Applied Mathematical Modelling 37 (2013) 8225–8236

Contents lists available at SciVerse ScienceDirect

Applied Mathematical Modelling

journal homepage: www.elsevier.com/locate/apm

Dynamical analysis and control strategies on malware propagation model

Liping Feng [a,b,*], Xiaofeng Liao [a], Qi Han [c], Huaqing Li [a]

[a] State Key Lab. of Power Transmission Equipment and System Security, College of Computer Science, Chongqing University, Chongqing 400044, China
[b] Department of Computer Science and Technology of Xinzhou Normal University, Xinzhou, ShanXi 034000, China
[c] School of Electrical and Information Engineering, Chongqing University of Science and Technology, Chongqing 401331, China

ARTICLE INFO

Article history:
Received 6 March 2012
Received in revised form 17 March 2013
Accepted 25 March 2013
Available online 3 April 2013

Keywords:
Malware
Epidemic model
Time delay
Hopf bifurcation
Stability

ABSTRACT

A variable infection rate is more realistic to forecast dynamical behaviors of malware (malicious software) propagation. In this paper, we propose a time-delayed *SIRS* model by introducing temporal immunity and the variable infection rate. The basic reproductive number R_0 which determines whether malware dies out is obtained. Furthermore, using time delay as a bifurcation parameter, some necessary and sufficient conditions ensuring Hopf bifurcation to occur for this model are derived. Finally, numerical simulations verify the correctness of theoretical results. Most important of all, we investigate the effect of the variable infection rate on the scale of malware prevalence and compare our model with stationary analytical model by simulation. According to simulating results, some strategies that control malware rampant are given, which may be incorporated into cost-effective antivirus policies for organizations to work quite well in practice.

1. Introduction

For all kinds of malicious programs which propagate on Internet, malware is a generic term including spyware, worms, Trojan horses, viruses etc. [1]. Since its first prevalence from several decades ago, the spread of malware has been accounting for an important share of financial losses in the field of computer security [2]. And, with widespread application of information technology (IT) in all walks of life, the threat of malware has become an increasing major issue of concern. It is thus imperative to understand in depth how malware spread for constraining effectively its rampant.

To this goal, based on the existing mathematical modeling and epidemic threshold theories [3,4], Kephart et al. [5] analyzed and predicted the dynamical features of computer virus propagation in different network topologies. Then, Kephart et al. [6] further improved their model by adding the effect of the "kill signal" idea on virus prevalence. In [7], Billings et al. predicted the long and short actions of computer virus spread by constructing a continuous *SIS* (susceptible-infected-susceptible) model and a discrete-time Markov chain dynamical system, respectively. These works lay a good foundation for later computer epidemiology. Zou et al. mainly focused their attentions on the dynamics of worm propagation [8–11]. Recently, based on the classical Kermack–Mckendrick model [12,13], a lot of malware propagation models with or without time delays [14–19] have been developed, which are all deterministic models and are effective on reflecting the prevalence of malware in homogenous computer networks. From a different perspective, Chen et al. performed a thorough study on the propagation of topological malware [20]. The authors proposed the spatial–temporal model to investigate the propagation of

* Corresponding author at: State Key Lab. of Power Transmission Equipment and System Security, College of Computer Science, Chongqing University, Chongqing 400044, China.
E-mail address: fenglp@yeah.net (L. Feng).

0307-904X/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.apm.2013.03.051

topological malware that take different scanning measures. Their results provide wide insight for modeling malware propagation and taking effective countermeasures. The authors in [21] investigate explicitly the information dissemination among mobile nodes for context awareness in a way similar to virus spreading. The key result of this study is multiepidemic S_aIS model is efficient for analyzing multiepidemic-based context dissemination. This modeling approach can help us to understand a wide range of malware propagation behavior on Internet.

It is worth noting that the above-mentioned works on malware modeling assume that the infection rate is a constant. In the existing epidemic modeling fields, only a handful work has been done on a variable infection rate. For instance, the work in [22] derived a two-factor model to characterize Code Red worm propagation. The experimental results show that the two-factor model matches better with observed Code Red worm data than simple epidemic model. This demonstrates the mathematical model with a variable infection rate is more accurate to reflect malware propagation. In fact, the large-scale worm propagation or other some unknown causes always lead to network congestion and trouble to some Internet routers [23–25], thus slow down worm scanning process. We therefore present a malware propagation model with variable infection rate, motivated by the work [22] and the reports in [23,25].

The remainder of this paper is organized as follows. In Section 2, modeling approach is described explicitly. In Sections 3, we investigate the existence of equilibria and analyze their dynamical behaviors. Mathematical results are illustrated by numerical simulations and some control strategies are given in Section 4. Finally, we summarize our work and propose the future focuses.

2. Modeling malware propagation

This section describes the model of malware propagation with a variable infection rate. Our goal is trying to create a realistic model which can provide wide insight into predicting malware prevalence in networks.

To model the propagation of malware throughout Internet, we assume that the total number of nodes (end-hosts, routers or servers) in the network is $N(t)$ at time t. Each node changes over time among three states: susceptible (S), infected (I) and recovered (R) due to the spread of malware. We describe these three states in details as follows.

(1) Susceptible (S): A node has the software vulnerability that the malware can exploit.
(2) Infected (I): A node is infected by malware, which means the node can infect its neighbors with this malware, and the malware has not been moved from the node.
(3) Removed (R): A node has installed a detection tool that can identify and remove a malware, or a node has installed a software patch to eliminate the node vulnerability exploited by a malware.

There are four state transitions among these three states.

(1) Propagating malware: nodes in the "susceptible" state will change to the "infected" state with the infection rate $\beta(t)$. An infection rate is affected by many factors. For example, for worms, the factors include the number of susceptible nodes, payload scale of malware copy, exploited node vulnerability, network congestion. For e-mail virus, the factors include the size of an e-mail address book, user awareness to an e-mail attachment [20].
(2) Immunizing nodes from susceptible state: nodes in the "susceptible" state will change to the "recovered" state at the proportion φ if corresponding nodes take countermeasures e.g., antivirus software, patching, firewall, intrusion detection system (IDS). The immune rate is affected by many factors, for example, user vigilance, the ability of malware to disguise and the performance of IDS [20].
(3) Immunizing nodes from infected state: nodes in the "infected" state will change to the "recovered" state at the proportion γ if corresponding nodes take antivirus countermeasures.
(4) Re-infecting nodes from recovered state: nodes in the "recovered" state will change to the "susceptible" states at the propagation δ after some time τ due to updates of virus-bases, reinstalling operating system etc.

Let $S(t)$, $I(t)$, $R(t)$ be the number of nodes in states S, I, R at time t, respectively, then at any time t, we have

$$S(t) + I(t) + R(t) = N(t). \tag{1}$$

Moreover, we believe the total number of nodes is changing, i.e., at any time, some nodes might die out at the proportion μ for encountering an unexpected network error, and meanwhile some new nodes may recruit. This assumption is suitable in practice, and consistent with other existing efforts [26–28].

From the above description, our model can be represented as a flow chart (see Fig. 1) or as a set of coupled differential equations (ODES) as follows.

$$\begin{cases} \frac{dS}{dt} = p\Lambda - \beta(t)I(t)S(t) - (\mu+\varphi)S(t) + \delta R(t-\tau), \\ \frac{dI}{dt} = \beta(t)I(t)S(t) - (\mu+\gamma)I(t), \\ \frac{dR}{dt} = (1-p)\Lambda + \varphi S(t) + \gamma I(t) - \delta R(t-\tau) - \mu R(t). \end{cases} \tag{2}$$

For clarity, we list the meanings of parameters of model (2) in Table 1.

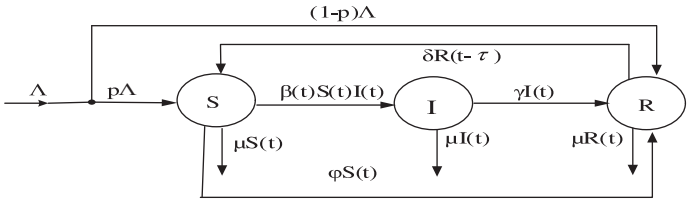

Fig. 1. Flow diagram for the SIRS model. The ODE formulation of this model is given by system (2).

Table 1
Symbols and their meanings of model 2.

Parameters	Notes
p	The susceptible rate of new nodes
Λ	The number of the new nodes
δ	The loss rate of immunity of the recovered nodes
$\beta(t)$	The infection rate at time t
μ	The replacement rate of the nodes
φ	The real-time immune rate of antivirus strategies
γ	The recovered rate of infected nodes

In the following, we will discuss the expression of $\beta(t)$. $\beta(t)$ is determined by the spreading efficiency of the malware on Internet infrastructure and human antivirus countermeasures. When malware outbreaks, the number of infected hosts will reach its maximum value in a short time, then will decrease because of network congestion, antivirus software, patching, upgrading susceptible hosts, setting up firewalls and disconnecting networks and so on. So, we can reflect the change of $\beta(t)$ with time t by the change of contact rate between I and S. Let β_0 express the initial infection rate, we model the infection rate $\beta(t)$ by the following equation:

$$\beta(t) = \beta_0 f_1(I(t)), \tag{3}$$

where f_1 is a nonlinear function of I. Let $f(I(t)) = f_1(I(t))I(t)$, Hence, system (2) can be rewritten as follows:

$$\begin{cases} \frac{dS}{dt} = p\Lambda - \beta_0 f(I(t))S(t) - (\mu+\varphi)S(t) + \delta R(t-\tau), \\ \frac{dI}{dt} = \beta_0 f(I(t))S(t) - (\mu+\gamma)I(t), \\ \frac{dR}{dt} = (1-p)\Lambda + \varphi S(t) + \gamma I(t) - \delta R(t-\tau) - \mu R(t), \end{cases} \tag{4}$$

where τ is the temporary immune period, and the function $f(I)$ is assumed to have the following properties [27]:

(H1) $f_1(I) \neq 0$,

(H2) $f_1'(I) < 0$,

(H3) $\lim_{t\to\infty} f(I) = C < +\infty$.

In particular, if the function $f_1(I) \equiv C$ (C is a constant), then the system (4) becomes a stationary *SIRS* model w. r. t the infection rate (i.e., the case that β is constant).

The system (4) has the following initial conditions:

$$\begin{aligned} &S(t) \geqslant 0, t \in [0,\infty), \\ &I(t) \geqslant 0, t \in [0,\infty), \\ &R(t) \geqslant 0, t \in [-\tau,\infty). \end{aligned} \tag{5}$$

Summing up the three equations of system (4), one can obtain the following equation

$$\frac{dN(t)}{dt} = \Lambda - \mu N(t). \tag{6}$$

Hence, solutions of system (4) need to satisfy the following condition:

$$S(t) + I(t) + R(t) \leqslant \frac{\Lambda}{\mu}. \tag{7}$$

It is easy to verify that the positive cone R^3_+ is a positive invariant set with respect to system (4), where $R^3_+ = \{(S,I,R) \in R^3 : S > 0, I > 0, R > 0\}$. Moreover, the feasible solutions of system (4) are bounded and enter the region D, where

$$D = \left\{ (S,I,R) \in R^3 : S > 0, I > 0, R > 0, S + I + R \leqslant \frac{\Lambda}{\mu} \right\}. \tag{8}$$

3. Mathematical analysis for equilibria

Explicit mathematical analysis can provide good theoretical foundation for predicting malware propagation. In this section, we will find the equilibria of system (4) and investigate their dynamical features.

Define

$$R_0 = \frac{\beta_0 \Lambda (p\mu + \delta) f'(0)}{\mu(\mu+\gamma)(\mu+\delta+\varphi)}. \tag{9}$$

Then the following conclusion holds.

Theorem 1. *If $R_0 \leqslant 1$, then system (4) has only a virus-free equilibrium E_0; if $R_0 > 1$, then system (4) has a virus-epidemic equilibrium $E_1^* = (S_1^*, I_1^*, R_1^*)$ besides E_0^*, where*

$$E_0^* = (S_0^*, I_0^*, R_0^*) = \left(\frac{(p\mu+\delta)\Lambda}{\mu(\mu+\delta+\varphi)}, 0, \frac{(1-p)\Lambda + \varphi S_0^*}{\delta+\mu} \right).$$

(*The* proof is given in Appendix A).

3.1. Virus-free equilibrium and its stability

The characteristic equation of system (4) at E_0^* is:

$$\det \begin{pmatrix} -\beta_0 f(0) - (\mu+\varphi) - \lambda & -\beta_0 S_0^* f'(0) & \delta e^{-\lambda\tau} \\ \beta_0 f(0) & \beta_0 S_0^* f'(0) - (\mu+\gamma) - \lambda & 0 \\ \varphi & \gamma - & \delta e^{-\lambda\tau} - \mu - \lambda \end{pmatrix} = 0,$$

which is equivalent to

$$\left[\beta_0 S_0^* f'(0) - (\mu+\gamma) - \lambda\right]\left(\lambda^2 + (2\mu+\varphi)\lambda + \mu(\mu+\varphi) + \delta(\lambda+\mu)e^{-\lambda\tau}\right) = 0. \tag{10}$$

Eq. (10) has a characteristic root $\lambda_1 = \beta S_0^* f'(0) - (\mu+\gamma) \equiv \frac{\beta_0\Lambda(p\mu+\delta)f'(0) - \mu(\mu+\gamma)(\mu+\delta+\varphi)}{\mu(\mu+\delta+\varphi)}$ and the roots of the equation

$$\lambda^2 + (2\mu+\varphi)\lambda + \mu(\mu+\varphi) + \delta(\lambda+\mu)e^{-\lambda\tau} = 0. \tag{11}$$

Combining Eq. (9), λ_1 can be rewritten as $\lambda_1 = (\mu+\gamma)(R_0 - 1)$. Obviously, if $R_0 > 1$, then $\lambda_1 > 0$; and if $R_0 < 1$, then $\lambda_1 < 0$.

Next, we focus on the sign of the roots of Eq. (11). Let

$$f(\lambda, \tau) = \lambda^2 + (2\mu+\varphi)\lambda + \mu(\mu+\varphi) + \delta(\lambda+\mu)e^{-\lambda\tau} = 0. \tag{12}$$

For $\tau = 0$, one can get

$$f(\lambda, 0) = \lambda^2 + (2\mu+\varphi+\delta)\lambda + \mu(\mu+\varphi+\delta) = 0. \tag{13}$$

Obviously, in accordance with the relationship between roots and coefficients of quadratic equation, there is no positive real part characteristic root of Eq. (13).

For $\tau > 0$, let $\lambda = i\omega, (\omega > 0)$. Rewrite Eq. (12) according to real parts and imaginary parts as

$$\begin{cases} -\omega^2 + \mu(\mu+\varphi) + \delta[\mu\cos(\omega\tau) + \omega\sin(\omega\tau)] = 0, \\ \omega(2\mu+\varphi) + \delta[\omega\cos(\omega\tau) - \mu\sin(\omega\tau)] = 0. \end{cases} \tag{14}$$

Furthermore, solving Eq. (14), one can get

$$\omega^4 + \left[(\mu+\varphi)^2 + \mu^2 - \delta^2\right]\omega^2 + [\mu(\mu+\varphi) + \delta][\mu(\mu+\varphi) - \delta] = 0. \tag{15}$$

Let $m = (\mu+\varphi)^2 + \mu^2 - \delta^2$ and $n = \mu(\mu+\varphi) - \delta$. Then, when $m > 0$and $n > 0$, Eq. (15) has no positive real part characteristic roots. Hence, the following Lemma holds.

Lemma 1. *If $R_0 < 1$, $m > 0$ and $n > 0$, then the virus-free equilibrium E_0^* of system (4) is locally asymptotically stable; if $R_0 > 1$, then the virus-free equilibrium E_0^* of system (4) is unstable.*

In what follows, we discuss the global stability of the free-equilibrium E_0^* of system (4).

Lemma 2. *When $R_0 \leqslant 1$, the solutions of system (4) satisfy $(S(t), I(t), R(t)) \to \left(\frac{(p\mu+\delta)\Lambda}{\mu(\mu+\delta+\varphi)}, 0, \frac{(1-p)\Lambda+\varphi S_0^*}{\delta+\mu}\right)$ as $t \to \infty$.*

(The proof is completed in Appendix B).

Combining Lemma 1 with Lemma 2, we can conclude the following theorem.

Theorem 2. *If Lemma 1 holds, then the virus-free equilibrium E_0^* of system (4) is globally asymptotically stable for any time delay τ. Otherwise, if $R_0 > 1$, then the virus-free equilibrium E_0^* of system (4) is unstable for any time delay τ.*

3.2. Endemic-equilibrium and dynamical properties

In this subsection, using time delay as the bifurcation parameter, we investigate the Hopf bifurcation for system (4). The Jacobian matrix of system (4) at E_1^* is

$$J(E_1^*) = \begin{pmatrix} -\beta_0 f(I_1) - (\mu+\varphi) & -\beta_0 S_1^* f'(I_1) & \delta e^{-\lambda\tau} \\ \beta_0 f(I_1) & \beta_0 S_1^* f'(I_1) - (\mu+\gamma) & 0 \\ \varphi & \gamma & -\mu - \delta e^{-\lambda\tau} \end{pmatrix}.$$

The corresponding characteristic equation of $J(E_1^*)$ can be described as

$$\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 + (a_4\lambda^2 + a_5\lambda + a_6)e^{-\lambda\tau} = 0, \tag{16}$$

where

$$\begin{aligned} a_1 &= \beta f(I_1) + 3\mu + \varphi + \gamma - \beta S_1 f'(I_1), \\ a_2 &= 3\mu^2 + 2\varphi\mu + 2\gamma\mu + \varphi\gamma + \beta(2\mu+\gamma)f(I_1) - 2\beta S_1(\mu+\varphi)f'(I_1), \\ a_3 &= \mu[\beta(\mu+\gamma)f(I_1) + (\mu+\varphi)(\mu+\gamma) - \beta S_1(\mu+\varphi)f'(I_1)], \\ a_4 &= \delta, \\ a_5 &= \delta[\beta f(I_1) + 2\mu + \gamma - \beta S_1 f'(I_1)], \\ a_6 &= \delta[\beta\mu f(I_1) + \mu(\mu+\gamma) - \beta\mu S_1 f'(I_1)]. \end{aligned}$$

When $\tau = 0$, Eq. (16) reduces to

$$\lambda^3 + b_1\lambda^2 + b_2\lambda + b_3 = 0, \tag{17}$$

where $b_1 = a_1 + a_4$, $b_2 = a_2 + a_5$, $b_3 = a_3 + a_6$. By the Routh–Hurwitz criteria, all roots of Eq. (17) have negative real parts if and only if $b_i > 0$, $(i = 1, 2, 3)$ and $A > 0$, where

$$A = \begin{vmatrix} b_1 & 1 \\ b_3 & b_2 \end{vmatrix}$$

So, we can reach the following Lemma.

Lemma 3. *If virus-endemic equilibrium E_1^* exists, then it is locally asymptotically stable when $\tau = 0$ and $b_i > 0$, $(i = 1, 2, 3)$, $A > 0$. When $\tau > 0$, assume $\lambda = v + i\omega (v, \omega \in R)$ and rewrite* Eq. (16) *according to its real and imaginary parts as*

$$\begin{cases} v^3 - 3\omega^2 v + a_1(v^2 - \omega^2) + a_2 v + a_3 + [a_4(v^2 - \omega^2) + a_5 v + a_6]e^{-v\tau}\cos\omega\tau + (2a_4 v\omega + a_5\omega)e^{-v\tau}\sin\omega\tau = 0, \\ 3v^2\omega - \omega^3 + 2a_1 v\omega + a_2\omega + (2a_4 v\omega + a_5\omega)e^{-v\tau}\cos\omega\tau - [a_4(v^2 - \omega^2) + a_5 v + a_6]e^{-v\tau}\sin\omega\tau = 0. \end{cases} \tag{18}$$

Let τ_0 be such that $v(\tau_0) = 0$, then Eq. (18) *is reduced to*

$$\begin{cases} -a_1\omega_0^2 + a_3 + (-a_4\omega_0^2 + a_6)\cos(\omega_0\tau_0) + a_5\omega_0\sin(\omega_0\tau_0) = 0, \\ -\omega_0^3 + a_2\omega_0 + a_5\omega_0\cos(\omega_0\tau_0) + (a_4\omega_0^2 - a_6)\sin(\omega_0\tau_0) = 0. \end{cases} \tag{19}$$

By squaring and adding, it follows that

$$\omega_0^6 + c_1\omega_0^4 + c_2\omega_0^2 + c_3 = 0, \tag{20}$$

where $c_1 = a_1^2 - 2a_2 - a_4^2$, $c_2 = a_2^2 - 2a_1a_3 - a_5^2 + 2a_4a_6$, $c_3 = a_3^2 - a_6^2$. Let $z = \omega_0^2$ and rewrite Eq. (20) as

$$z^3 + c_1 z^2 + c_2 z + c_3 = 0. \tag{21}$$

Denote

$$h(z) = z^3 + c_1 z^2 + c_2 z + c3.$$

Since $\lim_{z\to\infty} h(z) = +\infty$, *then* Eq. (21) *at least has a positive real root when* $c_3 < 0$.*Suppose*

$(H4) c_3 < 0$.

In the following, we will discuss the distributions of the positive roots of Eq. (21).

Lemma 4. *Define*

$$\Delta = \frac{4}{27}c_2^3 - \frac{1}{27}c_1^2 c_2^2 + \frac{4}{27}c_1^3 c_3 - \frac{2}{3}c_1 c_2 c_3 + c_3^2.$$

Then, the necessary and sufficient conditions for Eq. (21) *to have one simple positive real root for z are*

(i) either $c_1 > 0, c_2 \geqslant 0$ and $c_1^2 > 3c_2$, or$c_2 < 0$; and
(ii) $\Delta < 0$.

(The proof is given in Appendix C)

Assuming that z_0 is a positive root of Eq. (21), then Eq. (20) has one positive root $\omega_0 > \sqrt{z_0}$. It follows from Eq. (19) that

$$\cos(\omega_0\tau_0) = \frac{e_1 e_4 + e_2 e_3}{e_3^2 + e_4^2},$$

where $e_1 = a_1\omega_0^2 - a_3, e_2 = \omega_0^3 - a_2\omega_0, e_3 = a_5\omega_0, e_4 = a_6 - a_4\omega_0^2$.

Therefore

$$\tau_0^j = \frac{1}{\omega_0}\left[\arccos\left(\frac{e_1 e_4 + e_2 e_3}{e_3^2 + e_4^2}\right)\right], \quad j = 0, 1, 2, \ldots.$$

Then $\pm i\omega_0$ is a pair of purely imaginary roots of Eq. (16) with τ_0^j. Define

$$\tau_0 = \min\{\tau_0^j\}. \tag{22}$$

Further, we need to verify the transversality condition

$$\left.\frac{d\mathrm{Re}(\lambda(\tau))}{d\tau}\right|_{\tau=\tau_0} \neq 0. \tag{23}$$

Taking the derivative of λ with respect to τ in Eq. (14), it is easy to obtain:

$$(3\lambda^2 + 2a_1\lambda + a_2)\frac{d\lambda}{d\tau} + (2a_4\lambda + a_5)e^{-\lambda\tau}\frac{d\lambda}{d\tau} + (a_4\lambda^2 + a_5\lambda + a_6)e^{-\lambda\tau}\left(-\tau\frac{d\lambda}{d\tau} - \lambda\right) = 0.$$

It follows that:

$$\frac{d\lambda}{d\tau} = \frac{(a_4\lambda^2 + a_5\lambda + a_6)e^{-\lambda\tau}\lambda}{3\lambda^2 + 2a_1\lambda + a_2 + \left[2a_4\lambda + a_5 - \tau(a_4\lambda^2 + a_5\lambda + a_6)\right]e^{-\lambda\tau}}. \tag{24}$$

Let $\lambda(\tau) = v(\tau) + i\omega(\tau)$ be the root of Eq. (13) satisfying $v(\tau_0) = 0$, $\omega(\tau_0) = \omega_0$. Then Eq. (18) can be rewritten as

$$\left.\frac{d\lambda}{d\tau}\right|_{\tau=\tau_0} = \frac{d_1 + id_2}{d_3 + id_4},$$

where

$$\begin{aligned}
d_1 &= \omega_0(a_6\sin\omega_0\tau_0 - a_5\omega_0\cos\omega_0\tau_0 - a_4\omega_0^2\sin\omega_0\tau_0),\\
d_2 &= \omega_0(a_6\cos\omega_0\tau_0 + a_5\omega_0\sin\omega_0\tau_0 - a_4\omega_0^2\cos\omega_0\tau_0),\\
d_3 &= 2a_4\omega_0\sin\omega_0\tau_0 + a_5\cos\omega_0\tau_0 - \tau(a_6 - a_4\omega_0^2)\cos\omega_0\tau_0 - \tau a_5\omega_0\sin\omega_0\tau_0,\\
d_4 &= 2a_4\omega_0\cos\omega_0\tau_0 - a_5\sin\omega_0\tau_0 - \tau a_5\omega_0\cos\omega_0\tau_0 + \tau(a_6 - a_4\omega_0^2)\sin\omega_0\tau_0.
\end{aligned}$$

Therefore

$$\left.\frac{d\mathrm{Re}(\lambda(\tau))}{d\tau}\right|_{\tau=\tau_0} = \frac{d_1 d_3 - d_2 d_4}{d_3^2 + d_4^2}.$$

In order to obtain the main results in this paper, we make the following assumption:

$$(\mathrm{H5})\left.\frac{d\mathrm{Re}(\lambda(\tau))}{d\tau}\right|_{\tau=\tau_0} \neq 0.$$

By using Ref. [29] and summarizing the above discussions, we have the following theorem.

Theorem 3. *Suppose that* Lemmas 3 and 4, H(4) *and* H(5) *are satisfied, by combing* Ref. [29], *the following results hold: when* $\tau < \tau_0$, *the virus-endemic equilibrium* E_1^* *of system* (4) *is locally asymptotically stable, and unstable when* $\tau > \tau_0$, *as well as system* (4) *undergoes a Hopf bifurcation at the virus-endemic equilibrium* E_1^* *when* $\tau = \tau_0$.

4. Numerical analysis and control strategies

4.1. Numerical examples

System (4) is a general malware model with an undetermined dynamic parameter $f(I(t))$. To verify the correctness of Theorems 2 and 3, first we need to determine the dynamical equation describing $f(I(t))$. Choosing nonlinear function $f_1(I(t)) = \frac{1}{1+\alpha I(t)}$, we have $f(I(t)) = \frac{I(t)}{1+\alpha I(t)}$, where α is used to adjust the infection rate sensitivity to the number of infected nodes $I(t)$. $\alpha = 0$ means the constant infection rate.

In what follows, we verify Theorems 2 and 3 by choosing other parameter values in system (4).

(i) For the parameter $\Lambda = 0.8$, $\mu = 0.1$, $p = 0.5$, $\gamma = 0.2$, $\beta_0 = 0.02$, $\varphi = 0.2$, $\delta = 0.01$, $\alpha = 1$. By calculation, we have $R_0 = 0.1032 < 1$, $m = 0.0999$, $n = 0.02$. The corresponding waveform is shown in Fig. 2. From Fig. 2, we can see that malware will die out after some time. The conclusion agrees with Theorem 2.

(ii) For the parameters $\Lambda = 1$, $\mu = 0.3$, $p = 0.9$, $\gamma = 0.2$, $\beta_0 = 0.8$, $\varphi = 0.46$, $\delta = 0.7$, $\alpha = 1$. By calculation, we have $R_0 = 3.5434 > 1, b_1 = 2.4405, b_2 = 1.4173, b_3 = 0.2654, A = 3.1935, c_3 = -0.0054$, $\Delta = -0.0034$, $c_2 = -0.1633$ and $\tau_0 = 10.03$. We depict the dynamical behavior of the virus-endemic equilibrium E_1^* of system (4) at $\tau = 7.3$ and $\tau = 10.3$ in Figs. 3 and 4, respectively. Fig. 3 shows that the trajectory converges to the virus-endemic equilibrium when $\tau = 7.3 < \tau_0$. Fig. 4 shows that system (4) has periodic solutions when $\tau = \tau_0 = 10.3$. The conclusion agrees with Theorem 3.

From the conclusion of Theorems 2 and 3, we learn out that it is necessary for eliminating malware prevalence in networks to make $R_0 < 1$ by corresponding antivirus measures.

For the purpose of comparison, we plot the Fig. 5 (for parameters $\Lambda = 1$, $\mu = 0.3$, $p = 0.9$, $\gamma = 0.2$, $\beta_0 = 0.8$, $\phi = 0.46$, $\delta = 0.7$). Comparing simulating curve of our model ($\alpha = 1$) with the simulation curve of stationary SIRS model ($\alpha = 0$), we observe that the scale of malware spreading predicted by our model infection is much smaller than the scale predicted by stationary SIRS

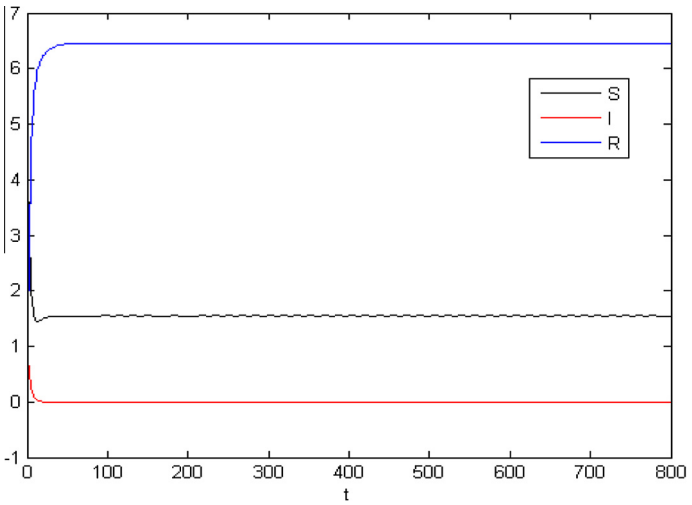

Fig. 2. The waveform plot of malware propagation results with $R_0 = 0.1032 < 1$.

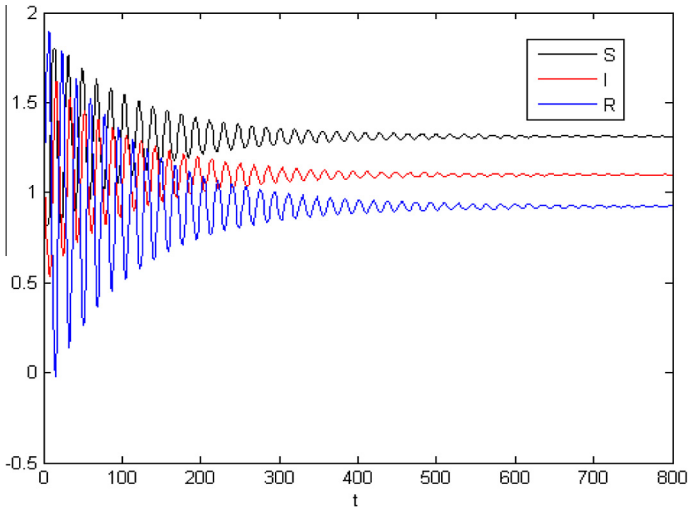

Fig. 3. The waveform plot of malware propagation results with $R_0 = 3.5434 > 1$ and $\tau = 7.3 < \tau_0$.

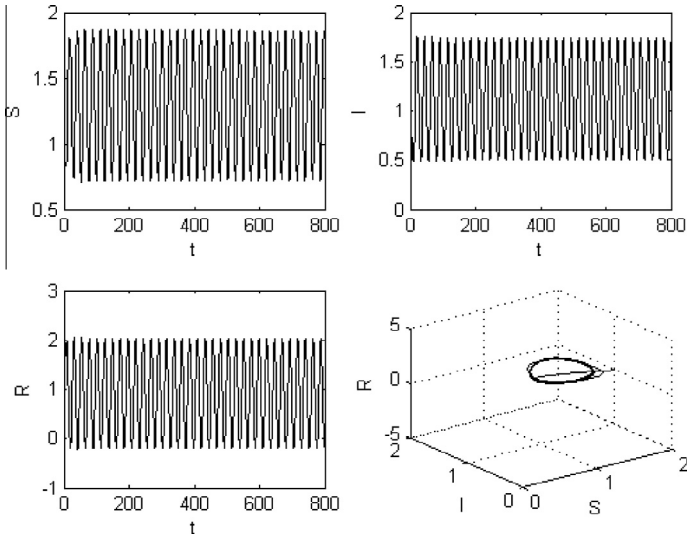

Fig. 4. The bifurcating periodic solutions from endemic equilibrium E_1^* occurs when $\tau = \tau_0 = 10.03$.

model. As part of ongoing work, we also plan trace the real data to verify that our model is more realistic than stationary SIRS model for analyzing the malware propagation.

4.2. Control strategies

Here, we consider influences of infection rate $\beta(t)$ on the dynamics of malware propagation. To obtain effective malware containment strategies, we get the relationship between α (a adjustable parameter of $\beta(t)$) and the proportion of infected hosts $I(t)$ by repeated numerical simulations with $\Lambda = 1$, $\mu = 0.3$, $p = 0.9$, $\gamma = 0.2$, $\beta_0 = 0.8$, $\delta = 0.7$ (in Fig. 6(a)) and $\delta = 0$ (in Fig. 6(b)). Simulation results are shown in Fig. 6(a) and (b). From these two figures, we can conclude that:

(i) There always exists a threshold for α, below which a small increase about α will lead to the proportion of infected hosts disproportionately largely decrease. Otherwise the change of the proportion of infected hosts is slight. So, organizations can choose appropriate infection rate $\beta(t)$ by adjusting to α to constrain malware prevalence with the least expensive antivirus policies.
(ii) Increasing real-time immune rate φ is a feasible method for decreasing the proportion of infected hosts.

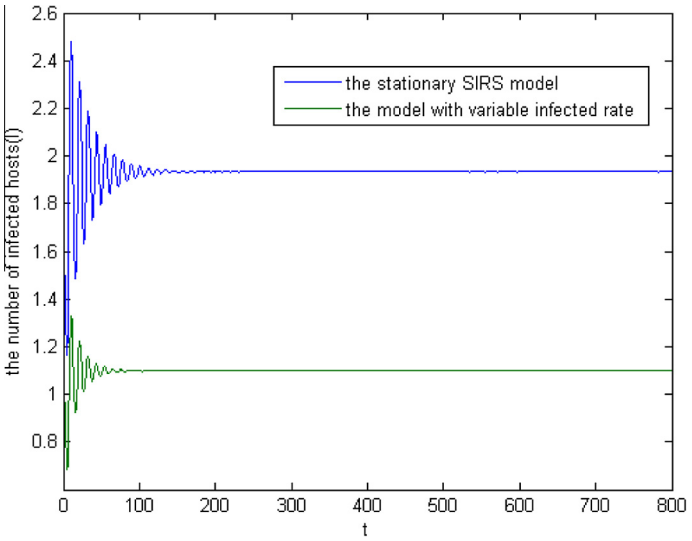

Fig. 5. Comparison between the stationary SIRS model and our model.

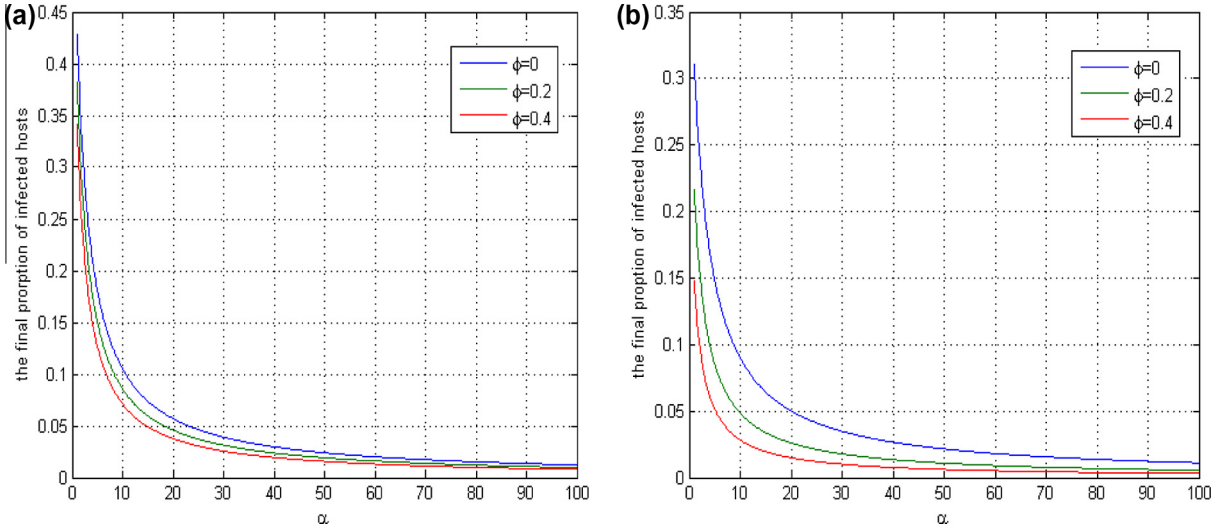

Fig. 6. The relationship between final proportion infected hosts and α.

(iii) Below the threshold of α, the final proportion of infected hosts in Fig. 6(b) is smaller than that in Fig. 6(a), which is because the number of susceptible hosts reduces when $\delta = 0$ in Fig. 6(b). Hence, reducing the number of susceptible hosts is effective for constraining the prevalence of malware.

5. Conclusions

The objective of this work is to model the malware prevalence in the network, and then to find out certain workable means of controlling malware propagation.

We explore the SIRS model with variable infection rate for investigating long-term actions of malware propagation. Based on this model, a control parameter R_0 that completely determines the global dynamics of malware propagation has been obtained by the explicit mathematical analysis. From Theorems 2 and 3, we learn out that malware may die out in the network when $R_0 < 1$, and they will be prevalent otherwise. Also, using time delay as a bifurcating parameter, we obtain a necessary and sufficient condition for occurring of Hopf bifurcation. Furthermore, numerical simulations verify the correctness of theoretical analyses. More importantly, we investigate the effect of a variable infection rate on the scale of malware prevalence in networks. Simulation results show that there is a threshold of the infection rate. When the value of infection rate is larger than this threshold, the change of infection rate is sensitive to the final scale of malware prevalence. When the value of

infection rate is smaller than this threshold, the number of infected nodes cannot create a large change with the varied infection rate. Meanwhile, we provide some antivirus strategies according to simulating results. In addition, we compare our model with the stationary *SIRS* model, and results show that the scale of malware spreading predicted by our model is much smaller than the scale predicted by stationary SIRS model. This is noteworthy for analysis and prediction of future malware prevalence. We think our analysis can provide some insight into malware countermeasures. In real world, this result can help antivirus companies or related organizations to make cost-effective countermeasures to work well.

Our model is suitable for Internet malware without topology constraint, like red worms, Nimda and so on. For predicting the dynamics of malware prevalence in more realistic way, we need do more efforts to trace real data to test out model. Furthermore, considering bifurcation is an undesirable phenomenon in malware propagation, we will continue our research according to dynamical optimal control method [30,31].

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 60973114, Grant 61170249 and Grant 61003247, in part by the Natural Science Foundation project of CQCSTC under Grant 2009BA2024, and in part by the State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University, under Grant 2007DA10512711206.

Appendix A. Proof of Theorem 1

Proof. Steady states of system (4) satisfy the following equations:

$$\begin{cases} p\Lambda - \beta_0 f(I(t))S(t) - (\mu+\varphi)S(t) + \delta R(t) = 0, \\ \beta_0 f(I(t))S(t) - (\mu+\gamma)I(t) = 0, \\ (1-p)\Lambda + \varphi S(t) + \gamma I(t) - \delta R(t) - \mu R(t) = 0. \end{cases} \tag{25}$$

When $I(t) = 0$, since $f(0) = 0$, solving the system (25), it is easy to obtain

$$E_0^* = (S_0^*, I_0^*, R_0^*) = \left(\frac{(p\mu+\delta)\Lambda}{\mu(\mu+\delta+\varphi)}, 0, \frac{(1-p)\Lambda + \varphi S_0^*}{\delta+\mu}\right).$$

When $I(t) > 0$, and from the second equation of system (25), it follows that

$$S = \frac{(\mu+\gamma)I}{\beta_0 f(I)}. \tag{26}$$

Similarly, from the third equation of system (25) it follows that

$$R = \frac{(1-p)\Lambda + \varphi S\gamma I}{\delta+\mu}. \tag{27}$$

Since system (25) is a nonlinear delay differential equation and infection rare is a function of I, it is difficult to find an explicit expression for I. Hence, in what follows, we will prove that there exists an endemic equilibrium. Substituting Eqs. (26) and (27) into the first equation of system (9), we obtain the following equation for I:

$$H(I) = p\Lambda - \frac{\mu(\mu+\delta+\gamma)}{\delta+\mu}I - \frac{\mu(\mu+\gamma)(\mu+\delta+\varphi)}{\beta_0(\delta+\mu)f(I)}I + \frac{\delta\Lambda(1-p)}{(\delta+\mu)} = 0.$$

It is easy to see that the function $H(I)$ is negative for enough large positive I. Next, we determine the sign of its derivative:

$$H'(I) = -\frac{\mu(\mu+\delta+\gamma)}{(\delta+\mu)} - \frac{\mu(\mu+\gamma)(\mu+\delta+\varphi)(f(I) - If'(I))}{\beta_0(\delta+\mu)f^2(I)}.$$

From $f_1'(I) < 0$, we can conclude that $f(I) - If'(I) > 0$ hold for all $I > 0$, and consequently, $H'(I) < 0$ hold for all $I > 0$. Therefore, for a positive root of $H(I) = 0$, $H(I)$ must satisfy $H(0) > 0$, i.e.,

$$H(0) = \frac{\mu(\mu+\gamma)(\mu+\delta+\varphi)}{\beta_0(\delta+\mu)f'(0)}(R_0 - 1) > 0.$$

Hence, a virus-endemic equilibrium exists if and only if $R_0 > 1$. the proof is completed. □

Appendix B. Proof of Lemma 2

Proof. Combining the first equation of system (4) with Eq. (1), we have

$$\dot{S}(t) \leqslant p\Lambda - (\mu+\varphi)S(t) + \delta(N(t) - I(t) - S(t)) \leqslant p\Lambda + \delta N(t) - (\delta+\mu+\varphi)S(t).$$

Thus

$$S(t) \leqslant \frac{p\Lambda + \delta N(t)}{\delta + \mu + \varphi} + \left(S(0) - \frac{p\Lambda + \delta N(t)}{\delta + \mu + \varphi}\right) \exp[-(\delta + \mu + \varphi)t].$$

When $t \to +\infty$, we obtain $S(t) \leqslant \frac{p\Lambda+\delta N(t)}{\delta+\mu+\varphi} = \frac{p\Lambda+\delta\frac{\Lambda}{\mu}}{\delta+\mu+\varphi} = \frac{\Lambda(p\mu+\delta)}{\mu(\delta+\mu+\varphi)}$.

Hence,

$$S(t) \leqslant \frac{\Lambda(p\mu + \delta)}{\mu(\delta + \mu + \varphi)}. \tag{28}$$

From Eq. (9), we can obtain that for all $I > 0$, if $R_0 < 1$, then $\frac{\beta_0\Lambda(p\mu+\delta)}{\mu(\delta+\mu+\varphi)} f(I(t)) < (\mu + \gamma)I(t)$. Hence, substituting Eq. (28) into the second equation of system (4), we have

$$\dot{I}(t) \leqslant \frac{\beta_0\Lambda(p\mu + \delta)}{\mu(\delta + \mu + \varphi)} f(I(t)) - (\mu + \gamma)I(t) < 0,$$

i.e., there exists an enough small positive constant ε such that

$$\frac{dI(t)}{dt} \leqslant -\varepsilon. \quad \frac{dI(t)}{dt} \leqslant -\varepsilon I(t). \tag{29}$$

Solving Eq. (29), we can obtain $I(t) \leqslant I(0)e^{-\varepsilon t}$.

Hence,

$$\lim_{t\to\infty} I(t) = 0. \tag{30}$$

From Eqs. (1) and (7), we have $\lim_{t\to\infty} N(t) = \frac{\Lambda}{\mu}$. Substituting Eq. (30) into the first equation of system (25), we can get

$$\lim_{t\to\infty} \dot{S}(t) \geqslant \frac{\Lambda(p\mu + \delta)}{\mu} - (\mu + \varphi + \delta)\frac{\Lambda(p\mu + \delta)}{\mu(\mu + \varphi + \delta)} = 0.$$

Hence,

$$\lim_{t\to\infty} S(t) = \frac{\Lambda(p\mu + \delta)}{\mu(\delta + \mu + \varphi)}.$$

Similarly, we can prove that

$$\lim_{t\to\infty} R(t) = \frac{(1 - p)\Lambda + \varphi S_0^*}{\delta + \mu}.$$

The proof is completed. □

Appendix C. Proof of Lemma 4

Proof. Derivative $h(z)$, one can get

$$h'(z) = 3z^2 + 2c_1z + c_2. \tag{31}$$

If $h(z) = 0$ has a positive simple real root, it must have three simple real roots. Hence $h(z)$ must have two real turning points, and the second turning point must occur at positive of z.Solving Eq. (31), we can obtain two turning points: $z_1 = \frac{1}{3}(-c_1 - \sqrt{c_1^2 - 3c_2})$ and $z_2 = \frac{1}{3}(-c_1 + \sqrt{c_1^2 - 3c_2})$. For Eq. (31) having two strictly negative real roots (or one strictly negative and one zero real root) we must have $c_1 > 0, c_2 \geqslant 0 \text{and} c_1^2 > 3c_2$, and for Eq. (31) having one strictly negative and one strictly positive real root we must have $c_2 < 0$ in addition as $h(z_1) < 0$ and $h(z_2) > 0$, we must have $\Delta = h(z_1)\,h(z_2) < 0$ from Eq. (31), we can obtain

$$z_1 + z_2 = -\frac{2}{3}c_1, z_1z_2 = \frac{c_2}{3}. \tag{32}$$

Hence

$$\begin{aligned}\Delta = h(z_1)h(z_2) &= (z_1^3 + c_1z_1^2 + c_2z_1 + c_3)(z_2^3 + c_1z_2^2 + c_2z_2 + c_3)\\ &= (z_1z_2)^3 + c_1(z_1z_2)^2(z_1 + z_2) + c_2(z_1z_2)(z_1^2 + z_2^2) + c_3(z_1^3 + z_2^3) + c_1^2(z_1z_2)^2 + c_1c_2(z_1z_2)(z_1 + z_2) + c_1c_3(z_1^2 + z_2^2)\\ &\quad + c_2c_3(z_1 + z_2) + c_3^2 + c_2^2(z_1z_2).\end{aligned}$$

Using Eq. (32) and the following relationships

$$z_1^2 + z_2^2 = (z_1 + z_2)^2 - 2z_1z_2, \quad z_1^3 + z_2^3 = (z_1 + z_2)^3 - 3z_1z_2(z_1 + z_2),$$

one can derive that

$$\Delta = \frac{4}{27}c_2^3 - \frac{1}{27}c_1^2c_2^2 + \frac{4}{27}c_1^3c_3 - \frac{2}{3}c_1c_2c_3 + c_3^2.$$

It is straightforward to show the conditions of Lemma 4 are also sufficient for $h(z) = 0$ to have a simple real root.

If $h(z) = 0$ has no less than two positive real root, then $h'(z)$ must have two strictly positive real roots, i.e., $z_1 > 0 \text{and} z_2 > 0$. Since the condition $c_1 > 0$, it is impossible for $z_1 > 0$. Hence, Eq. (21) has only one simple positive real root. The proof is completed. □

Appendix D. Supplementary data

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.apm.2013.03.051.

References

[1] M. Garetto, W.B. Gong, D. Towsley, Modeling malware spreading dynamics, in: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications (INFOCOM 2003), vol. 3, 2003, pp. 1869–1879.
[2] S. Datta, H. Wang, The effectiveness of vaccinations on the spread of email-borne computer viruses, in: Proceedings of the Conference on Electrical and, Computer Engineering, 2005, pp. 219–223.
[3] D. Bernoulli, Essai d'une nouvelle analyse de la mortalité causée la petite vérole et des avantages de l'inoculation pour la prévenir, Mém. Math. Phys. Acad. Roy. Sci. Paris (1760) 1–45.
[4] N.T.J. Bailey, The Mathematical Theory Of Infectious Diseases and its Applications, Oxford University Press, New York, 1975.
[5] J.O. Kephart, S.R. White, Directed-graph epidemiological models of computer viruses, in: Proceedings of the IEEE Computer Society Symposium on Security and Privacy, 1991, pp. 343–359.
[6] J.O. Kephart, S.R. White, Measuring and modeling computer virus prevalence, in: Proceedings of the IEEE Computer Society Symposium on Security and Privacy, 1993, pp. 2–15.
[7] L. Billings, W.M. Spears, I.B. Schwartz, A unified prediction of computer virus spread in connected networks, Phys. Lett. A 297 (3) (2002) 261–266.
[8] C.C. Zou, W.B. Gong, D. Towsley, L.X. Gao, The monitoring and early detection of internet worms, IEEE-ACM Trans. Networking 13 (5) (2005) 961–974.
[9] C.C. Zou, D. Towsley, W.B. Gong, On the performance of Internet worm scanning strategies, Perform. Eval. 63 (7) (2006) 700–723.
[10] C.C. Zou, D. Towsley, W.B. Gong, S.l. Cai, Routing worm: A fast, selective attack worm based on IP address information, in: Proceedings of the 19th Workshop on Principles of Advanced and Distributed, Simulation, 2005, pp. 199–206.
[11] C.C. Zou, D. Towsley, W.B. Gong, Modeling and simulation study of the propagation and defense of Internet email worm, IEEE Trans. Dependable Secure Comput. 4 (2) (2007) 105–118.
[12] D.J. Daley, J. Gani, Epidemic Modeling: An Introduction, Cambridge University Press, New York, 1999.
[13] W.O. Kermack, A.G. McKendrick, Contributions to the mathematical theory of epidemics, Bull. Math. Biol. 53 (1) (1991) 33–55.
[14] K.M. Bimal, K.S. Dinesh, SEIRS epidemic model with delay for transmission of malicious objects in computer network, Appl. Math. Comput. 188 (2) (2007) 1476–1482.
[15] R. Xu, Z.E. Ma, Z.P. Wang, Global stability of a delayed SIRS epidemic model with saturation incidence and temporary immunity, Comput. Math. Appl. 59 (9) (2010) 3211–3221.
[16] X. Han, Q.L. Tan, Dynamical behavior of computer virus on Internet, Appl. Math. Comput. 217 (6) (2010) 2520–2526.
[17] L.P. Song, Z. Jin, G.Q. Sun, J. Zhang, X. Han, Influence of removable devices on computer worms: dynamic analysis and control strategies, Comput. Math. Appl. 61 (7) (2011) 1823–1829.
[18] S.J. Wang, Q.M. Liu, X.F. Yu, Y. Ma, Bifurcation analysis of a model for network worm propagation with time delay, Math. Comput. Model. 52 (3) (2010) 435–447.
[19] K.M. Bimal, K.P. Samir, Fuzzy epidemic model for the transmission of worms in computer network, Nonlinear Anal.: Real World Appl. 11 (5) (2010) 4335–4341.
[20] Z.S. Chen, C.Y. Ji, Spatial-temporal modeling of malware propagation in networks, IEEE Trans. Neural Networks 16 (5) (2005) 1291–1303.
[21] C. Anagnostopoulos, S. Hadjiefthymiades, E. Zervas, Information dissemination between mobile nodes for collaborative context awareness, IEEE Trans. Mobile Comput. 10 (12) (2011) 1710–1725.
[22] C.C. Zou, W. Gong, D. Towsley, Code red worm propagation modeling and analysis, in: Proceedings of the 9th ACM Conference on Computer and Communications, Security, 2002, pp 138–147.
[23] J. Cowie, A. Ogielski, Global routing instabilities during code red II and Nimda worm propagation, 2001. http://www.renesys.com/tech/presentations/.
[24] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. Wu, L. Zhang, Observation and analysis of BGP behavior under stress, in: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet, measurement, 2002, pp. 183–195.
[25] J. Cowie, A. Hobgood, R. Meharwal, The curious incident of 7 NOV 2011. http://www.renesys.com/tech/presentations/.
[26] L.P. Feng, X.F. Liao, H.Q. Li, Q. Han, Hopf bifurcation analysis of a delayed viral infection model in computer networks, Math. Comput. Model. 56 (2012) 167–179.
[27] S.M. Moghadas, A.B. Gumel, Global stability of a two-stage epidemic model with generalized non-linear incidence, Math. Comput. Simul. 60 (1) (2002) 107–118.
[28] D.K. Saini, A mathematical model for the effect of malicious object on computer network immune system, Appl. Math. Model. 35 (8) (2011) 3777–3787.
[29] J. Hale, S.M. Lunel, Introduction to Functional Differential Equations, Springer-Verlag, 1993.
[30] H.Q. Li, F.X. Liao, R.J. Liao, A unified approach to chaos suppressing and inducing in a periodically forced family of nonlinear oscillators, IEEE Trans. Circuits Syst. – I: Regular Papers 59 (4) (2012) 784–795.
[31] H.Q. Li, F.X. Liao, U. Saleem, L. Xiao, Analytical proof on the existence of chaos in the generalized Duffing-type oscillator with fractional-order deflection, Nonlinear Anal. Ser. B: Real World Appl. 13 (6) (2012) 2724–2733.