융합망 환경에서 인터넷 웜 확산 방식 연구

정회원 신 원*

The Spread of Internet Worms on Convergence Networks

Weon Shin* *Regular Member*

요 약

최근 빠른 속도로 확산되는 인터넷 웜은 인터넷은 물론 융합망에서도 주요한 위협이 될 것으로 예상된다. 이러한 인터넷 웜에 대응하기 위해서는 웜의 확산 방식과 웜 확산에 영향을 끼치는 융합 요소를 연구하는 것이 필수적이다. 본 논문은 융합망 환경에서 웜 확산에 대한 정확한 모델링을 그 목표로 한다. 이를 위하여 다양한 실험을 통하여 융합망 환경에서 웜 확산의 양상을 분석한다.

Key Words : Internet Worm, Convergence Network, Worm Spreading, Infection Rate

ABSTRACT

Fast spreading Internet worms will be sure to become one of the new major threats of convergence networks as well as the Internet. In order to defend and respond them, it is necessary to study how Internet worms propagate and what factors affect worm spreading. In this paper, we try to describe the correct spread of worms on convergence network environments. Therefore we propose a spreading model and analyze the spreading effects by various experiments.

Ⅰ. 서 론

세계적으로 보편화된 인터넷 기술은 유무선 기술을 통합하더니 급기야 방송 기술과 통신 기술까지도 흡수하여 새로운 융합망으로 거듭나고 있다. 최근 인터넷 기술을 기반으로 양질의 멀티미디어 서비스가 가능하도록 한 광대역 통합망인 BcN(Broadband convergence Network), 통신과 방송의 경계를 허물고 있는 IPTV(Internet Protocol Television), 인터넷 상에서 음성 통신이 가능하도록 하는 VoIP(Voice over Internet Protocol) 등 다양한 융합 기술들이 선보이고 있다. 그러나, 새로운 인터넷 융합 및 응용 기술이 등장함에 따라 다양한 역기능들도 함께 증가하고 있다. 대표적인 역기능으로 시스템의 취약성을 이용한 인터넷 웜 및 컴퓨터 바이러스 공격, 운영체제의 취약성과 서버 구성 상의 오류를 이용한 해킹, Bot 및 좀비 PC들을 이용한 분산서비스 거부 공격 등이 막대한 피해를 끼치고 있다. 그 중 세계적으로 빈번하게 이루어져서 많은 피해를 끼치는 공격이 서버 또는 네트워크 구조와 온라인 서비스의 가용성에 치명적 피해를 유발하는 인터넷 웜 공격이다.

인터넷 웜은 "독립적으로 자기복제를 실행하여 번식하는 빠른 전파력을 가진 컴퓨터 프로그램 또는 실행 가능한 코드"로 정의된다[1]. 인터넷 웜이 발생시키는 대량의 코드는 패킷 형태로 전송되는데, 이는 다른 작업을 방해하는 직접적인 원인이 되기도 하지만, 피해 시스템들이 가해 시스템이 되어 네트워크 하부구조에 대량의 트래픽을 발생시켜 네트워크 자체를 마비시키는 서비스 거부 공격을 수행

※ 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. KRF-2008-331-D00576)
* 동명대학교 정보보호학과 (shinweon@tu.ac.kr)
논문번호 : KICS2009-12-633, 접수일자 : 2009년 12월 28일, 최종논문접수일자 : 2010년 3월 15일

한 것과 같은 간접적인 효과를 유발하기도 한다.

본 논문에서는 기존 네트워크 환경뿐만 아니라 융합망에 적합한 새로운 인터넷 웜 확산 모델을 개발하고, 현재 인터넷 및 융합망 환경에서 웜 확산과 각 요인에 따른 영향을 분석하고자 한다. 먼저 2장에서는 웜 확산 모델을 살펴보고, 3장에서 융합망 환경을 고려한 새로운 확산 모델을 제안한다. 4장에서 융합망 환경에서 다양한 웜 확산 시뮬레이션을 수행하고 대응 방안을 살펴본 후 마지막 5장에서 결론을 유도한다.

Ⅱ. 인터넷 웜 확산 모델

2.1 기존 웜 확산 모델

인터넷 웜은 인터넷 주소 공간을 대상으로 감염 가능한 취약 호스트를 물색하는 동작인 "스캐닝(Scanning)"을 수행한다. 이를 통하여 취약 호스트를 발견하여 자기 자신을 복제하고, 감염된 호스트에서 다시 동일한 동작을 무한 반복하여 확산한다. Cliff C. Zou 등[2]은 인터넷 웜의 스캐닝 방식에 따라 웜 확산 방식의 성능을 분석하였는데, 인터넷 주소 공간, 즉 IP 주소에 대해 무작위 스캐닝을 수행하는 RCS(Random Constant Spread) Worm의 동작에서 다음 식을 유도하여 인터넷 환경의 일반적인 웜 확산을 설명하였다.

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)],\ \beta = \frac{\eta}{\Omega}$$

여기서, β는 웜 확산율, η는 웜의 단위 시간 당 평균 스캐닝 수, Ω는 웜이 스캐닝할 수 있는 전체 호스트의 주소 공간(IP 주소), N은 감염가능한 전체 취약 호스트 수, $I(t)$는 시각 t에 감염된 호스트 수를 나타낸다.

한편, Two-factor Worm Model[3]에서는 웜 확산의 네트워크 오버헤드 등을 함께 고려하여 고정된 확산율 β 대신에 다음 식과 같은 시간에 따라 변화하는 함수 $\beta(t)$로 나타내었다.

$$\beta(t) = \beta_0 (1 - \frac{I(t)}{N})^{\phi}$$

여기서, β_0는 웜의 초기 확산율이고 ϕ는 감염 호스트 비율에 의해 변화하는 확산율을 반영하는 값이다. 만약, ϕ가 0이라면 확산율은 $\beta = \beta_0$로 고정되면서 RCS Worm에 해당한다.

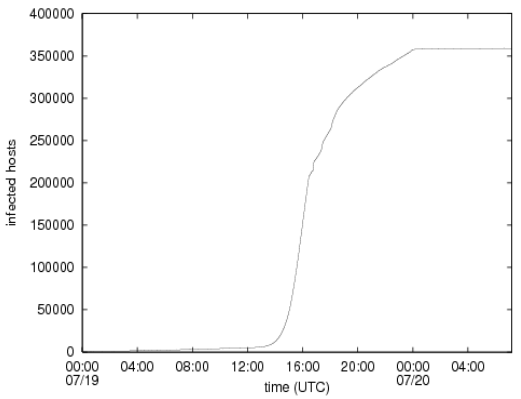

그림 1. Code Red Worm 확산 측정값

그림 1은 CAIDA[4]에서 2001년 7월 실제 측정한 값으로 Code Red Worm이 359,000대의 컴퓨터를 감염시킨 결과이고, 그림 2는 위 식을 이용하여 Code Red Worm의 확산 곡선을 그린 그래프이다. 여기서, 당시의 감염 가능한 전체 호스트 수는 $N = 359{,}000$으로 두고, 확산율을 Code Red Worm의 특성을 반영하여 $\beta = \beta_0 = 358/2^{32} = 8.34 \times 10^{-8}$로 설정하였다[5]. 그래프를 살펴보면 모델링에 의한 확산과 실제 측정값이 매우 비슷한 형태를 그리고 있는데, 특히 β가 고정인 원래 모델보다 시간에 따라 변화하는 함수 $\beta(t)$를 적용한 모델이 실제 측정값에 더 근접함을 알 수 있다. 이는 웜의 확산이 포화상태가 됨에 따라 오버헤드에 의해 감소되는 현상을 반영하고 있다.

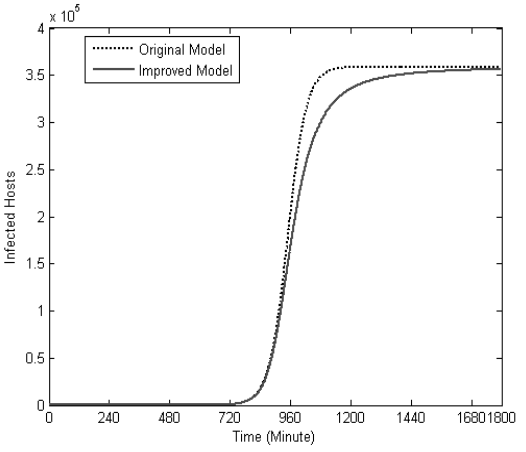

그림 2. 모델링에 의한 Code Red Worm 확산

2.2 대역폭에 따른 웜 확산

인터넷 웜이 네트워크로 확산하는 경우, 확산율은 해당 네트워크 대역폭 범위 내의 스캐닝 수 η에 의존하게 된다. 즉, 웜이 스캐닝할 때 발생하는 단위 시간 당 패킷은 해당 네트워크의 단위 시간 당 대역폭을 초과할 수 없으므로 다음이 성립한다[5].

$$\eta \times s \leq B$$

여기서, s는 웜의 크기, B는 해당 네트워크에서 물리적인 최대 대역폭을 나타낸다.

예를 들어, 코드 크기만 376바이트인 Slammer Worm이 10Mbps IPv4 환경에서 확산할 때, IP(Internet Protocol) 상에서 UDP(User Datagram Protocol)로 확산한다는 사실이 알려져 있으므로, 이를 보편적인 Ethernet 환경의 프레임 크기로 환산하면 Slammer Worm의 전체 크기가 430바이트이다. 위 식을 이용하면 Slammer Worm의 최대 스캐닝 수는 $\eta = 2906$임을 알 수 있다. 단, 감염 호스트의 성능이나 패킷 오버헤드 등은 무시한다고 가정한다.

$$\eta \leq \frac{B}{s} = \frac{10 \times 1000 \times 1000\ (bps)}{430 \times 8\ (bit)} = 2906.976\cdots$$

또한, Slammer Worm은 IPv4 주소 공간 전체를 스캐닝한다는 사실이 알려져 있으므로, 이를 이용하여 계산하면 확산율은 $\beta = 6.77 \times 10^{-7}$이다[5].

$$\beta = \frac{\eta}{\Omega} = \frac{2906}{2^{32}} = 0.0000006766\cdots$$

즉, Slammer Worm은 10Mbps 속도의 IPv4 네트워크에서는 초당 2906회 스캐닝을 수행하고 $\beta = 6.77 \times 10^{-7}$의 확산율로 확산한다.

실제 인터넷 웜에 대한 관찰 결과를 살펴보면 Code Red Worm은 4KB 크기로 당시 분당 평균 358개의 IP 주소를 스캔한 것으로 확인되었고[6], Slammer Worm은 404바이트 크기로 2003년 당시 초당 평균 4,000개의 IP 주소를 스캔한 것으로 확인되었다[7]. 특히, Slammer Worm은 100Mbps 대역폭 네트워크 환경에서 최고 26,000개를 스캐닝할 수 있는 것으로 관찰되었다[7].

Ⅲ. 융합망을 고려한 새로운 웜 확산 모델의 제안

이 장에서는 기존 확산 모델을 개선하여 융합망에 적용가능한 새로운 인터넷 웜 확산 모델을 제안한다. 표 1은 본 논문에서 사용하는 표기법이다.

표 1. 본 논문의 표기법

표기	정 의
N	감염 가능한 전체 호스트 수
$S_x(t)$	t시점에서 네트워크 x 내의 취약 호스트 수
$I_x(t)$	t시점에서 네트워크 x 내의 감염 호스트 수
$\beta_x(t)$	t시점에서 네트워크 x의 웜 확산율

3.1 제안 웜 확산 모델

제안 확산 모델은 융합망과 같은 네트워크 환경에서 인터넷 웜 확산을 설명하기 위한 모델이다. 즉, 단일 네트워크 환경의 확산을 설명하는 기존 모델과는 달리 융합망에서 속도가 서로 다른 네트워크 환경 또는 속도가 서로 다른 매체에서 확산하는 인터넷 웜의 동작 모두를 설명할 수 있다. 이를 위하여 다음을 가정한다.

<가정>

1. 인터넷 웜은 해당 네트워크 환경에서 낼 수 있는 최고 속도로 확산한다.
2. 각 호스트는 동일한 웜에 여러 번 중복으로 감염되지 않는다.
3. 인터넷 웜에 면역성을 가지는 호스트의 경우 감염되지 않는다.
4. 감염 호스트의 성능, 라우터 및 스위치의 패킷 오버헤드 등은 무시한다.

서로 격리된 2개의 네트워크 i와 j는 그림 3과

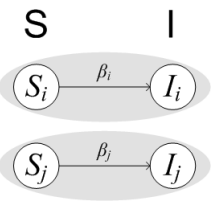

그림 3. 개별 네트워크의 웜 확산

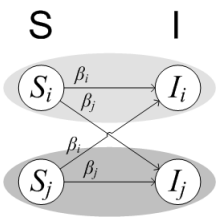

그림 4. 융합망 환경에서 웜 확산

같이 독립적인 확산율로 웜이 각각 확산하면, 서로 영향을 끼치지 않는다. 그러나, 서로 다른 네트워크 i와 j가 연결되어 있는 융합망의 경우에는 그림 4와 같이 자체 네트워크로도 확산이 이루지지만 서로의 네트워크에 영향을 끼치면서 확산한다. 즉, 융합망에서는 한 가지 형태로 고정되어 있는 기존의 확산과는 달리 각각의 네트워크에서 개별적인 확산을 수행하면서 서로의 확산에 영향을 끼치게 된다. 그러나, 어떠한 환경이라도 각 호스트는 감염가능한 취약한 상태 S(Susceptible)와 웜에 감염된 상태 I(Infectious)의 2가지 상태를 가진다. 특히, 융합망에서 인터넷 웜 확산율은 각 호스트의 상태전이에 따라 표 2와 같은 의미를 가진다.

2개의 네트워크 i, j가 연결되어 융합망이 구성되어 있고 각각의 속도로 웜이 확산된다면 t시점의 감염 호스트 수는 다음 식과 같다.

$$\begin{aligned}\frac{dI_i(t)}{dt} &= \beta_i(t)I(t)S_i(t)\sigma_i(t)+\beta_i(t)I(t)S_j(t)\sigma_j(t)\\ &= \beta_i(t)I(t)\left[\sigma_i(t)S_i(t)+\sigma_j(t)S_j(t)\right]\\ \frac{dI_j(t)}{dt} &= \beta_j(t)I(t)S_j(t)\sigma_j(t)+\beta_j(t)I(t)S_i(t)\sigma_i(t)\\ &= \beta_j(t)I(t)\left[\sigma_i(t)S_i(t)+\sigma_j(t)S_j(t)\right]\\ \frac{dI(t)}{dt} &= \frac{dI_i(t)}{dt}+\frac{dI_j(t)}{dt}\end{aligned}$$

여기서, $I_x(t)$는 네트워크 x에서 t시점의 감염된 호스트 수를 나타내고, $S_x(t)$는 네트워크 x에서 t시점의 취약 호스트 수로 $N-I_x(t)$와 같다. 또한, $\sigma_x(t)$와 $\beta_x(t)$ 함수는 다음 식과 같이 정의된다.

$$\sigma_x(t)=\frac{S_x(t)}{N},\ \beta_x(t)=\beta_x(1-\frac{I_x(t)}{N})^{\phi}$$

여기서, $\sigma_x(t)$는 네트워크 x에서 전체 호스트 수에 대한 취약 호스트 수의 t시점에서 비율 함수이고, $\beta_x(t)$는 네트워크 x에서 t시점의 확산율 함수이다. 제안 모델에서는 확산율을 Two-factor Worm Model[3]처럼 시간에 따라 변화하는 함수 $\beta_x(t)$로 나타낸다. 특히 상수 β_x는 네트워크 x에서 최초의 웜 확산율이다.

기존 확산 모델은 단일 네트워크에서 웜이 같은 비율로 확산하는 것을 고려하였지만, 융합망에서는 서로 다른 성질의 네트워크가 연결되면서 동일한 웜일지라도 각각의 확산율이 다르고 이로 인해 취약 호스트가 감염 호스트에 끼치는 영향도 다르다. 이를 반영하기 위해 제안 모델에서는 함수 $\sigma_x(t)$를 도입한다. 즉, $\sigma_x(t)$는 개별 네트워크에서 실시간으로 취약 호스트가 감염 호스트로 상태가 변경되면서 각각의 네트워크에게 영향을 끼치는 $\beta_x(t)$에서 $I_x(t)=N-S_x(t)$를 반영한 함수이다.

위 수식에 따라 유무선 인터넷이 연결되어 있는 환경에서 웜 확산을 실험하면 그림 5와 같다. 여기서, 유선 인터넷은 IEEE 802.3 10Mbps 속도를, 무선 인터넷은 802.11b 11Mbps를 내고, Slammer 웜이 유선 인터넷 환경의 호스트 1대에서 시작하여 유선 인터넷 환경의 취약 호스트 7,000대와 무선

표 2. 상태전이에 따른 의미

확산율	상태전이	의미
β_i	$S_i \rightarrow I_i$	네트워크 i에 있는 호스트가 같은 네트워크 내에서 발생한 웜에 감염
β_j	$S_i \rightarrow I_j$	네트워크 i에 있는 호스트가 네트워크 j에서 발생한 웜에 감염
β_i	$S_j \rightarrow I_i$	네트워크 j에 있는 호스트가 네트워크 i에서 발생한 웜에 감염
β_j	$S_j \rightarrow I_j$	네트워크 j에 있는 호스트가 같은 네트워크 내에서 발생한 웜에 감염

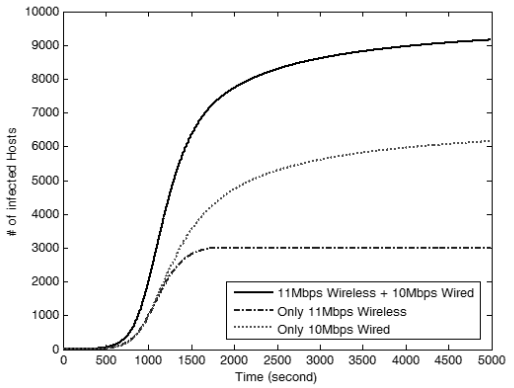

그림 5. 저속도 유무선 인터넷에서 웜 확산

인터넷 환경의 취약 호스트 3,000대를 대상으로 확산한다고 가정한다.

3.2 제안 확산 모델의 분석

단일 네트워크에서 웜 확산을 고려하여 작성된 기존의 확산 모델은 인터넷 및 정보통신 기술이 발전함에 따라 다양한 네트워크를 통합한 융합망에 적용하기에는 현실적인 어려움이 존재한다. 즉, 동일한 인터넷 웜이라도 유선 인터넷 망과 무선 인터넷 망에서 확산은 각각 다른 양상을 띠게 되며, 이들이 함께 통합한 유무선 인터넷 망에서는 각각의 방식과도 다른 제 3의 방식으로 웜이 확산하게 된다. 이러한 차이를 고려하여 웜 확산을 좀 더 정확하게 설명하기 위한 모델이 바로 제안 모델이다. 제안 모델의 특징을 정리하면 다음과 같다.

- 융합망 환경에서 확산 모델은 고정된 한 가지 방식으로 확산되는 것과는 달리 개별 네트워크에서 각각의 방식으로 웜이 확산되고 서로의 확산에 영향을 끼침으로써 복잡하게 진행된다.
- 융합망 환경에서 초기 확산율 β_x는 물리적인 네트워크의 특성에 따라 지역성을 가지는 고유한 값이며, 확산 함수 $\beta_x(t)$는 감염가능한 취약 호스트 수가 줄어듦에 따라 함께 감소하게 된다.
- 융합망 환경의 취약 호스트는 자신의 네트워크뿐 아니라 다른 네트워크에서 발생한 웜에 감염될 수 있으며, 이로 인해 서로의 취약 호스트에 영향을 주어 전체적인 확산율에 영향을 미친다. $\sigma_x(t)$는 이를 반영한 함수이고, 전체 취약 호스트와 해당 네트워크 취약 호스트에 대한 비율 함수이다.
- 융합망 환경에서 전체 웜 확산 속도는 가장 높은 속도의 네트워크에서 웜 확산 속도와 가장 낮은 속도의 네트워크에서 웜 확산 속도 사이에 존재한다.

Ⅳ. 실험 내용과 결과 분석

4.1 다양한 환경에서 웜확산 실험

실험 1. 유선 인터넷과 무선 인터넷 환경에서 웜 확산 실험

앞의 수식에 따라 유무선 인터넷 환경에서 웜 확산을 실험하면 그림 6과 같다. 여기서, 감염가능한 전체 호스트 수를 10,000대($N=10,000$)로 두고, 유선 인터넷(IEEE 802.3)에서 100Mbps 속도를, 무선 인터넷(802.11g)에서 54Mbps 속도로 Slammer 웜이 호스트 1대에서 시작하여 유선 인터넷의 취약 호스트 7,000대와 무선 인터넷의 취약 호스트 3,000대를 대상으로 확산한다고 가정한다.

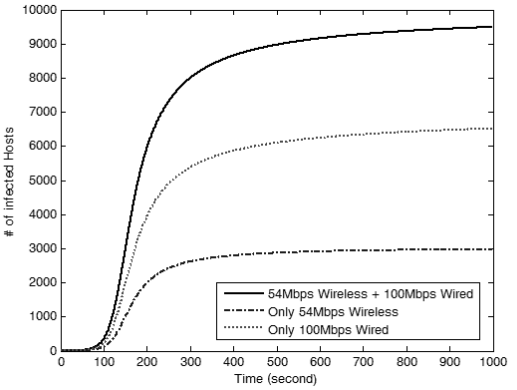

그림 6. 고속도 유무선 인터넷에서 웜 확산

실험 2. 감염 호스트 수에 따른 융합망 환경에서 웜 확산 실험

실험 1과 동일한 조건에서 최초 감염 호스트 수를 변화시킨 경우의 웜 확산 실험 결과는 그림 7과 같다. 여기서, 감염가능한 전체 호스트 수를 10,000대($N=10,000$)로 두고, 최초 감염 호스트의 수는 10대, 100대, 1,000대이다.

이 실험에서 웜은 최초 감염 호스트 수가 많으면 감염 호스트와 취약 호스트의 상호 작용이 증가하므로 더 빨리 확산한다는 사실을 확인할 수 있다.

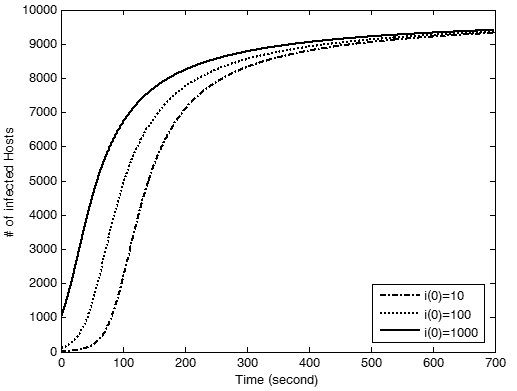

그림 7. 최초 감염 호스트 수에 따른 웜 확산

실험 3. 무선 인터넷 환경의 취약 호스트 수에 따른 융합망 환경에서 웜 확산 실험

유무선 인터넷 환경에서 취약 호스트 수에 따른 웜 확산을 실험하면 그림 8과 같다. 여기서, 감염가능한 전체 호스트 수를 10,000대($N=10,000$)로 두고, 무선 인터넷 환경의 취약 호스트를 1,000대, 4,000대, 7,000대로 차츰 증가시켜 실험하였다.

이 실험에서 무선 인터넷의 취약 호스트 수가 적고 유선 인터넷의 취약 호스트 수가 많을수록 인터넷 웜이 더 빠른 속도로 확산한다는 사실을 확인할 수 있다. 단, 무선 인터넷의 취약 호스트가 4,000대와 7,000대의 경우 유선 인터넷과의 속도차로 인하여 후반부에서는 역전 현상이 발생한다.

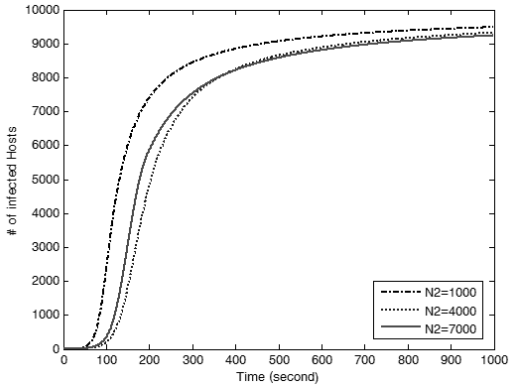

그림 8. 무선 인터넷 환경의 취약 호스트 증가에 따른 웜 확산

실험 4. 유무선 인터넷과 이동 인터넷으로 구성된 융합망에서 웜 확산 실험

유무선 인터넷 및 이동 인터넷 환경에서 웜 확산을 실험하면 그림 9와 같다.

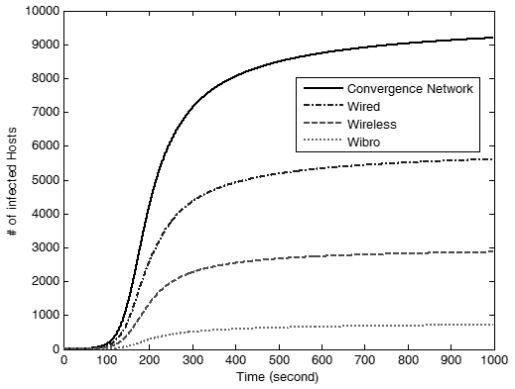

그림 9. 다양한 융합망 환경에서 웜 확산

여기서, 감염가능한 전체 호스트 수를 10,000대($N=10,000$)로 두고, 100Mbps 유선 인터넷 6,000대, 54Mbps 무선 인터넷 3,000대, 10Mbps Wibro 1,000대를 대상으로 확산하는 실험이다.

4.2 실험 결과 분석

앞에서 실시한 융합망 환경에서 다양한 웜 확산 실험 결과를 분석하면 웜 확산에 대해 다음과 같은 대응 방안을 유도할 수 있다.

- 최초 감염 호스트 수 $I_x(0)$가 적으면 웜은 느린 속도로 확산하므로, 취약 호스트가 감염되지 않도록 대비한다면 웜 확산을 늦출 수 있다.
- 웜 확산 대응 방안이 마련되어 있지 않다면 취약 호스트를 저속도 네트워크에 배치하는 것만으로도 확산 속도를 늦추는 효과를 가져온다.
- 웜 확산 대응 방안이 마련된 이후에는 고속도 네트워크의 감염 호스트를 먼저 치료하는 것이 효과적으로 확산 속도를 늦출 수 있다.
- 웜 확산에 대한 대응이 빠르면 빠를수록 확산은 효과적으로 감소한다(그림 10은 대응 시점이 200초, 400초, 600초인 경우의 웜 확산 곡선).

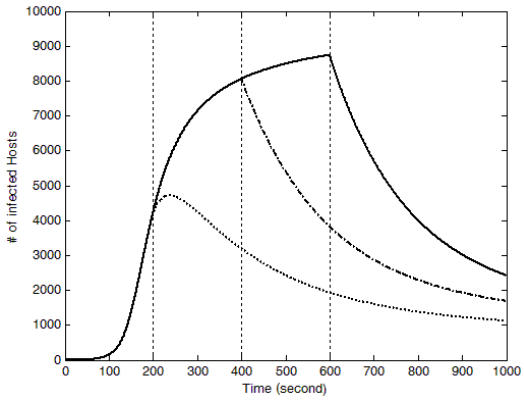

그림 10. 대응 시점에 따라 감소하는 웜 확산

V. 결 론

전 세계를 단일 네트워크로 연결한 인터넷은 서로 다른 네트워크 기술을 통합하더니 이제는 다양한 서비스와 기술을 도입한 융합망으로 거듭나고 있다. 그러나 기술과 서비스의 융합 인터넷 환경이 바이러스, 악성봇, 인터넷 웜이 확산하기 위한 천혜의 환경을 제공하는 결과를 가져왔다. 이로 인해 각종 시스템을 사용하지 못하도록 하는 직접적인 효

과와 인터넷 기반 구조의 신뢰성에 심각한 타격을 주는 간접적인 가능성도 함께 내포하고 있다. 단적인 예로, 2003년 Slammer Worm에 의해 발생한 1.25 대란과 2009년 DDoS에 의해 발생한 7.7 대란은 인터넷을 통한 초고속 정보화 사회를 지향하는 한국에 있어서 인터넷 하부구조 보안, 사이버 테러에 대한 조기 대응, 콘트롤 타워에 의한 정보보호 정책 시행에서 중요한 시사점을 제시하고 있다.

본 논문에서는 현재 문제가 되고 있는 인터넷 웜 확산 모델을 분석하고, 향후 융합망 환경에 적용가능한 새로운 모델을 제안하여 융합망에서 인터넷 웜 확산을 예측하고, 감염 호스트 수, 인터넷 속도, 주소체계를 고려한 다양한 환경에서 그 영향을 분석하였다. 본 논문의 결과는 인터넷의 융합화에 따른 웜 확산을 초기에 예측하고 다양한 환경에서 대응 방안을 마련하는데 활용할 수 있을 것이다.

참 고 문 헌

〔1〕 *"인터넷침해사고 동향 및 분석월보"*, *한국정보보호진흥원*, 2008.

〔2〕 Cliff Changchun Zou, Don Towsley, Weibo Gong, "On the Performance of Internet Worm Scanning Strategies," *Elsevier Journal of Performance Evaluation*, Vol.63, No.7, pp.700-723, 2006.

〔3〕 Cliff Changchun Zou, Weibo Gong, Don Towsley, "Code Red Worm Propagation Modeling and Analysis," 9th ACM Conference on Computer and Communication Security (CCS'02), pp.138-147, 2002.

〔4〕 "The Spread of the Sapphire/Slammer Worm," http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

〔5〕 신원, "IPv6 환경에서 인터넷 웜 확산 방식 연구", *Telecommunications Review*, 제19권 1호, pp.118-128, 2009.

〔6〕 Cliff Changchun Zou, Lixin Gao, Weibo Gong, Don Towsley, "Monitoring and Early Warning for Internet Worms," 10th ACM Conference on Computer and Communication Security (CCS'03), pp.190-199, 2003.

〔7〕 D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver. "Inside the Slammer Worm". *IEEE Magazine on Security and Privacy*, Vol.1, No.4, pp.33-39, 2003.

〔8〕 An Analysis of Conficker's Logic and Rendezvous Points, http://mtc.sri.com/Conficker/

〔9〕 Phillip Porras and Hassen Sa¨ıdi and Vinod Yegneswaran, "A Multi-perspective Analysis of the Storm (Peacomm) Worm", CSL Technical Note, SRI International, 2007.

〔10〕 Akamai Technologies, "The State of the Internet, 1Q 2009", 2009.

〔11〕 Pele Li, Mehdi Salour and Xiao Su, "A Survey of Internet Worm Detection and Containment", *IEEE Communications Surveys & Tutorials*, 1st Quarter 2008, Vol.10, No.1, pp.20-35, 2008.

신 원 (Weon Shin) 정회원

2001년 8월 부경대학교 전자계산학과 이학박사

2002월 3월~2005년 1월 (주)안철수연구소 선임연구원

2005년 3월~현재 동명대학교 정보보호학과 조교수

<관심분야> 악성코드 확산, 디지털 포렌식, 소프트웨어 보안, 암호 프로토콜 응용