JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 12 : 2858~2864 Dec. 2015

복수 인터넷 웜의 확산 방식 연구

신 원*

The Propagation Dynamics of Multiple Internet Worms

Weon Shin*

Department of Information Security, Tongmyong University, Busan, 48520, Korea

요 약

최근 인터넷 웜은 악성코드 중 가장 빠른 속도로 확산하면서 정보 유출, 시스템 결함 등을 일으킬 수 있는 주요한 위협이 되고 있다. 특히, 복수의 인터넷 웜과 변종 웜이 동시 다발적으로 확산하면서 기존 인터넷 웜 대응 방식으로는 한계가 된다는 것을 여실히 보여주고 있다. 이러한 다양한 인터넷 웜에 효과적으로 대응하기 위해서는 복수 웜의 확산 방식을 이해하는 것이 필수적이다. 본 논문에서는 기존의 단일 웜 확산 모델을 개선하여 복수 변종 웜 확산에 대한 정확한 모델링을 목표로 하고, 다양한 실험을 통하여 복수 웜 확산의 양상을 분석한다.

ABSTRACT

Internet worms have been the major Internet threats may disclose important information and can bring about faults of computer systems, which spread with the fastest speed among malicious codes. Simultaneously spreading multiple worms and its variants are revealing the limitation of conventional responses based on single worms. In order to defend them effectively, it is necessary to study how multiple worms propagate and what factors affect worm spreading. In this paper, we improve the existed single worm spreading models and try to describe the correct spreads of multiple worms. Thus we analyze the spreading effects of multiple worms and its variants by various experiments.

키워드 : 인터넷 웜, 변종 웜, 확산 모델링, 웜 확산, 복수 웜 확산

Key word : Internet worm, Worm variants, Propagation modeling, Worm spreading, Multiple worm spreading

Received 13 August 2015, **Revised** 04 September 2015, **Accepted** 18 September 2015

* **Corresponding Author** Weon Shin (E-mail:shinweon@tu.ac.kr, Tel:+82-51-629-1284)
Department of Information Security, Tongmyong University, Busan, 48520, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.12.2858 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

세계적으로 널리 보급되고 있는 인터넷 기술은 시간적 제약과 공간적 한계를 극복하여 다양한 실생활의 서비스들이 인터넷의 가상생활에서도 실현될 수 있도록 진화하고 있다. 그러나 새로운 인터넷 기술이 등장함에 따라 이에 따른 역기능들도 함께 증가하고 있다. 특히 정보보호 측면에서 시스템 취약점을 이용한 악성코드 공격, 운영체제 취약점 또는 시스템 구성 상의 오류를 이용한 해킹, 좀비 PC들을 이용한 분산서비스 거부 공격 등이 기하급수적으로 증가하고 있으며, 매년 엄청난 피해를 끼치고 있다. 그러나 그 중에서도 세계적인 규모로 발생하여 인터넷 환경에 막대한 피해를 끼칠 수 있는 공격이 바로 인터넷 웜을 이용한 공격으로, 대표적으로 과거의 Code Red worm, Slammer worm 등의 사례를 살펴보면 이러한 사실을 직접 확인할 수 있다.

인터넷 웜은 "많이 사용하는 서비스의 보안 취약점이나 정책 결함을 악용하여 스스로 네트워크를 통해 전파하는 프로그램"으로 정의된다[1]. 즉, 인터넷 웜은 소프트웨어의 구현 버그, 설계 결함 등의 취약성을 이용하여 시스템의 권한을 획득하고 자기 자신을 복제하여 허가되지 않은 동작을 수행하는 악성 코드(Malicious Code)이다. 이 과정 중에 수행되는 코드와 발생되는 패킷은 시스템 및 운영체제에 오버헤드를 초래할 뿐만 아니라 정상적인 네트워크 서비스가 불가능하도록 만든다. 따라서, 우리나라와 같은 초고속 인터넷 환경에서 인터넷 웜의 확산은 단순한 악성 코드의 확산을 의미할 뿐만 아니라 인터넷 기반구조를 사용불능으로 만드는 분산 서비스 거부 공격과 같은 의미를 가질 수 있다. 또한, 최근 인터넷 웜 공격의 특징은 하나의 웜이 제작되면 관련 소스가 배포되거나 공개되어 이를 이용한 유사 웜 또는 변종 웜이 제작되어 확산되고 있다. 그래서, 최초의 웜에 대한 대응 방안을 마련하였다하더라도 유사 웜 또는 변종 웜 대응에는 또 다른 대응 방안을 마련하여 개별적으로 대응해야한다는 문제점을 가진다.

본 논문에서는 단일 웜 기반의 기존 웜 확산 방식을 개선하여 다중 인터넷 웜에 적합한 새로운 복수 웜 확산 모델링을 수행한다. 이를 활용하여 현재 인터넷 환경에서 다중 또는 변종 웜 확산과 각 확산 요인에 따른 영향을 분석하고자 한다. 먼저 2장에서는 웜 확산 모델을 살펴보고, 복수 변종 웜을 고려한 새로운 확산 모델을 제안한다. 3장에서 인터넷 환경에서 다양한 웜 확산 실험을 수행한 후 4장에서 실험 내용을 분석한다. 마지막 5장에서 결론을 유도한다.

Ⅱ. 복수 인터넷 웜의 확산 모델링

2.1. 기존 웜 확산 모델

인터넷 웜 확산에서 가장 많이 사용하는 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. SI 모델을 개선한 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 수식 (1)과 같다. 여기서, $S(t)$는 t시점에 취약한 호스트 수, $I(t)$는 t시점에 감염 호스트 수, $R(t)$는 t시점에 복구된 호스트 수이다.

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

인터넷 웜은 "스캐닝(Scanning)"을 수행하여 사용 가능한 주소 공간을 대상으로 감염 가능한 취약 호스트를 물색한다[1,4]. 스캐닝을 통하여 취약 호스트에 자기 자신을 복제하여 감염시키고, 감염된 호스트에서 다시 스캐닝을 반복하여 확산한다. Zou 등[5]은 인터넷 웜의 스캐닝에 따른 성능을 분석하였는데, 단위시간당 균등 스캐닝을 수행하는 RCS(Random Constant Spread) Worm의 동작에서 수식 (2)를 유도하여 인터넷 환경의 웜 확산을 설명하였다.

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)], \beta = \frac{\eta}{\Omega} \qquad (2)$$

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

한편, Two-factor Worm Model[6]에서는 웜 확산 속도 감소 정도를 반영하여 확산율 β를 시간에 따라 변화

하는 함수 $\beta(t)$를 적용한 수식(3)을 보여준다.

$$\beta(t) = \beta_0(1 - \frac{I(t)}{N})^{\phi} \quad (3)$$

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

실제적으로 Code Red worm 확산 당시 Goldsmith와 Eichman이 네트워크 트래픽에 대한 데이터를 수집하였다[7,8]. Fig. 1은 두 데이터의 평균값을 점으로 표기하였고, 제안 확산 모델에 따른 웜 확산을 실선으로 표기하였다. 그래프를 살펴보면 모델링에 의한 확산과 실제 측정값이 매우 비슷한 형태임을 알 수 있다.

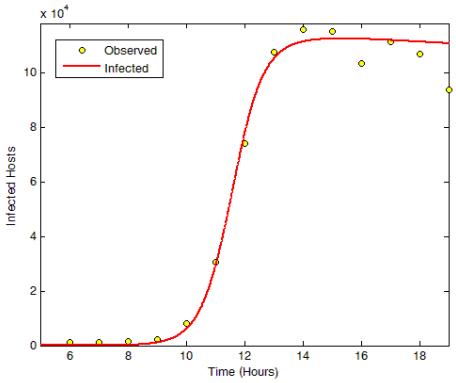

Fig. 1 The observed results of Code Red worm and the estimation by modeling

2.2. 새로운 복수 웜 확산 모델

이 장에서는 단일 웜에 기반하는 기존 확산 모델을 개선하여 복수 웜 확산에 적용할 수 있는 새로운 확산 모델을 제안한다. 기존의 웜 확산 모델은 하나의 웜을 가정하여 작성되었으므로 단일 웜이 확산하는 경우를 잘 설명할 수 있지만, 여러 개의 변종 웜이 발생하여 동시에 인터넷으로 확산하는 경우 복수 웜의 동작을 설명할 수 없다[9]. 따라서 이를 위한 수정과 새로운 가정이 불가피하다. 제안 모델의 가정은 다음과 같다.

<가정>

① 각 호스트는 동일한 웜에 여러 번 중복으로 감염되지 않는다.

② 각 호스트가 웜에 감염된 경우, 해당 웜의 변종 웜에는 감염되지 않지만 다른 웜에는 감염될 수 있다.

③ 인터넷 웜은 확산을 시작하는 호스트의 해당 네트워크 속도에 맞추어 확산한다.

④ 미시적 관점에서 다루는 감염 호스트 성능이나 라우터와 같은 네트워크 장비에서 발생하는 패킷 오버헤드 등은 무시한다.

Table 1은 본 논문에서 사용하는 표기법이다.

Table. 1 Notations used in this paper

Notation	Explanation
N	Total number of vulnerable hosts
W_x	The x-th variant of the worm W
$S(t)$	Number of susceptible hosts at time t
$I_x(t)$	Number of hosts infected with worm W_x at time t
$R(t)$	Number of recovered hosts at time t
$\beta_x(t)$	Infection rate of W_x at time t
$\gamma_x(t)$	Recovery rate of W_x at time t

복수 웜 확산 모델에서는 모든 호스트는 기존 확산 모델과 마찬가지로 S, I, R의 3가지 상태를 가진다. Fig. 2는 인터넷 웜 W_0이 확산하여 각 호스트가 S에서 I_0(W_0에 감염된 상태)로 전이된 이후 R로 복구되는 경우인데, 웜은 자신의 확산율 $\beta_0(t)$로 확산하고 복구율 $\gamma_0(t)$로 복구한다.

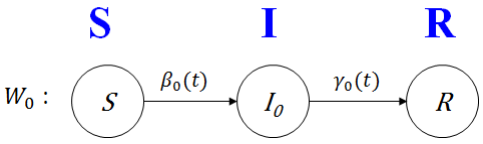

Fig. 2 The new SIR spread model of a worm

Fig. 3은 1개의 인터넷 웜을 시작으로 n개의 인터넷 웜이 함께 확산하여 각 호스트가 S에서 I_0(W_0에 감염된 상태) 또는 I_n(W_n에 감염된 상태)으로 전이된 이후 R로 복구되는 경우인데, 각 웜은 확산율 $\beta_0(t),\cdots,\beta_n(t)$로 각각 확산하고, 복구율 $\gamma_0(t),\cdots,\gamma_n(t)$으로 각각 복구한다.

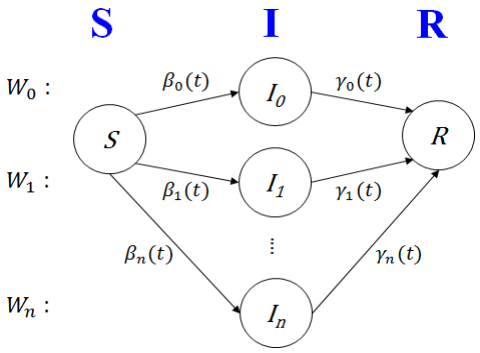

Fig. 3 The new SIR spread model of multiple worms

여러 개의 웜 $W_0, W_1, \cdots, W_n$이 각각의 확산율로 웜이 확산되는 경우, t시점에서 감염된 호스트 수는 다음 식을 이용하여 계산할 수 있다. 서로 다른 웜은 서로의 확산에 영향을 미치지 않고 개별적으로 확산하며, 각 호스트는 웜 $W_0, W_1, \cdots, W_n$에 중복 감염될 수 있다. 다음 수식(4)에 의해 감염 호스트 수를 계산할 수 있다.

$$\begin{aligned}
\frac{dI_0(t)}{dt} &= \beta_0(t)I_0(t)[N-I_0(t)]-\gamma_0 I_0(t) \\
\frac{dI_1(t)}{dt} &= \beta_1(t)I_1(t)[N-I_1(t)]-\gamma_1 I_1(t) \\
&\vdots \\
\frac{dI_n(t)}{dt} &= \beta_n(t)I_n(t)[N-I_n(t)]-\gamma_n I_n(t)
\end{aligned} \tag{4}$$

변종 웜은 이미 공개된 소스 또는 툴킷 등을 활용하거나 여러 키를 이용하여 암호화 또는 다양한 방식의 압축하는 방식을 적용한다[10]. 특히 변종 웜인 경우 서로에게 영향을 끼치며 확산하고, 각 호스트는 웜 $W_0, W_1, \cdots, W_n$에 중복 감염되지 않는데 다음 수식 (5)에 의해 감염 호스트 수를 계산할 수 있다.

$$\begin{aligned}
\frac{dI_0(t)}{dt} &= \beta_0(t)I_0(t)[N-I_0(t)-I_1(t)\cdots-I_n(t)]-\gamma_0 I_0(t) \\
&= \beta_0(t)I_0(t)[N-I(t)]-\gamma_0 I_0(t) \\
\frac{dI_1(t)}{dt} &= \beta_1(t)I_1(t)[N-I_0(t)-I_1(t)\cdots-I_n(t)]-\gamma_1 I_1(t) \\
&= \beta_1(t)I_1(t)[N-I(t)]-\gamma_1 I_1(t) \\
&\vdots \\
\frac{dI_n(t)}{dt} &= \beta_n(t)I_n(t)[N-I_0(t)-I_1(t)\cdots-I_n(t)]-\gamma_n I_n(t) \\
&= \beta_n(t)I_n(t)[N-I(t)]-\gamma_n I_n(t)
\end{aligned} \tag{5}$$

단, $I(t) = I_0(t) + I_1(t) + \cdots + I_n(t)$

Ⅲ. 복수 인터넷 웜 확산 실험

인터넷 웜에 대한 확산율 $\beta(t)$는 앞에서 설명한 바와 같이 전체 취약 호스트 수와 네트워크 대역폭에 따라 좌우된다.

복구율 $\gamma(t)$은 Two-factor Worm Model[6]과 같이 사용하고 편의상 모두 같은 값으로 사용한다. 한편, Akamai가 조사한 2015년 1분기 인터넷 평균 속도 측정 결과에 따르면 한국이 23.6Mbps, 전세계 평균 인터넷 속도는 5.0Mbps로 조사되었다[11]. 본 논문에서는 이 결과를 변종 웜 확산에 적용하여 다양한 실험을 수행한다. 실험에서 웜은 전체 IP 주소를 균일하게 스캔하면서 인터넷 평균 속도로 확산하고 패킷 오버헤드는 따로 고려하지 않는다고 가정한다.

3.1. 다중 인터넷 웜의 개별 확산

Fig. 4는 200KB 크기의 인터넷 웜 W가 호스트 1대를 감염시켜 확산한 후 24시간 후 150KB의 다른 인터넷 웜 X가 확산한 실험결과이다. 여기서, $N = 10{,}000$이고, Total은 웜 W 또는 웜 X 중 하나 이상에 감염된 호스트 수의 합이다.

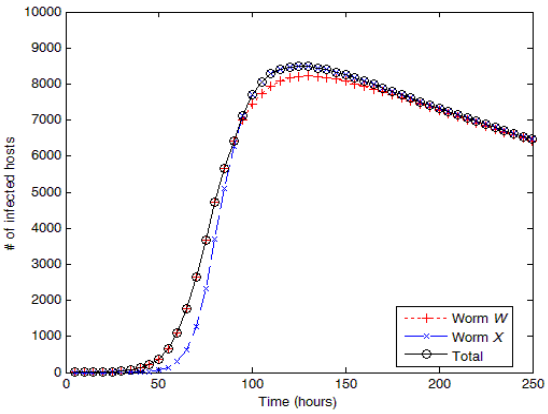

Fig. 4 The spread of multiple worms

인터넷 웜 X가 인터넷 웜 W보다 24시간 늦게 확산을 시작하였으나 크기가 작으므로 확산 속도가 역전함을 확인할 수 있다. 또한, 인터넷 웜 X와 인터넷 웜 W는 서로 다른 웜이므로 중복으로 취약 호스트에 감염하여 확산한다.

3.2. 복수 변종 웜의 개별 확산

Fig. 5는 200KB 크기의 인터넷 웜 W가 호스트 1대를 감염시켜 확산한 후 24시간 후 150KB의 변종 웜 W_1이 확산한 실험결과이다. 여기서, $N=10{,}000$이고, Total은 웜 W와 웜 W_1에 감염된 호스트 수의 합이다.

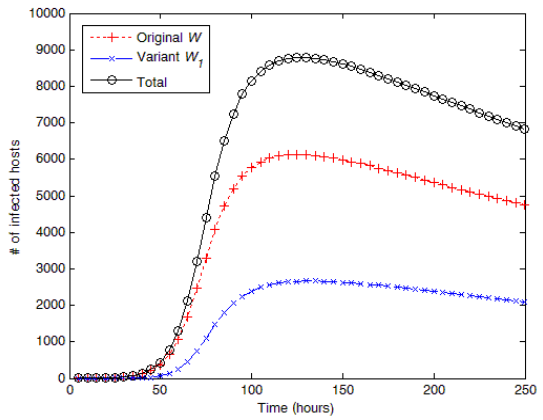

Fig. 5 The spread of worm variants

변종 웜 W_1는 인터넷 웜 W가 보다 24시간 늦게 확산을 시작하였으므로 인터넷 웜 W가 감염되지 않은 취약 호스트를 대상으로 확산을 시작한다. 즉, 인터넷 웜 W와 변종 웜 W_1는 같은 특성을 가진 웜이므로 취약 호스트가 두 웜에 중복으로 감염되지 않는다.

3.3. 복수 변종 웜의 확산

Fig. 6은 200KB 크기의 인터넷 웜 W가 호스트 1대를 감염시켜 확산한 후 24시간 후 150KB의 다른 웜 X가 확산하고 다시 24시간 후 150KB의 변종 웜 W_1이 확산한 실험결과이다. 여기서, Total은 웜 W, 웜 X, 웜 W_1 중 하나 이상에 감염된 호스트 수의 합이다.

인터넷 웜 W이 확산 후 48시간이 지났을 때 변종 웜 W_1이 확산을 시작하는데, 이미 W에 의해 취약 호스트 수가 매우 감소한 상태이므로 W_1의 확산이 거의 진행되지 않는다. 다른 웜 X는 W와 변종 웜 W_1에 감염된 호스트도 중복해서 감염될 수 있으므로 대규모로 확산이 진행되는 것을 확인할 수 있다.

Fig. 7은 200KB 크기의 인터넷 웜 W가 호스트 1대를 감염시켜 확산한 후 24시간 후 150KB의 변종 웜 W_1가 확산하고 다시 24시간 후 150KB의 다른 웜 X가 확산한 실험결과로, Fig. 6에서 다른 웜과 변종 웜의 순서만 바꾼 것이다. 여기서, $N=10{,}000$이고, Total은 웜 W, 웜 X, 웜 W_1 중 하나 이상에 감염된 호스트 수의 합이다.

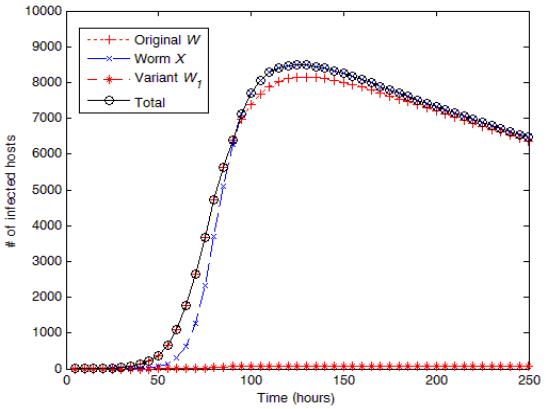

Fig. 6 The spread of multiple worms and worm variants

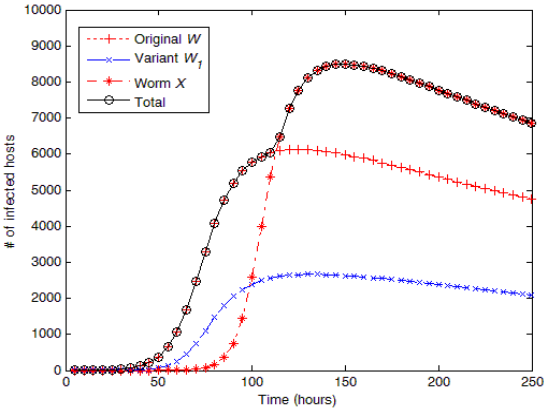

Fig. 7 The spread of worm variants and multiple worms

인터넷 웜 W이 확산 후 24시간이 지났을 때 변종 웜 W_1이 확산을 시작하는데, W에 의해 취약 호스트 수가 감소한 상태라 하더라도 아직 취약 호스트가 남아있으므로 W_1은 확산이 소규모로 발생한다. 다른 웜 X는 W와 변종 웜 W_1에 감염된 호스트도 중복해서 감염될 수 있으므로 대규모로 확산이 진행되는 것을 확인할 수 있다.

3.4. 복수 변종 웜의 동시 확산

Fig. 8은 인터넷 웜 W과 확산을 시작한 24시간 이후에 변종 웜 W_1, 다른 웜 X가 동시에 확산한 실험결과이다. 여기서, $N=10{,}000$이고, Total은 웜 W, 웜 X, 웜 W_1 중 하나 이상에 감염된 호스트 수의 합이다.

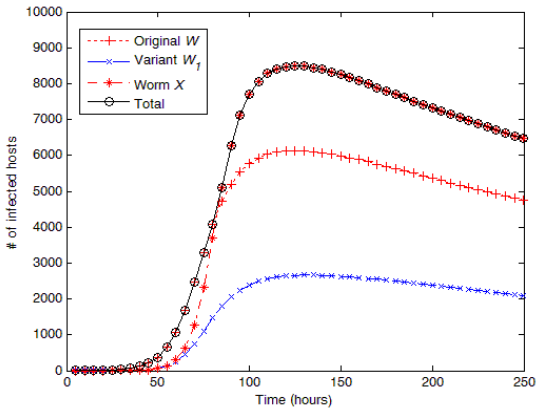

Fig. 8 The simultaneous spread of multiple worms and worm variants

인터넷 웜 W이 확산 후 24시간이 지났을 때 변종 웜 W_1와 다른 웜 X가 확산을 시작하는데, 이미 W에 의해 취약 호스트 수가 감소한 상태이므로 W_1의 확산이 소규모로 발생한다. X는 중복으로 감염될 수 있으므로 다른 웜 감염과 관련없이 확산이 증가하는 것을 확인할 수 있다. 즉, Fig. 6과 유사한 결과이지만, X가 더 일찍 확산한 결과이다.

Ⅳ. 실험 내용 분석

앞의 복수 웜 확산 실험 내용을 분석하면 다음과 같은 중요 내용을 얻어낼 수 있다.

① 미시적 관점의 감염 호스트 성능이나 네트워크 장비의 패킷 오버헤드 등을 무시하는 경우, 웜 확산의 가장 큰 영향을 끼치는 것은 웜 자체의 크기이다.

② 서로 다른 웜 확산에서는 확산 시기도 중요하지만 웜 자체의 크기와 인터넷 속도에 따라 확산 속도가 좌우된다.

③ 변종 웜은 원형 웜 확산 속도에 영향을 받는다. 변종 웜은 취약 호스트에 원형 웜과 중복 감염될 수 없으므로, 원형 웜이 감염되지 않은 취약 호스트를 대상으로 확산되기 때문에 확산 속도는 늦어질 수밖에 없다.

④ 서로 다른 웜은 취약 호스트에 중복으로 감염될 수 있으므로, 확산 속도는 각각의 웜에 따라 독립적이다.

⑤ 복수 웜을 가능한 한 짧은 시차를 두고 확산시키는 것이 확산 효과가 크다. 특히, 동시에 확산시키는 것이 확산 효과가 가장 크며, 시차가 커지면 단일 웜 확산과 사실상 차이가 없다.

이 내용을 기반으로 인터넷 웜을 개발하여 공격하는 경우 다음과 같이 하는 것이 효과가 크다는 것을 확인할 수 있다.

① 서로 다른 웜을 동시에 개발하여 확산시키는 것이 피해를 더 키울 수 있다. 단, 웜 개발자 입장에서는 인터넷 웜 여러 개를 동시에 제작하는 것은 현실적으로 어려운 문제이다.

② 서로 다른 웜을 동시에 개발하는 것이 어려운 경우, 변종 웜을 개발하여 확산시키는 것이 효과가 있다. 단, 가능한 같은 시기에 확산시키는 것이 효과가 더 크다.

③ 인터넷 웜을 가능한 작은 크기로 제작하는 것이 가장 큰 피해를 끼칠 수 있다. 이는 인터넷 웜 확산의 핵심사항으로 웜 개발자 입장에서는 매우 중요한 문제이다.

④ 한국과 같은 인터넷 속도가 빠른 국가에서 인터넷 웜을 확산시키는 것이 웜 확산 피해가 더 크다.

Ⅴ. 결 론

컴퓨터 바이러스, 인터넷 웜, 트로이 목마, 루트킷과 같은 다양한 종류의 악성코드는 인터넷 기술에 대한 역기능으로써 국가적 규모의 피해를 끼칠 심각한 위협으로 인식되고 있다. 그 중 컴퓨터 시스템의 취약점을 이용하여 확산되는 인터넷 웜은 인터넷 기반 구조를 공격하여 시스템의 결함을 유발하여 신뢰성에 타격을 주는 특징을 가진다. 과거에 세계적으로 확산되어 막대한 피해를 끼쳤던 Code Red Worm, Conficker Worm, Stuxnet Worm 등은 자체 웜의 피해는 물론 이들의 변종

웜에 의한 피해가 광범위하게 이루어졌다[6, 12, 13]. 이로 인해 단일 웜에 대한 시그니처 기반 대응 방식의 한계를 드러내면서 기존 악성코드 대응 방식에 새로운 시사점을 제시하였다.

본 논문에서는 현재 심각한 문제가 되고 있는 인터넷 웜의 다중 확산에 대한 모델링을 수행하고, 여러 웜의 확산 방식과 그 영향을 분석하였다. 본 논문의 결과는 향후 등장 가능한 다양한 인터넷 웜 확산을 정확히 예측하고 대응 방안을 마련하는데 유용하게 활용될 수 있을 것이다.

REFERENCES

[1] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A taxonomy of computer worms," *in Proceeding 2003 ACM workshop on Rapid malcode,* New York, pp.11-18, 2003.

[2] Herbert W. Hethcote, "The Mathematics of Infectious Diseases," *SIAM Review*, vol. 42, no. 4, pp.599-653, 2000.

[3] James D. Murray, Mathematical Biology: I. An Introduction, Third Edition, New York, Springer, 2001.

[4] Yini Wang, Sheng Wen, Yang Xiang, and Wanlei Zhou, "Modeling the Propagation of Worms in Networks: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 2, pp. 942-960, 2014.

[5] Cliff C. Zou, Don Towsley and Weibo Gong, "On the Performance of Internet Worm Scanning Strategies," *Elsevier Journal of Performance Evaluation*, vol. 63, no. 7, pp.700-723, Jul. 2006.

[6] Cliff C. Zou, Weibo Gong and Don Towsley. "Code Red Worm Propagation Modeling and Analysis," *in Proceeding 9th ACM Conference on Computer and Communication Security*, pp.138-147, New York, USA, 2002.

[7] Possible CodeRed Connection Attempts [Internet]. Available: http://lists.jammed.com/incidents/2001/07/0149.html

[8] Re: Possible CodeRed Connection Attempts [Internet]. Available: http://lists.jammed.com/incidents/2001/07/0159.html

[9] Weon Shin, "Propagation Modeling of Multiple Internet Worm Variants," *Journal of Security Engineering,* vol. 12, no. 3, pp.247-258, 2015.

[10] Sounak Paul and Bimal Kumar Mishra, "Survey of Polymorphic Worm Signatures," *International Journal of u- and e- Service, Science and Technology*, vol.7, no.3, pp.129-150, 2014.

[11] Akamai, (Q1 2015), The State of the Internet, 2015 Report, vol. 8, no. 1, Available: https://www.stateoftheinternet.com/resources-web-security-2015-q1-internet-security-report.html

[12] Kelly Burton, The Conficker Worm [Internet]. Available: https://www.sans.org/security-resources/malwarefaq/conficker-worm.php

[13] David Kushner, The Real Story of Stuxnet [Internet]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

신원 (Shin, Weon)

2001년 8월 : 부경대학교 전자계산학과 이학박사 졸업
2002년 3월 ~ 2005년 1월 ㈜안랩(구, ㈜안철수연구소) 선임연구원
2005년 3월 ~ 현재 동명대학교 정보보호학과 조교수, 부교수
※ 관심분야 : 소프트웨어 보안, 악성코드 확산, 디지털 포렌식