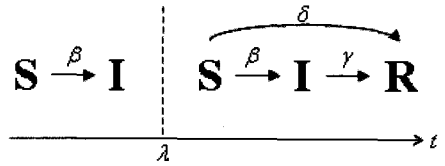
여기서, 초기 조건은 $s(\lambda) = s_\lambda$, $i(\lambda) = i_\lambda$, $r(\lambda) = 0$이고, $\lambda \leq t \leq \infty$인 모든 t에 대해 $s(t)+i(t)+r(t)=1$, $\frac{di}{dt}+\frac{ds}{dt}+\frac{dr}{dt}=0$을 만족한다. 단, 제안 모델의 대응 단계에서 t가 대응을 시작하는 λ에서 무한대까지 값을 가진다.

위 미분 방정식은 오일러의 방법(Euler's Method)[6]을 통하여 아래와 같은 식으로 나타낼 수 있다.

$$s(n)=s(n-1)-\{\beta s(n-1)i(n-1)-\delta s(n-1)\}\Delta t$$
$$i(n)=i(n-1)+\{\beta s(n-1)i(n-1)-\gamma i(n-1)\}\Delta t$$
$$r(n)=r(n-1)+\{\gamma i(n)+\delta s(n)\}\Delta t$$

보다 정밀한 값을 구하기 위해서는 개선된 오일러의 방법(Improved Euler's Method)[7]을 사용할 수도 있지만, Δt를 0.001~0.1 시간 정도로 충분히 작게 하면 오일러의 방법으로도 충분히 높은 정밀도로 근사값을 구할 수 있으므로 본 논문에서는 오일러의 방법을 사용하기로 한다.

(그림 3)은 확산 단계와 대응 단계를 함께 표현한 제안 모델을 도식화하여 보여준다. 확산 단계에서 SI 모델을 기반으로 인터넷 웜의 확산이 진행되다가 λ 시점부터 대응 단계로 바뀌면서 개선된 SIR 모델을 기반으로 웜 확산 및 복구가 함께 이루어진다.



(그림 3) 제안 인터넷 웜 확산 모델

3.2 제안 확산 모델의 분석

인터넷 및 광대역 통합망에서 인터넷 웜의 확산을 SI 모델에만 적용하는 경우에는 웜 확산에 대한 설명은 가능하지만 치료 및 대응에 따른 웜 확산의 감소는 알 수 없다. 또한, SIR 모델에 적용하는 경우에는 감염되는 호스트만이 복구될 수 있으므로 감염되기 이전에 인터넷 웜 대응에 따른 효과를 분석할 수 없는 문제점이 있다. 이러한 문제점을 해결하고 웜 확산을 좀 더 정확하게 설명하기 위한 모델이 제안 모델인 "SI-SIR 모델"이다. 제안 SI-SIR 모델의 특징을 정리하면 다음과 같다.

1. 인터넷 웜의 확산은 전체 감염 가능한 호스트 수 N에 의존하는 것이 아니라 최초 감염 비율 $s(0)$와 확산율 β에 의존한다. 여기서, $s(0)$는 최초 감염된 호스트의 비율이고, β는 웜의 동작 방식, 네트워크 속도에 따라 결정되는 고유한 값으로 웜에 따라 다른 값을 가진다. 역으로 β를 통하여 웜을 판단할 수 있다.
2. 대응 시점 λ가 0에 가까울수록 인터넷 웜의 확산이 둔화되고, 둔화 속도는 γ, δ에 의존한다. 즉, 웜 대응에 따른 복구율과 면역율이 크면 클수록 빠른 속도로 인터넷 웜에 감염된 호스트 수는 감소한다.
3. 대응 시점 λ이후 S 상태에서 I 상태를 거치지 않고 R 상태로 직접 변경되는 복구율 δ가 존재한다. 이는 웜에 대한 대응을 수행하여 취약한 호스트가 취약하지 않은 호스트가 되었음을 의미한다.
4. 인터넷 웜의 확산이 일정시간 동안 거의 증가하지 않다가 폭발적으로 증가하기 시작하는 시점은 웜에 따라 고유한 값을 가진다. 역으로 그 값을 통해 특정 웜을 결정할 수도 있다. 예를 들어, Code Red는 $t=11.9$(시간), Slammer Worm은 $t=30.145$(분)이다.

앞에서 설명한 바와 같이 제안 SI-SIR 모델은 SI 모델과 SIR 모델의 특징을 결합하여 개선한 모델로써 인터넷 웜 확산은 웜에 대한 대응을 시작하는 시점인 λ부터 서로 다른 형태를 가진다. 즉, $\lambda\simeq 0$이면 개선한 SIR 모델과 유사하게 동작하고 λ가 충분히 크면 SI 모델과 유사하게 동작한다.

제안 SI-SIR 모델 중 웜의 확산에 관련한 함수 $i(t)$는 다음과 같이 다시 쓸 수 있다.

$$\frac{di(t)}{dt}=\begin{cases}\beta s(t)i(t), & 0\le t<\lambda\\ \beta s(t)i(t)-\gamma i(t), & \lambda\le t\le\infty\end{cases}$$

여기서, λ부터 대응 이후 감염 호스트 비율을 $i_\lambda=i(\lambda)$, 감염가능한 호스트 비율을 $s_\lambda=s(\lambda)$로 각각 두었을 때 $t=\lambda$인 경우

$$\left.\frac{di}{dt}\right|_{t=\lambda}>0 \rightarrow \beta s_\lambda i_\lambda-\gamma i_\lambda>0 \rightarrow s_\lambda>\frac{\gamma}{\beta}$$

를 만족한다. 위 계산에 의하면 시각 λ에서 감염된 호스트의 비율 i_λ과 상관없이 감염 가능한 호스트 비율 s_λ이 γ/β보다 작다면 즉, $s_\lambda<\gamma/\beta$이면 감염을 통한 웜의 확산은 더 이상 발생하지 않는다. 또한, γ를 충분히 크게 하여 $\beta s_\lambda<\gamma$로 만들면, 시각 λ에서 감염 가능한 호스트 비율 s_λ과 확산율 β에 대한 복구율 γ보다 작다면 웜은 역시 확산할 수 없다.

SIR 모델에서 γ는 I 상태에서 R 상태로만 변경되는 비율로 웜 감염 후 실패하여 정지되거나 복구되는 비율 모두를 포함한다. 반면에 제안 SI-SIR 모델은 S 상태에서 R 상태로 변경되는 비율 δ이 존재하고, I 상태에서 R 상태로 변경되는 비율 γ가 존재한다. 전자의 경우 웜에 대한 대응을 통하여 면역이 생겨 감염되지 않는 경우이고 후자의 경우 감염 후 치료하여 복구된 경우와 실패하여 정지되는 경우 모두를 포함한다.

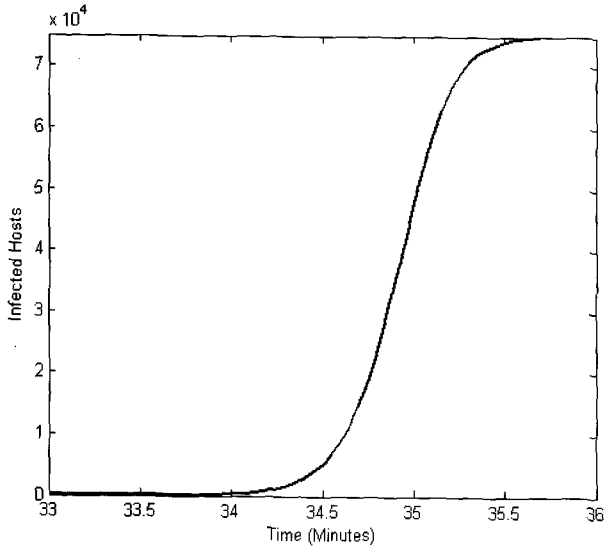
4. 제안 모델의 적용

본 장에서는 각각의 확산 모델에 대하여 2003년 1.25 대란을 일으켰던 Slammer Worm(또는 SQL_Overflow Worm, Sapphire Worm)을 적용하여 결과를 살펴보고 현재 네트워크 환경을 가정하여 실험한다.

4.1 Slammer Worm 확산 분석

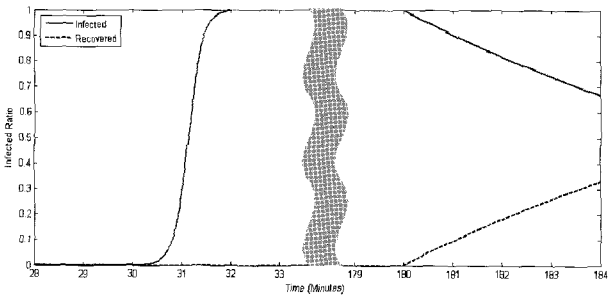
Slammer Worm은 일반적인 웜과 같이 파일형태로 저장되어 감염되는 것이 아니라 메모리상에 상주하는 악성코드로

Windows 네트워크 관련 API를 사용하여 임의의 IP 주소로 UDP(User Datagram Packet) 패킷을 보내게 된다. 보내지는 패킷의 크기는 404 바이트이며 Microsoft SQL-Monitor 포트인 1434 포트를 사용하는데, 이 패킷을 받은 취약한 Microsoft's SQL Server나 MSDE(Microsoft SQL Server Desktop Engine) 2000은 무한루프를 돌면서 서버가 종료될 때까지 패킷을 보내게 되어 실제적으로 DoS를 유발하는 결과를 낳게 된다. 이미 알려진 Slammer Worm의 초기 확산율은 분당 6.7이고 감염 호스트가 8.5±1초마다 2배로 증가되었다[8]. Code Red가 시간 단위로 확산되는데 반해, Slammer Worm은 초 단위로 확산하여 전세계 취약한 호스트의 90%가 10분 내에 감염되는 초유의 사태가 발생하였다. 이러한 데이터를 바탕으로 Slammer Worm을 각각의 확산 모델에 적용시키면 (그림 4)와 같은 결과를 얻을 수 있다. 단, $N=75,000$, $\beta=6.7$이고 네트워크 속도는 모두 동일하다고 가정한다.



(그림 4) Slammer Worm의 확산 ($33 \leq t \leq 36$)

위 결과를 분석하면, Slammer Worm 확산이 진행된 이후 34분까지는 거의 확산이 진행되지 않다가 약 2분간 폭발적인 증가세를 보인 후 36분경에는 감염 가능한 거의 대부분의 호스트가 감염되었다. CAIDA의 Slammer Worm 확산을 조사한 결과에 따르면 2003년 1월 25일 05:29 UTC 에서 06:00 UTC 사이에 여러 국가의 서버 74,855대가 웜에 감염된 것을 확인할 수 있다[9]. 국내에서는 14:00경부터 네트워크 장애 신고가 들어오기 시작하였으며, 14:30경부터 약 9시간동안 원활한 인터넷 사용이 어렵게 되었다. 정보통신부에서는 긴급 대책반을 15:30경에 구성하여 17:00경부터 ISP(Internet Service Provider)에서 이상 트래픽이 발생하는 포트를 차단하기 시작하였다[10]. 이러한 Slammer Worm의 동작은 SI 모델 또는 SIR 모델만으로는 설명할 수 없으나 본 논문에서 제안한 SI-SIR 모델은 가능하다. SI-SIR 모델을 사용하여 Slammer Worm 확산과 대응까지 모든 과정을 살펴보면 다음 (그림 5)와 같다.

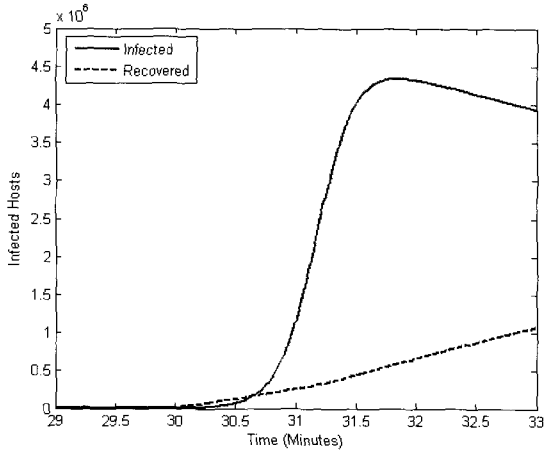


(그림 5) Slammer Worm의 확산과 대응 ($28 \leq t \leq 184$)

여기서, 실제 조사 결과와 확산 모델의 결과와는 약 5분의 차이가 나는데, 웜 확산의 진행이 처음 33분간은 감염 호스트의 숫자가 거의 0에 가깝기 때문에 확산을 발견할 수 없는 시간대가 존재한다. 즉, 실제 인터넷 웜이 확산하기 시작한 최초 시각과 인터넷 웜이 확산하여 누군가에 의해 발견되는 시각이 다르기 때문에 발생하는 시간차가 존재한다.

4.2 국내 인터넷 환경에서 웜 확산 분석

본 장에서는 Slammer Worm이 국내 인터넷 환경에서 확산한다고 가정하고 제안 SI-SIR 모델을 적용하여 내용을 분석한다. 먼저, 정보통신부의 인터넷 통계에 따르면 대한민국은 2005년 5월 현재 36,274,432개의 IPv4 주소를 보유하고 있으며, 2005년 4월 현재 12,203,290명이 초고속 인터넷에 가입하였다[11]. 여기서, 초고속 인터넷 가입자 중 5,000,000명이 각각 1대의 PC를 가지고 있고 모두가 Slammer Worm에 감염될 수 있는 취약한 PC라고 가정한다. 현재 국내 초고속 인터넷망을 통하여 확산된다고 하면, (그림 6)과 같은 결과를 얻을 수 있다. 단, $N=5,000,000$, $\beta=6.7$, $\gamma=0.1$, $\delta=0.05$, $\lambda=30$이고 네트워크 속도는 모두 동일하다고 가정한다.



(그림 6) Slammer Worm의 확산 ($29 \leq t \leq 33$)

(그림 6)은 Slammer Worm이 확산을 시작한 후 30분부터 0.1의 복구율을 가지는 경우로 확산이 32분경에 최고에 다다른 후 진정되기 시작하여 확산이 점차 감소하고 있다. 이러한 인터넷 웜 확산은 초기에 그 징후를 파악하여 얼마나 빨리

대응하느냐와 얼마나 빠른 복구율로 시스템을 치료하느냐가 가장 중요한 요소가 된다.

S. Staniford 등[3]은 매 분당 취약한 호스트 수십 대를 감염시킬 수 있는 웜을 "Warhol Worm"으로, 매 초당 취약한 호스트 수십 대를 감염시킬 수 있는 웜을 "Flash Worm"으로 정의하였다. 이 정의에 따르면 Warhol Worm은 전 세계 취약한 호스트 대부분을 15분 이내에 감염 시킬 수 있으며 Slammer Worm은 지금까지 나온 인터넷 웜 중 가장 Warhol Worm에 근접한 웜으로 알려져 있다. 또한 Flash Worm도 고속화, 통합화되는 네트워크 기술의 발전에 힘입어 곧 현실화될 것으로 예상된다.

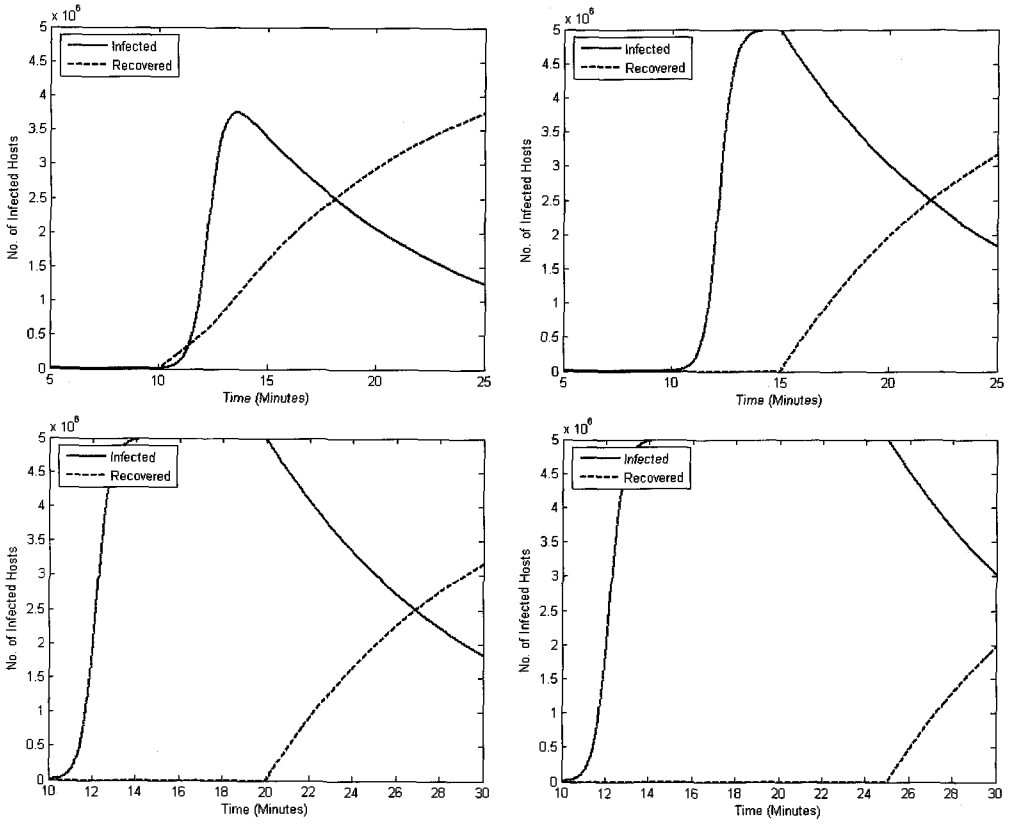
위 내용을 토대로 Slammer Worm보다 빠른 확산율을 가지는 가상의 "Warhol Worm"[3]을 가정하고, 국내 인터넷 환경에서 확산 모델을 분석한다. 단, $N=5,000,000$, $\beta=3$, $\gamma=0.1$, $\delta=0.05$이고 네트워크 속도는 모두 동일하다고 가정하면, (그림 7)과 같은 결과를 얻을 수 있는데, 동일한 조건하에서 대응 시점 λ를 10분, 15분, 20분, 25분씩 증가하여 살펴보았다. 보다시피 Warhol Worm은 15분 내에 전 세계 인터넷망에 확산할 수 있는 웜이므로 확산을 시작한지 10분에서 15분 사이에 폭발적인 증가세를 보인다. λ가 15분 이상인 경우는 Warhol Worm이 이미 확산되어 전체 네트워크를 마비시킨 후의 대응으로 제2의 1.25 대란의 재현이 발생하는 상황이다. (그림 7)의 결과에서 Warhol Worm에 대응하기 위해서는 웜 확산에 대한 조기 대응이 필수적이며 최소 15분 이전에 시작되어야 한다.

고속도의 인터넷 웜 확산을 막기 위해서는 다음과 같은 대응이 이루어져야 한다.

1. 인터넷 웜이 확산되기 시작하였을 때 대응을 신속하게 수행하여 대응 시점 λ를 0에 가깝게 해야 한다. 이를 위해서는 라우터나 침입차단시스템(Firewall) 또는 침입탐지시스템(IDS, Intrusion Detection System)의 네트워크 레벨에서 특정 IP 주소 및 포트, 패킷 등을 차단해야 한다.
2. γ와 δ를 가능한 한 높은 비율로 하여 대응한다. 즉, 감염된 호스트는 백신 프로그램이나 제거 프로그램을 이용하여 높은 γ 비율로 빠른 시간 내에 복구되어야 하고 취약한 호스트는 높은 δ 비율로 패치(Patch)되어야 한다. 취약성이 있는 운영체제 및 어플리케이션의 패치와 대응 정책을 내려서 개별적인 대응이 함께 이루어져야 한다.
3. 네트워크 기술의 발전과 인터넷 웜의 진화에 따른 β의 예측이 가능해야 하고, 이를 기반으로 신속한 대응 정책을 수립해야 한다. 웜에 대한 지속적인 모니터링을 통하여 네트워크 인프라를 다루는 기관에서는 λ를 작게 하는 것에 초점을 맞추고, 기업이나 특정 조직에서는 δ를 높이는 것에 초점을 맞추는 방법이 있다.

4.3 광대역 통합망에서 웜 확산

광대역 통합망(BcN)은 통신, 방송, 인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊김없이



(그림 7) 제안 모델에 따른 Warhol Worm의 확산

편리하고 안전하게 광대역으로 사용할 수 있는 차세대 통합 네트워크로 정의된다[12]. 다양한 서비스 개발이 용이한 개방형 플랫폼(Open API)을 기반으로 하여 보안, 품질보장, IPv6를 지원하는 차세대 통합 네트워크이다. 기술적인 측면에서 BcN은 IP(Internet Protocol), MPLS(Multi Protocol Label Switching), ATM(Asynchronous Transfer Mode), Ethernet의 모든 기술을 융합하는 패킷 기반 네트워크이며 IP-managed Network로 정의하고 있다[12]. 즉, BcN은 All-IP 기반으로 구현될 예정이며 기존의 모든 인터넷 기술이 적용됨을 의미한다. 광대역 통합망의 서비스를 살펴보면 통신·방송의 융합, 유·무선 통합, 음성·데이터의 통합, 미디어의 통합 등 4가지 측면을 가지는 디지털 컨버전스 서비스로 볼 수 있는데, 실제로 서비스는 통화 기반 서비스, 데이터 기반 서비스, 방송 기반 서비스, 홈 기반 서비스, 유·무선 통합 서비스, 기타 부가 및 복합 서비스가 제공될 예정이다. 부가적으로 QoS (Quality of Service) 보장형 서비스를 위한 대역폭 관리, 자원 관리 등이 요구되며 서드 파티 서비스 수용을 위한 Open API를 채용한다. 또한 망관리와 안전성 확보를 위한 OAM (Operations, Administration and Maintenance), 시큐리티 기능도 포함될 예정이다.

광대역 통합망의 구축에 있어서 핵심망은 IP 및 패킷 스위치 기반으로 통합되고 있는 추세이며, 유선 사업자뿐만 아니라 무선 사업자들도 IP 기반 멀티미디어 서비스 제공을 준비하고 있다. 구체적으로 설명하면 가입자망에서는 기본의 초고속 인터넷망을 활용한 유선망, 3G망과 WLAN(Wireless LAN)의 확대를 통한 무선망, Digital CATV 및 지상파/위성 DMB(Digital Multimedia Broadcasting) 망의 구축을 통한 방송망, 홈게이트웨이 보급을 통한 홈네트워크를 융합할 예정이고, 전달망에서는 QoS, 시큐리티, IPv6, Open API 등을 제공할 예정이다. 즉, 모든 정보기기들은 All-IP 기반으로 구현되어 IP 주소를 부여 받을 예정이다. 따라서, 광대역 통합망에서 인터넷 웜 확산은 광대역 통합망 기반 구조 자체가 기존의 인터넷망 기반 위에서 구축되는 IP-managed Network이고, 새롭게 등장할 다양한 서비스도 이를 기반으로 하고 있으므로 현재의 초고속 인터넷망에서의 확산과 크게 다르지 않으므로 앞의 제안 확산 모델을 그대로 적용할 수 있을 것으로 예상된다. 단, 광대역 통합망에 직접 적용하기 위해서는 네트워크 전송 속도 및 호스트 플랫폼의 특성에 따른 확산율 β, 대응 방식에 따른 γ와 δ의 적절한 조정이 필수적이다.

5. 결 론

인터넷은 전세계를 하나의 네트워크로 연결하여 누구나 원하는 정보를 얻을 수 있도록 한 네트워크의 네트워크(Network of Network)이다. 전세계 수천만 대의 컴퓨터가 인터넷을 통하여 다양한 정보들이 전송되고 있으며, 최근 전자상거래의 등장으로 수많은 기업 간, 국가 간 거래들이 인터넷을 통하여 전송되고 있다. 광대역 통합망(BcN)은 구축된 인터넷 기반 위에 통신, 방송, 인터넷이 융합되는 차세대 통합 네트워크이다. 즉, 이러한 기술적인 융합은 이미 구축된 인터넷 하부 구조를 그대로 수용할 수 있는 장점이 있는 반면에 기존의 인터넷 환경에서 발생하는 해킹, 바이러스, 사기, 컴퓨터 범죄 등의 다양한 위협이 광대역 통합망에도 동일하게 적용됨을 의미한다. 그 중 운영체제 및 네트워크의 취약점을 이용하여 급속도로 확산되는 인터넷 웜은 대상을 가리지 않고 무차별적으로 네트워크 기반 구조를 공격하는 분산 서비스 거부 공격의 형태를 가진다. 따라서, 인터넷 웜의 확산은 직접적으로는 해당 네트워크에서 시스템의 정상적인 동작을 못하도록 할 뿐만 아니라 간접적으로는 인터넷 및 광대역 통합망 서비스의 신뢰성에 심각한 타격을 주는 특징을 가진다. Slammer Worm에 의해 발생한 1.25 대란의 예는 초고속 인터넷을 통한 정보화 사회를 지향하는 한국에 있어 순기능과 역기능을 함께 생각하게 하였으며, 네트워크 기반 구조 보호에 대한 새로운 시각을 제시하였다.

본 논문에서는 현재 문제가 되고 있는 인터넷 웜의 확산에 대한 새로운 모델을 제안함으로써 광대역 통합망과 같은 고성능 네트워크 환경에서 그 영향을 분석하였다. 이를 위하여 관련 연구에 대하여 살펴보고, 이미 발생한 인터넷 웜이 웜 확산 모델에 따라 동작함을 보였으며, 현재 네트워크 환경에서 발생 가능한 인터넷 웜 확산을 실험하였다. 본 논문의 결과는 인터넷의 진화에 따른 방송·인터넷·멀티미디어가 융합하는 BcN 등에 적용할 수 있을 뿐만 아니라 네트워크의 고성능화에 따른 인터넷 웜 확산의 대응 방안을 마련하는데 있어 예측 자료로 활용할 수 있을 것이다. 이를 기반으로 향후 국내 광대역 통합망의 네트워크 위상(Topology)에 따른 웜 확산 모델링에 대한 연구 및 서로 이질적인 네트워크 환경에서 웜 확산과 대응에 대한 연구도 활발하게 진행될 것으로 예상된다.

참 고 문 헌

[1] H. W. Hethcote, "The Mathematics of Infectious Diseases", SIAM Review, Vol.42, No.4, 2000

[2] James D. Murray, "Mathematical Biology", SpringerVerlag, 1993.

[3] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time", Proceedings of the USENIX Security Symposium, pp.149-167, 2002.

[4] J. Kim, S. Radhakrishnan, S. K. Dhall, "Measurement and Analysis of Worm Propagation on Internet Network Topology", International Conference on Computer Communications and Networks(ICCCN'04) 2004, 2004.

[5] Cliff C. Zou, Weibo Gong, Don Towsley. "Code Red Worm Propagation Modeling and Analysis", 9th ACM Conference on Computer and Communication Security (CCS'02), 2002.

[6] "Euler's Method," http://www.shodor.org/refdesk/Resources/Algorithms/EulersMethod/index.php

[7] "Improved Euler's Method," http://www.shodor.org/refdesk/Re-

sources/Algorithms/ImprovedEulersMethod/index.php

[8] D. Moore, C. Shanning and K. Claffy, "Code-Red : a case study on the spread and victims of an Internet worm", Proceedings of the 2nd Internet Measurement Workshop, pp.273 - 284, 2002.

[9] "The Spread of the Sapphire/Slammer Worm", http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

[10] 정관진, 이희조, "인터넷 웜과 바이러스의 진화와 전망", 한국정보처리학회지, 제 10권 제 2호, pp.27-37, 2003.

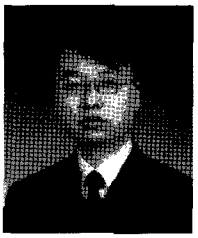
[11] "인터넷통계정보검색시스템", http://isis.nic.or.kr/

[12] 김철수, 김해숙, 강성수, 박영식, "BcN 표준모델", 한국통신학회지, Vol.21, No.5, pp.29-42, 2004.

[13] Z. Chen and L. Gao and K. Kwiat, "Modeling the Spread of Active Worms", IEEE INFOCOM, 2003.

[14] D. Moore, C. Shannon, G. Voelker, and S. Savage, "Internet quarantine : Requirements for containing self-propagating code", Proceedings of 22nd Annual Joint Conference of IEEE Computer and Communication societies(INFOCOM 2003), 2003.

[15] 전용희, "정보통신 인프라의 웜 전파 분석 및 모델링", 한국통신학회지, Vol.21, No.9, pp.106-119, 2004.



신 원

e-mail : shinweon@tit.ac.kr

1996년 부경대학교 전자계산학과(이학사)

1998년 부경대학교 대학원 전자계산학과(이학석사)

2001년 부경대학교 대학원 전자계산학과(이학박사)

2002년~2005년 (주)안철수연구소 선임연구원

2005년~현재 동명정보대학교 정보보호학과 전임강사

관심분야 : 소프트웨어 보안, 악성코드, 이동에이전트 보안, 암호학 응용