

Research Article

A Novel Computer Virus Propagation Model under Security Classification

Qingyi Zhu¹ and Chen Cen²

¹College of Cyber-Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

²College of Computer Science, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Correspondence should be addressed to Qingyi Zhu; zhuqy@cqupt.edu.cn

Received 28 February 2017; Revised 30 April 2017; Accepted 2 May 2017; Published 25 May 2017

Academic Editor: Jose R. C. Piqueira

Copyright © 2017 Qingyi Zhu and Chen Cen. 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.

In reality, some computers have specific security classification. For the sake of safety and cost, the security level of computers will be upgraded with increasing of threats in networks. Here we assume that there exists a threshold value which determines when countermeasures should be taken to level up the security of a fraction of computers with low security level. And in some specific realistic environments the propagation network can be regarded as fully interconnected. Inspired by these facts, this paper presents a novel computer virus dynamics model considering the impact brought by security classification in full interconnection network. By using the theory of dynamic stability, the existence of equilibria and stability conditions is analysed and proved. And the above optimal threshold value is given analytically. Then, some numerical experiments are made to justify the model. Besides, some discussions and antivirus measures are given.

1. Introduction

With the rapid development of the Internet, the spread of computer virus has brought a lot of potential safety problems, which not only caused huge waste to the network resources but also harmed the interests of individuals and the masses. The traditional way of antivirus is constantly updating the virus library of antivirus software. But it is a passive mechanism to prevent viruses. In this context, the macroscopical study of computer virus propagation is regarded as a very important approach to antivirus and has received more and more attention from scholars.

In 1991, Kephart and White firstly used the model of biological infectious virus to study the spread of computer viruses [1]. Since then, a lot of dynamical models of computer virus have been presented. These models can be simply divided into two broad categories: homogeneous models and heterogeneous models according to whether the network is fully connected or not.

In recent years, more and more scholars have begun to study heterogeneous models. Kjaergaard and his partners

followed the time evolution of information propagation through communication networks by using the susceptible-infected (SI) model with empirical data on contact sequences [2]. Castellano and Pastor-Satorras studied the threshold of epidemic models in quenched networks with degree distribution given by a power-law for the susceptible-infected-susceptible (SIS) model [3]. Zhu et al. investigated a new epidemic SIS model with nonlinear infectivity, as well as birth and death of nodes and edges [4]. Taking into account the power-law degree distribution of the Internet, Yang et al. proposed a novel epidemic model of computer viruses and presented the spreading threshold for the model [5]. L.-X. Yang and X. Yang proposed an epidemic model of computer viruses over a reduced scale-free network [6]. Yang and his partners proposed a node-based susceptible-latent-breaking-susceptible (SLBS) model which addresses the impact of the structure of the viral propagation network on the viral prevalence [7]. To understand the impact of available information in the control of malicious network epidemics, Mishra and three others proposed a 1- n - n -1 type differential epidemic model, where the differentiability allows

a symptom based classification [8]. All these models assume that the spread of viruses can only be through the topological neighbors.

In fact, a lot of viruses can propagate without dependence on the topology, such as Code Red (2001), Slammer (2003), Blaster (2003), Witty (2004), and Conficker (2009). By probing the entire IPv4 space or localized IP addresses, these viruses can infect an arbitrary vulnerable computer. In this condition, the propagation network can be regarded as fully connected. Besides, there are still some fully interconnected networks, such as virtual cluster in cloud [9–12]. So the study of homogeneous models is also an important branch of computer virus dynamical models. A portion of infected external computers could enter the Internet and removable storage media could carry viruses, based on the two facts. Gan et al. established a series of dynamical models [13–16]. Amador and Artalejo investigated the dynamics of computer virus spreading by considering a stochastic SIRS model where immune computers send warning signals to reduce the propagation of the virus among the rest of computers in the network [17]. Liu and Zhong presented and analyzed an SDIRS model describing the propagation of web malware based on the assumption of homogeneity [18]. Yuan and three others presented a nonlinear force of infection function for e-SEIR model to study the crowding and psychological effects in network virus prevalence [19].

In order to protect the security and stability of information systems, the concept of information security classified protection is proposed and has been a basic strategy of construction of national information. But to our knowledge, nearly all previous models describing the spread of computer viruses ignore the impacts of security classifications. In order to study how these factors affect the spread of computer viruses on the Internet, this paper proposes a novel computer virus propagation model. A thorough analysis of this model shows that some equilibria existed and are globally asymptotically stable in a specific situation. Besides, some simulation experiments are performed to examine the conclusion got from this model. In the end, some effective strategies for controlling virus spreading are recommended.

The subsequent materials are organized in this fashion: The idea of modeling is introduced in Section 2. The new model is established in Section 3. The analysis of four equilibria is addressed in Section 4. The local and global stabilities of these equilibria are investigated in Sections 5 and 6, respectively. Simulation experiments and some discussions are presented in Section 7. Finally, this work is outlined in Section 8.

2. Idea of Modeling

In a security classification network, blindly increasing the security level of computer will result in both waste of resource and increase of cost. Therefore, reinforcing the security level of computer must be targeted. About security classification of computer, the influential criteria are “Trusted Computer System Evaluation Criteria (TcsEC)” issued by United States

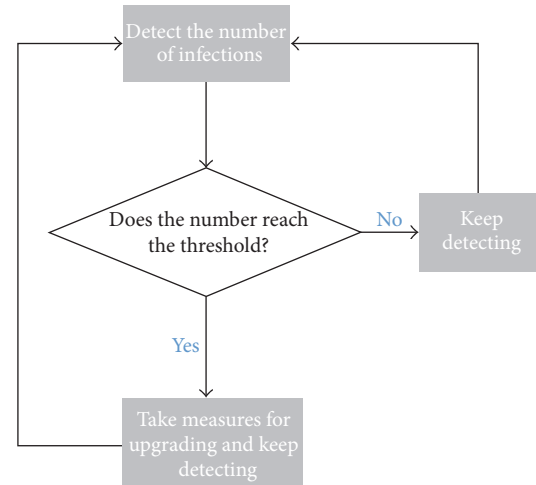


FIGURE 1: Flow diagram of upgrading.

Department of Defense [20]. By using these criteria, computers in the network can be divided into four divisions. From high to low, they are Levels A, B, C, and D, respectively.

Low Security Level: Divisions D and C. In this level, it is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class. Classes in this level provide for discretionary (need-to-know) protection and it can only provide a review of protection.

High Security Level: Divisions B and A. The security-relevant sections of a system are mentioned throughout this document as the Trusted Computing Base (TCB) [21]. Computers in this level must carry the sensitivity labels with most data structures in the system and the system developer should provide the security policy model based on TCB. By using formal security verification methods, this level requires that each operation in the system must have a formal documentation and can only be made by the administrator.

Obviously, computers with low security level are more likely to be infected by virus. This is the first breakthrough point for modeling.

In the network with security classification, administrators usually do not take any measures to upgrade the computers with low security level if there are only few threats for the sake of cost. With the increase of the infected computers number in the network, the administrators will upgrade the security level of computers ultimately. Here we assume that there exists a threshold value. If the number of infected computers is above the threshold value, some countermeasures will be taken to level up the security of a fraction of computers with low security level. Further, assume that the probability of taking upgrading measures for one uninfected computer is proportional to the number of infected computers. The flow diagram in Figure 1 can briefly express these operations. How the threshold value and the fraction of upgraded computers affect the propagation of computer virus is the concern in this paper.

3. Model Formulation

According to the situation of computer virus infection and the level of computer security, all computers in the network are divided into three compartments.

- S_l -compartment: the set of uninfected or susceptible computers in low security level
- S_h -compartment: the set of uninfected or susceptible computers in high security level
- I -compartment: the set of infected computers

For the modeling purpose, a series of parameters are introduced and some assumptions are made.

- One can assume that the average probabilities per unit time of S_l and S_h computers connecting to the network are b_l and b_h , respectively.
- Every computer in the system is got out for some reasons with the average probability per unit time μ , where μ is positive constant.
- Due to possible contact with infected computers in the network, every S_l and S_h computer is infected with the average probabilities β_l and β_h per unit time, respectively, where β_l and β_h are positive constant and $\beta_l > \beta_h$.
- Assume that one I computer becomes an S_l computer (or an S_h computer) with the average probability per unit time γ_l (or γ_h), where γ_l, γ_h are positive constants.
- As mentioned in Section 2, the upgrading probability of an S_l computer is denoted by a piecewise function $f(I)$. The expression of $f(I)$ is as follows:

$$f(I) = \begin{cases} 0, & \text{if } 0 \leq I < I_{\max}, \\ \alpha I, & \text{if } I \geq I_{\max}. \end{cases} \quad (1)$$

I_{\max} denotes the threshold value and α denotes the a fraction of upgrading computers.

Let $S_l(t)$, $S_h(t)$, and $I(t)$ denote, at time t , the average numbers of S_l -, S_h -, and I -compartment computers, respectively. Let $N(t)$ denote the total number of all computers in the system at time t . Unless otherwise stated in the following content, they will be abbreviated as N , S_l , S_h , and I , respectively. Then, $S_l + S_h + I = N$. The collection of the above parameters and assumptions can be schematically depicted in Figure 2, from which the dynamical model is formulated as the following differential system:

$$\begin{aligned} \dot{S}_l &= b_l + \gamma_l I - f(I) S_l - \beta_l S_l I - \mu S_l, \\ \dot{S}_h &= b_h + \gamma_h I + f(I) S_l - \beta_h S_h I - \mu S_h, \\ \dot{I} &= \beta_l S_l I + \beta_h S_h I - \gamma_l I - \gamma_h I - \mu I. \end{aligned} \quad (2)$$

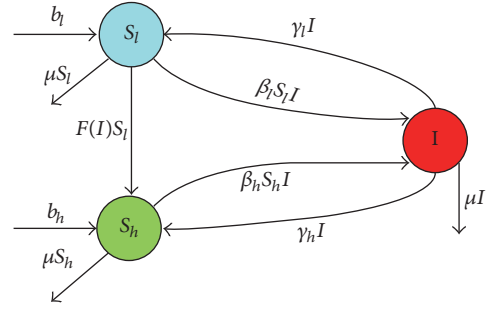


FIGURE 2: Transition diagram of the new model.

Considering that $S_l + S_h + I = N$, system (2) can be reduced to the following system:

$$\begin{aligned} \dot{N} &= b_l + b_h - \mu N, \\ \dot{S}_h &= b_h + \gamma_h I + f(I) (N - S_h - I) - \beta_h S_h I - \mu S_h, \\ \dot{I} &= \beta_l (N - S_h - I) I + \beta_h S_h I - \gamma_l I - \gamma_h I - \mu I. \end{aligned} \quad (3)$$

Solving the first equations of system (3), it is easy to obtain $\lim_{t \rightarrow \infty} N = N^* = (b_l + b_h)/\mu$. Therefore, system (3) can be reduced to the following limiting system [22, 23]:

$$\begin{aligned} \dot{S}_h &= b_h + \gamma_h I + f(I) (N^* - S_h - I) - \beta_h S_h I - \mu S_h, \\ \dot{I} &= \beta_l (N^* - S_h - I) I + \beta_h S_h I - \gamma_l I - \gamma_h I - \mu I. \end{aligned} \quad (4)$$

The feasible region for system (4) is

$$\Omega = \{(S_h, I) \mid S_h \geq 0, I \geq 0, 0 \leq S_h + I \leq N^*\}, \quad (5)$$

which is positively invariant.

4. Equilibria

In this section, all equilibria of system (4) are calculated. To obtain all potential equilibria, system (4) can be written as

$$\begin{aligned} b_h + \gamma_h I - \beta_h S_h I - \mu S_h &= 0, \\ \beta_l (N^* - S_h - I) I + \beta_h S_h I - \gamma_l I - \gamma_h I - \mu I &= 0, \end{aligned} \quad (6)$$

if $0 \leq I < I_{\max}$,

$$\begin{aligned} b_h + \gamma_h I + \alpha I (N^* - S_h - I) - \beta_h S_h I - \mu S_h &= 0, \\ \beta_l (N^* - S_h - I) I + \beta_h S_h I - \gamma_l I - \gamma_h I - \mu I &= 0, \end{aligned} \quad (7)$$

if $I \geq I_{\max}$.

From (6) the fact that there always exists a virus-free equilibrium can be got:

$$E_0^* = \left(S_{h0}^* = \frac{b_h}{\mu}, I_0^* = 0 \right), \quad (8)$$

and the basic reproduction number is

$$R_0 = \frac{\beta_l b_l + \beta_h b_h}{\mu (\gamma_l + \gamma_h + \mu)}. \quad (9)$$

Let

$$\begin{aligned} C &= \mu(\gamma_l + \gamma_h + \mu) - \beta_l b_l - \beta_h b_h \\ &= \mu(\gamma_l + \gamma_h + \mu)(1 - R_0), \end{aligned} \quad (10)$$

$$A_1 = \beta_l \beta_h,$$

$$B_1 = \beta_l \beta_h N^* - \beta_l \gamma_h - \beta_l \mu - \beta_h \gamma_l - \beta_h \mu, \quad (11)$$

$$\Delta_1 = B_1^2 - 4A_1 C,$$

$$A_2 = \beta_l \beta_h + \alpha \beta_h,$$

$$\begin{aligned} B_2 &= (\beta_l \beta_h + \alpha \beta_h) N^* - \beta_l \gamma_h - \beta_l \mu - \beta_h \gamma_l - \beta_h \mu \\ &\quad - \alpha(\gamma_l + \gamma_h + \mu), \end{aligned} \quad (12)$$

$$\Delta_2 = B_2^2 - 4A_2 C.$$

The quadratic equation of I can be got from system (6) and (7) as follows:

$$A_1 I^2 - B_1 I + C = 0 \quad \text{if } 0 \leq I < I_{\max}, \quad (13)$$

$$A_2 I^2 - B_2 I + C = 0, \quad \text{if } I \geq I_{\max}. \quad (14)$$

Considering that $I_1^* = (B_1 + \sqrt{\Delta_1})/2A_1$, $I_2^* = (B_1 - \sqrt{\Delta_1})/2A_1$ are the roots of (13) and $I_3^* = (B_2 + \sqrt{\Delta_2})/2A_2$, $I_4^* = (B_2 - \sqrt{\Delta_2})/2A_2$ are the roots of (14) ($I_1^* \neq I_3^*$), the solution of (6) and (7) can be got as follows:

$$\begin{aligned} I_1^* &= \frac{B_1 + \sqrt{\Delta_1}}{2A_1}, \\ S_{h1}^* &= \frac{b_h + \gamma_h I_1^*}{\mu + \beta_h I_1^*}, \\ I_2^* &= \frac{B_1 - \sqrt{\Delta_1}}{2A_1}, \\ S_{h2}^* &= \frac{b_h + \gamma_h I_2^*}{\mu + \beta_h I_2^*}, \\ I_3^* &= \frac{B_2 + \sqrt{\Delta_2}}{2A_2}, \\ S_{h3}^* &= \frac{b_h + \gamma_h I_3^* + \alpha I_3^* (N - I_3^*)}{\mu + \beta_h I_3^*}, \\ I_4^* &= \frac{B_2 - \sqrt{\Delta_2}}{2A_2}, \\ S_{h4}^* &= \frac{b_h + \gamma_h I_4^* + \alpha I_4^* (N - I_4^*)}{\mu + \beta_h I_4^*}. \end{aligned} \quad (15)$$

(13) and (14) can be deduced as follows:

$$\begin{aligned} &A_1 (I_1^{*2} - I_3^{*2}) - B_1 (I_1^* - I_3^*) - \alpha \beta_h I_3^{*2} \\ &\quad + (B_2 - B_1) I_3^* = 0, \\ &(I_1^* - I_3^*) [A_1 (I_1^* + I_3^*) - B_1] \\ &\quad = I_3^* [\alpha \beta_h I_3^* - (B_2 - B_1)], \\ &(I_1^* - I_3^*) [A_1 (I_1^* + I_3^*) - B_1] \\ &\quad = I_3^* [\alpha \beta_h I_3^* - \alpha \beta_h N^* + \alpha(\gamma_l + \gamma_h + \mu)], \\ &(I_1^* - I_3^*) [A_1 (I_1^* + I_3^*) - B_1] \\ &\quad = \alpha I_3^* [\beta_h I_3^* - \beta_h N^* + \beta_l (N^* - I_3^* - S_{h3}^*)], \\ &(I_1^* - I_3^*) [A_1 (I_1^* + I_3^*) - B_1] \\ &\quad = \alpha I_3^* (\beta_l - \beta_h) (N^* - I_3^* - S_{h3}^*), \end{aligned} \quad (16)$$

because of $\beta_l > \beta_h$ and $I_3^* + S_{h3}^* \leq N^*$, $\alpha I_3^* (\beta_l - \beta_h) (N^* - I_3^* - S_{h3}^*) \geq 0$. Then

$$(I_1^* - I_3^*) [A_1 (I_1^* + I_3^*) - B_1] \geq 0. \quad (17)$$

Assuming $I_1^* < I_3^*$, then $A_1 (I_1^* + I_3^*) - B_1 > 2A_1 I_1^* - B_1 = \sqrt{\Delta_1} > 0$ and $(I_1^* - I_3^*) [A_1 (I_1^* + I_3^*) - B_1] < 0$, which contradicts with (17). So $I_1^* > I_3^*$. In the same way, one can get

$$I_2^* < I_4^* < I_3^* < I_1^*. \quad (18)$$

Theorem 1. *There are only two viral equilibria $E_1^* = (S_{h1}^*, I_1^*)$ (or $E_3^* = (S_{h3}^*, I_3^*)$) and $E_2^* = (S_{h2}^*, I_2^*)$ (or $E_4^* = (S_{h4}^*, I_4^*)$) in this model if*

- (1) $R_0 < 1$;
- (2) $B_1 > 0, \Delta_1 > 0$ (or $B_2 > 0, \Delta_2 > 0$);
- (3) $I_1^* > I_{\max}$ (or $I_2^* > I_{\max}$).

Proof. System (13) has two real roots if $\Delta_1 > 0$. From (10) one can get that $C > 0$ if $R_0 < 1$; then $C/A_1 > 0$. So the fact that $I_1^* > 0, I_2^* > 0$ if $B_1 > 0$ can be got (in the same way, the fact that $I_1^* > 0, I_2^* > 0$ can be got if $B_2 > 0, \Delta_2 > 0$) and there are only two viral equilibria E_1^*, E_2^* (or E_3^*, E_4^*) if $I_1^* > I_{\max}$ (or $I_2^* > I_{\max}$) from (18). \square

Theorem 2. *System (4) has only three viral equilibria $E_2^* = (S_{h2}^*, I_2^*), E_3^* = (S_{h3}^*, I_3^*)$, and $E_4^* = (S_{h4}^*, I_4^*)$ if*

- (1) $R_0 < 1$;
- (2) $B_1 > 0, \Delta_1 > 0$;
- (3) $B_2 > 0, \Delta_2 > 0$;
- (4) $I_2^* < I_{\max} \leq I_4^*$.

Proof. Like the proof of Theorem 1, it does not need to be stated. \square

Theorem 3. System (4) has only one viral equilibrium $E_1^* = (S_{h1}^*, I_1^*)$ (or $E_3^* = (S_{h3}^*, I_3^*)$) if

- (1) $R_0 > 1$;
- (2) $I_1^* < I_{\max}$ (or $I_3^* \geq I_{\max}$).

Proof. One can get $C < 0$ if $R_0 > 1$ and $\Delta_1 > 0$, $\Delta_2 > 0$, $C/A_1 < 0$, $C/A_2 < 0$. So $I_1^* > 0$, $I_2^* < 0$ and $I_3^* > 0$, $I_4^* < 0$. Then the fact that only E_1^* (or E_3^*) existed if $I_1^* < I_{\max}$ (or $I_3^* \geq I_{\max}$) from (18) can be got. \square

5. The Local Stability Analysis

To examine the local stability of the equilibria of system (4), its Jacobian matrices should be got as follows:

$$J_1 = \begin{pmatrix} -\beta_h I - \mu & \gamma_h - \beta_h S_h \\ -\beta_l I + \beta_h I & \beta_l N^* - \beta_l S_h - 2\beta_l I + \beta_h S_h - \gamma_l - \gamma_h - \mu \end{pmatrix},$$

if $0 \leq I < I_{\max}$,

$$J_2 = \begin{pmatrix} -\beta_h I - \mu - \alpha I & \gamma_h - \beta_h S_h + \alpha(N^* - S_h - 2I) \\ -\beta_l I + \beta_h I & \beta_l N^* - \beta_l S_h - 2\beta_l I + \beta_h S_h - \gamma_l - \gamma_h - \mu \end{pmatrix},$$

if $I \geq I_{\max}$.

Theorem 4. E_0^* is locally asymptotically stable if $R_0 < 1$.

Proof. The associated characteristic equation of E_0^* can be got from J_1 as follows:

$$(\lambda + \mu) \left(\lambda + \gamma_l + \gamma_h + \mu - \beta_l \frac{b_l}{\mu} - \beta_h \frac{b_h}{\mu} \right). \quad (20)$$

Then

$$\begin{aligned} \lambda_1 &= -\mu < 0, \\ \lambda_2 &= -\gamma_l - \gamma_h - \mu + \beta_l \frac{b_l}{\mu} + \beta_h \frac{b_h}{\mu} \\ &= (\gamma_l + \gamma_h + \mu)(R_0 - 1). \end{aligned} \quad (21)$$

Based on the Lyapunov theorem [24], only if $R_0 < 1$ are all eigenvalues of (17) negative. At this situation, E_0^* is locally asymptotically stable. \square

Theorem 5. E_1^* (or E_3^*) is locally asymptotically stable if system (4) follows Theorem 1 or 2 or 3.

Proof. The associated characteristic equations of E_1^* can be got from J_1 as follows:

$$\lambda^2 + k_1 \lambda + k_2 = 0, \quad (22)$$

where

$$\begin{aligned} k_1 &= \beta_l I_1^* + \beta_h I_1^* + \mu > 0, \\ k_2 &= I_1^* [\beta_l (\beta_h I_1^* + \mu) - (\beta_l - \beta_h) (\beta_h S_{h1}^* - \gamma_h)] \\ &= I_1^* [2\beta_l \beta_h I_1^* + \beta_l \mu - \beta_l \beta_h S_{h1}^* + \beta_l \gamma_h + \beta_2^2 S_{h1}^* \\ &\quad - \beta_h \gamma_h - \beta_l \beta_h I_1^* + \beta_l \beta_h N^* - \beta_l \beta_h N^*] \\ &= I_1^* [2\beta_l \beta_h I_1^* + \beta_l \mu + \beta_l \gamma_h - \beta_h \gamma_h \\ &\quad + \beta_h (\beta_l N^* - \beta_l S_{h1}^* - \beta_l I_1^* + \beta_h S_{h1}^*) - \beta_l \beta_h N^*] \\ &= I_1^* [2\beta_l \beta_h I_1^* + \beta_l \mu + \beta_l \gamma_h - \beta_h \gamma_h \\ &\quad + \beta_h (\gamma_l + \gamma_h + \mu) - \beta_l \beta_h N^*] = I_1^* [2\beta_l \beta_h I_1^* + \beta_l \mu \\ &\quad + \beta_l \gamma_h + \beta_h \gamma_l + \beta_h \mu - \beta_l \beta_h N^*] \\ &= I_1^* \left(2A_1 \frac{B_1 + \sqrt{\Delta_1}}{2A_1} - B_1 \right) = I_1^* \sqrt{\Delta_1} > 0. \end{aligned} \quad (23)$$

The associated characteristic equations of E_3^* can be got from J_2 as follows:

$$\lambda^2 + k_3 \lambda + k_4 = 0, \quad (24)$$

where

$$\begin{aligned} k_3 &= \alpha I_3^* + \beta_l I_3^* + \beta_h I_3^* + \mu > 0, \\ k_4 &= I_3^* [\beta_l (\alpha I_3^* + \beta_h I_3^* + \mu) \\ &\quad - (\beta_l - \beta_h) (\alpha S_{h3}^* + 2\alpha I_3^* - \alpha N^* + \beta_h S_{h3}^* - \gamma_h)] \\ &= I_3^* [2(\beta_l \beta_h + \beta_h \alpha) I_3^* \\ &\quad + \alpha (\beta_l N^* - \beta_l I_3^* - \beta_l S_{h3}^* + \beta_h S_{h3}^*) \\ &\quad + \beta_h (\beta_l N^* - \beta_l I_3^* - \beta_l S_{h3}^* + \beta_h S_{h3}^*) + \beta_l \mu + \beta_l \gamma_h \\ &\quad - \beta_h \gamma_h - N^* (\beta_l \beta_h + \beta_h \alpha)] = I_3^* [2A_2 I_3^* \\ &\quad + \alpha (\gamma_l + \gamma_h + \mu) + \beta_h (\gamma_l + \gamma_h + \mu) + \beta_l \mu + \beta_l \gamma_h \\ &\quad - \beta_h \gamma_h - N^* (\beta_l \beta_h + \beta_h \alpha)] = I_3^* [2A_2 I_3^* - B_2] \\ &= I_3^* \left[2A_2 \frac{B_2 + \sqrt{\Delta_2}}{2A_2} - B_2 \right] = I_3^* \sqrt{\Delta_2} > 0. \end{aligned} \quad (25)$$

$k_1 > 0$, $k_2 > 0$ (or $k_3 > 0$, $k_4 > 0$); the Hurwitz criterion follows [24], so E_1^* (or E_3^*) is locally asymptotically stable. \square

6. The Global Stability Analysis

This section will discuss the global stability of the equilibrium of system (4). To get global stability, let us investigate the following lemmas.

Lemma 6. For system (4), there is no periodic solution in the interior of Ω .

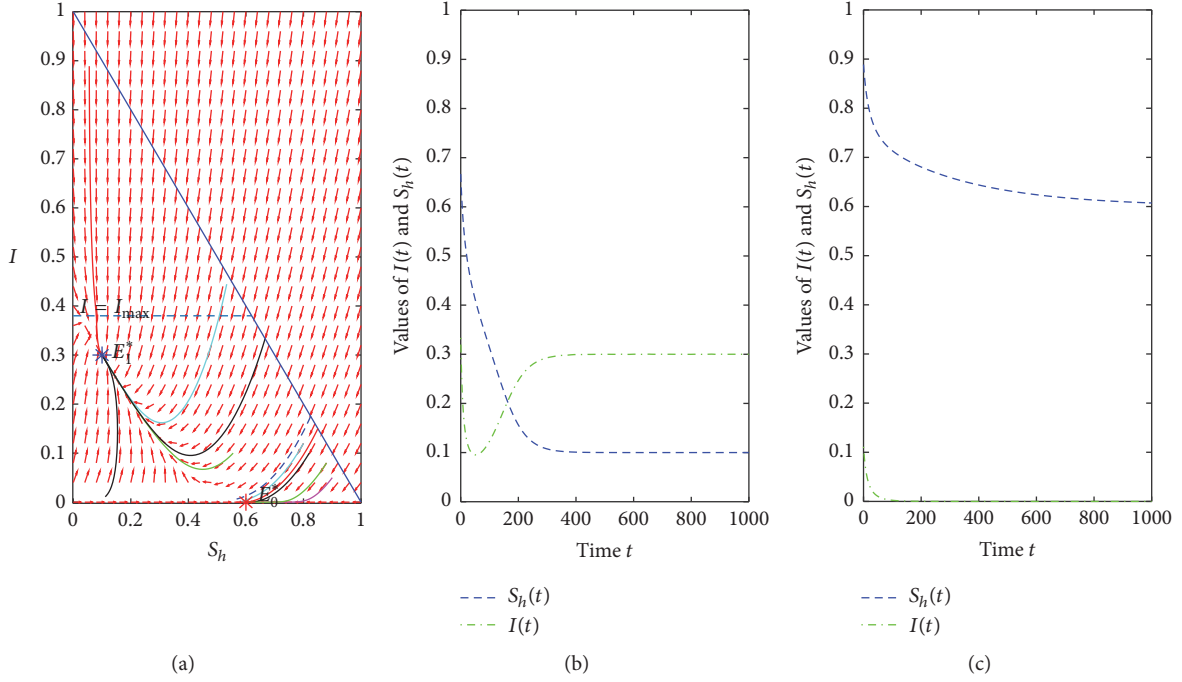


FIGURE 3: Trajectory figure and time plots of Example 1.

Proof. Let

$$\begin{aligned} G(S_h, I) &= b_h + \gamma_h I + f(I)(N^* - S_h - I) - \beta_h S_h I \\ &\quad - \mu S_h, \\ H(S_h, I) &= \beta_l(N^* - S_h - I)I + \beta_h S_h I - \gamma_l I - \gamma_h I \\ &\quad - \mu I, \\ B(S_h, I) &= \frac{1}{I}, \end{aligned} \quad (26)$$

and then

$$\begin{aligned} \frac{\partial(GB)}{\partial S_h} + \frac{\partial(HB)}{\partial I} &= -\beta_h - \frac{\mu}{I} - \beta_l < 0, \\ &\text{if } 0 \leq I < I_{\max}, \\ \frac{\partial(GB)}{\partial S_h} + \frac{\partial(HB)}{\partial I} &= -\beta_h - \frac{\mu}{I} - \beta_l - \alpha < 0, \\ &\text{if } I \geq I_{\max}. \end{aligned} \quad (27)$$

Thus, the claimed result follows from the Bendixson-Dulac criterion [24]. \square

Lemma 7. For system (4), there is no periodic solution that passes through a point on $\partial\Omega$, the boundary of Ω .

Proof. Consider an arbitrary point (\bar{S}_h, \bar{I}) , on the boundary of Ω . From (5), $\partial\Omega$ consists of the following three possibilities:

- (a) $\bar{S}_h = 0$. Then $\dot{S}_h|_{(\bar{S}_h, \bar{I})} = b_h + \gamma_h \bar{I} > 0$, if $0 \leq I < I_{\max}$, and $\dot{S}_h|_{(\bar{S}_h, \bar{I})} = b_h + \gamma_h \bar{I} + \alpha \bar{I}(N^* - \bar{I}) > 0$, if $I_{\max} \leq I \leq N^*$.

TABLE 1: Related instructions.

N	Not existing
E	Only existing
EL	Existing and locally asymptotically stable
EG	Existing and globally asymptotically stable

(b) $\bar{I} = 0$, $0 \leq \bar{S}_h \leq N^*$. Then $\dot{I}|_{(\bar{S}_h, \bar{I})} = 0$.

(c) $\bar{S}_h + \bar{I} = N^*$. Then $(d(\bar{S}_h + \bar{I})/dt)|_{(\bar{S}_h, \bar{I})} = -b_l - \gamma_l \bar{I} < 0$.

In view of the orbit smoothness, combining the above discussions can get the claimed result. \square

In view of Lemmas 6 and 7 and Theorems 3–5, the main result of this section can be got as follows.

7. Numerical Examples and Discussions

In this section, some numerical examples are used to verify the results obtained in the previous section.

Example 1. Suppose $\beta_l = 0.24$, $\beta_h = 0.08$, $\gamma_l = 0.146$, $\gamma_h = 0.003$, $b_l = 0.0012$, $b_h = 0.0018$, $\mu = 0.003$, $\alpha = 0.005$, and $I_{\max} = 0.38$. In this situation, $R_0 < 1$, $I_1^* < I_{\max}$. Some trajectories of initial points are displayed in Figure 3(a) and the time plots about two of them are shown in Figures 3(b) and 3(c). In Figure 3(a), the blue dashed line divides Ω into Ω_1 (above the blue dashed line) and Ω_2 (under the blue dashed line). The initial points in Ω_1 are finally stable at E_1^* and in Ω_2 are finally stable at E_0^* , which complies with the third rows of Table 2. And the abbreviation notations of Table 2 are shown in Table 1.

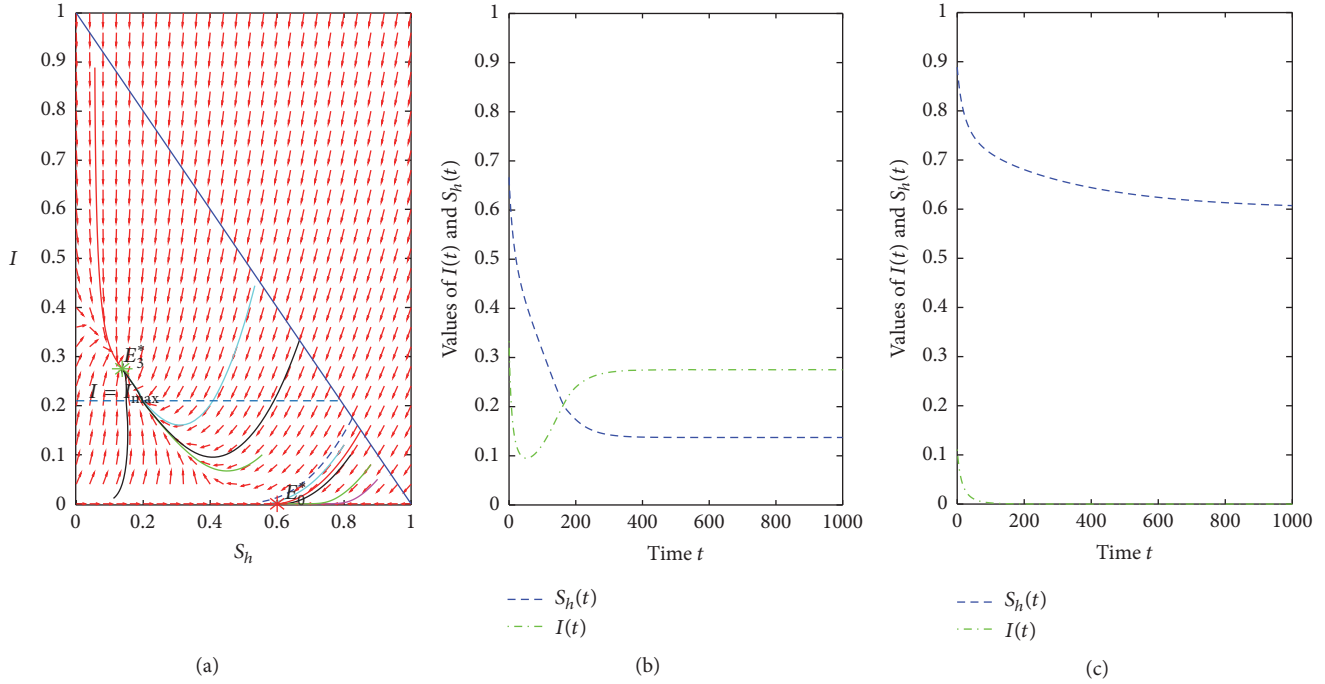


FIGURE 4: Trajectory figure and time plots of Example 2.

TABLE 2: Main result of Section 6.

Conditions			E_0^*	E_1^*	E_2^*	E_3^*	E_4^*
$R_0 < 1$			EG	N	N	N	N
$R_0 < 1$	$B_1 > 1, B_2 > 1, \Delta_1 > 0, \Delta_2 > 0$	$I_1^* < I_{\max}$	EL	EL	E	N	N
		$I_3^* \geq I_{\max} > I_2^*$	EL	N	E	EL	E
		$I_2^* > I_{\max}$	EL	N	N	EL	E
		$I_1^* < I_{\max}$	E	EG	E	N	N
$R_0 > 1$			E	N	N	EG	E

Example 2. Suppose $\beta_l = 0.24, \beta_h = 0.08, \gamma_l = 0.146, \gamma_h = 0.003, b_l = 0.0012, b_h = 0.0018, \mu = 0.003, \alpha = 0.005$, and $I_{\max} = 0.21$. In this situation, $R_0 < 1, I_3^* > I_{\max}$. Some trajectories of initial points are displayed in Figure 4(a) and the time plots about two of them are shown in Figures 4(b) and 4(c). In Figure 4(a), the blue dashed line divides Ω into Ω_1 (above the blue dashed line) and Ω_2 (under the blue dashed line). The initial points in Ω_1 are finally stable at E_3^* and in Ω_2 are finally stable at E_0^* , which complies with lines 4-5 of Table 2.

Example 3. Suppose $\beta_l = 0.24, \beta_h = 0.08, \gamma_l = 0.146, \gamma_h = 0.043, b_l = 0.0012, b_h = 0.0018, \mu = 0.003, \alpha = 0.005$, and $I_{\max} = 0.21$. In this situation, $R_0 < 1$ and there is only E_0^* in the system. Some trajectories of initial points are displayed in Figure 5(a) and the time plots about two of them are shown in Figures 5(b) and 5(c). The initial points in are finally stable at E_0^* , which complies with line 2 of Table 2.

Example 4. Suppose $\beta_l = 0.3, \beta_h = 0.09, \gamma_l = 0.056, \gamma_h = 0.043, b_l = 0.0012, b_h = 0.0018, \mu = 0.003, \alpha = 0.06$,

and $I_{\max} = 0.38$. In this situation, $R_0 > 1, I_1^* < I_{\max}$. Some trajectories of initial points are displayed in Figure 6(a) and the time plots about two of them are shown in Figures 6(b) and 6(c). The initial points in are finally stable at E_1^* , which complies with line 6 of Table 2.

Example 5. Suppose $\beta_l = 0.3, \beta_h = 0.09, \gamma_l = 0.056, \gamma_h = 0.043, b_l = 0.0012, b_h = 0.0018, \mu = 0.003, \alpha = 0.06$, and $I_{\max} = 0.2$. In this situation, $R_0 > 1, I_3^* > I_{\max}$. Some trajectories of initial points are displayed in Figure 7(a) and the time plots about two of them are shown in Figures 7(b) and 7(c). The initial points in are finally stable at E_3^* , which complies with the last row of Table 2.

By introducing random factors and model adaptive behavior, a series of simulations run are used to approximate closer to actual worm propagation due to the unavailability of real-world data. Hosts (used IP addresses) here appear as abstractions in the simulations. Instead of modeling various operating systems and services, each host is simply considered to be one of the following: susceptible nodes with

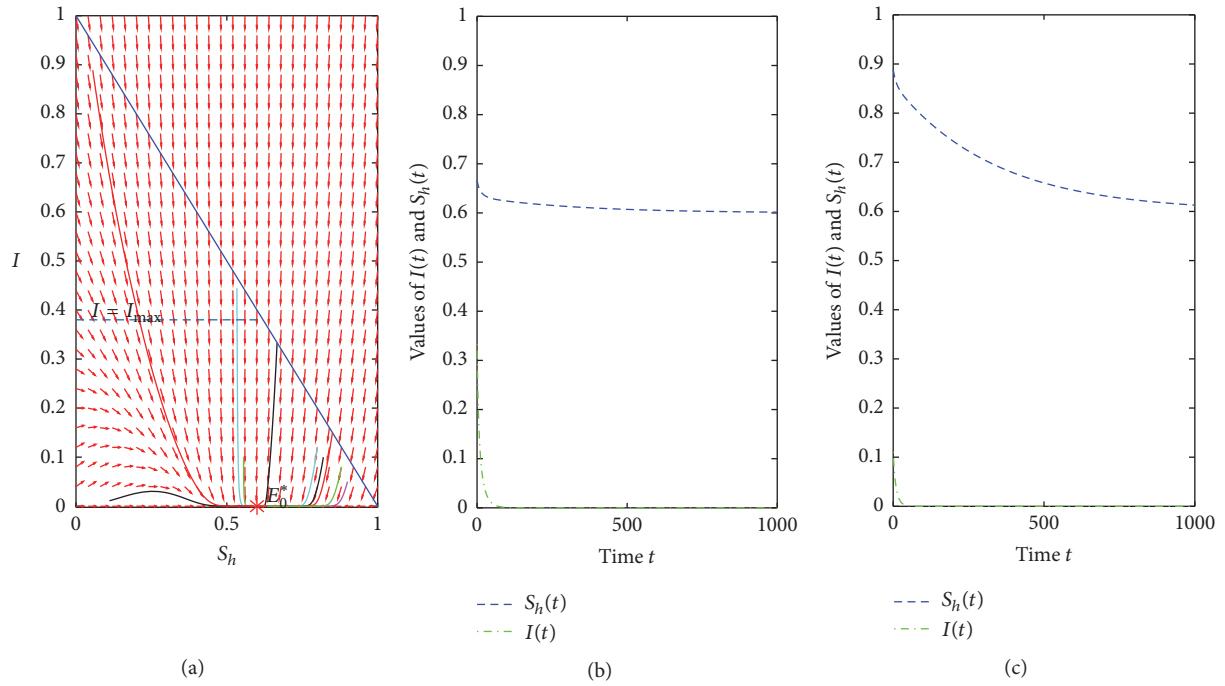


FIGURE 5: Trajectory figure and time plots of Example 3.

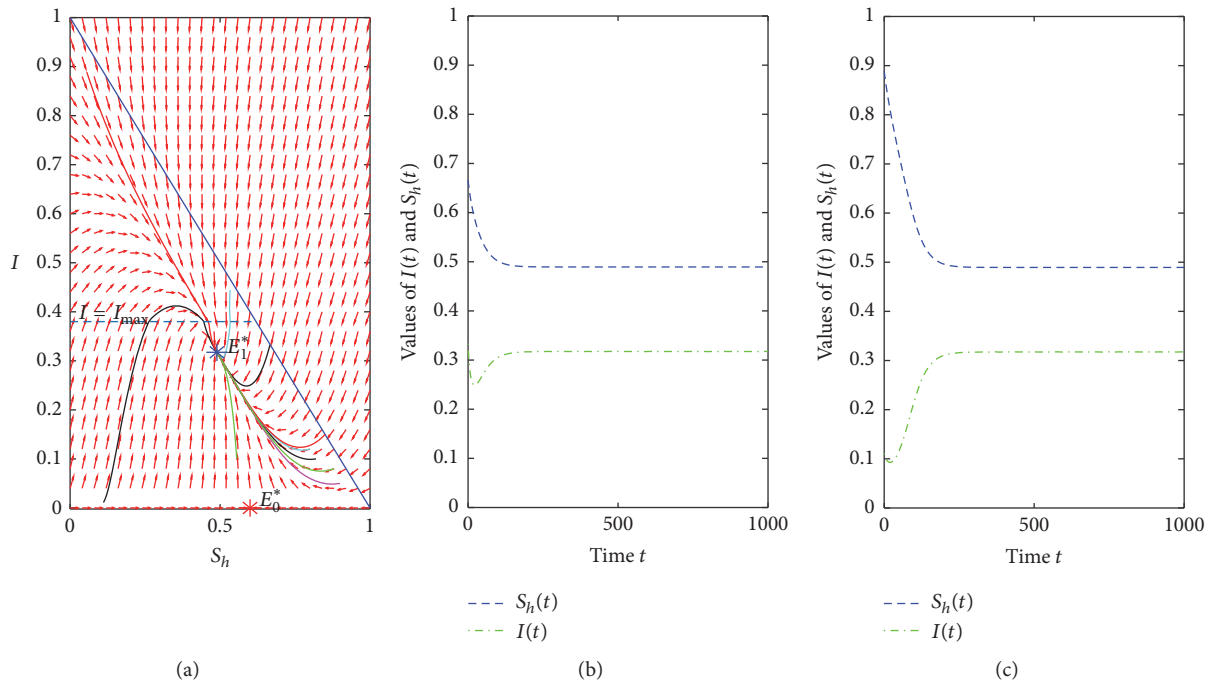


FIGURE 6: Trajectory figure and time plots of Example 4.

high security level, susceptible nodes with low security level, and infected nodes. Here a complete network with initial 10000 nodes is applied for numerical evaluation. And we focus on how the mechanisms of security classification and intervention affect the propagation of network viruses. So we simulate three scenarios for the spread of viruses: (1) non-SC

non-INTVIN scenario, (2) with SC non-INTVIN scenario, and (3) with SC and INTVIN scenario (see Figure 8), where SC and INTVIN are short for security classification and intervention, respectively. And the parameters I_{\max} and α determine when to intervene and the strength of interventions, respectively. For evaluation purpose, the values of the

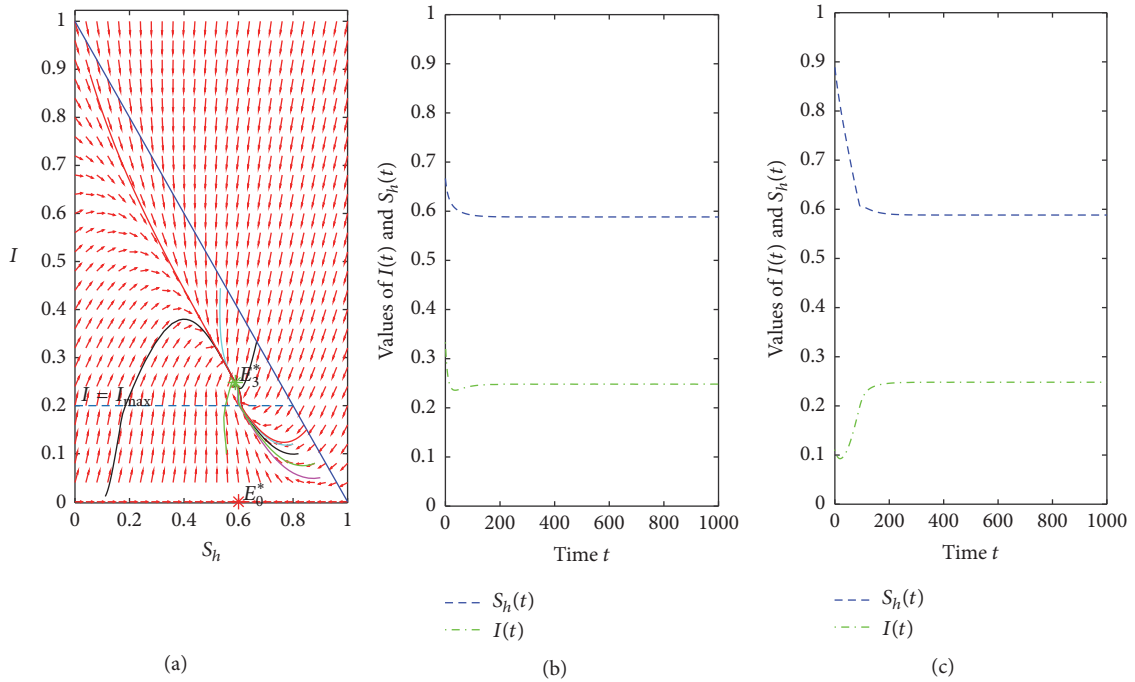


FIGURE 7: Trajectory figure and time plots of Example 5.

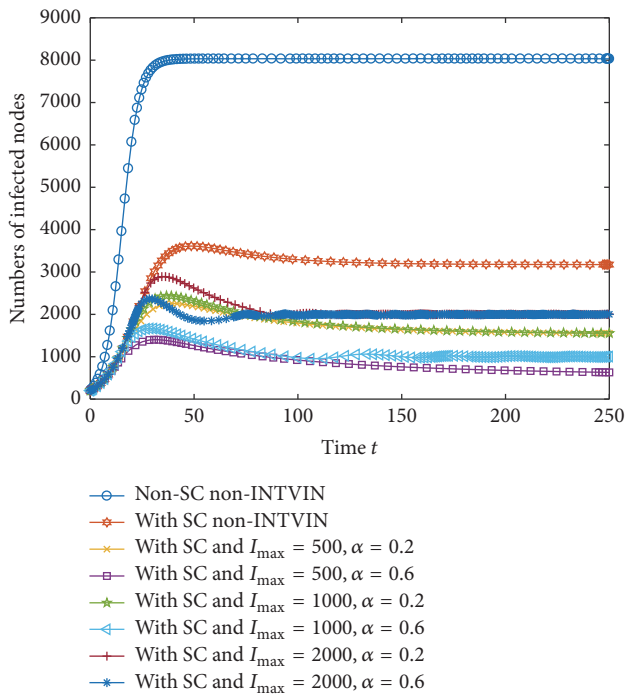


FIGURE 8: Time evolution of the infected nodes in different scenarios.

model parameters are set as follows: $\beta_l = 0.3$, $\beta_h = 0.09$, $\gamma_l = 0.056$, $\gamma_h = 0.043$, $b_l = 0.0012$, $b_h = 0.0018$, $\mu = 0.003$, and other parameters are shown in Figure 8. In general, simulation results show that the intervention mechanism

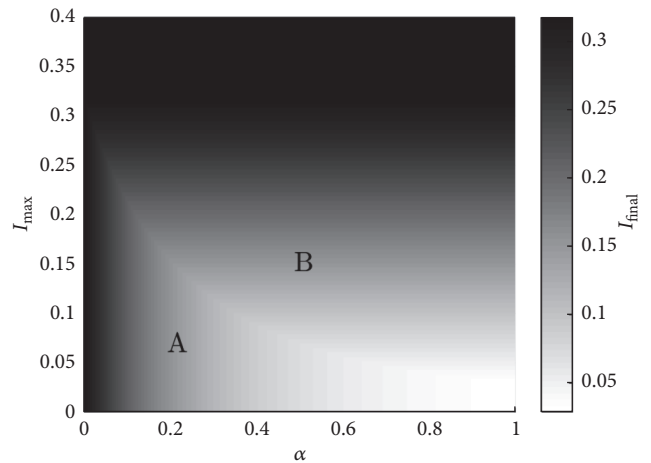


FIGURE 9: Influence of I_{max} and α on I_{final} . I_{max} and I_{final} are the proportions of infected nodes in all nodes. Moreover, I_{final} is the average of 100 values for $t > 10000$. Here all other parameters are the same as Figure 8.

proposed in this paper can be applied to curbing the spread of virus effectively. Moreover, a large number of simulations are conducted to study how the combination of I_{max} and α affects the propagation scale (see Figure 9). Obviously, the earlier (the lower I_{max}) and stronger (the higher α) the intervention is introduced, the fewer the nodes finally get infected. We divide the parameter subspace $\{(\alpha, I_{max}): \alpha > 0, I_{max} > 0\}$ into two parts, numbered as A and B (as shown in Figure 9). Simulation results lead the following conclusion.

- (1) If $(\alpha, I_{\max}) \in A$, the value of I_{final} (defined in Figure 9) only depends on the value of α . So in Figure 8 the number of infected nodes in scenarios with $I_{\max} = 500$ is the same as the one with $I_{\max} = 1000$, where $\alpha = 0.2$, and it is higher than the one with $I_{\max} = 500$ and $\alpha = 0.6$. More precisely, the value of I_{final} decreases as α increasing.
- (2) If $(\alpha, I_{\max}) \in B$, the value of I_{final} only depends on the value of I_{\max} (4). So in Figure 8 the number of infected nodes in scenarios with $\alpha = 0.2$ is the same as the one with $\alpha = 0.6$, where $I_{\max} = 2000$, and it is higher than the one with $I_{\max} = 1000$ and $\alpha = 0.6$. Note that I_{final} does not always decrease with the increase of I_{\max} , because the intervention is never involved for large I_{\max} (see the dark black part for $I_{\max} > 0.3$ in Figure 9).

Remark 6. The simulations here do not take into account latency issues, hop-count, bandwidth limitations, and transfer times or connectivity issues. Since the scale of simulated network is quite small compared with the real Internet, all parameters are assumed on that scale. But the scale factor can also make the real-world more complex.

Table 2 suggests that, to eradicate viruses from the Internet, one should take necessary actions to control the system parameters so that R_0^* is well below 1 and not let system meet the lines 3–5 of Table 2. After simple calculations, the following can be got:

$$\begin{aligned}
\frac{\partial R_0}{\partial \beta_1} &= \frac{b_1}{\mu(\gamma_l + \gamma_h + \mu)} > 0, \\
\frac{\partial R_0}{\partial \beta_h} &= \frac{b_h}{\mu(\gamma_l + \gamma_h + \mu)} > 0, \\
\frac{\partial R_0}{\partial b_1} &= \frac{\beta_1}{\mu(\gamma_l + \gamma_h + \mu)} > 0, \\
\frac{\partial R_0}{\partial b_h} &= \frac{\beta_h}{\mu(\gamma_l + \gamma_h + \mu)} > 0, \\
\frac{\partial R_0}{\partial \mu} &= -\frac{\gamma_l + \gamma_h + 2\mu}{\mu^2(\gamma_l + \gamma_h + \mu)^2} < 0, \\
\frac{\partial R_0}{\partial \gamma_l} &= -\frac{1}{\mu(\gamma_l + \gamma_h + \mu)^2} < 0, \\
\frac{\partial R_0}{\partial \gamma_h} &= -\frac{1}{\mu(\gamma_l + \gamma_h + \mu)^2} < 0.
\end{aligned} \tag{28}$$

Thus, R_0 is increasing with $\beta_1, \beta_h, b_1, b_h$ and is decreasing with μ, γ_l, γ_h .

Based on the above discussions, an incomplete list of effective measures for users to contain the virus prevalence is presented below:

- (1) Timely acquire the updated versions of the antivirus software, so that the two infecting probabilities, β_1 and

β_h , are both reduced and the curing probabilities, γ_l and γ_h , are enhanced.

- (2) Do not connect computers to the Internet when unnecessary, so that the recruitment rate, μ , is lowered.
- (3) For both cost and security, let the threshold value of computer virus lead administrator to take measures to upgrade the security level approaching the value of stable infections in the stage of taking measures.

8. Conclusions

In this paper, we presented a novel intervention mechanism to restrain the virus spreading under the framework of security classification. The model reflects a realistic scenario how the intervention is applied when the number of infected nodes reaches the intervention threshold. Theoretical analysis and numerical evaluation are used to study how I_{\max} , α affect the propagation behaviors. The main results are listed as follows: (1) The dynamic behaviors of computer virus under security classification are different with common circumstance. Obviously, much higher security computers will lead to fewer infections. (2) The earlier and the stronger the intervention is introduced, the fewer the nodes finally get infected. (3) According to the brief parameter analysis, some other effective measures in reality are presented. Viewed from a real-world perspective, in order to make better use of this intervention mechanism, one of the most important things is how to detect the exact number of infected nodes. Although an in-depth discussion of this is outside this paper's scope, we are forced to point out that the measured value is below the actual one. In this case, the actual value of intervention threshold must be set below the theoretical one.

Our future work will be focused on studying such intervention mechanism in heterogeneous networks, such as small-world network and scale-free network.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by Chongqing Engineering Research Center of Mobile Internet Data Application, Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant nos. KJ1500415, KJ1400414, KJ1500434, and KJ1704080), Doctoral Scientific Research Foundation of Chongqing University of Posts and Telecommunications (Grant no. A2015-02), and the National Natural Science Foundation of China (no. 61672004).

References

- [1] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 343–359, Oakland, Calif, USA, May 1991.

- [2] M. Kjaergaard, S. Brander, and F. M. Poulsen, "Small but slow world: how network topology and burstiness slow down spreading," *Physical Review E*, vol. 83, no. 83, pp. 602–608, 2010.
- [3] C. Castellano and R. Pastor-Satorras, "Thresholds for epidemic spreading in networks," *Physical Review Letters*, vol. 105, no. 21, Article ID 218701, 2010.
- [4] G. Zhu, X. Fu, and G. Chen, "Global attractivity of a network-based epidemic SIS model with nonlinear infectivity," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 6, pp. 2588–2594, 2012.
- [5] L.-X. 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] L.-X. Yang and X. Yang, "The spread of computer viruses over a reduced scale-free network," *Physica A: Statistical Mechanics and Its Applications*, vol. 396, pp. 173–184, 2014.
- [7] L.-X. Yang, M. Draief, and X. Yang, "The impact of the network topology on the viral prevalence: a node-based approach," *PLoS ONE*, vol. 10, no. 9, Article ID e0134507, 2015.
- [8] B. K. Mishra, K. Haldar, and D. N. Sinha, "Impact of information based classification on network epidemics," *Scientific Reports*, vol. 6, Article ID 28289, 2016.
- [9] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, vol. E98B, no. 1, pp. 190–200, 2015.
- [10] Q. Liu, W. Cai, J. Shen, Z. Fu, X. Liu, and N. Linge, "A speculative approach to spatial-temporal efficiency with multi-objective optimization in a heterogeneous cloud environment," *Security and Communication Networks*, vol. 9, no. 17, pp. 4002–4012, 2016.
- [11] G. Juve and E. Deelman, "Wrangler: Virtual cluster provisioning for the cloud," in *Proceedings of 20th ACM International Symposium on High-Performance Parallel and Distributed Computing, HPDC'11*, pp. 277–278, San Jose, Calif, USA, June 2011.
- [12] L. H. Zeng, B. F. Zhang, and L. H. Zhang, "Virtual cluster constructing based on cloud computing platform," *Microelectronics Computer*, vol. 27, no. 8, pp. 31–39, 2010.
- [13] C. Gan, X. Yang, and Q. Zhu, "Propagation of computer virus under the influences of infected external computers and removable storage media: modeling and analysis," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1349–1356, 2014.
- [14] C. Gan and X. Yang, "Theoretical and experimental analysis of the impacts of removable storage media and antivirus software on viral spread," *Communications in Nonlinear Science and Numerical Simulation*, vol. 22, no. 1–3, pp. 611–622, 2014.
- [15] C. Gan, X. Yang, W. Liu, and Q. Zhu, "A propagation model of computer virus with nonlinear vaccination probability," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 92–100, 2014.
- [16] C. Gan, "Modeling and analysis of the effect of network eigenvalue on viral spread," *Nonlinear Dynamics*, vol. 84, no. 3, pp. 1727–1733, 2016.
- [17] J. Amador and J. R. Artalejo, "Stochastic modeling of computer virus spreading with warning signals," *Journal of the Franklin Institute. Engineering and Applied Mathematics*, vol. 350, no. 5, pp. 1112–1138, 2013.
- [18] W. Liu and S. Zhong, "Web malware spread modelling and optimal control strategies," *Scientific Reports*, vol. 7, Article ID 42308, 2017.
- [19] H. Yuan, G. Liu, and G. Chen, "On modeling the crowding and psychological effects in network-virus prevalence with nonlinear epidemic model," *Applied Mathematics and Computation*, vol. 219, no. 5, pp. 2387–2397, 2012.
- [20] L. Qiu, Y. Zhang, F. Wang, H. R. Mahajan, and M. Kyung, "Trusted computer system evaluation criteria," *Classified Information*, 2007.
- [21] J. Noorman, P. Agten, W. Daniels et al., "Sancus: low-cost trustworthy extensible networked devices with a zero-software trusted computing base," in *Proceedings of the Usenix Conference on Security*, pp. 479–494, 2013.
- [22] L.-X. Yang and X. Yang, "The effect of infected external computers on the spread of viruses: a compartment modeling study," *Physica A. Statistical Mechanics and Its Applications*, vol. 392, no. 24, pp. 6523–6535, 2013.
- [23] H. R. Thieme, "Asymptotically autonomous differential equations in the plane," *The Rocky Mountain Journal of Mathematics*, vol. 24, no. 1, pp. 351–380, 1994.
- [24] R. C. Robinson, *An Introduction to Dynamical System: Continuous and Discrete*, Prentice Hall, New Jersey, NJ, USA, 2004.



Hindawi

Submit your manuscripts at
<https://www.hindawi.com>

