ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

온라인 소셜 네트워크에서 구조적 파라미터를 위한 확산 모델

Propagation Models for Structural Parameters in Online Social Networks

공 종 환[1] 김 익 균[2] 한 명 묵[1*]
Jong-Hwan Kong Ik Kyun Kim Myung-Mook Han

요 약

단순한 소통 미디어였던 소셜 미디어가 최근에는 트위터, 페이스북을 중심으로 활성화되면서 소셜 네트워크 서비스의 활용 및 중요성이 점차 커지고 있다. 기업들은 소셜 네트워크의 빠른 정보 확산 능력을 통해 마케팅에 적극 활용하고 있지만, 정보 확산 능력이 커지면서 이에 대한 역기능 또한 증가하고 있다. 소셜 네트워크는 사용자들의 친분 및 관계를 기반으로 형성되고 소통하기 때문에 스팸, 악성코드 유포에 대한 효과 및 확산 속도가 매우 빠르다. 이에 본 논문에서는 소셜 네트워크 환경에서 악성 데이터 확산에 영향을 미치는 파라미터들을 도출하고, XSS Worm과 Koobface Worm의 확산 실험을 통해 각각의 파라미터들의 확산 능력을 비교 분석한다. 또한, 소셜 네트워크 환경에서의 구조적 특징을 고려하여 정보 확산에 영향을 미치는 파라미터에 기반 한 악성 데이터 확산 모델을 제안한다. 본 논문이 제안하는 방법의 실험을 위해 역학 모델인 SI 모델을 기반으로 BA모델과 HK모델을 구성하여 실험을 진행하고, 실험의 결과로 XSS Worm과 Koobface Worm의 확산에 영향을 미치는 파라미터는 군집도와 근접 중심성임을 확인할 수 있었다.

☞ 주제어 : 악성 데이터, 확산모델, 소셜 네트워크, 인터넷 웜

ABSTRACT

As the social media which was simple communication media is activated on account of twitter and facebook, it's usability and importance are growing recently. Although many companies are making full use of its the capacity of information diffusion for marketing, the adverse effects of this capacity are growing. Because social network is formed and communicates based on friendships and relationships, the spreading speed of the spam and mal-ware is very swift. In this paper, we draw parameters affecting malicious data diffusion in social network environment, and compare and analyze the diffusion capacity of each parameters by propagation experiment with XSS Worm and Koobface Worm. In addition, we discuss the structural characteristics of social network environment and then proposed malicious data propagation model based on parameters affecting information diffusion. n this paper, we made up BA and HK models based on SI model, dynamic model, to conduct the experiments, and as a result of the experiments it was proved that parameters which effect on propagation of XSS Worm and Koobface Worm are clustering coefficient and closeness centrality.

☞ keyword : Malicious data, Propagation Model, Social Network, Internet worm

1. 서 론

최근 스마트폰의 보급이 확대되고 모바일 및 인터넷 환경이 활성화됨에 따라 소셜 네트워크 서비스 이용이 급증하고 있다. 이로 인해 사람들은 시간과 장소의 제약 없이 소셜 네트워크 서비스에 접속하여 사용자 및 참여자들 간의 다양한 정보나 소식들을 전달하면서 정보의 확산 뿐만 아니라 사용자들 간의 사회적 상호작용을 통해 여론을 형성하는 등 큰 영향력을 발휘하고 있다.

이전에 단순한 소통 미디어였던 소셜 미디어가 최근에는 트위터, 페이스북을 중심으로 활성화되면서 파급효과는 더욱 커지고 있다. 이에 각 기업들은 트위터, 페이스북 등의 소셜 네트워크 서비스를 활용하여 마케팅에 적극 활용하였다. 기업들은 그들의 공식 소셜 네트워크 환경의 프로필 상에서 노출전략 및 정보 확산전략을 이용하여 기업에 대한 기본적인 설명, 공식 홈페이지로의 링크 제공, 로고 노출, 담벼락 및 미디어의 활용 등을 통해 기업의 홍보 및 제품의 홍보 수단으로 마케팅에 적극 활용하였다. 이와 같이 소셜 네트워크 환경에서의 정보 확산의 영향력이 커짐에 따라 이에 대한 역기능 또한 증

1 Depart of Computer Engineering, Gachon University, Seongnam, 461-701, Korea
2 Cyber Security Research Division, Electronics and Telecommunications Research Institute, Daejeon, 305-700 Korea
* Corresponding author (mmhan@gachon.ac.kr)
[Received 5 December 2013, Reviewed 13 December 2013, Accepted 31 December 2013]
☆ 본 연구는 미래창조과학부가 지원한 2013년 정보통신·방송(ICT)연구개발사업의 연구결과로 수행되었음

가하고 있다. 소셜 네트워크상에 경쟁 기업을 비하하는 글을 작성하거나, 허위 광고 및 이용자들이 원치 않는 정보에 대한 스팸성 메시지가 증가하고 있다. 특히 최근에는 자극적인 단어가 포함된 메시지와 악성코드감염을 위한 악성URL 확산을 통해 사용자들의 관심을 유발하고, 악성코드를 감염 및 전파시키는 등의 지능적인 공격이 빠르게 늘어나고 있고, 사용자들 간의 관계를 기반으로 소통하는 소셜 네트워크의 특성으로 인해 악성코드의 확산속도는 급증하고 있다. 또한 이러한 소셜 네트워크 환경에서의 데이터 확산분석을 위한 데이터의 양은 매우 방대하고, 전체 네트워크의 구성 및 분석이 어렵기 때문에 소셜 네트워크 환경의 구조적 특징이 잘 반영된 Sample Network를 활용하여 악성 데이터의 확산을 분석하는 연구가 이루어지고 있다[1-3][9].

이에 본 논문에서는 소셜 네트워크 환경에서의 악성 데이터 확산 분석을 위해 기존의 소셜 네트워크의 구조적 특징을 잘 표현할 수 있는 그래프 이론에 기반 한 랜덤그래프 알고리즘을 분석 및 생성하고, 소셜 네트워크에서 발생 가능한 공격으로 Cross Site Scripting(XSS) Worm과 Koobface Worm을 분석한다. 또한 소셜 네트워크의 구조적 특징 중 악성 데이터 확산에 영향을 미치는 파라미터들을 역학 모델인 Susceptible Infectious(SI) 모델을 기반으로 실험하여 악성 데이터 확산에 가장 큰 영향을 미치는 파라미터를 도출한다. 실험에 대한 결과로 사용자의 행위적 특성을 고려하지 않았을 때 XSS Worm의 경우 확산에 가장 큰 영향을 미치는 구조적 파라미터는 근접 중심성(Closeness Centrality)이고, Koobface Worm은 군집도(Clustering Coefficient)였다. 이러한 결과를 기반으로 소셜 네트워크 환경에서 악성 데이터의 확산을 조기에 탐지하거나 늦출 수 있을 것이다.

2장에서는 관련 연구로서 기존 연구의 문제점과 전반적인 이론적 배경을 소개하고, 3장에서는 XSS Worm과 Koobface Worm의 확산 분석을 위하여 소셜 네트워크의 구조적 특징을 반영한 악성 데이터 확산모델을 제안한다. 4장에서는 XSS Worm과 Koobface Worm의 확산 실험을 통하여 확산에 영향을 미치는 파라미터들을 분석하고, 이를 바탕으로 각각의 공격에 대한 악성 데이터 확산에 영향을 미치는 파라미터들을 분석한다. 마지막 5장에서는 이에 대한 결과를 도출하고, 향후 연구방향을 제시한다.

2. 관련 연구

2.1 기존 연구

최근 소셜 네트워크 환경에서의 악성 데이터 확산 연구가 많이 이루어지고 있다. 이러한 연구들의 대부분은 유행성 질병의 확산 분석을 기반으로 하며, 대상 네트워크는 작은 세상 네트워크(Small world Network)[17], 척도 없는 네트워크(Scale free Network)[6,7], 실제 소셜 네트워크에 기반 한 모델이 주를 이루고 있다. 소셜 네트워크의 특정 유형인 E-mail, IM 네트워크와 모바일 네트워크를 대상으로 악성 데이터의 확산 연구[6][9], 소셜 네트워크 환경에서 XSS Worm 및 Trojan Worm에 대한 확산 분석으로 SI 모델 기반 연구가 이루어졌다[1-3][9]. 또한 소셜 네트워크의 특징을 반영한 네트워크를 구성하여 악성 데이터의 확산 분석을 수행하고, 네트워크 특징 중 군집도(Clustering Coefficient)에 따른 Worm의 확산 속도를 분석하는 연구[9]가 있으며, 사용자의 행위적 특성을 고려한 확산 분석의 연구가 이루어졌다[1-3][18]. 실제 소셜 네트워크 환경의 데이터(Orkut, Hi5, Myspace, Linkedln, Flicker)를 기반으로 사용자의 활동에 초점을 맞춘 연구 및 correlation-based 방식으로 Worm의 확산을 완화할 수 있는 방안에 초점을 맞춘 연구가 이루어졌다[18][19].

기존의 연구에서는 사용자의 행위에 대한 분석을 기반으로 사용자의 소셜 네트워크 환경에서의 행위적 파라미터들을 가정하여 악성 데이터의 확산 실험을 수행한 연구가 이루어졌다. 하지만 실제 소셜 네트워크에서 데이터 확산에 영향을 미치는 파라미터들은 다수 존재하는데, 기존의 연구는 이러한 구조적 특징 중 군집도만을 이용하여 악성 데이터의 확산 분석을 수행하였다. 따라서 본 논문에서는 사용자의 행위적 특성 및 실제 소셜 네트워크의 구조적 특징을 고려한 악성 데이터 확산 모델을 도출한다.

2.2 소셜 네트워크의 특징

온라인 소셜 네트워크 환경에서의 악성 데이터 확산의 분석 및 시뮬레이션을 위해 소셜 네트워크의 토폴로지적 특징에 대한 이해가 필요하다. 실제 소셜 네트워크는 일반적으로 0.1~0.7정도의 높은 클러스터링 된 군집도를 보이는 작은 세상 네트워크의 특징을 보이고 있으며[8], 차수 분포(Degree Distribution)가 멱함수 법칙(Power-law Distribution)을 따르는 특징을 보인다[7][8]. 또

한 소셜 네트워크에서 평균 네트워크 거리가 낮은 특징을 보이고 있다. 이는 Stanley Milgram의 작은 세상 현상에 관한 연구에서와 같이 사회는 공간적인 제약 없이 평균 6단계를 거치면 그 사람을 알 수 있다는 여섯 단계 현상(Six Degree Phenomenon)을 보인다[16]. 즉, 많은 간선을 가진 허브(Hub)역할을 수행하는 노드들에 의해 연결되며 평균 네트워크 거리가 낮아진다는 점이다.

2.3 소셜 네트워크 환경에서의 악성 데이터

2.3.1 XSS Worm

Cross Site Scripting Worm은 악의적인 공격자가 Client-side script를 다른 사용자가 열람하는 웹 페이지에 삽입하도록 허용하는 웹 어플리케이션에서 전형적으로 발견되는 컴퓨터 보안 취약점 중 하나이다. Cross Site Scripting은 해커가 동일 근원 보안 정책(Same origin policy)과 같은 접근 제어를 우회하는데 사용될 수 있다. 또한 2007년 Symantec에서 발행한 보고서에 의하면 웹페이지에서 발생하는 보안 취약점의 약 80%를 차지하고 있는 것으로 분석된다. XSS 취약점은 1990년대부터 보고되었고, Twitter, Facebook, MySpace, Orkut 등과 같은 유명한 소셜 네트워크 사이트들도 공격을 받았으며, 보안 담당자들에 의하면 웹 사이트의 68%가 XSS공격의 대상이 될 수 있을 것으로 예상하고 있다.

XSS Worm은 실행 가능한 악성 코드를 웹페이지에 삽입한 뒤 다른 사용자가 악성 코드가 삽입된 웹페이지를 보게 하여 사용자의 컨텍스트에서 악성코드를 실행하는 기법으로 비 지속적 공격(Non-Persistent Attack)과 지속적 공격(Persistent Attack)의 2가지 유형으로 분류할 수 있다[11].

2.3.2 Koobface Worm

Koobface는 소셜 네트워크를 통해 확산되는 웜으로써, Facebook의 철자를 바꾼 이름으로 Facebook을 통해 주로 확산되고 손상된 시스템을 사용하여 P2P 봇넷을 구축하는 웜이다. 손상된 시스템은 다른 손상된 시스템에 연결하여 P2P방식으로 명령을 수신하고, 봇넷은 손상된 시스템에 PPI(Pay-Per-Install) 악성코드를 설치하는 한편 검색 조회를 하이재킹하여 광고를 표시하는데 사용된다. Koobface는 주로 소셜 네트워크 환경에서 동영상 링크를 통해 확산된다. 동영상을 호스팅하는 웹 사이트를 사용자가 방문할 때 동영상 코덱 또는 동영상 재생에 필요한 다른 필요 업데이트를 다운로드 및 실행을 유도하는 것으로 실제는 Worm의 복제본이다. Koobface는 소셜 네트워크 사이트를 대상으로 사회 공학 기술을 사용하여 확산되며, 사용자는 친구나 지인이 게시한 것으로 보이는 링크는 안전한 것으로 판단하는 실수에 빠지기 쉽다는 점을 악용한 공격으로 친구가 게시한 링크인지 웜이 게시한 링크인지 판단하기가 쉽지 않은 공격이다[15].

2.4 네트워크 그래프 모델

2.4.1 Barabasi-Albert Model(BA Model)

척도 없는 네트워크는 현실 네트워크들의 끊임없이 성장하는 속성의 자연스러운 결과로서 대표적인 모델은 BA Model이다[7]. BA Model은 현실 세계의 네트워크에 대하여 두 가지 메커니즘을 전제로 하고 있다. 첫째, 네트워크는 새로운 노드가 지속적으로 추가된다는 네트워크의 확장성과 둘째, 새로운 노드는 어떤 특정한 규칙적인 방법으로 연결되는 것이 아닌 이미 잘 연결되어있는 노드에 우선적인 연결(Preferential Attachment)을 수행한다. 즉, 규칙적인 연결이 아닌 인접한 이웃이 많은, Degree가 높은 노드에 우선적으로 연결된다는 메커니즘을 기반으로 하고 있다. 이러한 선호적 연결에 따라 균등하지 않은 링크 수를 가지는 특성을 나타내고, 이는 실제 세상과 매우 유사하다고 볼 수 있다. 실제 세상 및 소셜 네트워크 환경에서도 평균 이상으로 극단적 연결을 가진 형태를 많이 볼 수 있다. BA Model은 다음과 같이 정의 된다.

- Initial condition : 연결이 되지 않은 N_0개의 네트워크로 시작한다.
- Growth : 각 Time step마다 새로운 노드가 생성된다.
- Preferential attachment(PA) : 새로운 노드에 $m \leq N_0$개의 간선이 추가되는데 기존의 n_i가 새로운 연결을 받을 확률은 식(1)과 같다.

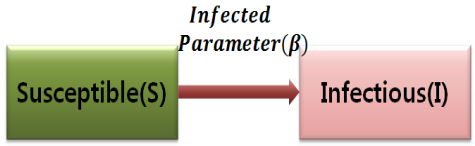
$$P(n_i) = \frac{k_i}{\sum_j k_j} \tag{1}$$

t time step 후에 네트워크는 $N_N(t) = N_0 + t$의 노드수와 $N_E(t) = mt$의 간선 수를 갖게 된다. BA model은 링크를 많이 가진 노드일수록 더 많은 링크를 받을 가능성이 높다는 Rich-get-richer dynamic의 특성을 설명할 수 있다.

2.4.2 Holme & Kim Model(HK Model)

HK Model은 척도 없는 네트워크의 대표 모델인 BA Model을 기반으로 'Triad Formation'단계를 추가하여 실제 소셜 네트워크의 특징인 High Clustering Coefficient를 만족하는 모델을 제안하였다[8]. 이는 BA Model의 PA단계 후에 추가된 노드와 기존의 임의 노드간의 연결 상태를 확인하고, 연결되어 있을시 임의 노드의 이웃노드와 임의적인 연결을 수행하는 Triad Formation(TF)단계를 추가하여 군집도의 값을 높여 소셜 네트워크의 특징을 반영하는 네트워크를 제안하였다.

2.5 Susceptible-Infectious(SI) Model



(그림 1) SI 모델
(Figure 1) Susceptible Infectious(SI) Model

일반적인 SI 모델은 네트워크 내에 모든 호스트들의 상태를 (그림 1)과 같이 취약한 상태(Susceptible)와 감염된 상태(Infectious)로 표현하는 모델로써 전체 호스트의 수 N, 기준시간 t, 취약한 호스트의 수 $S(t)$, 감염된 호스트의 수 $I(t)$, 감염 속도에 영향을 주는 파라미터 β로 구성된다. 취약한 호스트의 수와 감염된 호스트의 증분에 대한 수학적 표현은 식(2), (3)과 같다.

$$\frac{dS(t)}{dt} = -\beta I(t)[N - I(t)] \tag{2}$$

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)] \tag{3}$$

식 (2)은 시간에 따른 취약한 호스트 수의 감소량을 나타내며, 감염 파라미터 $-\beta$에 비례하는 것을 의미한다. 식 (3)는 감염 파라미터 β, 시간 t에서 감염 호스트 수 $I(t)$와 취약한 호스트 수 $S(t)$에 비례하는 것을 의미한다.

3. 제안하는 악성 데이터 확산 모델

3.1 소셜 네트워크의 구조적 파라미터 분석

소셜 네트워크의 구조적 특징 중 데이터의 확산에 영향을 주는 파라미터는 다음과 같다.

① 근접 중심성(Closeness Centrality) : 한 노드가 그를 제외한 다른 노드에서 얼마나 가까이에 위치하는 지를 평가하는 것으로써, 특정 노드와 직접적으로 연결된 노드뿐만 아니라 네트워크내 간접적으로 연결된 모든 노드들 간의 최단거리의 평균을 계산함으로써 노드의 중심성을 측정하는 요소이다. 이에 대한 계산은 식(4)와 같다.

$$C_c(n_i) = \left[\sum_{j=1}^{g} d(n_i, n_j)\right]^{-1} \tag{4}$$

② 밀도(Density) : 네트워크 내에서 연결이 얼마나 많은지를 상대적으로 나타낸 정도로써, 네트워크 내 전체 노드가 서로 얼마나 많은 관계를 맺고 있는지를 표현한 개념이다. 밀도가 높은 노드 혹은 네트워크 일수록 정보의 수집 및 확산 경로가 많아지므로 데이터의 확산 속도가 빨라진다. 네트워크에 L개의 연결이 존재한다면 밀도(ρ)는 식(5)와 같이 최대 가능한 연결 수 대비 L이 되며 0~1사이의 값을 갖는다.

$$\rho = \frac{L}{g(g-1)/2} = \frac{2L}{g(g-1)} \tag{5}$$

③ 군집도(Clustering Coefficient) : 임의의 한 노드에 연결된 두 노드가 서로 간에 얼마나 알고 있는지를 나타내는 지표다. 노드의 군집도가 높다는 것은 해당 노드를 중심으로 많은 연결을 갖고 있다는 의미이다. 임의의 노드 v가 k_v의 이웃 노드와 연결되어 있을 때 노드 v에 대한 군집도는 식(6)과 같고, 전체 노드가 N개인 네트워크의 평균 군집도는 식(7)과 같다.

$$C_v = \frac{k_v(k_v - 1)}{2} \tag{6}$$

$$C_N = \frac{1}{N}\sum_{i=1}^{n} C_i \tag{7}$$

3.2 소셜 네트워크의 특징을 고려한 SI모델

[1]에서는 사용자 행위에 대한 가정을 고려한 모델을 제안하였다. 기존의 SI 모델에서 사용자의 행위에 대한 가정을 기반으로 감염 파라미터 β의 변화에 따른 웜의 확산 속도를 비교하였다. [10]에서는 네트워크의 군집도를 적용한 SI 모델을 제안하고 확산속도를 분석하였다. 이를 기반으로 소셜 네트워크의 구조적 특징을 감염 파라미터 β에 적용하였다.

소셜 네트워크 환경에서 기존에 제안된 SI 모델에 악성 데이터 확산모델에 근접 중심성, 밀도, 군집도를 적용한 SI 모델을 제안하며 식 (8)과 같다. $P(k)$는 네트워크에서 k의 차수(degree)를 가질 확률이며, $E[k]$는 네트워크의 평균 차수와 같다. $f(c)$는 [8]에서 제안하는 네트워크의 군집도를 나타내는 파라미터이며 $g(p)$는 [3]에서 제안하는 사용자의 행위 기반 특성을 나타내는 확률을 의미한다. $C_c(n)$은 네트워크의 근접 중심성을 나타내는 파라미터이며, $D(\rho)$는 네트워크의 밀도를 나타내는 파라미터이다.

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)]\theta(t)g(p)f(c)C_c(n)D(\rho) \quad (8)$$

$$\theta(t) = \frac{\sum_n nP(n)i_n(t)}{\sum_n nP(n)} = \frac{\sum_n nP(n)i_n(t)}{E[k]}$$

$$C_c(n_i) = \left[\sum_{j=1}^{g} d(n_i, n_j)\right]^{-1}$$

$$D(\rho) = \frac{2L}{g(g-1)}$$

네트워크에서 확산에 영향을 미치는 파라미터 $C_c(n)$과 $D(\rho)$, $f(c)$에 대하여 각각의 파라미터에 따른 악성 데이터의 확산 속도 분석을 수행한다.

4. 실험 및 결과

4.1 실험 환경 실험 시나리오

Python 2.6을 활용하여 BA모델과 HK모델의 네트워크 그래프를 구성하고, 악성 데이터 확산 모델의 구현 및 시뮬레이션을 수행하였다. BA모델과 HK모델의 네트워크적 모델의 특징은 (표 1)과 같다. 악성데이터의 확산 실험으로 공격의 두 가지 유형인 XSS Worm과 Koobface Worm에 대한 시나리오를 생성하고, 웜에 확산속도에 각각의 파라미터가 미치는 영향에 대하여 실험을 수행한다. 실험은 BA모델과 HK모델을 기반으로 도출된 네트워크의 특징을 기반으로 각각의 웜에 대한 확산 속도를 비교분석한다. 실험은 단위시간동안 악성 데이터의 확산이 이루어진다고 가정을 하고 수행하며 10회 반복 수행한다. 각 공격에 대한 실험 시나리오는 (표 2, 3)과 같다. 각 공격에 대하여 공격 Worm에 대한 특징을 반영하는 사용자의 행위 기반 특성에 기반 한 실험과 네트워크의 구조적 특징을 고려한 파라미터에 대한 확산 속도 실험을 수행한다.

(표 1) 네트워크 특징(BA Model, HK Model)
(Table 1) Network Characteristic(BA Model, HK Model)

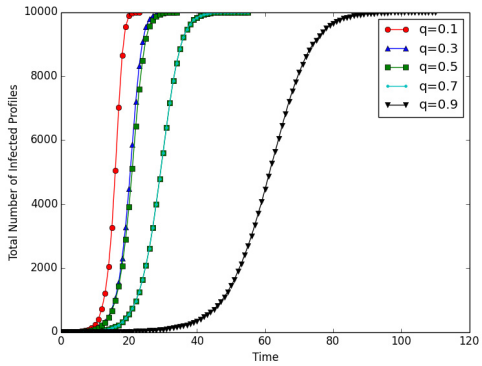
특징 \ 모델	BA Model	HK Model
Number of Vertices	10,000	10,000
Number of Edges	19997	19996
Average Shortest Path Length	5.0183	5.103
Average Node Degree	3.9994	3.9992
Average Clustering Coefficient	0.004	0.225
Density	3.997E-4	3.995E-4
Closeness Centrality	0.2015	0.1983

(표 2) XSS Worm 실험 시나리오
(Table 2) XSS Worm test scenario

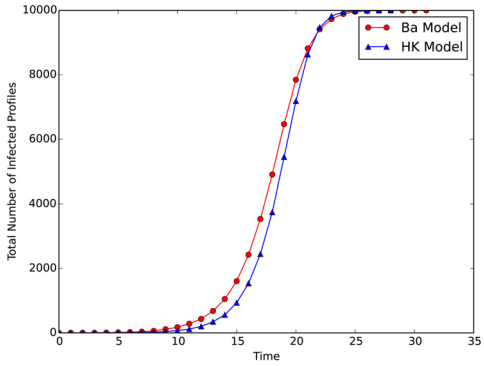
XSS Worm 시나리오
1. 사용자의 행위 기반 특성
- 친구 노드 방문 확률에 따른 확산속도 비교
2. 네트워크 구조적 특징
- 군집도에 따른 확산속도 비교
- 밀도에 따른 확산 속도 비교
- 근접 중심성에 따른 확산 속도 비교

(표 3) Koobface Worm 실험 시나리오
(Table 3) Koobface Worm test scenario

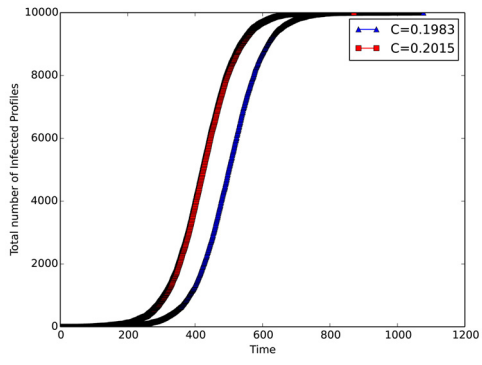
Koobface Worm 시나리오
1. 사용자의 행위 기반 특성
- 사용자가 악성 URL을 실행할 확률에 따른 확산 속도 비교
2. 네트워크 구조적 특징
- 군집도에 따른 확산속도 비교
- 밀도에 따른 확산 속도 비교
- 근접 중심성에 따른 확산 속도 비교



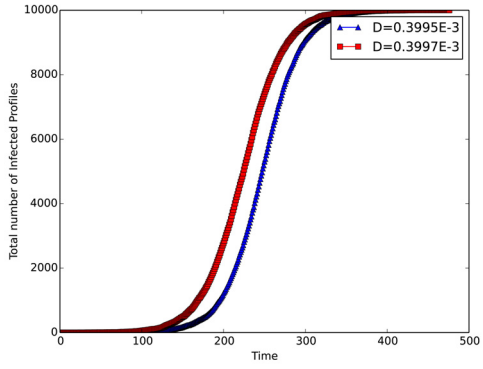
(그림 2(a)) 방문확률 q에 따른 XSS Worm
(Figure 2(a)) XSS Worm depending on visiting rate q



(그림 2(b)) 군집도에 따른 XSS Worm
(Figure 2(b)) XSS Worm depending on Clustering Coefficient



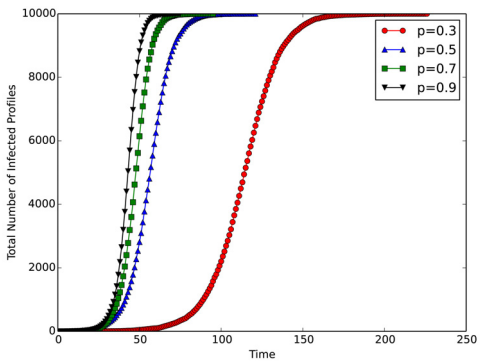
(그림 2(c)) 근접 중심성에 따른 XSS Worm
(Figure 2(c)) XSS Worm depending on Closeness Centrality



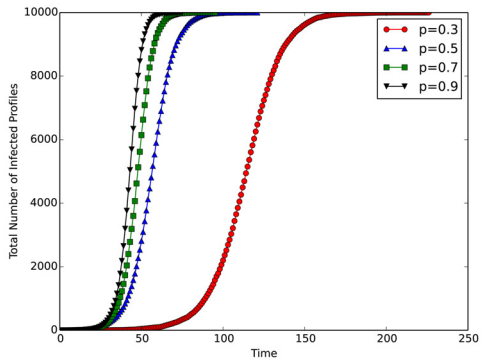
(그림 2(d)) 밀도에 따른 XSS Worm
(Figure 2(d)) XSS Worm depending on Density

4.2 실험 결과 및 분석

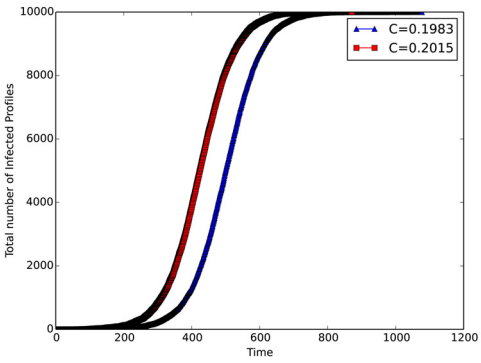
XSS Worm에 대한 실험은 사용자 방문확률 q값에 따른 XSS Worm의 확산속도 비교, 군집도에 따른 확산속도 비교, 밀도에 따른 확산속도 비교, 근접 중심성에 따른 확산속도 비교를 수행하였다. 각각의 파라미터별 실험 시 해당 파라미터를 제외한 다른 파라미터들의 값은 동일하게 설정함으로써 각각의 파라미터가 확산속도에 미치는 영향을 비교할 수 있다. (그림 2(a))는 사용자의 행위기반 특성으로 사용자 방문확률 값을 변화시키면서 확산 속도를 비교하였다. 친구 방문확률이 0.9일 때 XSS Worm의 확산속도가 느리게 측정되었으며 낮선 사용자의 노드에 방문할 확률이 높을수록 XSS Worm의 확산 속도는 급격히 증가하는 것을 볼 수 있다. (그림 2(b))에서는 군집도에 따른 XSS Worm의 확산속도를 비교한 그래프로써 낮은 수치의 군집도를 갖는 BA모델과 비교적 높은 수치를 갖는 HK모델의 군집도 수치를 적용하여 결과를 도출하였다. XSS Worm의 경우 군집도에 따른 확산속도 증가율은 크게 차이가 나지 않았는데, 이는 XSS Worm의 확산 방식이 수동적이기 때문이다. 다른 사용자가 감염된 프로파일에 방문했을 경우에 감염되기 때문에 군집도는 XSS Worm에 큰 영향을 미치지는 않았다. (그림 2(c))는 근접 중심성에 의한 악성 데이터의 확산 속도이다. 자신을 제외한 다른 노드들과의 위치가 얼마나 가까이 위치한지에 대한 수치로써 근접 중심성의 수치가 높을수록 XSS Worm의 확산 속도는 높게 측정되었다. 이는 근접 중심성이 높은 노드는 많은 연결을 갖게 되고 이를 방문하는 사



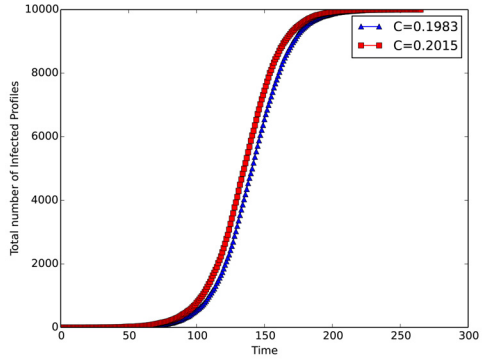
(그림 3(a)) 군집도에 따른 Koobface Worm(HK model)
(Figure 3(a)) Koobface Worm depending on Clustering Coefficient(HK Model)



(그림 2(b)) 군집도에 따른 XSS Worm
(Figure 2(b)) XSS Worm depending on Clustering Coefficient



(그림 3(c)) 근접 중심성에 따른 Koobface Worm
(Figure 3(c)) Koobface Worm depending on Closeness Centrality

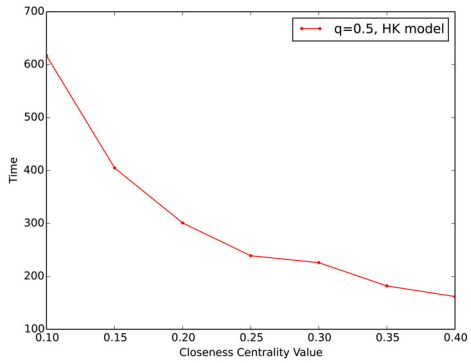


(그림 3(d)) 밀도에 따른 Koobface Worm
(Figure 3(d)) Koobface Worm depending on Density

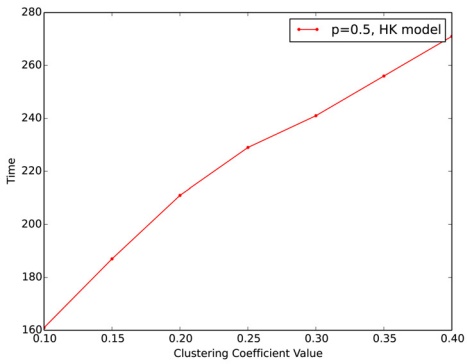
용자가 많을 확률이 높기 때문이다. (그림 2(d))는 밀도에 의한 XSS Worm의 확산 속도로써 두 모델의 수치가 매우 낮게 측정되었지만, 밀도가 낮을수록 XSS Worm의 확산 속도가 느리다는 것을 알 수 있다. 밀도가 낮을수록 네트워크 내의 연결이 적다는 의미이기 때문에 확산 속도는 낮아질 수밖에 없다.

Koobface Worm의 실험은 XSS Worm과 달리 사용자들 간의 방문에 의한 감염이 아닌 공격자는 악성 URL이 포함된 메시지를 전송하고 이에 대한 URL을 실행했을 경우 감염되는 특징을 갖고 있기 때문에 사용자의 행위 기반 특성은 악성 URL 메시지를 실행할 확률 p로 정의한다[3]. 그러나 Koobface Worm의 경우 악성 URL을 실행할 확률이 높을수록 확산속도가 빨라지는 것은 당연한 결과이므로, 이에 대한 실험은 생략하며 XSS Worm과 같이 군집도, 근접 중심성, 밀도에 대하여 확산 속도를 비교 분석하며, 해당 파라미터를 제외한 다른 파라미터들의 값은 동일하게 설정하여 실험을 수행한다.

(그림 3(a))는 군집도가 높은 HK모델에서 사용자가 Worm에 대하여 실행할 확률을 변화시키면서 해당 p값에 따른 확산 속도를 나타낸 그래프이고, (그림 3(b))는 군집도가 낮은 BA모델에서 Worm을 실행할 확률에 따른 확산 속도를 나타낸 그래프이다. 두 그래프를 비교해보면 군집도가 낮은 BA모델에서의 확산속도가 매우 빠른 것을 확인할 수 있다. 이는 기존의 연구[10]에서와 같이 군집도가 높은 것은 사용자들 간에 알고 있을 확률이 높은 경우로써 공격자의 악성 메시지에 의한 초기 감염이 늦으며, 확



(그림 4) 근접 중심성에 따른 확산 속도
(Figure 4) Propagation speed depending on Closeness Centrality



(그림 5) 군집도 차이에 따른 확산 속도
(Figure 5) Propagation speed depending on Closeness Centrality

산 속도가 낮다는 것을 의미한다. XSS Worm은 군집도에 의한 영향을 적게 받는 것을 볼 수 있었는데 이는 각 Worm의 감염 특징에 의한 차이로 볼 수 있다. (그림 3(c))는 HK모델과 BA모델의 근접 중심성에 의한 확산 속도를 나타낸 그래프이며 p의 값은 0.5로 고정하여 실험을 수행하였다. 근접 중심성에 의한 확산속도의 결과가 거의 비슷하게 측정되는 것을 볼 수 있는데 이는 Koobface Worm의 특징에 의한 결과로 볼 수 있다. Koobface Worm에 감염된 노드는 현재 자신과 연결된 이웃 노드들에게 악성 URL이 포함된 메시지를 자동적으로 전송하는 능동적인 확산 형태를 지니면서 매우 빠른 확산 속도를 보이는 공격이므로 수동적인 확산과정을 보이는 XSS Worm에 비하여 근접 중심성에 의한 영향이 적은 것으로 해석할 수 있다. (그림 3(d))는 밀도에 따른 Koobface Worm의 확산 속도를 나타낸다. XSS Worm과 유사한 결과를 확인할 수 있으며 악성 Worm의 특징에 의해 영향을 받는 파라미터이기 보다는 네트워크의 공통적인 특징으로 정보의 확산에 영향을 주는 파라미터인 것으로 볼 수 있다.

따라서 XSS Worm의 확산에 영향을 미치는 파라미터는 근접 중심성, Koobface Worm의 확산에 영향을 미치는 파라미터는 군집도임을 확인할 수 있었다. 이러한 결과에 대해 HK모델을 기반으로 (그림 4)와 (그림 5)에서 각 파라미터의 수치를 변화시키면서 전체 노드를 감염시키기 위해 필요한 단위 시간을 측정하고 이를 그래프로 나타내었다. (그림 4)는 XSS Worm에서 친구노드를 방문할 확률을 $q=0.5$, 군집도는 HK모델의 값으로 고정시키고 근접 중심성의 값을 변화시킨 그래프이다. (그림 4)에서와 같이 근접 중심성이 낮은 네트워크 일수록 전체 노드를 감염시키는데 걸리는 시간이 적었고, 근접 중심성의 값이 0.25 이상일 경우부터는 확산 속도의 차이가 줄어드는 것을 확인할 수 있었다. (그림 5)는 HK모델의 특징을 기반으로 하고, Koobface Worm에서 악성 URL을 실행할 확률 $p=0.5$로 가정하여 군집도의 값을 변화시킨 그래프이다. 군집도의 수치가 높은 네트워크 일수록 전체 노드를 감염시키는데 걸리는 시간은 증가하였다. 실험 결과와 같이 수동적인 확산 특징을 갖는 XSS Worm의 경우 악성 데이터의 확산은 근접 중심성에 영향을 받고, 능동적인 확산 특징을 갖는 Koobface Worm은 군집도에 영향을 받는 것을 확인할 수 있었다. 이런 결과를 기반으로 네트워크에서 각 공격에 대해 노드의 근접 중심성이 가장 높은 노드 또는 군집도가 낮은 노드에 대해 주기적으로 모니터링을 수행한다면 악성 데이터의 확산을 조기에 파악할 수 있고 대응이 가능할 것이다.

5. 결론 및 향후 연구

최근 트위터, 페이스북을 중심으로 소셜 네트워크 환경의 규모와 영향력은 점차 증대되고 있다. 이에 대한 역기능으로 공격자들은 소셜 네트워크의 특징으로 빠른 확산 능력을 보이고 있는 점을 악용하여 소셜 네트워크에서 보안 의식이 취약한 사용자들을 타깃으로 악성 데이터를 확산시키고 있다. 이에 본 논문에서는 이러한 소셜 네트워크의 특징을 기반으로 악성 데이터의 확산에 영향을 미치는 파라미터들을 분석하기 위한 확산분석 모델을 제안하였다. 기존의 연구[1-3]는 사용자의 행위 기반 특성으로 친구 방문 확률, 악성 데이터를 실행할

확률을 가정하여 각 공격에 대한 확산 속도를 분석하거나, 네트워크의 구조적 특징 중 군집도만을 선택하여 확산 분석을 수행하였다. 그러나 본 논문에서는 기존의 연구에서와 같이 사용자의 행위 기반 특성을 기반으로 하며, 네트워크의 구조적 파라미터인 근접 중심성, 밀도, 군집도와 같은 정보 확산에 영향을 미치는 파라미터들을 고려하여 소셜 네트워크 환경에서 발생할 수 있는 공격 유형들에 대한 확산 속도를 분석하였다. 또한 소셜 네트워크의 구조적 특징 파라미터를 선택하여 제안하는 SI 모델에 적용시킴으로써 각각의 파라미터가 확산에 미치는 영향력을 분석할 수 있었다. 위 실험을 통한 분석 결과는 소셜 네트워크의 구조적 특징 또는 사용자 개개인의 노드별 특징을 산출하여 악성 데이터의 확산에 가장 큰 영향을 미칠 수 있는 노드를 선택하여 주기적으로 모니터링 함으로써 악성 데이터의 확산을 늦출 수 있을 것이다.

따라서 향후에는 소셜 네트워크 환경에서 영향력이 높은 노드를 산출하고, 해당 노드가 악성 데이터에 감염되었는지에 대한 여부를 탐지 및 분석하는 연구를 하고자 한다.

참 고 문 헌(Reference)

[1] Faghani, Mohammad Reza, and Hossein Saidi. "Malware propagation in online social networks." Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on. IEEE, 2009.

[2] Faghani, Mohammad Reza, and Hossein Saidi. "Social networks' XSS worms." Computational Science and Engineering, CSE'09. International Conference on. Vol. 4. IEEE, 2009.

[3] Faghani, Mohammad Reza, Ashraf Matrawy, and Chung-Horng Lung. "A Study of Trojan Propagation in Online Social Networks." New Technologies, Mobility and Security(NTMS), 2012 5th International Conference on. IEEE, 2012.

[4] Zou, Cliff Changchun, Weibo Gong, and Don Towsley. "Code red worm propagation modeling and analysis." Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002.

[5] Su, Fei, Zhao-Wen Lin, and Yan Ma. "Modeling and analysis of Internet worm propagation." The Journal of China Universities of Posts and Telecommunications 17.4. 63-68, 2010.

[6] Mannan, Mohammad, and Paul C. van Oorschot. "On instant messaging worms, analysis and countermeasures." Proceedings of the 2005 ACM workshop on Rapid malcode. ACM, 2005.

[7] Barabási, Albert-László, and Réka Albert. "Emergence of scaling in random networks." science 286.5439 , 509-512, 1999.

[8] Holme, Petter, and Beom Jun Kim. "Growing scale-free networks with tunable clustering." Physical Review E 65.2, 026107, 2002.

[9] Zou, Cliff Changchun, Don Towsley, and Weibo Gong. "Modeling and simulation study of the propagation and defense of internet e-mail worms." Dependable and Secure Computing, IEEE Transactions on 4.2, 105-118. 2007.

[10] Wu, Xiaoyan, and Zonghua Liu. "How community structure influences epidemic spread in social networks." Physica A: Statistical Mechanics and its Applications 387.2, 623-630, 2008.

[11] Grossman, Jeremiah (July 30, 2006). "The origins of Cross-Site Scripting (XSS)". Retrieved September 15, 2008.

[12] Moreno, Yamir, Romualdo Pastor-Satorras, and Alessandro Vespignani. "Epidemic outbreaks in complex heterogeneous networks." The European Physical Journal B-Condensed Matter and Complex Systems 26.4, 521-529, 2002.

[13] Yan, Guanhua, et al. "Malware propagation in online social networks: nature, dynamics, and defense implications." Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, 2011.

[14] Kyung-moon Woo, Chong-kwon Kim. "Internet Worm Propagation Modeling using a Statistical Method". The Korean Institute of Communication and Information Sciences. vol.37B, 2012.

[15] Thomas, Kurt, and David M. Nicol. "The Koobface botnet and the rise of social malware." Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on. IEEE, 2010.

[16] Milgram, Stanley. "The small world problem."

Psychology today 2.1, 60-67, 1967.
[17] Watts, Duncan J., and Steven H. Strogatz. "Collective dynamics of 'small-world'networks." nature 393.6684 440-442, 1998.
[18] Benevenuto, Fabrício, et al. "Characterizing user behavior in online social networks." Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference. ACM, 2009.
[19] Xu, Wei, Fangfang Zhang, and Sencun Zhu. "Toward worm detection in online social networks." Proceedings of the 26th Annual Computer Security Applications Conference. ACM, 2010.

◐ 저 자 소 개 ◑

공 종 환(Jong-Hwan Kong)
2012년 2월 경원대학교 컴퓨터소프트웨어학과 졸업(공학사)
2012년~현재 가천대학교 일반대학원 전자계산학과(석사과정)
관심분야 : Network Security, Information Security
E-mail : ball3314@naver.com

김 익 균(Ik Kyun Kim)
1994년 경북대학교 컴퓨터공학과 공학사 .
1996년 경북대학교 컴퓨터공학과 석사
2009년 경북대학교 컴퓨터공학과 공학박사
1996년~현재 한국 전자통신연구원 책임연구원, 네트워크보안연구실 실장
2004년~2005년 미국 Purdue University 객원연구원
관심분야 : 네트워크보안, 컴퓨터네트워크, 클라우드컴퓨팅, 스마트그리드 보안, 빅데이터 보안분석
E-mail : ikkim21@etri.re.kr

한 명 묵(Myung-Mook Han)
1980년 연세대학교 공과대학 졸업 (공학사)
1987년 뉴욕공과대학교 컴퓨터공학과 석사 졸업 (공학석사)
1997년 오사카시립대학교 정보공학부 졸업(공학박사)
1998년~현재 가천대학교 IT대학 교수
1998년~현재 한국인터넷정보학회 부회장
관심분야 : Security, Algorithm, Data Mining
E-mail : mmhan@gachon.ac.kr