Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 207457, 14 pages
http://dx.doi.org/10.1155/2014/207457

Research Article

Modeling the Propagation of Mobile Phone Virus under Complex Network

Wei Yang,[1] Xi-liang Wei,[2] Hao Guo,[3] Gang An,[4] Lei Guo,[2] and Yu Yao[2,5]

[1] *Software College, Northeastern University, Shenyang 110819, China*
[2] *College of Information Science and Engineering, Northeastern University, Shenyang 110819, China*
[3] *Quality and Technology Department, Liaoning Provincial Institute of Measurement, Shenyang 110004, China*
[4] *Information Center, Panjin Finance Bureau, Panjin 124000, China*
[5] *Key Laboratory of Medical Image Computing, Northeastern University, Ministry of Education, Shenyang 110819, China*

Correspondence should be addressed to Wei Yang; yangwei@mail.neu.edu.cn

Received 14 March 2014; Accepted 26 June 2014; Published 15 July 2014

Academic Editor: Fei Yu

Mobile phone virus is a rogue program written to propagate from one phone to another, which can take control of a mobile device by exploiting its vulnerabilities. In this paper the propagation model of mobile phone virus is tackled to understand how particular factors can affect its propagation and design effective containment strategies to suppress mobile phone virus. Two different propagation models of mobile phone viruses under the complex network are proposed in this paper. One is intended to describe the propagation of user-tricking virus, and the other is to describe the propagation of the vulnerability-exploiting virus. Based on the traditional epidemic models, the characteristics of mobile phone viruses and the network topology structure are incorporated into our models. A detailed analysis is conducted to analyze the propagation models. Through analysis, the stable infection-free equilibrium point and the stability condition are derived. Finally, considering the network topology, the numerical and simulation experiments are carried out. Results indicate that both models are correct and suitable for describing the spread of two different mobile phone viruses, respectively.

1. Introduction

More and more rogue programs called mobile phone virus, which can take control of a mobile device by exploiting its vulnerabilities, can be written to propagate from one phone to another. Security issues of mobile phones have become increasingly prominent. Though attacks from the mobile phone virus have not caused greater damage up to now, it is just a matter of time before it breaks out [1]. The large population of mobile users and the wide coverage of mobile communication network [2] create a breeding ground for the propagation of mobile phone virus. The propagation of mobile phone virus may be more potentially destructive than the computer virus. In this regard, mobile phone virus encounters a similar situation of Internet worms, so it is necessary to research the propagation behavior of mobile phone virus in the real world and design effective containment strategies to suppress them.

The usual ways for mobile phone virus to propagate include multimedia messaging service (MMS) [3] interface and e-mail services on that mobile phone. MMS messages are intended to contain media content such as photos, audios, and videos, but they can also contain infected malicious codes [4]. One noteworthy example is Commwarrior [5], which is the first mobile phone virus that can propagate via MMS. It searches for phone number through a user's local address book and sends MMS messages containing infected files to other users in the address book. It is an easy way for mobile phone virus to carry out because people are more likely to open and download the contents that they received from their friends. So the mobile phone virus could be sent out in just one click and travel to any mobiles all over the world with a larger chance of success in propagation [4].

The mobile phone virus is in the time of high-speed development. In the present, it only reproduces and propagates by tricking mobile phone users, called user-tricking virus, but does not spread automatically. According to the development rules of the computer virus, the future trend of the mobile phone virus is that it can propagate by exploiting vulnerabilities existing in mobile phone operating systems or application software. That is, the propagation of such mobile phone virus called vulnerability-exploiting virus can be realized by itself without human participants.

The possible path through which mobile phone virus spreads depends on the social relationship of a user by exploiting the local address book or recent call records. Communications based on social network provide the environment for the spread of the mobile phone virus. And the social network will greatly influence the spread of the mobile phone virus. Recently some researchers have studied the structures of social network topologies [6–8]. They found that all of these networks are complex network and they have power-law degree distributions. Existing work on studying mobile phone virus [9, 10] does not take into account the capability of mobile phone virus to spread under complex network. Consequently this paper focuses on researching the behavior of the user-tricking virus in the present and the vulnerability-exploiting virus in the future combining the topology of the complex network.

Many particular factors can affect the propagation of mobile phone virus and its behavior is very complicated depending on the social relationship of mobile phone users. So an extremely fundamental and effective way to study the mobile phone virus is using the epidemiological models. Epidemiological models are the usual method used to understand and predict the propagation of Internet worms by many researchers [11–20].

The mobile phone virus has some commons with the Internet worms. As the behavior of mobile phone virus is more complex than that of Internet worms, it is necessary to construct a new model for virus propagation. Due to the characteristic of exponential propagation exhibited by mobile phone virus through complex network, it is challenging to model the user-tricking and vulnerability-exploiting mobile phone virus.

Through above observations, this paper models the propagation of mobile phone virus considering the characteristics of mobile phone viruses and the network topology structure. The contributions of this paper are as follows.

(i) Two different propagation models of mobile phone viruses under the complex network are proposed in this paper. One is intended to describe the propagation of user-tricking virus, and the other is to describe the propagation of the vulnerability-exploiting virus.

(ii) A detailed analysis is conducted to analyze the propagation models. Through analysis, the stable infection-free equilibrium point and the stability condition are derived.

(iii) Considering the network topology, the numerical and simulation experiments are carried out. Results indicate that both models are correct and suitable for describing the spread of two different mobile phone viruses, respectively.

The rest of this paper is organized as follows. Section 2 presents related work about modeling the mobile phone virus. Section 3 conducts and analyzes the mobile phone virus SIS propagation model (M-SIS) and obtains the stability condition and the infection-free equilibrium point. Section 4 proposes the propagation model of vulnerability-exploiting mobile phone virus, which is called the mobile phone virus SIR propagation model (M-SIR). Section 5 describes the constructing process of complex network which is used to simulate the spread of the mobile phone virus. Section 6 concludes the paper and provides future research directions.

2. Related Work

Mobile phone users communicate and share files with their friends and they also take part in some activities or join groups online [21]. These characteristics give hackers the opportunities to attack mobile users. As a result, the mobile phone virus can spread quickly. More and more researchers pay attention to the area of mobile phone virus. But the research on the mobile phone virus is just in the beginning stage. Fundamental research works on it have been gradually carried out in order to raise the security awareness among users.

Leavitt lists some mobile phone viruses, such as Cabir, Skulls, and Mosquito and points out increasing virus attacks to mobile phones [1]. But he deems that a method always can be found to cope with the security issue caused by the mobile phone virus. Dwan takes the mobile phone virus “Cabir” as an example to emphasize the lack of security mechanism and expects to take certain security measures from both mobile phones’ software and hardware [22]. Jamaluddin et al. state the damage of the mobile phone virus and predict that the mobile phone virus will develop along the path of the computer virus and cause serious security problems [23]. Dagon et al. describe the security threat with which mobile users are faced and propose several security advices to mobile users [24].

With the popularity of Android platform based mobile phones, more and more attention is paid to the protection of mobile phones. Zhang et al. propose a browser-free multilevel smart phone privacy protection system by means of short message system [25]. Based on the specific network of short message, Jin et al. proposed an epidemic model of mobile phone virus based on the efficiency of immunization to reveal the spreading rule of mobile phone virus [26].

Based on the similarity between a malicious worm and a biological virus, some epidemic models representing worm propagation were presented to depict the propagation of worms, for example, SIS model (susceptible-infectious-susceptible) and SIR model (susceptible-infectious-recovered) [27]. Yao et al. research the worm propagation model by considering the time delay [28]. They found that time delay may lead to Hopf bifurcation phenomenon which will make the worm propagation system unstable and uncontrollable.

Propagation models and the stability of mobile phone virus become an attractive research field in recent years since it facilitates worm prediction, detection, analysis and prevention, and so forth. There have been some models to simulate the mobile phone virus propagation.

Wang et al. modeled the mobility of mobile phone users in order to study the fundamental spreading patterns that characterize a mobile virus outbreak [29]. Their results explain the lack of a major mobile virus breakout so far and predict that once a mobile operating system's market share reaches the phase transition point, viruses will pose a serious threat to mobile communications. Zheng et al. analyze the communication of Bluetooth between mobile users and put forward a propagation model of the mobile phone virus which spreads through Bluetooth technique [30]. Xuetao et al. propose and evaluate a SI_1I_2S, a competition model that describes the spread of two mutually exclusive mobile viruses across heterogeneous composite networks [31].

Existing propagation models of mobile phone virus focus on the specific kind of virus. This kind of virus spreads using Bluetooth or short message, which is completely different from the virus spreading using MMS.

Mobile phone virus that spreads using MMS typically exploits the social network of users to propagate from one mobile device to another. So the topology of network is a key factor for this kind of mobile virus using MMS to propagation. As far as I know no one has studied the propagation model of this kind virus. So considering the characteristics of mobile phone virus and the social network relationship, two different propagation models of mobile phone viruses under the complex network are proposed in this paper to understand how particular factors can affect their propagation and design effective containment strategies to suppress mobile phone virus.

3. Modeling the Propagation of the User-Tricking Mobile Phone Virus

3.1. M-SIS Model. The user-tricking virus only reproduces and propagates by tricking when mobile phone users are in just one click. In this regard, the following assumption is made that the propagation path of a mobile virus can be approximated by the social network of mobile devices. Given that a user A has a higher probability to open and download a message from B with whom he periodically exchanges messages, the pair of users, A-B, would be considered more vulnerable. In contrast, if user A does not exchange messages with user C, the user A is unlikely to be infected by a mobile phone virus sent by C and hence the pair of A-C is considered less likely to be included in the propagation path of the mobile virus. This kind of virus is now prevailing on current mobile phone system and is difficult to kill completely. It will mislead users to install and then execute a norm application. Even if it removed, it can do the same thing with another guise again.

An undirected graph $G = (V, E)$ consisting of a set of vertices V and a set of edges E is used to denote mobile phone communication system. Each vertex $u \in V$ denotes a mobile in the cellular network and each edge $e(u, v)$ denotes that at least one traffic flow was exchanged between mobiles u and v. Let d_i denote the degree of any vertex $i \in V$. According to the spread property of user-tricking mobile phone virus, the epidemic states of a mobile are divided as follows: susceptible state (S) and infectious state (I).

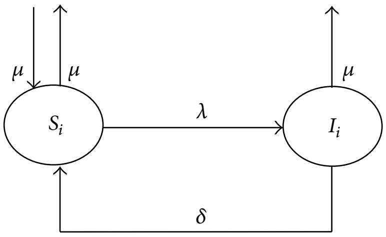


Figure 1: State transition graph of the ith kind of mobiles in M-SIS model.

Susceptible state (S): nodes have not been infected by any user-tricking virus but are prone to infection.

Infectious state (I): nodes have been infected by user-tricking virus and they may infect some mobiles in state S.

Mobile users who have larger groups of friends in social network tend to appear in the contact list of many others [32]. Different nodes with different vertex's degree have different behavior to the spread of mobile phone virus. So it is necessary to study the propagation process of mobile nodes with different node's degree.

According to the nodes' degrees, these vertices in the undirected graph are classified into n kinds of nodes. The nodes with the same degree belong to a class. Let N_i denote the number of the ith kinds of nodes while the value of i ranges from 1 to n. It is assumed that there are totally N mobiles deployed in the communication network. So the sum of n kinds of mobiles is expressed as follows:

$$N = N_1 + N_2 + \cdots + N_i + N_n. \tag{1}$$

Let $S_i(t)$ represent the number of the ith kinds of mobiles in the susceptible state at t time. $I_i(t)$ is defined as the number of the ith kinds of mobiles in the infected state at t time. So the number of the ith kinds of mobiles can be obtained as follows:

$$S_i(t) + I_i(t) = N_i. \tag{2}$$

In the social network, a mobile can leave or join the network randomly. So the "death" of a mobile is defined to refer to the fact that a phone drops out of the network for certain reason, such as breakdown. The "birth" means that the network adds a new mobile. But it is assumed that the system is a closed system and the number of "dead" rates of mobile is the same as that of the "birth" one.

The propagation modeling of user-tricking mobile phone virus under complex network called M-SIS model is proposed, which means mobile phone virus SIS (susceptible-infectious-susceptible) propagation model. In the M-SIS model, M represents mobile phone, and S stands for the susceptible state while I stands for the infectious state. The state transforming process of any kind of mobiles in M-SIS model is illustrated in Figure 1.

A node may change its states as follows.

Node i of any kind can transit to the infectious state if it is at the susceptible state. The infection probability, also called contact infection rate, is presented by λ.

Table 1: Parameters description in the M-SIS model.

Parameter	Meaning
N	The total number of mobiles
$S_i(t)$	The number of the ith kinds of mobiles in the susceptible state at time t
$I_i(t)$	The number of the ith kinds of mobiles in the infectious state at time t
N_i	The number of the ith kinds of mobiles at time t
λ	The contact infection rate
δ	The infection recovery rate
μ	The "birth/death" rate

A mobile is not permanently immune against the virus and has a risk of reinfection. So a mobile at the infectious state can kill the virus and recover to the susceptible state. The infection recovery rate is presented by δ.

To maintain the balance of the network system, the "death" rate and the "birth" rate are all μ. The "new born" mobiles are all in the susceptible state.

The description of related parameters in M-SIS model is showed in Table 1.

Based on the above analysis and compartment model of ith kind presented in Figure 1, given a topology of a mobile communication network, the number of susceptible and infected nodes of the ith kind at time t in the M-SIS model can be formulated by the equations as follows:

$$\begin{aligned} \frac{dS_i(t)}{dt} &= \mu N_i - \mu S_i(t) - \lambda k_i S_i(t)\Theta(t) + \delta I_i(t), \\ \frac{dI_i(t)}{dt} &= \lambda k_i S_i(t)\Theta(t) - \mu I_i(t) - \delta I_i(t). \end{aligned} \tag{3}$$

In (3), k_i is the degree of the ith kind of mobile phone nodes, where $i = 1, 2, \ldots, n$. $\Theta(t)$ is the infected probability that any of neighbor nodes of one mobile phone node and the expression of $\Theta(t)$ are as

$$\Theta(t) = \frac{\sum_{i=1}^{n} k_i P(k_i) I_i(t)}{\langle k\rangle}. \tag{4}$$

In (4), $\langle k\rangle$ means the average degree of nodes in the network, which can be expressed as

$$\langle k\rangle = \sum k_i P(k_i), \tag{5}$$

where $P(k_i)$ is the probability density of nodes with the degree k_i. So the differential equations of the M-SIS model can be concluded as the following equation:

$$\begin{aligned} \frac{dS(t)}{dt} &= \sum_{i=1}^{n} \frac{dS_i(t)}{dt}, \\ \frac{dI(t)}{dt} &= \sum_{i=1}^{n} \frac{dI_i(t)}{dt}. \end{aligned} \tag{6}$$

3.2. Infection-Free Equilibrium Point. The infection-free equilibrium refers to the fact that the mobile virus gets removed and the number of infected mobiles remains 0. To derive the infection-free equilibrium point, let both $dS_i(i)/dt$ and $dI_i(i)/dt$ be equal to 0, and the following expression is obtained as

$$\begin{aligned} \mu N_i - \mu S_i(t) - \lambda k_i S_i(t)\Theta(t) + \delta I_i(t) &= 0, \\ \lambda k_i S_i(t)\Theta(t) - \mu I_i(t) - \delta I_i(t) &= 0. \end{aligned} \tag{7}$$

When $I_i = 0$, $S_i(t)$ and $I_i(t)$ can be calculated as follows, where $i = 1, 2, \ldots, n$:

$$\begin{aligned} S_i(t) &= N_i, \\ I_i(t) &= 0. \end{aligned} \tag{8}$$

The number of the ith kinds of mobile phones in the susceptible state is N_i, while that of the ith kinds of mobile phones in the infectious state is 0. The infection-free equilibrium point of the mobile phone virus propagation system under the M-SIS model is thus $E_0^*(N_1, 0, N_2, 0, \ldots, N_n, 0)$.

3.3. Stability of the Infection-Free Equilibrium. Though the user-tricking virus is difficult to completely kill and mobiles are not permanently immune, it is ensured that the number of infected mobiles can dynamically remain 0. It means that the infection-free equilibrium can be achieved. Its stability for the propagation system of the mobile phone virus will be discussed.

Theorem 1. *If the basic reproduction number $R_0 < 1$, the propagation system under the M-SIS model of mobile phone virus will stabilize at the infection-free equilibrium point:*

$$R_0 = \frac{\lambda}{(\mu + \delta) N \langle k\rangle} \sum_{i=1}^{n} k_i^2 N_i^2. \tag{9}$$

Proof. Let $i = 1$ and put it into (3); the following equation can be obtained:

$$\begin{aligned} \frac{dS_1(t)}{dt} &= \mu N_1 - \mu S_1(t) - \lambda k_1 S_1(t)\Theta(t) + \delta I_1(t), \\ \frac{dI_1(t)}{dt} &= \lambda k_1 S_1(t)\Theta(t) - \mu I_1(t) - \delta I_1(t). \end{aligned} \tag{10}$$

Two equations from (10) are given the partial derivative with the aspects of $S_1, I_1, S_2, I_2, \ldots, S_n, I_n$ and then set $I_i = 0$. $A2 \times 2n$ dimensional matrix is obtained, where $g(j) = k_j P(k_j)/\langle k\rangle$, $j = 1, 2, \ldots, n$:

$$\begin{pmatrix} -\mu & -\lambda k_1 S_1 g(1) & \cdots & 0 & -\lambda k_1 S_1 g(j) & \cdots & 0 & -\lambda k_1 S_1 g(n) \\ 0 & -(\mu+\delta)+\lambda k_1 S_1 g(1) & \cdots & 0 & \lambda k_1 S_1 g(j) & \cdots & 0 & \lambda k_1 S_1 g(n) \end{pmatrix}. \tag{11}$$

Similarly, when $i = 2, 3, \ldots, n$, we take the derivative of formula (3) with the aspects of $S_1, I_1, \ldots, S_n, I_n$ and then set $I_i = 0$. With matrix (11), a $2n \times 2n$ dimensional matrix is obtained:

$$\begin{pmatrix} -\mu & -\lambda k_1 S_1 g(1) & \cdots & 0 & -\lambda k_1 S_1 g(j) & \cdots & 0 & -\lambda k_1 S_1 g(n) \\ 0 & -(\mu+\delta)+\lambda k_1 S_1 g(1) & \cdots & 0 & \lambda k_1 S_1 g(j) & \cdots & 0 & \lambda k_1 S_1 g(n) \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & -\lambda k_j S_j g(1) & \cdots & -\mu & -\lambda k_j S_j g(j) & \cdots & 0 & -\lambda k_j S_j g(n) \\ 0 & \lambda k_j S_j g(1) & \cdots & 0 & -(\mu+\delta)+\lambda k_j S_j g(j) & \cdots & 0 & \lambda k_j S_j g(n) \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & -\lambda k_n S_n g(1) & \cdots & 0 & -\lambda k_n S_n g(j) & & -\mu & -\lambda k_n S_n g(n) \\ 0 & \lambda k_n S_n g(1) & \cdots & 0 & \lambda k_n S_n g(j) & & 0 & -(\mu+\delta)+\lambda k_n S_n g(n) \end{pmatrix}. \tag{12}$$

According to [33], n eigen values of matrix (12) are all equal to $-u$. Lines or columns including any of these n eigen values are removed, and a $n \times n$ dimensional matrix is obtained:

$$\begin{pmatrix} -(\mu+\delta)+\lambda k_1 S_1 g(1) & \lambda k_1 S_1 g(2) & \cdots & \lambda k_1 S_1 g(j) & \cdots & \lambda k_1 S_1 g(n) \\ \lambda k_2 S_2 g(1) & -(\mu+\delta)+\lambda k_2 S_2 g(2) & & \lambda k_2 S_2 g(j) & & \lambda k_2 S_2 g(n) \\ \vdots & \vdots & & \vdots & & \vdots \\ \lambda k_j S_j g(1) & \lambda k_j S_j g(2) & & -(\mu+\delta)+\lambda k_j S_j g(j) & & \lambda k_j S_j g(n) \\ \vdots & \vdots & & \vdots & & \vdots \\ \lambda k_n S_n g(1) & \lambda k_n S_n g(2) & & \lambda k_n S_n g(j) & & -(\mu+\delta)+\lambda k_n S_n g(n) \end{pmatrix}. \tag{13}$$

A series of transformations for matrix (13) are performed, and then the following matrix is given:

$$\begin{pmatrix} -(\mu+\delta) & 0 & \cdots & 0 & \cdots & \lambda k_1 S_1 g(n) \\ 0 & -(\mu+\delta) & \cdots & 0 & \cdots & \lambda\left(k_1 S_1 g(1) + k_2 S_2 g(2)\right) \dfrac{g(n)}{g(2)} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & -(\mu+\delta) & \cdots & \lambda \sum_{i=1}^{j} \left[k_i S_i g(i)\right] \dfrac{g(n)}{g(j)} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & -(\mu+\delta) + \lambda \sum_{i=1}^{n} \left[k_i S_i g(i)\right] \end{pmatrix}. \tag{14}$$

Obviously, the matrix (14) has an upper triangular one, and its characteristic equation is as follows:

$$[\lambda + (\mu + \delta)]^{n-1} \cdot \left[\lambda + (\mu + \delta) - \lambda \sum_{i=1}^{n} [k_i S_i g(i)]\right] = 0. \quad (15)$$

From (15), the characteristic values are obtained:

$$\lambda_1 = -(\mu + \delta), \qquad \lambda_2 = -(\mu + \delta) + \lambda \sum_{i=1}^{n} [k_i S_i g(i)]. \quad (16)$$

According to Routh-Hurwitz criterion, if and only if all of characteristic values are less than zero, the propagation system will eventually be stable at the equilibrium point E_0. Obviously, λ_1 are negative and the stability relies on λ_2. If λ_2 is less than 0, the equilibrium will be achieved. By transformation, the stability condition is derived as

$$R_0 = \frac{\lambda}{(\mu + \delta) N \langle k \rangle} \sum_{i=1}^{n} k_i^2 N_i^2 < 1. \quad (17)$$

The proof is complete. □

Corollary 2. *When the degree of a mobile node grows, the basic reproduction number R_0 gets increased, which means that it increases difficulty in realizing the stability for the propagation system of the mobile phone virus.*

Proof. Equation (17) can be converted into the following inequality:

$$R_0 = \frac{\lambda}{(\mu + \delta) N \langle k \rangle} \cdot \frac{\sum_{i=1}^{n} k_i^2 N_i^2}{\sum_{i=1}^{n} k_i N_i} < 1. \quad (18)$$

Obviously, $\sum_{i=1}^{n} k_i^2 N_i^2 / \sum_{i=1}^{n} k_i N_i$ is a monotonic function of k_i. When the degree k_i of the mobile phone node is increased, R_0 will also grow. It makes (18) more difficult to be satisfied. Corollary 2 is thus drawn. □

4. Modeling the Propagation of the Vulnerability-Exploiting Mobile Phone Virus

4.1. M-SIR Model. According to the development of virus, the mobile virus will eventually become a mobile worm which is called vulnerability-exploiting virus. The vulnerability-exploiting virus will automatically propagate by exploiting vulnerabilities existing in mobile phone operating systems or application software. Patching can be applied to repair vulnerabilities and then protect mobile phones from attacks. According to the spread property of vulnerability-exploiting virus, the epidemic state of a node is divided as follows: susceptible state (S), infectious state (I), and recovered state (R).

Susceptible state (S): nodes have not been infected by any user-tricking virus but are prone to infection. Infectious state (I): nodes have been infected by vulnerability-exploiting virus and they may infect some nodes in state S. Recovered state (R): nodes are cleaned of vulnerability-exploiting virus and immune to the same type of cleaned virus.

The propagation modeling of vulnerability-exploiting mobile phone virus under complex network called M-SIR model is proposed, which means mobile phone virus SIR (susceptible-infectious-recovered) propagation model. The state transforming process of any kind of nodes in M-SIR model is illustrated in Figure 2.

In the M-SIR model, a node in the kth kind can transit to the infectious state if it is at the susceptible state. The infection probability is presented by λ. The infectious node can clean the virus through patching with the immune rate γ. Once patched, the mobile is immune to the virus permanently. The susceptible node can also be patched in advance of infection with patching rate ω and transits to the recovered state. To maintain the balance of the network system, the "death" rate and the "birth" rate are all μ. The "new born" mobiles are all in the susceptible state. But the "new born" mobiles become not only susceptible ones but also "immune" ones, because new mobiles may install new versions of software with patches. The description of related parameters in M-SIR model is shown in Table 2.

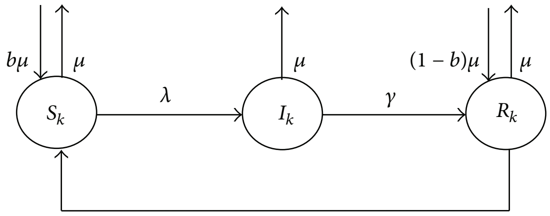


Figure 2: State transition graph of the kth kind of nodes in M-SIR model.

Table 2: Notations in the M-SIR model.

Parameter	Meaning
N	The total number of mobiles
$S_i(t)$	The number of the ith kinds of mobiles in the susceptible state at time t
$I_i(t)$	The number of the ith kinds of mobiles in the infected state at time t
$R_i(t)$	The number of the ith kinds of mobiles in the "immune" state at time t
N_i	The number of the ith kinds of mobiles at time t
λ	The contact infection rate
γ	The "immune" rate for infected mobiles
ω	The "immune" rate for susceptible mobiles
μ	The "birth/death" rate
b	The probability of new "born" susceptible mobiles
$1 - b$	The probability of new "born" immune mobiles

Define $R_i(t)$ as the number of the ith kinds of immune mobiles at time t. A mobile can be in one of three states for a time, and the sum for three classes of mobiles is as

$$S_i(t) + I_i(t) + R_i(t) = N_i. \tag{19}$$

According to the above analysis and state transition graph in Figure 2, given a topology of a social network, the number of susceptible, infected, and recovered nodes of the ith kind at time t in the M-SIR model can be presented by

$$\begin{aligned}\frac{dS_i(t)}{dt} &= b\mu N_i - \mu S_i(t) - \lambda k_i S_i(t)\,\Theta(t) - \omega S_i(t),\\ \frac{dI_i(t)}{dt} &= \lambda k_i S_i(t)\,\Theta(t) - \mu I_i(t) - \gamma I_i(t),\\ \frac{dR_i(t)}{dt} &= (1-b)\,\mu N_i + \gamma I_i(t) - \mu R_i(t).\end{aligned} \tag{20}$$

There are n kinds of nodes in the network, so the differential equations of the M-SIR model can be concluded as the following equation:

$$\begin{aligned}\frac{dS(t)}{dt} &= \sum_{i=1}^{n} \frac{dS_i(t)}{dt},\\ \frac{dI(t)}{dt} &= \sum_{i=1}^{n} \frac{dI_i(t)}{dt},\\ \frac{dR(t)}{dt} &= \sum_{i=1}^{n} \frac{dR_i(t)}{dt}.\end{aligned} \tag{21}$$

4.2. Infection-Free Equilibrium Point. In order to obtain the infection-free equilibrium point, (20) is converted into the following equation:

$$\begin{aligned}b\mu N_i - \mu S_i(t) - \lambda k_i S_i(t)\,\Theta(t) - \omega S_i(t) &= 0,\\ \lambda k_i S_i(t)\,\Theta(t) - \mu I_i(t) - \gamma I_i(t) &= 0,\\ (1-b)\,\mu N_i + \gamma I_i(t) - \mu R_i(t) &= 0.\end{aligned} \tag{22}$$

Solving (22), $S_i(t)$, $I_i(t)$, and $R_i(t)$ are derived as follows:

$$\begin{aligned}S_i &= \frac{b\mu}{\mu+\omega} N_i,\\ I_i &= 0,\\ R_i &= N_i - \frac{b\mu}{\mu+\omega}.\end{aligned} \tag{23}$$

There are total n kinds of nodes. Each kind of nodes has an infection-free equilibrium point. So the infection-free equilibrium point of the mobile phone virus propagation system under the M-SIR model is $E_1^*(S_1, 0, R_1, S_2, 0, R_2 \ldots, S_n, 0, R_n)$, where

$$S_i = \frac{b\mu}{\mu+\omega} N_i, \qquad I_i = 0, \qquad R_i = N_i - \frac{b\mu}{\mu+\omega}. \tag{24}$$

4.3. Stability of the Infection-Free Equilibrium

Theorem 3. *If the basic reproduction number $R_1 < 1$, the mobile phone virus propagation system under the M-SIR model will stabilize at the infection-free equilibrium point:*

$$R_1 = \frac{\lambda b\mu}{(\mu+\gamma)(\mu+\omega)N\langle k\rangle} \cdot \sum_{i=1}^{n} i^2 N_i^2. \tag{25}$$

Proof. Take the partial derivative of three equations to the right in (20) with the aspects of $S_1, I_1, S_2, I_2, \ldots, S_n, I_n$. With $I_i = 0$, a $2n \times 2n$ dimensional matrix is given:

$$\begin{pmatrix} -\mu-\omega & -\lambda k_1 S_1 g(1) & \cdots & 0 & -\lambda k_1 S_1 g(j) & \cdots & 0 & -\lambda k_1 S_1 g(n)\\ 0 & -(\mu+\gamma)+\lambda k_1 S_1 g(1) & \cdots & 0 & \lambda k_1 S_1 g(j) & \cdots & 0 & \lambda k_1 S_1 g(n)\\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots\\ 0 & -\lambda k_j S_j g(1) & \cdots & -\mu-\omega & -\lambda k_j S_j g(j) & \cdots & 0 & -\lambda k_j S_j g(n)\\ 0 & \lambda k_j S_j g(1) & \cdots & 0 & -(\mu+\gamma)+\lambda k_j S_j g(j) & \cdots & 0 & \lambda k_j S_j g(n)\\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots\\ 0 & -\lambda k_n S_n g(1) & \cdots & 0 & -\lambda k_n S_n g(j) & & -\mu-\omega & -\lambda k_n S_n g(n)\\ 0 & \lambda k_n S_n g(1) & \cdots & 0 & \lambda k_n S_n g(j) & & 0 & -(\mu+\gamma)+\lambda k_n S_n g(n) \end{pmatrix}, \tag{26}$$

where $g(j) = k_j P(k_j)/\langle k\rangle$, $j = 1, 2, \ldots, n$.

Removing the lines and columns including $-\mu + \omega$, a matrix of $n \times n$ dimensional is given as follows:

$$\begin{pmatrix} -(\mu+\gamma)+\lambda k_1 S_1 g(1) & \lambda k_1 S_1 g(2) & \cdots & \lambda k_1 S_1 g(j) & \cdots & \lambda k_1 S_1 g(n) \\ \lambda k_2 S_2 g(1) & -(\mu+\gamma)+\lambda k_2 S_2 g(2) & & \lambda k_2 S_2 g(j) & & \lambda k_2 S_2 g(n) \\ \vdots & \vdots & & \vdots & & \vdots \\ \lambda k_j S_j g(1) & \lambda k_j S_j g(2) & & -(\mu+\gamma)+\lambda k_j S_j g(j) & & \lambda k_j S_j g(n) \\ \vdots & \vdots & & \vdots & & \vdots \\ \lambda k_n S_n g(1) & \lambda k_n S_n g(2) & & \lambda k_n S_n g(j) & & -(\mu+\gamma)+\lambda k_n S_n g(n) \end{pmatrix}. \tag{27}$$

The second column of the matrix (26) multiplying by $-g(1)/g(2)$ is added to the first column, and then the third column multiplying by $-g(2)/g(3)$ is added to the second column and so on. After that, the first row multiplying by $g(1)/g(2)$ is added to the second row, and then the second row multiplying by $g(2)/g(3)$ is added to the third row and so on. The following matrix is thus obtained:

$$\begin{pmatrix} -(\mu+\gamma) & 0 & \cdots & 0 & \cdots & \lambda k_1 S_1 g(n) \\ 0 & -(\mu+\gamma) & & 0 & & \lambda\left[k_1 S_1 g(1) + 2k_2 S_2 g(2)\right] \dfrac{g(n)}{g(2)} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & & -(\mu+\gamma) & & \lambda \sum_{i=1}^{j} \left[k_i S_i g(i)\right] \dfrac{g(n)}{g(j)} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & & 0 & & -(\mu+\gamma) + \lambda \sum_{i=1}^{n} \left[k_i S_i g(i)\right] \end{pmatrix}. \tag{28}$$

The characteristic equation of (28) is showed as follows:

$$\left[\lambda + (\mu+\delta)\right]^{n-1} \cdot \left[\lambda + (\mu+\delta) - \lambda \sum_{i=1}^{n} \left[k_i S_i g(i)\right]\right] = 0. \tag{29}$$

The characteristic values are as follows:

$$\lambda_1 = -(\mu+\delta), \qquad \lambda_2 = -(\mu+\delta) + \lambda \sum_{i=1}^{n} \left[k_i S_i g(i)\right]. \tag{30}$$

According to Routh-Hurwitz criterion, if and only if all of the characteristic values are less than zero, the propagation system will eventually be stable at the equilibrium point E_1^*. By transformation of λ_2, the stability condition is obtained as

$$R_1 = \frac{\lambda \sum_{i=1}^{n} \left[i S_i g(i)\right]}{\mu+\gamma} = \frac{\lambda b \mu}{(\mu+\gamma)(\mu+\omega) N \langle k \rangle} \cdot \sum_{i=1}^{n} i^2 N_i^2 < 1. \tag{31}$$

The proof is complete. □

5. Constructing the Network Topology

The attacks target of the mobile virus is to infect the smart phone. The propagation path of mobile virus obeys the mobile user's social network, which has its own characters and greatly affects the propagation of the mobile phone virus. Thus it is indispensable to construct such a network to simulate the propagation of the mobile phone virus and validate our models.

The social network which is the propagation environment of mobile virus is a typical complex network. In the real world lots of networks have been proved to be complex network such as World Wide Web and email. The complex network has the following two characteristics: the degree of a node follows the power-law distribution and the network appears as small-world phenomenon. It is hard to put the real mobile virus into the real mobile network. So network topology generator called Inet3.0 is used to create a complex network to simulate the environment of mobile virus.

Inet is a topology generator developed by the University of Michigan and its current version has been upgraded to 3.0. When giving the total number of N nodes, Inet3.0 could output the information of N nodes including the position, degree, and the neighbors. Inet3.0 simulates the topology

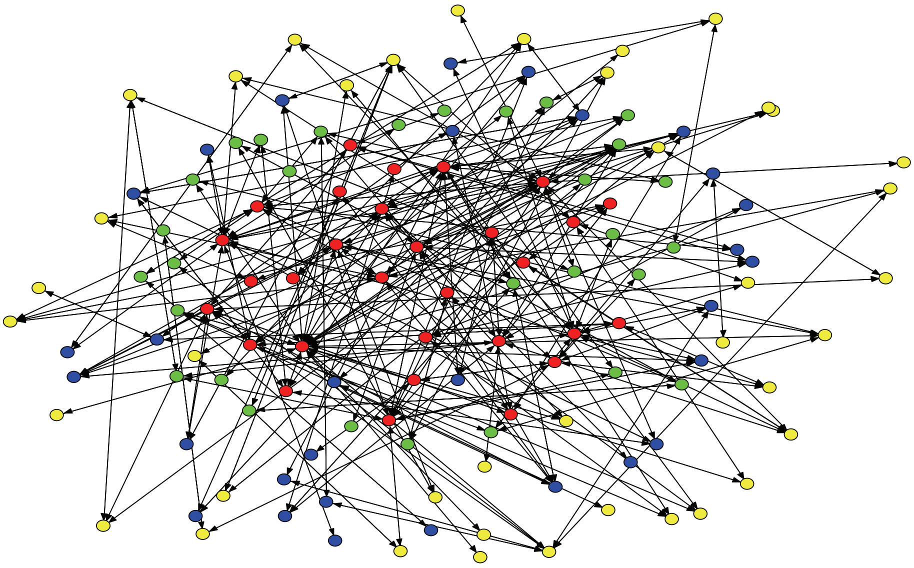


Figure 3: The distribution and connectivity of 130 nodes in the network generated by Inet3.0.

structure of the Internet and it accords with the characteristics of the complex network. Firstly, nodes' degrees generated by Inet3.0 follow the power-law distribution. Secondly, the characteristic path length created by Inet3.0 is short, which reflects the effect of the small-world phenomenon of social network. However, the clustering coefficient of the network built by Inet3.0 is relatively large. The network generated by Inet3.0 is much closed to the complex network and can be applied for simulating the propagation of the mobile phone virus.

In this paper, Inet3.0 is used to build a complex network which contains 10000 nodes. There are 118 different kinds of degrees among which the biggest value is 1799 and the least one is 1. Due to the high density of the topology and the page limit, it is difficult to differentiate the connectivity between nodes. Figure 3 shows the distribution and the connectivity of only 130 nodes in the topology structure, and the degrees of them are the biggest of all 10000 nodes.

Among the 130 nodes, the 30 red nodes are those with the biggest degrees; the 30 green ones are those with bigger degrees; the 30 blue ones are those with smaller degrees; the 40 yellow ones are those with the smallest degrees.

6. Numerical and Simulation Experiments

To verify the accuracy of theoretical analysis and the correctness of both M-SIS and M-SIR models, the numerical and simulation experiments are separately carried out. Numerical experiments are based on iterations of formulae and can directly reflect the property of the models. It is hard to simulate the real propagation environment of mobile phones virus. So the simulation experiments are carried out like other researchers [22–30]. Our simulation is a discrete-time simulation and well embodies the propagation of viruses in which node data are obtained on a time interval every second.

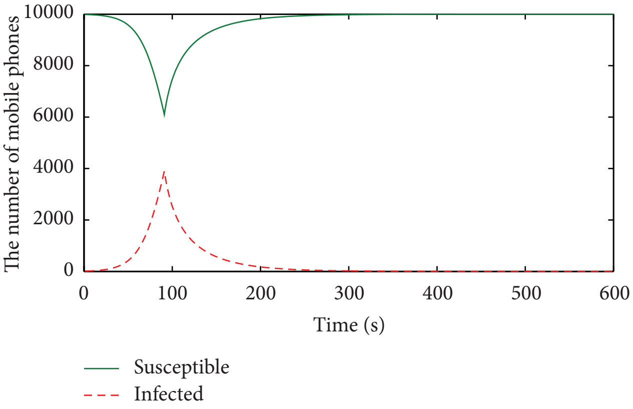


Figure 4: Numerical results in the M-SIS model.

Different from numerical experiments, the simulation imitates the real environment and is more closed to reality.

To raise the accuracy, the experiments under the same condition are carried out for 100 times, and the experiment result is derived from the average of 100 results. Algorithm 1 is the algorithm of the simulation which embodies the topology of the network. It is noted that one susceptible mobile can only be infected by its neighboring infected mobiles. The two-dimensional array Link_Matrix [][] is used to store the joined relationship between nodes.

6.1. Experiment for the M-SIS Model. The parameters in our experiments are chosen based on the research results of Zou et al. [34] and Wang et al. [35]. Due to the limit of computer memory and Inet3.0, 10,000 mobile phone nodes are set in our network system.

The contact infection rate λ of the mobile phone virus is set at 0.00003 with the same magnitude of the initial infection rate in Zou et al.'s research [34]. Similarly, the death/birth rate

```
for i = 0...virus_NUM-1
    if (node[i].status is susceptible)
        for j = 0...virus_NUM-1
            if (Link_Matrix[i][j] == 1 and node[j].status is infected)
                if (random number (rn) match the infection rate $\lambda$)
                    node[i].status become infected
                    break
                end if
            end if
        end for
        if (j > virus_NUM-1 and rn match the “immune” rate $\omega$)
            node[i].status become immune
        else if (j > virus_NUM-1 and rn match the “death” rate $\mu$)
            node[i].status become dead
        end if
    else if (node[i].status is infected)
        if (rn match the “immune” rate $\gamma$)
            node[i].status become immune
        else if (rn match the “death” rate $\mu$)
            node[i].status become dead
        end if
    else if (node[i].status is immunized)
        if (rn match the “death” rate $\gamma$)
            node[i].status become dead
        end if
    end if
end for
for i = 0...virus_NUM-1
    if (node[i].status is dead and rn match the probability b)
        node[i].status become susceptible
    else
        node[i].status become immune
    end if
end for
```

Algorithm 1

μ is assigned to be 0.00002 based on Wang et al.'s study [35]. The recovery rate δ is assumed to set 0.1. At the beginning, the mobile phone virus spreads along the edges of mobile phone nodes which own few contacts with others and then attacks core nodes. Therefore, there are 10 infected mobile phones with the degree of 1 initially, which means that the initial infected nodes only have one contact with other nodes.

The numerical results of the number of susceptible, infected mobile phones over time in M-SIS model are showed, respectively, in Figure 4.

To observe the propagation of the mobile user-tricking virus, virus-killing measure is taken after the 90 s, and sharp points appear in the curves at 90 s.

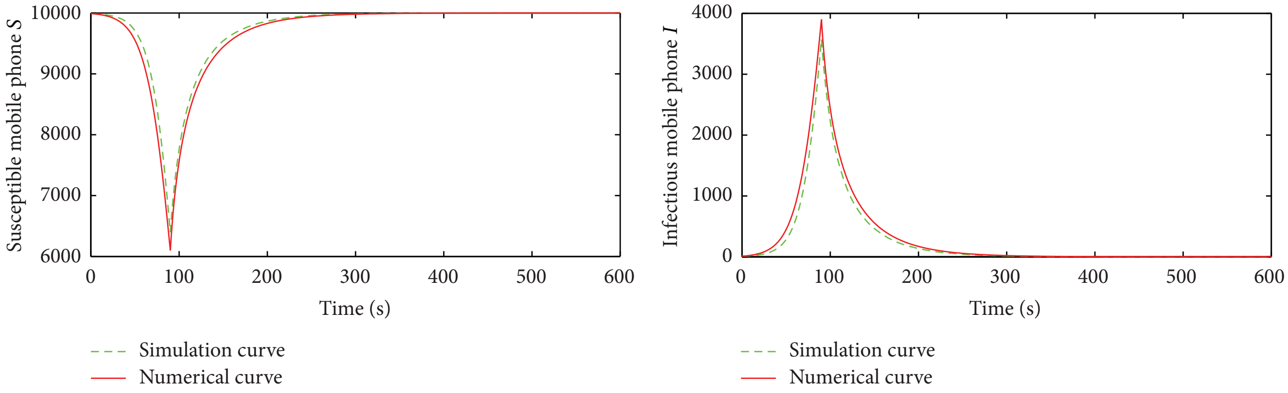
According to Theorem 1, the basic reproduction number R_0 is about 0.8 with the above parameters. It means that the propagation system of the mobile user-tricking virus under the M-SIS model will be eventually stable at its infection-free equilibrium point. Obviously, the number of infected mobile phones shrinks to 0 and that of susceptible ones is up to 10000 in Figure 4, which indicates that the infection-free equilibrium is achieved. The accuracy of theoretical analysis gets verified.

To check the correctness of M-SIS propagation model, the simulation experiments have been executed and the simulation results are compared with numerical results under the same parameters as shown in Figure 5.

Figure 5(a) compares the number of susceptible mobiles in numerical and simulation result and Figure 5(b) compares the number of susceptible mobiles. It is seen that the numerical curves match the simulation ones very well, which verifies the correctness of the M-SIS propagation model.

The affections of different parameters on the mobile user-tricking virus propagation model are tested. The contact infection rate λ is firstly discussed. λ is specified as 0.00002, 0.00003, 0.00004, 0.00005, 0.00006, and 0.00007, respectively, and other parameters remain unchanged. With different contact infection rates, the propagation trends of the mobile user-tricking virus are showed in Figure 6.

The increase of the contact infection rate can fasten the propagation of mobile user-tricking virus. But when it increases to certain extent, the impact of the mobile user-tricking virus goes down. The larger contact infection rate is, the more nodes are infected. So the contact infection rates can



(a) Compare the number of susceptible mobiles in numerical and simulation result

(b) Compare the number of infectious mobiles in numerical and simulation result

Figure 5: Comparison of numerical and simulation result.

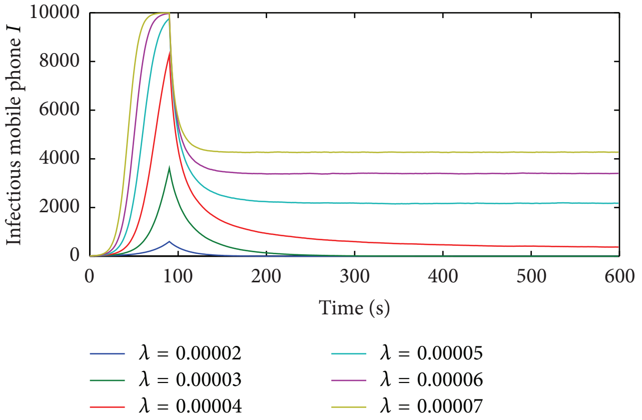


Figure 6: Impact of the contact infection rate λ on the M-SIS model.

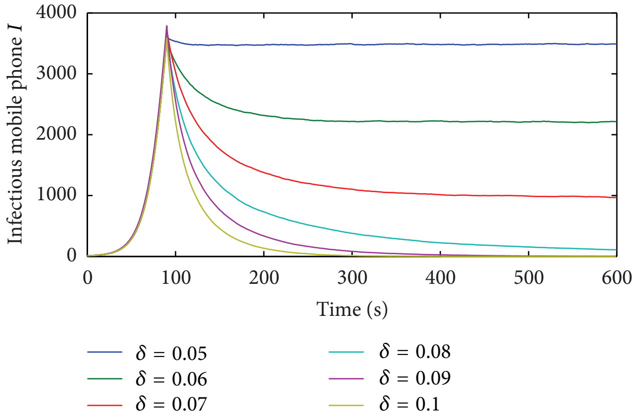


Figure 7: Impact of infection recovery rate δ on the M-SIS model.

rapid the propagation speed and wide the propagation scope of mobile user-tricking virus.

The infection recovery rate δ is also discussed while other parameters remain unchanged. δ is set at 0.05, 0.06, 0.07, 0.08, 0.09, and 0.1 respectively, and the propagations trends of the mobile user-tricking virus are given in Figure 7.

With the increase of δ, the number of infected nodes decreases, but all the curves reach the peak at the same time. It means that the infection recovery rate can only affect the spread scope of mobile user-tricking virus. It cannot rapid the propagation speed.

6.2. Experiment for the M-SIR Model. In this experiment, the patching rate γ for infected mobiles is 0.01 based on the research of Wang et al. [35]. The root of mobile vulnerability-exploiting virus existing is software vulnerabilities which are inevitable during the design and implementation process of software and hard to detect. Due to lots of bandwidth consumption the patch cannot be distributed in time, so the patching rate ω for susceptible mobile phones is relatively small and is set as 0.0001. And it is assumed that the probability b that the "new born" mobile phone becomes susceptible one is 0.6. Other parameters are set the same as the ones in the M-SIS model.

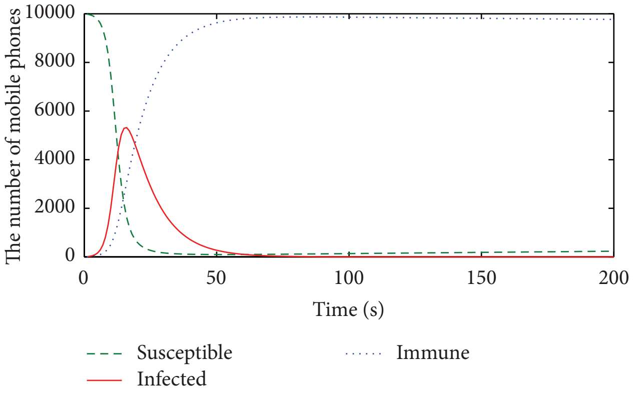
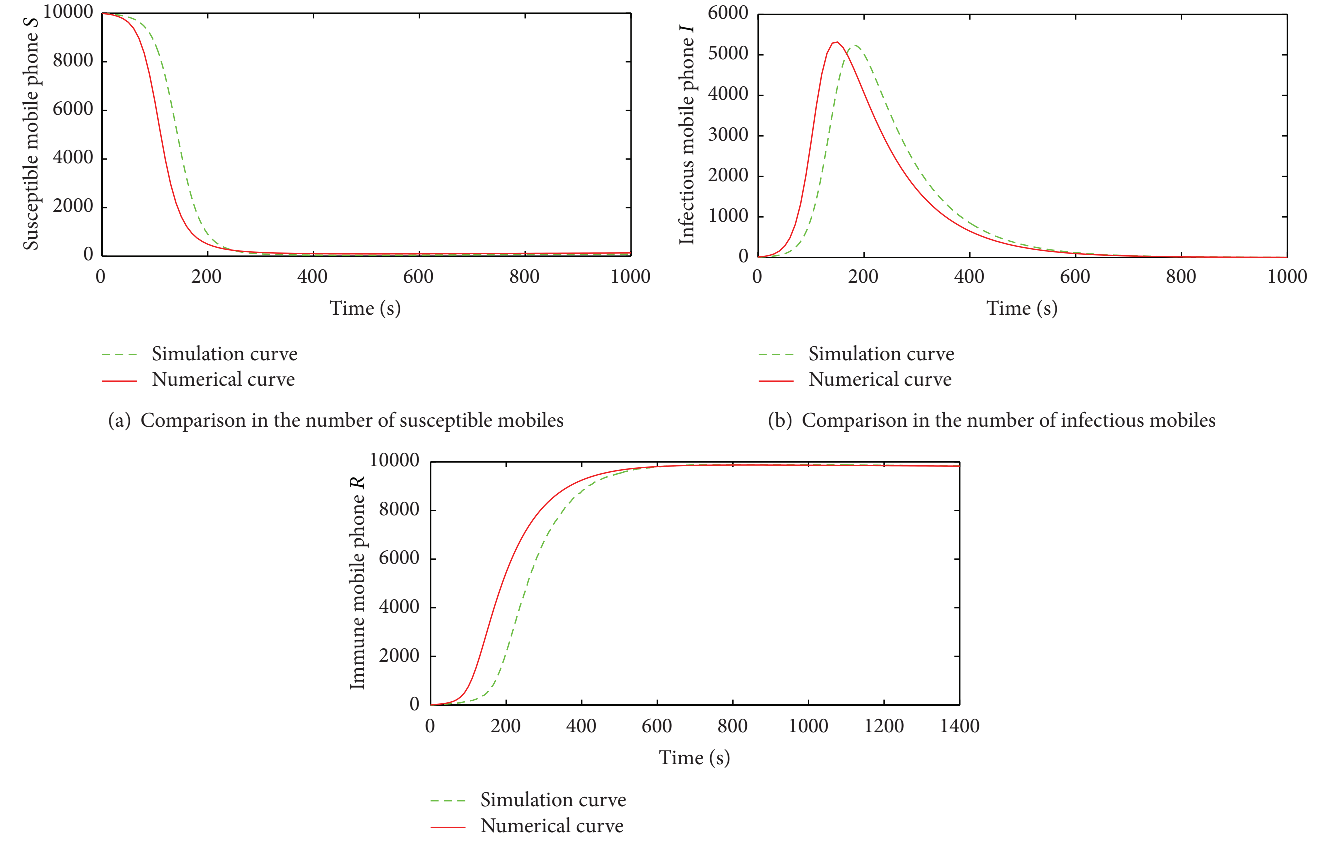


Figure 8: Numerical results in the M-SIR model.

The numerical results of the susceptible, infected, and immune mobile phones in the M-SIR model are given in Figure 8.



(a) Comparison in the number of susceptible mobiles

(b) Comparison in the number of infectious mobiles

(c) Comparison in the number of immune mobiles

Figure 9: Comparisons between numerical and simulation results in the M-SIR model.

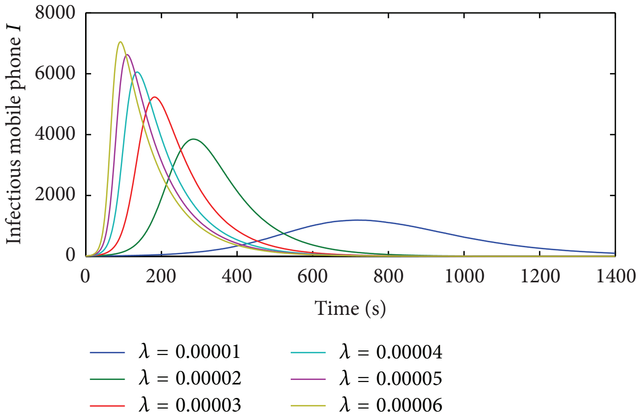


Figure 10: Effect of the contact infection rate λ in the M-SIR model.

All infected mobile phones vanish and the population in the long term is in an immune state. According to Theorem 3, the basic reproduction number R_1 is about $0.8 < 1$, which means that the propagation system of mobile phone virus under the M-SIR model will stabilize at its infection-free equilibrium point. In Figure 8 the susceptible, infected, and immune state mobile phones all reach their equilibrium points. This is fully consistent with the conclusions of Theorem 3.

The numerical results and simulation ones in susceptible, infected, and immune mobile phones, respectively, under the M-SIR model are shown in Figure 9.

The simulation curves of all states are almost consistent with the numerical ones which prove the correctness of the M-SIR model. The effect of contact infection rate to the propagation of vulnerability-exploiting mobile phone virus is shown in Figure 10.

Figure 10 shows the propagation trends of vulnerability-exploiting mobile phone virus with six different contact infection rates. With the increasing of the contact infection rate, the spread speed of the vulnerability-exploiting mobile phone virus is promoted, which makes the vulnerability-exploiting mobile phone virus reach the peak with little time. The scope of vulnerability-exploiting mobile phone virus also widens with the higher contact infection rate. The higher contact infection rate is the more nodes are infected. But the impact on the propagation is weakening with λ going up to some extent.

The performance of the immune rate to the propagation of vulnerability-exploiting mobile phone virus is discussed in Figure 11.

Figure 11 gives the propagations of the vulnerability-exploiting mobile phone virus with five different immune rates. The immune rate can affect the speed and scope of propagation. Obviously, the more the immune rate γ

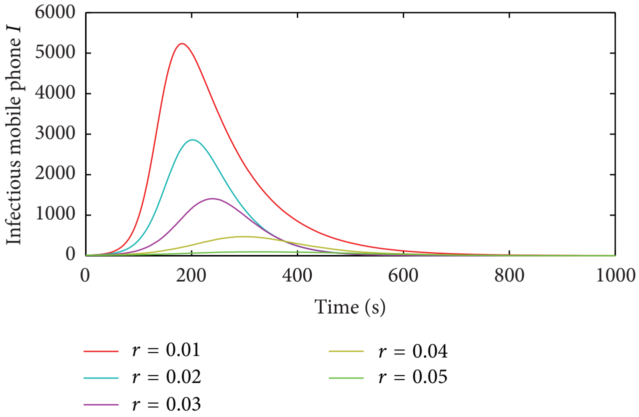


Figure 11: Effect of the immune rate γ in the M-SIR model.

is, the weaker the spread capability of the vulnerability-exploiting mobile phone virus is. Therefore, in order to guarantee normal applications of mobile phones and suppress the propagation speed and the propagation scope of mobile phone virus, we should choose a reasonable value for immune rate γ.

7. Conclusions

The objective of this paper is to model two kinds of mobile phone virus under two important factors (viz., the characteristics of mobile phone viruses and the network topology structure) and then to find out certain means to suppress the propagation of mobile phone virus. The M-SIS and M-SIR propagation models for mobile phone viruses are proposed, combining with the structural characteristics of the complex network.

The M-SIS propagation model is effective to predict the propagation of the user-tricking mobile phone virus. It reflects the characteristic of the mobile virus, which is difficult to completely remove, and the removed mobile phone virus can reinfect the same mobile phone.

The M-SIR propagation model is suitable to describe the vulnerability-exploiting mobile phone virus. It reflects the characteristic of the mobile virus, which spreads by exploiting vulnerabilities, and the mobile phone can be immune to the mobile phone virus after virus removal and patching.

Through analysis, the stable infection-free equilibrium point and the stability condition of the two propagation models are derived. The basic reproduction numbers R_0 and R_1 are given, which can determine whether the mobile phone virus extinguishes. When $R_0 < 1$ and $R_1 < 1$, the proposed M-SIS and M-SIR models have only a worm-free equilibrium, respectively, which is globally stable and implies that the worm dies out eventually. Then some numerical and simulation experiments are carried out which prove that our models are correct and fully consistent with the conclusions of our analysis. Our future work will expand this model which can characterize more features of mobile phone virus, for example, taking delay or impulse into consideration.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This paper is supported by the Fundamental Research Funds of the Central Universities under Grant no. N120317001, Program for New Century Excellent Talents in University (NCET-13-0113), Natural Science Foundation of Liaoning Province of China under Grant no. 201202059, and Program for Liaoning Excellent Talents in University under LR2013011.

References

[1] N. Leavitt, "Mobile phones: the next frontier for hackers?" *Computer*, vol. 38, no. 4, pp. 20–23, 2005.

[2] Ericsson, "Traffic and market data report," 2011, http://www.ericsson.com/res/docs/2012/tmd_report_feb_web.pdf.

[3] M. Ghaderi and S. Keshav, "Multimedia messagingservice: system description and performance analysis," in *Proceedings of the 1st International Conference on Wireless Internet*, pp. 198–205, 2005.

[4] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A social network based patching scheme for worm containment in cellular networks," in *Proceedings of the 28th IEEE International Conference on Computer Communications (IEEE INFOCOM '09)*, pp. 1476–1484, Rio de Janeiro, Brazil, April 2009.

[5] F-SECURE, "F-secure virus information pages: commwarrior," http://www.f-secure.com/v-descs/commwarrior.shtml.

[6] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and S. Bhattacharjee, "Measurement and analysis of online social networks," in *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, pp. 29–42, 2007.

[7] R. Kumar, J. Novak, and A. Tomkins, "Structure and evolution of online social networks," in *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 611–617, 2006.

[8] A. Yong-Yeol, H. Seungyeop, K. Haewoon, M. Sue, and J. Hawoong, "Analysis of topological characteristics of huge online social networking services," in *Proceedings of the 16th International Conference on World Wide Web*, pp. 835–844, 2007.

[9] C. Fleizach, M. Liljenstam, P. Johansson, G. M. Voelker, and A. Mehes, "Can you infect me now?: malware propagation in mobile phone networks," in *Proceedings of the ACM Workshop on Recurring Malcode*, pp. 61–68, 2007.

[10] F. Li, Y. Y. Yang, and J. Wu, "CPMC: an efficient proximity malware coping scheme in smartphone-based mobile networks," in *Proceedings of the 29th IEEE Conference on Information Communications (INFOCOM '10)*, pp. 2811–2819, San Diego, Calif, USA, 2010.

[11] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 343–361, 1991.

[12] J. O. Kephart and S. R. White, "Measuring and modeling computer virus prevalence," in *IEEE Computer Security Symposium on Security and Privacy*, pp. 2–15, 1993.

[13] R. W. Thommes and M. J. Coates, "Modeling virus propagation in peer-to-peer networks," in *Proceedings of the IEEE 5th*

International Conference on Information, Communications and Signal Processing, pp. 981–985, IEEE, Bangkok, Thailand, 2005.

[14] C. Zou Cliff, D. Towsley, and G. Weibo, "On the performance of internet worm scanning strategies," *Performance Evaluation*, vol. 63, no. 7, pp. 700–723, 2008.

[15] H. Yuan and G. Chen, "Network virus-epidemic model with the point-to-group information propagation," *Applied Mathematics and Computation*, vol. 206, no. 1, pp. 357–367, 2008.

[16] B. K. Mishra and S. K. Pandey, "Dynamic model of worms with vertical transmission in computer network," *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8438–8446, 2011.

[17] C. W. John and J. M. David, "Modelling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction," *Computational Statistics Data Analysis*, vol. 45, no. 1, pp. 3–23, 2004.

[18] Y. B. Kafai, "Understanding virtual epidemics: children's folk conceptions of a computer virus," *Journal of Science Education and Technology*, vol. 17, no. 6, pp. 523–529, 2008.

[19] F. Wang, Y. Zhang, C. Wang, J. Ma, and S. Moon, "Stability analysis of a SEIQV epidemic model for rapid spreading worms," *Computers and Security*, vol. 29, no. 4, pp. 410–418, 2010.

[20] J. R. C. Piqueira and V. O. Araujo, "A modified epidemiological model for computer viruses," *Applied Mathematics and Computation*, vol. 213, no. 2, pp. 355–360, 2009.

[21] W. Fan and K. H. Yeung, "Online social networks-Paradise of computer viruses," *Physica A: Statistical Mechanics and Its Applications*, vol. 390, no. 2, pp. 189–197, 2011.

[22] B. Dwan, "The mobile phone virus," *Network Security*, vol. 7, pp. 14–15, 2004.

[23] J. Jamaluddin, N. Zotou, R. Edwards, and P. Coulton, "Mobile phone vulnerabilities: a new generation of malware," in *Proceedings of the IEEE International Symposium on Consumer Electronics*, pp. 199–202, 2004.

[24] D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: the viruses are coming!," *Pervasive Computing*, vol. 3, no. 4, pp. 11–15, 2004.

[25] W. Zhang, H. He, Q. Zhang, and T.-H. Kim, "PhoneProtector: protecting user privacy on the android-based mobile platform," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 282417, 10 pages, 2014.

[26] C. Jin, X. Huang, and S. Jin, "Propagation model of mobile phone virus based on efficiency of immunization," in *Proceedings of the International Conference on MultiMedia and Information Technology (MMIT '08)*, pp. 500–502, 2008.

[27] J. Ren, X. Yang, Q. Zhu, L.-X. Yang, and C. Zhang, "A novel computer virus model and its dynamics," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 1, pp. 376–384, 2012.

[28] Y. Yao, W. Xiang, A. Qu, G. Yu, and F. Gao, "Hopf bifurcation in an SEIDQV worm propagation model with quarantine strategy," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 304868, 18 pages, 2012.

[29] P. Wang, M. C. González, C. A. Hidalgo, and A. L. Barabási, "Understanding the spreading patterns of mobile phone viruses," *Science*, vol. 324, no. 5930, pp. 1071–1076, 2009.

[30] H. Zheng, L. Dong, and G. Zhuo, "An epidemic model of mobile phone virus," in *Proceedings of the 1st International Symposium on Pervasive Computing and Applications*, pp. 1–5, IEEE, Urumqi, China, August 2006.

[31] W. Xuetao, N. C. Valler, M. Faloutsos, I. Neamtiu, B. A. Prakash, and C. Faloutsos, "Smartphone viruses propagation on heterogeneous composite networks," in *Proceedings of the IEEE 2nd Network Science Workshop*, pp. 106–109, 2013.

[32] M. E. J. Newman, S. Forrest, and J. Balthrop, "Email networks and the spread of computer viruses," *Statistical, Nonlinear, and Soft Matter Physics*, vol. 66, Article ID 035101, 2002.

[33] J. P. Zhang and Z. Jin, "The analysis of an epidemic model on networks," *Applied Mathematics and Computation*, vol. 217, no. 17, pp. 7053–7064, 2011.

[34] C. C. Zou, D. Towsley, and W. B. Gong, "Code red worm propagation modeling and analysis," in *Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS '02)*, pp. 138–147, 2002.

[35] F. W. Wang, Y. K. Zhang, and C. G. Wang, "Stability analysis of a SEIQV epidemic model for rapid spreading worms," *Computers & Security*, vol. 29, no. 4, pp. 410–418, 2010.

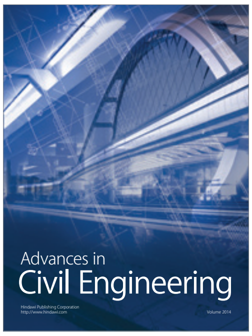
Journal of
Engineering

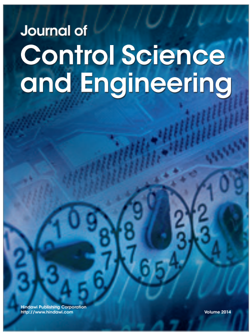
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

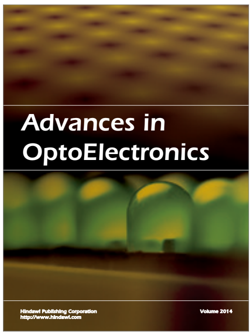
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

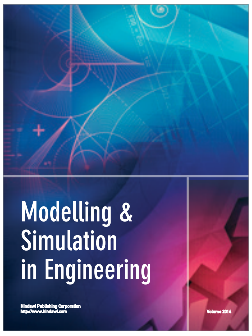
Journal of
Robotics

Journal of
Electrical and Computer Engineering

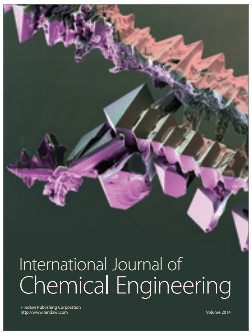

Advances in
OptoElectronics

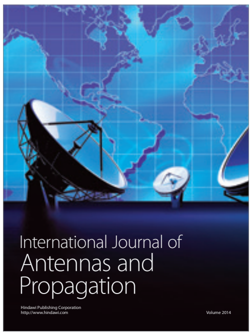
VLSI Design

International Journal of
Navigation and Observation

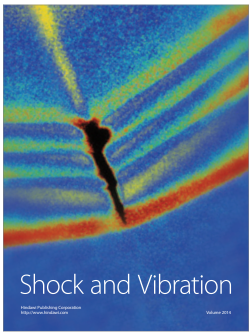

Modelling & Simulation in Engineering

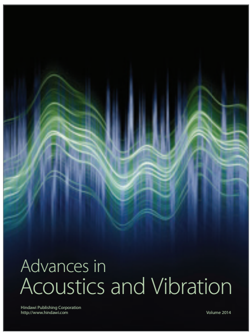
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration