情報保護學會論文誌
第16卷 第3號, 2006. 6

인터넷 환경에서 웜 확산 모델의 제안과 분석*

신 원[1†], 이 경 현[2‡]
[1]동명대학교, [2]부경대학교

An Improved Spreading Model for Internet Worms*

Weon Shin[1†], Kyung-Hyune Rhee[2‡]
[1]Tongmyong University, [2]Pukyong National University

요 약

누구나 인터넷에 접속할 수 있는 환경이 구축됨에 따라 해킹, 악성코드 등의 다양한 위협도 함께 등장하고 있다. 그 중 인터넷 웜은 1.25 대란과 같이 국가 기간망을 뒤흔들 수 있는 위협으로 인식되고 있다. 본 논문은 인터넷 환경에서 웜 확산의 모델링을 그 목표로 한다. 이를 위해 인터넷 웜에 적용 가능한 확산 모델을 제안하고, 인터넷 환경에서 웜에 적용하여 동작을 분석한다. 제안 모델은 고속의 인터넷 웜 확산에 따른 영향을 분석함으로써 인터넷 웜의 확산을 보다 정확하게 예측할 수 있다.

ABSTRACT

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 examine the existed spreading models and propose a new worm spreading model on Internet environment. We also predict and analyze the spreading effects of high-speed Internet worms. The proposed model leads to a better prediction of the worm spreading since various factors are considered.

Keywords : *Internet worm, Worm spreading model*

Ⅰ. 서 론

최근 다양한 인터넷 기술과 어플리케이션이 등장함에 따라 예상하지 못했던 수많은 역기능들도 함께 증가하고 있다. 인터넷 서비스를 제공하는 서버의 취약성이 노출되어 외부 침입으로 정상적인 서비스가 어려운 경우도 발생하고 있고, 일반 사용자 컴퓨터에 대한 다양한 해킹 시도, 바이러스 유포도 발생하고 있다. 그 중 서비스 거부 공격의 형태로 가용성에 피해를 가하기 위해 가장 많이 이루어지는 것이 인터넷 웜을 통한 공격이다.

인터넷 웜은 호스트 운영체제의 구현 버그, 설계 결함 등의 취약성을 이용한 후 비인가된 소프트웨어 코드를 실행하는 악성 소프트웨어로, 대부분 같은 취약성을 가진 다른 호스트로 인터넷 망을 이용하여 자기 자신을 복제하도록 구현되어 있다. 이 과정 중에 수행되는 무한 루프와 발생되는 패킷은 시스템 및 네트워크 환경에 오버헤드를 초래하여 인터넷을 통한 정상적인 서비스가 불가능하도록 만든다. 따라서, 인

접수일: 2006년 4월 17일; 채택일: 2006년 5월 26일
* 본 연구는 한국과학재단 특정기초연구(R01-2006-000-10260-0) 지원으로 수행되었음.
† 주저자, shinweon@tu.ac.kr
‡ 교신저자, khrhee@pknu.ac.kr

터넷 환경에서 웜의 확산은 단순한 악성 소프트웨어 확산의 의미뿐만 아니라 웜의 회생자가 곧 또 다른 공격자가 되어 인터넷 전체를 사용불능으로 만드는 분산 서비스 거부 공격의 의미를 가진다.

본 논문에서는 인터넷 웜 확산 모델링을 인터넷 환경에 적용하여 그 영향을 분석하고자 한다. 먼저 2장에서 새로운 웜 확산 모델을 제안하여 분석하고, 3장에서 인터넷 환경을 고려한 시뮬레이션을 수행한다. 4장에서는 관련 연구에 대하여 살펴보고, 마지막 5장에서 결론을 맺는다.

Ⅱ. 새로운 인터넷 웜 확산 모델

현재 인터넷 웜의 연구는 탐지 및 대응, 실행 메커니즘, 스캐닝 전략, 웜의 전파 등이 주류를 이루고 있는데, 정확한 인터넷 웜 확산 모델을 통하여 웜의 행위를 예측하는 이유는 다음과 기술할 수 있다[1].

- 과거에 관찰된 웜 행위의 보다 나은 이해
- 웜 위협 잠재성의 평가
- 인터넷 상에서 미래의 웜에 대한 영향 평가
- 웜 확산에 대한 탐지 메커니즘 설계의 기초
- 웜 특성화에 대한 관련 있는 파라미터의 결정

본 논문은 그 중 인터넷 웜 확산에 대해 기제안된 SI 모델[2]과 SIR 모델[3]을 개선하여 웜 확산에 적합한 새로운 모델을 제안한다. 다음 표 1은 본 논문에서 사용하는 표기법이다.

표 1. 본 논문의 표기법

표기	정 의
N	감염 가능한 전체 호스트 수
$s(t)$	t시점의 취약한 호스트 비율
$i(t)$	t시점의 감염 호스트 비율
$r(t)$	t시점의 제거 또는 복구된 호스트 비율
$\beta(t)$	t시점의 인터넷 웜 확산율
$\gamma(t)$	t시점의 감염 호스트에 대한 복구율
$\delta(t)$	t시점의 취약한 호스트에 대한 면역율

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)에서 각 호스트는 SI 모델과 마찬가지로 S(Susceptible), I(Infectious)의 2가지 상태를 가진다. 해당되는 미분방정식은 SI 모델과 유사하다.

$$\frac{ds(t)}{dt} = -\beta(t)s(t)i(t)$$
$$\frac{di(t)}{dt} = \beta(t)s(t)i(t)$$

여기서, 초기 조건은 $s(0) = s_0 \simeq 1$, $i(0) = i_0 \simeq 0$이다. 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)에서 각 호스트는 SIR 모델과 마찬가지로 S(Susceptible), I(Infectious), R(Recovery)의 3가지 상태를 가진다. 그러나, 원래의 SIR 모델과는 달리 웜에 대한 대응을 시작하면서 S 상태에서 R 상태로 직접 변경되는 호스트가 존재한다. 각 상태에 대한 미분방정식은 다음과 같다.

$$\frac{ds(t)}{dt} = -\beta(t)s(t)i(t) - \delta(t)s(t)$$
$$\frac{di(t)}{dt} = \beta(t)s(t)i(t) - \gamma(t)i(t)$$
$$\frac{dr(t)}{dt} = \gamma(t)i(t) + \delta(t)s(t)$$

여기서, 초기 조건은 $s(\lambda) = s_\lambda$, $i(\lambda) = i_\lambda$, $r(\lambda) = 0$이다. 단, 제안 모델의 대응 단계에서 t가 대응을 시작하는 λ에서 무한대까지 값을 가진다.

그림 1은 확산 단계와 대응 단계를 함께 표현한 제안 모델을 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.

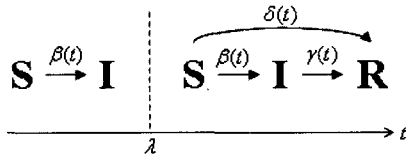

그림 1. 제안 인터넷 웜 확산 모델

이를 미분방적식으로 나타내면 다음과 같다.

$$\frac{ds(t)}{dt} = -\beta(t)s(t)i(t) - \delta(t)s(t)$$
$$\frac{di(t)}{dt} = \beta(t)s(t)i(t) - \gamma(t)i(t)$$
$$\frac{dr(t)}{dt} = \gamma(t)i(t) + \delta(t)s(t)$$
$$\begin{cases} \beta(t) \neq 0, \gamma(t) = 0, \delta(t) = 0 & (0 \leq t < \lambda) \\ \beta(t) \neq 0, \gamma(t) \neq 0, \delta(t) \neq 0 & (t \geq \lambda) \end{cases}$$

SI 모델과 SIR 모델에서 확산율 β가 고정된 상수값인데 반해 제안 모델에서는 Two-factor Worm Model[4]과 마찬가지로 시간에 따라 변화하는 함수 $\beta(t)$로 나타낸다.

$$\beta(t) = \beta(0)(1 - i(t))^{\phi}$$

여기서, $\beta(0)$는 초기 확산율이고, ϕ는 감염 호스트 비율에 의해 변화하는 감염율을 반영하는 값이다. 또한, Two-factor Worm Model에서 고려하지 않았던 $\gamma(t)$, $\delta(t)$도 시간에 따라 변화하는 함수로 다음과 같이 정의하였다. 여기서, $\gamma(0)$와 $\delta(0)$는 각각 초기 복구율과 초기 면역율이고, χ와 ψ는 실제 대응에 의해 변화하는 복구율과 면역율을 반영하는 값이다.

$$\gamma(t) = \gamma(0)(1 - r(t))^{\chi}$$
$$\delta(t) = \delta(0)(1 - r(t))^{\psi}$$

2. 제안 확산 모델의 분석

인터넷 환경에서 웜의 확산을 SI 모델에만 적용하는 경우 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 모델이다. 제안 모델의 특징을 정리하면 다음과 같다.

확산율 $\beta(t)$는 감염가능한 호스트 수 또는 네트워크 위상에 따라 감소한다. 복구율 $\gamma(t)$와 면역율 $\delta(t)$는 대응을 수행함에 따라 증가한다.

인터넷 웜의 확산이 일정시간 동안 거의 증가하지 않다가 폭발적으로 증가하기 시작하는 시점은 웜에 따라 고유한 값을 가진다. 알려진 값으로는 Code Red는 $t = 11.9(hour)$, Slammer Worm은 $t = 30.1(min)$이다.

대응 시점 λ이후 S 상태에서 I 상태를 거치지 않고 R 상태로 직접 변경되는 면역율 $\delta(t)$가 존재한다. 이는 웜에 대한 대응을 수행하여 취약한 호스트가 취약하지 않은 호스트가 되어 면역성을 가졌음을 의미한다.

대응 시점 λ가 0에 가까울수록 인터넷 웜의 확산이 조기에 둔화되고, 그 속도는 $\gamma(t)$, $\delta(t)$에 의존한다. 즉, 웜 대응에 따른 복구율과 면역율이 클수록 인터넷 웜에 감염된 호스트 수는 빠른 속도로 감소한다.

제안 모델은 SI 모델과 SIR 모델의 특징을 결합하여 반영한 모델로써 웜에 대한 대응을 시작하는 시점인 λ부터 서로 다른 형태를 가진다. 즉, $\lambda \simeq 0$이면 SIR 모델과 유사하게 동작하고 λ가 충분히 크면 SI 모델과 유사하게 동작한다.

Ⅲ. 제안 모델의 적용

본 장에서는 확산 모델에 대하여 2001년 7월에 발발했던 Code Red Worm과 2003년 1.25 대란을 일으켰던 Slammer Worm을 적용하여 결과를 살펴보고 현재 국내 인터넷 환경을 가정하여 실험한다.

1. Code Red Worm의 확산

Code Red Worm은 파일형태의 웜으로 임의의 IP 주소를 생성하여 Windows IIS 서버를 대상으로 취약점을 이용한 DoS를 유발한다. 당시 Goldsmith와 Eichman이 B 클래스의 네트워크 트래픽 데이터를 수집하였다[5][6]. 그림 2는 두 데이터의 평균값을 점으로 표기하였고, 제안 확산 모델에 따른 웜 확산을 실선으로 표기하였다. 여기서 $N = 118{,}000$, $\beta(0) = 1.8$, $\gamma(0) = 0.6$, $\delta(0) = 0.3$이다. 제안 모델을 통하여 Code Red의 확산을 설명할 수 있으나, 네트워크 확산이 최대치인 경우와 대응 시점 이후에 대해서는 측정 방식, 대응 시점에 따라 약간의 오차가 발생한다.

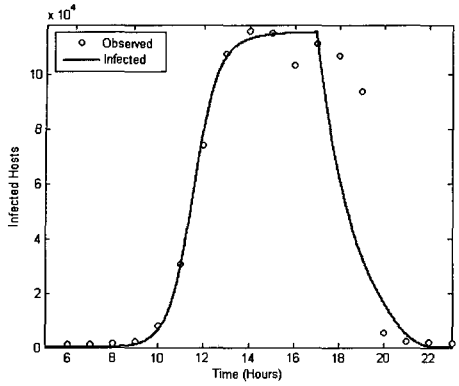

그림 2. Code Red 확산의 관찰값과 제안 모델

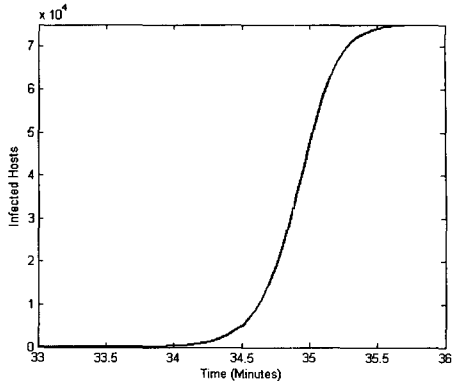

그림 3. Slammer Worm의 확산

위 결과를 분석하면, Code Red Worm 확산이 진행된 이후 10시간까지는 거의 확산이 진행되지 않다가 11에서 13시간 사이 약 2시간 동안 폭발적인 증가세를 보인다.

2. Slammer Worm의 분석

Slammer Worm은 파일형태로 저장되어 감염되는 일반적인 웜과는 달리 메모리상에 상주하여 무한루프를 돌면서 서버가 종료될 때까지 패킷을 보내게 되어 실제적으로 DoS를 유발하는 결과를 낳게 된다[7]. Code Red가 시간 단위로 확산되는데 반해, Slammer Worm은 초 단위로 확산하여 전세계 취약한 호스트의 90%가 30분 내에 감염되는 초유의 사태가 발생하였다. CAIDA가 조사한 결과에 따르면 2003년 1월 25일 05:29 UTC 에서 06:00 UTC 사이에 여러 국가의 서버 74,855대가 Slammer Worm에 감염된 것을 확인할 수 있다[8]. 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[9]. 이러한 사실과 조사된 데이터를 바탕으로 Slammer Worm의 확산을 재구성해보면 그림 3과 같다. Slammer Worm 확산이 진행된 이후 34분까지는 거의 확산이 진행되지 않다가 약 2분간 폭발적인 증가세를 보인 후 36분경에는 감염 가능한 거의 대부분의 호스트가 감염되었다. 여기서, $N=75{,}000$, $\beta(0)=6.7$, $\gamma(0)=0.2$, $\delta(0)=0.1$, $33 \le t \le 36$이다.

3. 국내 인터넷 환경에서 가상 웜의 확산

본 장에서는 Slammer Worm과 동일한 성질을 가지는 가상의 웜이 국내 인터넷 환경에서 확산한다고 가정하고 제안 모델을 적용하여 내용을 분석한다. 여기서, 1,000,000대의 PC가 가상 웜에 감염될 수 있는 취약한 PC라고 가정한다. 현재 국내 초고속 인터넷망을 통하여 확산된다고 하면, 그림 4와 같은 결과를 얻을 수 있다. 단, $N=1{,}000{,}000$, $\beta(0)=6.7$, $\gamma(0)=0.1$, $\delta(0)=0.05$, $\lambda=30$, $29 \le t \le 33$이고 네트워크 속도는 모두 동일하다고 가정한다.

그림 4는 가상 웜이 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 대응하느냐"가 가장 중요한 요소인데, 구체적으로 "얼마나 빠른 복구율로 시스템을 치료하느냐"와 "얼마나 빠른 면역율로 시스템을 면역시키느냐"이다.

S. Staniford 등[10]은 취약한 호스트 수십 대를 매 분당 감염시킬 수 있는 웜을 "Warhol Worm"으로, 취약한 호스트 수십 대를 매 초당 감염시킬 수 있는 웜을 "Flash Worm"으로 정의하였다. 이 정의에 따르면 Warhol Worm은 전 세계 취약한 호스트 대부분을 15분 이내에 감염 시킬 수 있다. Warhol Worm과 Flash Worm은 고속화, 통합화되는 네트워크 기술의 발전에 힘입어 곧 현실화될 것으로 예상된다.

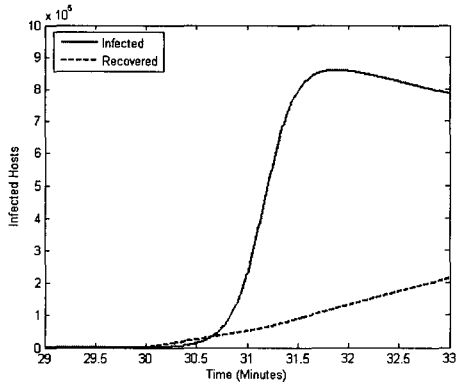

그림 4. 가상 웜의 확산

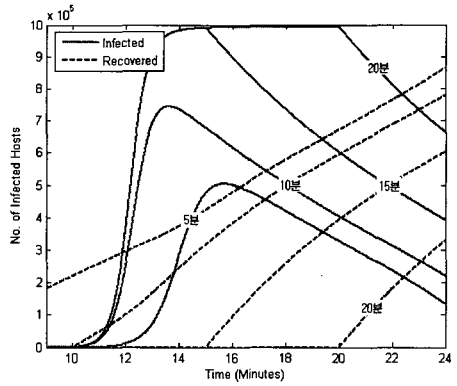

그림 5. 제안 모델에 따른 Warhol Worm의 확산과 대응

위 내용을 토대로 Slammer Worm보다 빠른 확산율을 가지는 가상의 "Warhol Worm"[10]을 가정하고, 국내 인터넷 환경에서 확산 모델을 분석한다. 단, $N=1{,}000{,}000$, $\beta(0)=3$, $\gamma(0)=0.1$, $\delta(0)=0.05$라고 가정하면, 그림 5와 같은 결과를 얻을 수 있는데, 동일한 조건 하에서 대응 시점 λ를 5분에서 20분까지 5분씩 증가하여 살펴보았다. Warhol Worm은 확산을 시작한지 10분에서 15분 사이에 폭발적인 증가세를 보이는데, λ가 15분 이상인 경우는 Warhol Worm이 이미 확산되어 전체 네트워크를 마비시키는 상황이다. 그림 5의 결과에서 Warhol Worm에 대응하기 위해서는 웜 확산에 대한 조기 대응이 최소 15분 이전에 시작되어야 한다.

4. 고속도 인터넷 웜의 대응

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

- 네트워크 기반 구조 담당 조직 : 인터넷 웜이 확산되기 시작하였을 때 조기 대응을 수행한다.
  - 네트워크 기술의 발전과 인터넷 웜의 진화에 따른 $\beta(0)=\beta_0$의 예측이 가능해야 하고, 이를 기반으로 신속한 대응 정책을 수립해야 한다.
  - 웜에 대한 지속적인 모니터링을 통하여 λ를 작게 하는 것에 초점을 맞춘다.
  - 네트워크 기반 구조 관점에서 대응 정책을 배포한다.
- 보안 업체 : 웜의 특성을 분석하여 해당되는 패치 및 백신 업데이트를 제공한다.
  - 높은 $\gamma(0)=\gamma_0$ 비율로 감염된 호스트에 대해 백신 업데이트나 웜 제거 프로그램을 제공한다.
  - 높은 $\delta(0)=\delta_0$ 비율로 취약한 호스트에 대해 패치소프트웨어를 제공한다.
  - 호스트 치료 및 패치에 대한 대응 정책을 배포한다.
- 일반 조직 및 개인 사용자 : 설정된 보안 정책을 적용하여 개별적인 대응을 수행한다.
  - 감염된 호스트는 백신 프로그램이나 제거 프로그램으로 치료하여 $\gamma(t)$를 높인다.
  - 취약성이 있는 운영체제 및 어플리케이션의 패치를 설치하여 $\delta(t)$를 높인다.
  - 라우터나 침입차단시스템(Firewall) 또는 침입탐지시스템(IDS, Intrusion Detection System)에서 특정 IP 주소 및 포트를 기준으로 해당 패킷들을 차단하여 $\beta(t)$를 감소시킨다.

Ⅳ. 관련연구

인터넷 웜 확산은 과거 질병 역학에서 연구한 전염병 확산에 대한 모델을 적용하여 해석할 수 있다. 이미 많은 학자들에 의해 여러 가지 모델이 제안되어 있으나 실제 동작하는 인터넷 웜에 적용하기에는 여러 전제 조건과 수정 사항이 필요하다. 본 장에서는 가장 대표적인 모델인 SI 모델[2], SIR 모델[3]과 기타 연구들을 설명한다.

SI 모델은 각 호스트가 2가지 상태 S(Susceptible), I(Infectious)를 가진다[2]. 호스트가 S 상태를 가지는 경우 β의 비율로 웜에 감염되어 I 상태로 변경된다. 이에 대한 미분방정식은 다음과 같다. 여기서, $I(t)$는 t시점에 감염 호스트 수이다.

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

위 식에서 감염된 호스트의 비율은 아래와 같다.

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

위 미분방정식의 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 6과 같다. 여기서, 감염 가능한 전체 수 $N=359{,}000$, 확산율 $\beta=1.8$, 초기값 $T=11.9$이다[10].

다음 그림 7은 CAIDA[10]에 의한 실제 측정치이다. 그림 6과 비교하여 최상단에 왜곡이 발생하지만 대체로 비슷한 유형임을 알 수 있다.

SIR 모델은 각 호스트가 3가지 상태 S(Susceptible), I(Infectious), R(Removed)를 가진다[3]. 호스트가 S 상태를 가지는 경우 β의 비율로 웜에 감염되어 I 상태로 변경되고, 감염되어 I 상태인 호스트는 γ의 비율로 제거된다. 이에 대한 미분방정식은 다음과 같다. 여기서, $S(t)$는 t시점에 취약한 호스트 수, $I(t)$는 t시점에 감염 호스트 수, $R(t)$는 t시점에 제거 또는 복구된 호스트 수이다.

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

위 식에서 웜에 감염된 호스트의 비율은 아래와 같이 나타낼 수 있다.

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

Code Red Worm 확산 이후 인터넷 웜 확산에 대한 관심이 고조되어 이를 분석하기 위해 많은 학자들이 다양한 방안들을 제안하였다. S. Staniford 등[10]은 Code Red 확산을 모델링하기 위하여 고전적 모델인 SI 모델을 적용하여 웜의 동작 방식을 분석하고 설계 방식와 확산 속도에 따라 웜을 분류하였다. J. Kim 등[11]은 SI 모델을 개선한 SIS 모델과 SIR 모델을 확장하여 웜 확산 모델을 제안하고 인터넷 위상에 따른 결과와 영향을 분석하였다. C. C. Zou 등[4]은 기존의 SI 모델을 개선하여 Two-factor Worm Model을 제안하였는데, 인터넷 웜 확산에서 사람의 대응이 확산을 둔화시킨다는 사실과 감염이 진행될수록 확산이 감소된다는 동적인 측면을 고려하여 보다 실제적인 모델을 제안하였다. Z. Chen 등[12]은 랜덤 스캐닝을 수행하는 웜을 대상으로 AAWP(Analytical Active Worm Propagation)를 제안하였는데, 연속 시간에서 미분 방정식을 도입한 다른 방안과 달리 이산 시간 모델에 기반하여 패치율, 웜 감염 시간, 동일 호스트 감염 등을 고려하였다.

V. 결 론

운영체제 및 네트워크의 취약점을 이용하여 급속

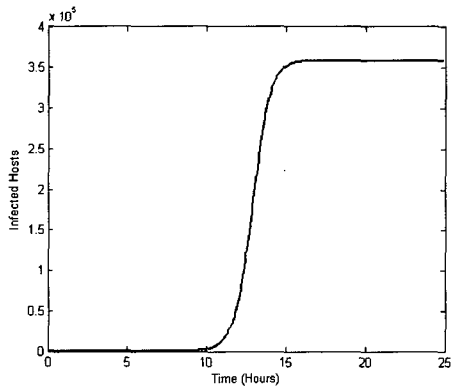

그림 6. Code Red 웜 확산 모델링

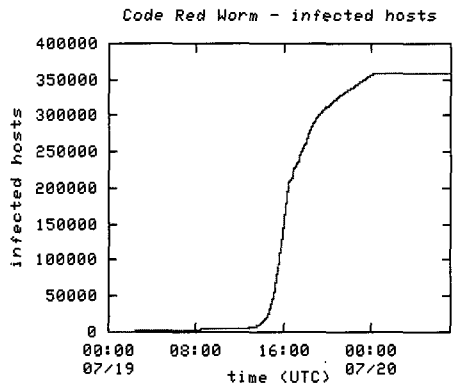

그림 7. Code Red 웜 확산(2001년 7월)

도로 확산되는 인터넷 웜은 무차별적으로 네트워크 기반 구조를 공격하는 가장 큰 위협 중 하나이다. 이러한 인터넷 웜의 확산은 직접적으로는 해당 네트워크에서 시스템의 정상적인 동작을 못하도록 할 뿐만 아니라 간접적으로는 인터넷 서비스의 신뢰성에 심각한 타격을 주는 특징을 가진다. Slammer Worm에 의해 발생한 1.25 대란은 초고속 인터넷을 통한 정보화 사회를 지향하는 한국에 있어 네트워크 기반 구조 보호에 대한 새로운 시각을 제시하였다.

본 논문에서는 현재 문제가 되고 있는 인터넷 웜 확산에 대한 새로운 모델을 제안함으로써 인터넷과 같은 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 네트워크의 고성능화에 따른 인터넷 웜 확산의 대응 방안을 마련하는데 있어 기반 연구로 활용할 수 있을 것이다. 이를 기반으로 향후 국내 광대역 통합망의 네트워크 위상에 따른 웜 확산 모델링에 대한 연구 및 서로 이질적인 네트워크 환경에서 웜 확산과 대응에 대한 연구도 진행되어야 한다.

참 고 문 헌

[1] A. Wagner and T. Dubendorfer, "Experiences with Worm Propagation Simulations", WORM '03, 2003

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

[3] James D. Murray, "Mathematical Biology", Springer-Verlag, 1993

[4] 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

[5] http://lists.jammed.com/incidents/2001/07/0149.html

[6] http://lists.jammed.com/incidents/2001/07/0159.html

[7] 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

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

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

[10] 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

[11] 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

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

[13] Thomas M. Chen, Jean-Marc Robert, "Worm Epidemics in High-Speed Networks", IEEE Computer Society, pp.48-53, 2004

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

[15] 전용희, "인터넷 웜의 탐지 및 대응기술 ", 한국통신학회지, 제 22권 8호, pp.1088-1103, 2005

[16] 신원, "고성능 네트워크에서 인터넷 웜 확산 모델링", 제 12-C 제 6호, pp.839-846, 2005

〈著者紹介〉

신 원 (Shin, Weon) 정회원
1996년 2월: 부경대학교 전자계산학과 졸업
1998년 2월: 부경대학교 전자계산학과 석사
2001년 8월: 부경대학교 전자계산학과 박사
2002년 3월~ 2005년 1월: (주)안철수연구소 선임연구원
2005년 3월 ~현재: 동명대학교 정보보호학과 전임강사
〈관심분야〉 소프트웨어 보안, 악성코드 확산, 암호학 응용

이 경 현 (Kyung-Hyune Rhee) 종신회원
1982년 2월: 경북대학교 수학교육과 졸업
1985년 2월: 한국과학기술원 응용수학과 석사
1992년 2월: 한국과학기술원 응용수학과 박사
1982년 2월 ~ 1993년 3월: 한국전자통신연구원 선임연구원
1993년 3월 ~ 현재: 부경대학교 전자컴퓨터정보통신공학부 교수
〈관심분야〉 암호이론, 암호프로토콜, 네트워크 보안