Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2013, Article ID 296940, 6 pages
http://dx.doi.org/10.1155/2013/296940

Research Article

Influence of Removable Devices' Heterouse on the Propagation of Malware

Xie Han,[1] Yi-Hong Li,[2] Li-Ping Feng,[3] and Li-Peng Song[1]

[1] *Department of Computer Science and Technology, North University of China, Taiyuan 030051, China*
[2] *Department of Mathematics, North University of China, Taiyuan 030051, China*
[3] *Department of Computer Science and Technology, Xinzhou Teachers University, Xinzhou 034000, China*

Correspondence should be addressed to Li-Peng Song; slp880@gmail.com

Received 5 September 2013; Accepted 30 September 2013

Academic Editor: Carlo Bianca

Copyright © 2013 Xie Han et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The effects of removable devices' heterouse in different areas on the propagation of malware spreading via removable devices remain unclear. As a result, in this paper, we present a model incorporating the heterogeneous use of removable devices, obtained by dividing the using rate into local area's rate, neighbour area's rate and global area's rate, and then getting the final rate by multiplying the corresponding area ratio. The model's equilibria and their stability conditions are obtained mathematically and verified by deterministic and stochastic simulations. Simulation results also indicate that the heterogeneity in using rate significantly changes the prospective propagation course of malware. Additionally, the thresholds of removable devices' using rate in neighbour area are given, which can guide us in designing effective countermalware method.

1. Introduction

The malicious programs or malware, including network worms, Trojan programs, and various botnets, have posed serious threats to the Internet [1–5]. Furthermore, removable devices have become a common propagation method by those recently detected malware, such as Stuxnet [6], Duqu [7], and Flame [8], which aim at controlling computers or other machinery, especially those physically isolated machines. Thus, it is very necessary to explore the propagation behavior and control strategies of such malware.

To capture the influences of removable devices on malware, some mathematical models have been proposed [9–13]. In [9], Song et al. presented the model by coupling a susceptible-infected-recovered (SIR) model with a susceptible-infected-susceptible (SIS) model [14]. In the model, a removable device would be infected with a certain rate if it was used on an infectious computer and then the infected removable device can infect other computers whenever it was used on them. To depict the computers which have been infected but are not yet infectious, Jin and Wang [10] put forward the susceptible-exposed-infected-recovered (SEIR) model by introducing the "exposed" state into the SIR model. L. X. Yang and X. Yang [11] further considered the model where the "exposed" state had limited infection ability. However, all of these models were homogeneous models. That is to say, each removable device was used with the same probability on all computers.

In [13], Peng et al. gave a model which divided the Internet into many subnets and assumed that removable devices were used equally within the subnet they belong to, but they were used with a lower probability outside the subnet. However, it is not a reasonable assumption that removable devices are homogeneously mixed with computers outside their subnet. Furthermore, under this assumption, they cannot give an effective defense method concerning removable devices' using area and rate. Hence, we present a heterogeneous model in this paper, which can give an effective countermalware method by exploring the influences of removable devices' using area and rate.

The remainder of this paper is organized as follows: we give the model and interpret the parameters' meanings in Section 2. After that, we analyze its dynamical behavior and illustrate our mathematical results by simulations in Section 3. Then, some containment strategies are given in Section 4. In the end, we summarize our work.

2. The Model

The basic models used in this paper are the SIR model and the SIS model. There are five compartments in our model: susceptible computers (S); infected computers (I); immunized computers (R); susceptible media (M_S)—removable devices without malicious programs; infected media (M_I)—removable devices which have carried the malicious programs and can propagate them to susceptible computers.

To depict the influences of removable devices' using area and rate, we divide the whole area into many subareas and each removable device belongs to an area named the local area of the device. We also assume that removable devices are used equally within the local area and used with a lower probability in their neighbour areas but hardly used in any other areas named global area here.

Let β_1 be the susceptible computer's infection rate caused by the successful scans of an infected computer. β_2 denotes susceptible computer's infection rate (susceptible medium's infection rate) due to an infected medium (an infected computer) in the same local area. N and M denote the total number of computers and the total number of removable devices, respectively. Here, we suppose that both N and M are constant. Then, the obsoleteness rate of computers (removable devices) is given by μ_1 (μ_2).

To model the random discovery of infection by antivirus program, the recovery rate of infected computers is given by δ_1. When infected devices are used on susceptible or immunized computers, the malicious programs carried by infected devices are likely to be detected. We denote this rate by δ_2.

Then, the model is given as follows:

$$\begin{aligned}
\dot{S} &= \mu_1 N - \frac{\beta_1 S I}{2^{32}} - \frac{D(\cdot)\beta_2 S M_I}{N} - \mu_1 S, \\
\dot{I} &= \frac{\beta_1 S I}{2^{32}} + \frac{D(\cdot)\beta_2 S M_I}{N} - \delta_1 I - \mu_1 I, \\
\dot{R} &= \delta_1 I - \mu_1 R, \\
\dot{M}_S &= \mu_2 M - \frac{D(\cdot)\beta_2 M_S I}{N} + \delta_2 \frac{R+S}{N} M_I - \mu_2 M_S, \\
\dot{M}_I &= \frac{D(\cdot)\beta_2 M_S I}{N} - \delta_2 \frac{R+S}{N} M_I - \mu_2 M_I,
\end{aligned} \tag{1}$$

where $D(\cdot)$ is the function of removable devices' using area and rate. For all removable devices, let α_1 (α_2) denote the ratio of using rate in neighbour area (global area) to the counterpart in local area and let λ_1 (λ_2) be the ratio of neighbour area's (global area's) radius to local area's radius. Without loss of generality, both removable devices' using rate in local area and local area's radius are set to 1. Then,

$$D(\cdot) = \frac{1}{\lambda_2^2} + \alpha_1 \frac{\lambda_1^2}{\lambda_2^2} + \alpha_2 \frac{\left(\lambda_2^2 - \lambda_1^2 - 1\right)}{\lambda_2^2}. \tag{2}$$

As $N = S + I + R$ and $M = M_S + M_I$, the model (1) can be rewritten as

$$\begin{aligned}
\dot{I} &= \frac{\beta_1 (N - I - R) I}{2^{32}} + \frac{D(\cdot)\beta_2 (N - I - R) M_I}{N} - \delta_1 I - \mu_1 I, \\
\dot{R} &= \delta_1 I - \mu_1 R, \\
\dot{M}_I &= \frac{D(\cdot)\beta_2 (M - M_I) I}{N} - \delta_2 \frac{N - I}{N} M_I - \mu_2 M_I.
\end{aligned} \tag{3}$$

Let

$$R_0 = \frac{\beta_1 N}{2^{32}(\delta_1 + \mu_1)} + \frac{D(\cdot)^2 \beta_2^2 M}{(\delta_1 + \mu_1)(\delta_2 + \mu_2) N}, \tag{4}$$

where R_0 is the basic reproduction number [15].

For system (3), there are two equilibria: disease-free equilibrium $E_0 = (0, 0, 0)$ and positive equilibrium $E^* = (I^*, R^*, M_I^*)$ when $R_0 > 1$. The positive equilibrium is given by

$$I^* = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \tag{5a}$$

$$R^* = \frac{\delta_1}{\mu_1} I^*, \tag{5b}$$

$$M_I^* = \frac{D(\cdot)\beta_2 M I^*}{(D(\cdot)\beta_2 - \delta_2) I^* + (\delta_2 + \mu_2) N}, \tag{5c}$$

where $a = (\beta_1(1 + (\delta_1/\mu_1))(D(\cdot)\beta_2 - \delta_2)N)/2^{32}$, $b = (\beta_1(1 + (\delta_1/\mu_1))(\delta_2 + \mu_2)N^2)/2^{32} + (\delta_1 + \mu_1)(D(\cdot)\beta_2 - \delta_2)N + D(\cdot)^2\beta_2^2(1 + (\delta_1/\mu_1))M - (\beta_1(D(\cdot)\beta_2 - \delta_2)N^2)/2^{32}$, and $c = (\delta_1 + \mu_1)(\delta_2 + \mu_2)N^2 - (\beta_1(\delta_2 + \mu_2)N^3)/2^{32} - D(\cdot)^2\beta_2^2 MN$.

3. Model Analysis

Theorem 1. *If $R_0 < 1$, E_0 is asymptotically stable.*

Proof. The characteristic equation of (3) at E_0 is given by

$$\det \begin{pmatrix} \lambda - \left(\frac{\beta_1 N}{2^{32}} - \delta_1 - \mu_1\right) & 0 & -D(\cdot)\beta_2 \\ -\delta_1 & \lambda + \mu_1 & 0 \\ -\frac{D(\cdot)\beta_2 M}{N} & 0 & \lambda + \delta_2 + \mu_2 \end{pmatrix} = 0. \tag{6}$$

Then, we have

$$(\lambda + \mu_1)\left[\left(\lambda - \frac{\beta_1 N}{2^{32}} + \delta_1 + \mu_1\right)(\lambda + \delta_2 + \mu_2) - \frac{D(\cdot)^2 \beta_2^2 M}{N}\right] = 0. \tag{7}$$

When $R_0 < 1$, corresponding to $(\delta_1+\mu_1-(\beta_1 N)/2^{32})(\delta_2+\mu_2)-(D(\cdot)^2\beta_2^2 M)/N > 0$, all eigenvalues of (7) have negative real parts. Thus, E_0 is asymptotically stable. The theorem is proven. □

Theorem 2. *If $R_0 > 1$, the endemic equilibrium E^* is asymptotically stable.*

Proof. The characteristic equation of (3) at E^* is given by

$$\det\begin{pmatrix} \lambda-\dfrac{\beta_1 N}{2^{32}}+\dfrac{\beta_1(2I^*+R^*)}{2^{32}}+\dfrac{D(\cdot)\beta_2 M_I^*}{N}+\delta_1+\mu_1 & \dfrac{\beta_1 I^*}{2^{32}}+\dfrac{D(\cdot)\beta_2 M_I^*}{N} & -\dfrac{D(\cdot)\beta_2(N-I^*-R^*)}{N} \\ -\delta_1 & \lambda+\mu_1 & 0 \\ -\dfrac{D(\cdot)\beta_2(M-M_I^*)}{N}-\dfrac{\delta_2 M_I^*}{N} & 0 & \lambda+\dfrac{D(\cdot)\beta_2 I^*}{N}+\delta_2\dfrac{N-I^*}{N}+\mu_2 \end{pmatrix}=0, \quad (8)$$

corresponding to

$$\begin{aligned}&\lambda^3+(a_{11}+a_{22}+a_{33})\lambda^2\\&\quad+(a_{11}a_{22}+a_{11}a_{33}+a_{22}a_{33}-a_{12}a_{21}-a_{13}a_{31})\lambda\\&\quad+a_{11}a_{22}a_{33}-a_{12}a_{21}a_{33}-a_{13}a_{31}a_{22}=0,\end{aligned} \quad (9)$$

where $a_{11}=-(\beta_1 N)/2^{32}+(\beta_1(2I^*+R^*))/2^{32}+(D(\cdot)\beta_2 M_I^*)/N+\delta_1+\mu_1$, $a_{12}=(\beta_1 I^*)/2^{32}+(D(\cdot)\beta_2 M_I^*)/N$, $a_{13}=-(D(\cdot)\beta_2(N-I^*-R^*))/N$, $a_{21}=-\delta_1$, $a_{22}=\mu_1$, $a_{31}=-(D(\cdot)\beta_2(M-M_I^*))/N-(\delta_2 M_I^*)/N$, and $a_{33}=(D(\cdot)\beta_2 I^*)/N+\delta_2(N-I^*)/N+\mu_2$.

According to the Hurwitz criteria [16, 17], we have

$$\begin{aligned}H_1&=a_{11}+a_{22}+a_{33}\\&=\frac{D(\cdot)\beta_2(N-I^*-R^*)M_I^*}{NI^*}+\frac{\beta_1 I^*}{2^{32}}+\frac{D(\cdot)\beta_2 M_I^*}{N}\\&\quad+\mu_1+\frac{D(\cdot)\beta_2 I^*}{N}+\delta_2\frac{N-I^*}{N}+\mu_2,\\H_2&=a_{11}^2a_{22}+a_{11}^2a_{33}+a_{11}a_{22}^2+a_{22}^2a_{33}+a_{11}a_{33}^2\\&\quad+a_{22}a_{33}^2+2a_{11}a_{22}a_{33}-a_{11}a_{12}a_{21}\\&\quad-a_{11}a_{13}a_{31}-a_{12}a_{21}a_{22}-a_{13}a_{31}a_{33}\\&>(a_{11}a_{33}-a_{13}a_{31})(a_{11}+a_{33})\\&>\Bigg[\left(-\frac{\beta_1(N-I^*-R^*)}{2^{32}}+\delta_1+\mu_1\right)\\&\qquad\times\left(\frac{\delta_2(N-I^*)}{N}+\mu_2\right)\\&\qquad-\frac{D(\cdot)\beta_2(N-I^*-R^*)}{N}\\&\qquad\times\left(\frac{D(\cdot)\beta_2(M-M_I^*)}{N}+\frac{\delta_2 M_I^*}{N}\right)\Bigg](a_{11}+a_{33})\\&=\left(-\frac{\beta_1(N-I^*-R^*)I^*}{2^{32}}+\delta_1 I^*+\mu_1 I^*\right.\\&\qquad\left.-\frac{D(\cdot)\beta_2(N-I^*-R^*)M_I^*}{N}\right)\left(\delta_2\frac{N-I^*}{NI^*}+\frac{\mu_2}{I^*}\right)\\&=0,\\H_3&=(a_{11}a_{22}a_{33}-a_{12}a_{21}a_{33}-a_{13}a_{31}a_{22})H_2\\&>(a_{11}a_{33}-a_{13}a_{31})a_{22}H_2\\&>0.\end{aligned} \quad (10)$$

If $R_0 > 1$, we have $H_1 > 0$, $H_2 > 0$, and $H_3 > 0$ and then all eigenvalues of (9) have negative real parts. Thus, there exists an endemic equilibrium E^* and it is asymptotically stable when $R_0 > 1$. The proof is completed. □

To validate the accuracy of Theorems 1 and 2, we used both deterministic method and stochastic method to simulate the system (3) with $N = 1000000$, $M = 400000$, $\mu_1 = \mu_2 = 0.00046$, and $\beta_2 = 0.098$ and two sets of other variables: (i) $\beta_1 = 0.24$, $\delta_1 = 0.05$, and $\delta_2 = 0.05$, where $R_0 \approx 5.98$; (ii) $\beta_1 = 0.05$, $\delta_1 = 0.1$, and $\delta_2 = 0.1$, where $R_0 \approx 0.85$.

As shown in Figure 1, when $R_0 > 1$, in both deterministic and stochastic simulations, the number of infected computers tends to the theoretical value predicted by (5a) finally, which indicates an endemic state E^*. However, in Figure 2, when $R_0 < 1$, the steady-state number of I is zero in accordance with the number predicted by disease-free state E_0.

4. Control Strategies

We first give the convergence proof of the numerical method, the improved Euler method, used in the simulation. Let $\mathbf{I} = (I, R, M_I)$. Then, we can rewrite the system (3) as $\dot{\mathbf{I}} = \mathbf{f}(t, \mathbf{I})$. Obviously, $\mathbf{f}$ is a continuous and differential function in R^4. Thus, $\mathbf{f}$ satisfies the Lipschitz condition and $\| f(t, \mathbf{I}^1) - f(t, \mathbf{I}^2)\| \leq L\|\mathbf{I}^1 - \mathbf{I}^2\|$, where L is a constant.

The Euler iteration equation is $\mathbf{I}_{n+1}^{(k+1)} = \mathbf{I}_n+(h/2)[\mathbf{f}(t_n, \mathbf{I}_n)+\mathbf{f}(t_{n+1}, \mathbf{I}_{n+1}^{(k)})]$ where $k = 0, 1, 2, \ldots$, $\mathbf{I}_{n+1}^{(0)} = \mathbf{I}_n + h\mathbf{f}(t_n, \mathbf{I}_n)$ and

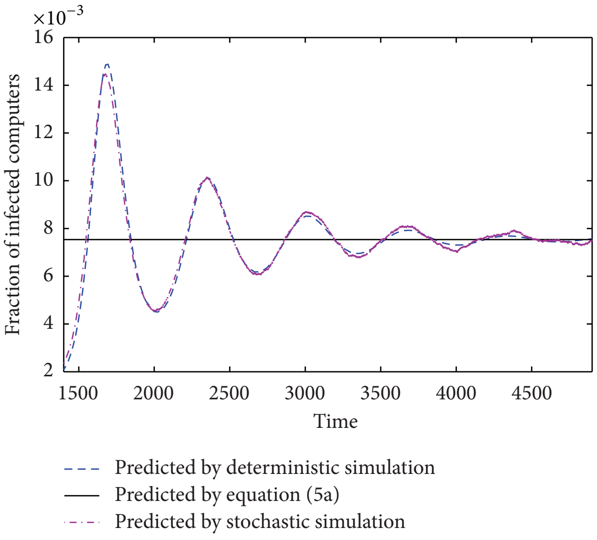


Figure 1: Fraction of infected computers when $R_0 > 1$. (a) Blue (dash line): deterministic simulation; (b) black (solid line): theoretical value; (c) purple (dot-dash line): stochastic simulation.

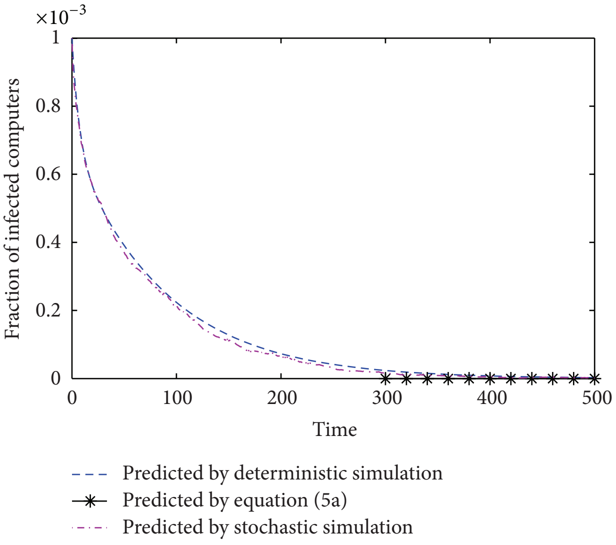


Figure 2: Fraction of infected computers when $R_0 < 1$. (a) Blue (dash line): deterministic simulation; (b) black (solid line): theoretical value; (c) purple (dot-dash line): stochastic simulation.

$n = 0, 1, 2, \ldots$. $h = t_{n+1} - t_n$, representing the step value in the Euler iteration algorithm. Then, we have

$$\begin{aligned}\left\|\mathbf{I}_{n+1}^{(k+1)} - \mathbf{I}_{n+1}^{(k)}\right\| &= \frac{h}{2}\left\|\mathbf{f}\left(t_{n+1}, \mathbf{I}_{n+1}^{(k)}\right) - \mathbf{f}\left(t_{n+1}, \mathbf{I}_{n+1}^{(k-1)}\right)\right\| \\ &\le \frac{hL}{2}\left\|\mathbf{I}_{n+1}^{(k)} - \mathbf{I}_{n+1}^{(k-1)}\right\| \\ &\le \left(\frac{hL}{2}\right)^2\left\|\mathbf{I}_{n+1}^{(k-1)} - \mathbf{I}_{n+1}^{(k-2)}\right\| \\ &\le \cdots \\ &\le \left(\frac{hL}{2}\right)^k\left\|\mathbf{I}_{n+1}^{(1)} - \mathbf{I}_{n+1}^{(0)}\right\|.\end{aligned} \tag{11}$$

Thus, the numerical technique used here is convergent as we can ensure that $hL/2 < 1$ by selecting a small value of h.

In this paper, we also use a Monte Carlo algorithm to simulate the propagation of malware [18, 19]. In all simulations given below, we set $N = M = 1000000$, $\mu_1 = \mu_2 = 0.00046$, $\beta_1 = 0.06$, $\beta_2 = 2$, $\delta_1 = 0.06$, $\delta_2 = 0.033$, $\alpha_2 = 0.0001$, and $\lambda_2 = 32$, where $\beta_1 \ll \beta_2$ because that malware such as Stuxnet is mainly spreading via removable devices to infect physically isolated machines. The initial numbers of I and M_I are set to 1000 and 0, respectively.

First, we compared three different models with the same parameters: homogeneous model presented in [9] where removable devices are assumed to be used with the same probability on all computers; heterogeneous model presented in [13] where the using rate of removable devices is divided into two rates (using rate on local computers and using rate on the other computers); and the model in this paper. We ran the simulation 100 times and got the average number of infected computers. Figure 3 shows the simulation results.

As shown in Figure 3, the model in this paper leads to the lowest infection rate and propagation speed. As it is established under the most reasonable assumptions among three models, its prediction is in accordance with the real propagation process to the most degree. The homogeneous model obtains the highest infection rate and the fastest propagation speed. Although the heterogeneity in removable devices' using rate is included in the model given in [13], this simplistic division of removable devices' using rate also leads to a great deviation.

We also simulated various α_1 and λ_1 to gain some insight into the containment of the malware considered in this paper. Figures 4(a) and 4(b) give the simulation results with fixed λ_1 and fixed α_1, respectively.

Figures 4(a) and 4(b) show that the radius of neighbour area (λ_1) and the using rate (α_1) in this area have great influences on the propagation of malware. The infection rate and speed decrease rapidly with the decrease of using rate (α_1) or neighbour area's radius (λ_1). In Figure 4(a) with fixed $\lambda_1(10)$, the malware dies out directly when $\alpha_1 = 0.05$, which means an effective countermalware method.

To get the effective countermalware thresholds under various values of λ_1, we further simulated the system (3) and got the values of α_1 below which the malware would die out. Figure 5 plots the simulation results.

As it is shown in Figure 5, the points in left area can guarantee the extinction of malware. However, the malware can self perpetuate in the right area. The threshold of α_1 decreases with the increase of λ_1 and this decrease is much faster in the area between two arrows ($\lambda_1^* < \lambda_1 < 5$). Furthermore, when the radius of neighbour area is less than two times of the radius of local area, corresponding to $\lambda_1 \le \lambda_1^*$ (=2), the malware will die out no matter what value α_1 is, which gives a promising countermalware threshold.

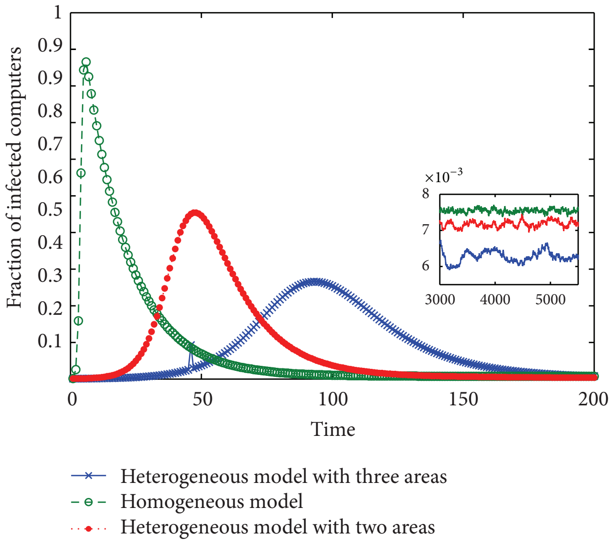


FIGURE 3: Fraction of infected computers based on the model in this paper (blue, heterogeneous model where three areas divided according to the removable device's using rate are considered) compared to the counterparts based on the model presented in [9] (green, homogeneous model) and in [13] (red, heterogeneous model where two areas are considered).

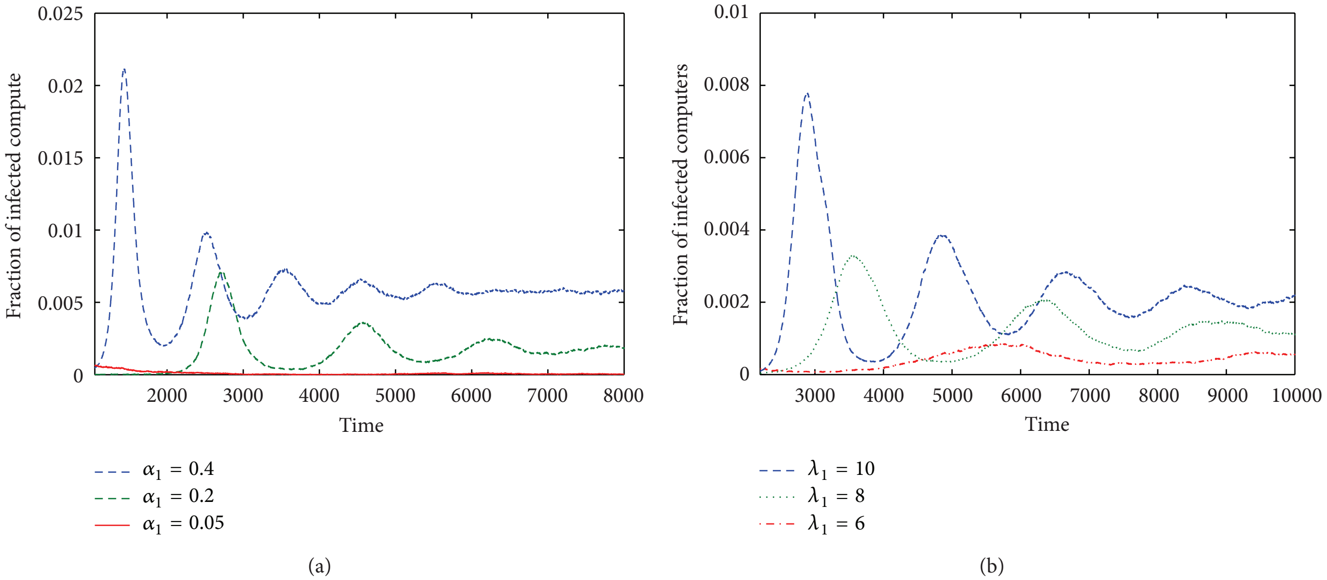


FIGURE 4: Fraction of infected computers based on model (3) with (a) $\alpha_1 = 0.4$ (blue), 0.2 (green), 0.05 (red), and $\lambda_1 = 10$; (b) $\lambda_1 = 10$ (blue), 8 (green), 6 (red), and $\alpha_1 = 0.2$. The other parameters are the same as in Figure 3.

5. Conclusion

Recently, the researches concerning malware have focused on those pieces malware spreading via removable devices [9–13]. Different from these researches, we present a model with a detailed depiction of the heterogeneity in removable devices' using rate. This consideration of heterogeneity can lead to an effective countermalware method by controlling the removable devices' using rate in neighbour area. Furthermore, when $\alpha_1 = \alpha_2 = 1$, the model presented in this paper corresponds to the model given in [9, 12]; when $\alpha_1 = \alpha_2 < 1$, it corresponds to the model given in [13]. Thus, the model in this paper is a more general model and can depict the malware's spreading process more precisely.

Mathematical analysis and stochastic simulations indicate that the dynamics are determined by the value of R_0. Simulation results have also shown that removable devices' using rate and the radius of neighbour area have great influences on the dynamics of malware. Specifically, we have obtained the thresholds of removable devices' using rate (α_1)

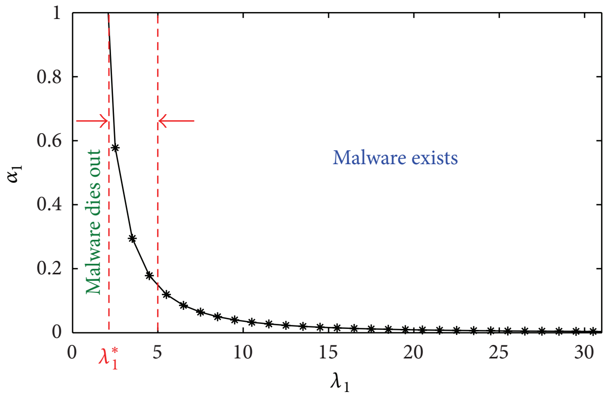


Figure 5: The relationship between α_1 and λ_1 under the phase transition condition where $\mu_1 = 0.00046$, $\mu_2 = 0.00046$, $\beta_1 = 0.06$, $\beta_2 = 2$, $\delta_1 = 0.06$, $\delta_2 = 0.033$, $\alpha_2 = 0.0001$, and $\lambda_2 = 32$.

when different values of λ_1 (the radius of neighbour area) are considered, which can guide us in designing effective countermalware method.

In the future, we plan to use real trace data to test our model, especially the special value of removable devices' using area (λ_1^*) and then get the most effective policy to help people in defending their devices and machines against malware.

Conflict of Interests

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

Acknowledgment

This work is supported by the National Natural Science Foundation of China (61379125, 61379080 and 11201434), Program for Basic Research of Shan'xi province (2012011015-3).

References

[1] C. C. Zou, D. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp. 106–118, 2007.

[2] Y. Li, J. X. Pan, and Z. Jin, "Dynamic modeling and analysis of the email virus propagation," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 472072, 22 pages, 2012.

[3] B. K. Mishra and S. K. Pandey, "Effect of anti-virus software on infectious nodes in computer network: a mathematical model," *Physics Letters A*, vol. 376, no. 35, pp. 2389–2393, 2012.

[4] L. P. Song, Z. Jin, and G. Q. Sun, "Modeling and analyzing of botnet interactions," *Physica A*, vol. 390, no. 2, pp. 347–358, 2010.

[5] L. Yang, X. Yang, J. Liu, Q. Zhu, and C. Gan, "Epidemics of computer viruses: a complex-network approach," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8705–8717, 2013.

[6] Symantec Security Response, http://www.symantec.com/connect/blogs/w32stuxnet-dossier.

[7] Kaspersky Security Bulletin, "Monthly Malware Statistics," February 2012, http://www.securelist.com/en/analysis/204792223.

[8] Flame (malware), http://en.wikipedia.org/wiki/Flame_(malware).

[9] L. P. Song, Z. Jin, G. Q. Sun, J. Zhang, and X. Han, "Influence of removable devices on computer worms: dynamic analysis and control strategies," *Computers & Mathematics with Applications*, vol. 61, no. 7, pp. 1823–1829, 2011.

[10] C. Jin and X. Y. Wang, "Analysis and control stratagems of flash disk virus dynamic propagation model," *Security and Communication Networks*, vol. 5, no. 2, pp. 226–235, 2012.

[11] L. X. Yang and X. Yang, "The spread of computer viruses under the influence of removable storage devices," *Applied Mathematics and Computation*, vol. 219, no. 8, pp. 3914–3922, 2012.

[12] Q. Zhu, X. Yang, and J. Ren, "Modeling and analysis of the spread of computer virus," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 5117–5124, 2012.

[13] Z. Z. Peng, L. P. Song, G. H. Li, and Y. H. Li, "Modeling and analyzing the spread of FlashDisk worms via multiple subnets," *International Journal of Computer Mathemati*. In press.

[14] J. D. Murray, *Mathematical Biology*, Springer, Berlin, Germany, 2003.

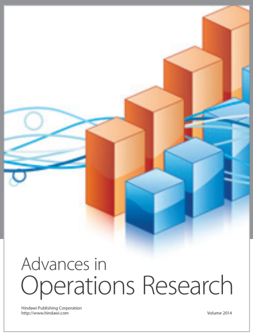
[15] R. M. Anderson, R. M. May, and B. Anderson, *Infectious Diseases in Humans: Dynamics and Control*, Oxford University Press, New York, NY, USA, 1991.

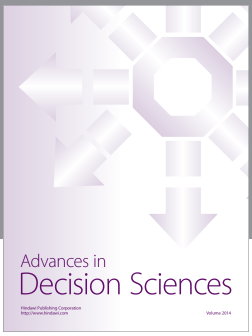
[16] E. A. Barbashin, *Introduction to the Theory of Stability*, Wolters-Noordhoff, Groningen, Netherlands, 1970.

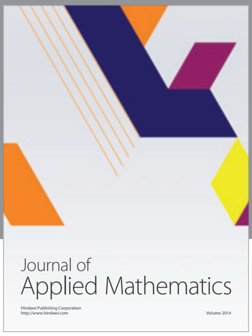
[17] J. P. LaSalle and S. Lefschetz, *Stability by Liapunov's Direct Method, with Applications*, Academic Press, New York, NY, USA, 1961.

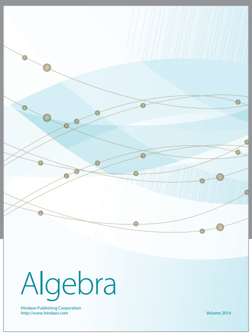
[18] D. T. Gillespie, "Exact stochastic simulation of coupled chemical reactions," *Journal of Physical Chemistry*, vol. 81, no. 25, pp. 2340–2361, 1977.

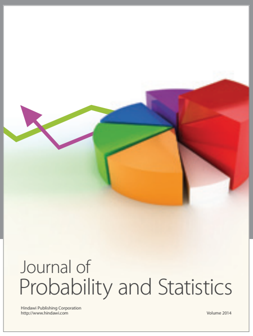
[19] D. Arnaud, F. Nando de, and G. Neil, Eds., *Sequential Monte Carlo Methods in Practice*, Springer, New York, NY, USA, 2001.











Hindawi

Submit your manuscripts at
http://www.hindawi.com