Applied Mathematical Modelling 39 (2015) 4121–4133

Contents lists available at ScienceDirect

Applied Mathematical Modelling

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

Investigation of the C-SEIRA model for controlling malicious code infection in computer networks

Inkyung Ahn [a], Hyeong-Cheol Oh [b], Jooyoung Park [c,*]

[a] Department of Mathematics, Korea University, Sejong 339-700, Republic of Korea
[b] Department of Electronics and Information Engineering, Korea University, Sejong 339-700, Republic of Korea
[c] Department of Control and Instrumentation Engineering, Korea University, Sejong 339-700, Republic of Korea

ARTICLE INFO

Article history:
Received 24 April 2013
Received in revised form 5 September 2014
Accepted 15 December 2014
Available online 24 December 2014

Keywords:
Malicious code infection
Computer worms
Epidemic model
Network population model
Stability
Optimal control

ABSTRACT

Recently, there has been great concern about the serious burden and damage caused by malicious objects, such as computer worms, on the Internet. Therefore, the establishment of efficient policies for preventing the propagation of malicious objects becomes an important issue in the operation of computer networks. Because the propagation of malicious code is similar in many aspects to the infectious spread of biological viruses, ordinary-differential-equation-based population models, frequently used in the field of epidemiology, are useful in studying the population change of infectious hosts in computer networks. In this paper, we propose the controlled susceptible-exposed-infectious-removed-antidotal (C-SEIRA) model, an epidemiological population model describing the state transitions of a computer network under malicious code infection. For the proposed model, we derive stability results for the infection-free state and the endemic state. In addition, we apply optimal control theory to the C-SEIRA model with the goal of minimizing the infectious compartment population and the system treatment cost of isolating infectious computers from the network. Simulation results show that the spread of malicious objects can be controlled reasonably well via the optimal control approach.

1. Introduction

As the Internet becomes increasingly prevalent in everyday life, there has been great concern about the serious burden and damage caused by malicious objects such as computer worms. In order to protect against such malicious actions, various human countermeasures based on anti-malicious software are developed and distributed each time a new malicious object appears. As a result, macroscopic approaches (e.g., [1–8]), which develop mathematical models for the malicious object propagation and/or establish efficient policies based on a model for controlling the malicious code infection, have become an important research issue in computer security. Because the propagation of malicious code is similar in many aspects to the infectious spread of biological viruses, ordinary differential equation (ODE)-based population models, frequently used in the field of epidemiology [9], are useful in studying the population change of infectious hosts in computer networks.

In this paper, we propose a controlled susceptible-exposed-infectious-removed-antidotal (C-SEIRA) model, which is an ODE-based epidemiological population model describing the state transitions of a computer network under malicious worm infection. A network worm is a malicious object that is designed to replicate itself and spread to other computers across a

[*] Corresponding author.
E-mail address: parkj@korea.ac.kr (J. Park).

http://dx.doi.org/10.1016/j.apm.2014.12.038
0307-904X/© 2014 Elsevier Inc. All rights reserved.

network. Worms, with or without payloads, often use up network resources and cause devastating events, such as denial-of-service (DoS) attacks or system shutdowns, on the network. Some recent worms, such as the much-talked-about Blaster worm, even allow malicious persons to remotely control the victims' computers. In the C-SEIRA model, we view the system treatment effort of isolating infectious hosts from the network as the control action. In general, it takes some time to develop and distribute such countermeasures for a new worm, so the worm may infect many computers on the network before countermeasures are put in place. This problem can be mitigated by detecting the infected computers as soon as possible, and then isolating them from the network until the proper countermeasures are developed and distributed. One way to detect the advent of a new network worm is to utilize the security gateways that monitor the aggressive scanning traffic that the worm sends out to look for susceptible computers [10]. The security system assumed in this paper operates against network worms in two phases. In its quarantine phase, the system detects the advent of a new worm and infected computers at the gateways, and isolates the infected computers from the network. In its vaccination phase, the worms, as for other malicious objects, are removed or cured locally on each infected computer. Fig. 1 shows a conceptual description of the operation of the security gateway assumed in this paper [11,12]. Internet data (packets) pass through the gateway to a router that contains an Ethernet switch connected to a number of computers. Packets from the computers also pass through the router and the gateway to the Internet. For the purpose of security, the gateway sends data to the monitor system before it passes them to the router or the Internet. The software or hardware of the monitor system can check all the packets. Once a computer infected with the new worm is detected, the gateways isolate the infected computer from the network by filtering out packets from that computer. After the countermeasures have taken place, the worms are removed or cured locally at computers or their firewall, as are other malicious objects. If the gateway checks all the packets and isolates all the infected computers until the countermeasures take place, the performance of the network can be significantly degraded due to the operation delay of the gateway. On the other hand, if the level (rate) of inspection and isolation is too low, the network can be full of infected computers. A similar quarantine method was discussed in [13], where the authors argue that it is difficult to find packets from unknown worms, meaning that many legitimate connections may be blocked. Thus, [13] proposed a dynamic quarantine method, in which a suspicious computer is quarantined and released automatically after a short time. In practice, it is a costly process for a security gateway to identify a worm packet in a high-speed (gigabit or terabit) network. For example, in order to identify a packet belonging to the "Code Red" worm, it is necessary to search packets for the string ".ida?" using deep packet inspection (DPI) [12–15], which is still too slow to be adopted in a gateway. The security gateway assumed in this paper does not inspect the packet payload; instead, it inspects the packet header to identify the address of the computer(s) that sent out the aggressive scanning traffic to look for victims. In this paper, we consider the case where the level (rate) of inspection and isolation is controlled. Hence, the exact meaning of the control input in the C-SEIRA model is the isolation rate of infectious computer hosts resulting from the system treatment effort of inspection and isolation. For the proposed C-SEIRA model, we derive stability results for the infection-free state and the endemic state. Optimal control theory is also applied to the C-SEIRA model, with the goal of minimizing the infectious compartment population and the system treatment cost of isolating infectious computers from the network. Simulation results show that the spread of malicious objects can be controlled reasonably well via the optimal control approach.

The remainder of this paper is organized as follows: in Section 2, we introduce the C-SEIRA model, an ODE-based epidemiological model for controlling the propagation of malicious objects. Section 3 presents a stability analysis for the infection-free equilibrium point and the endemic equilibrium point of the C-SEIRA model. Section 4 describes the optimal-control-based system treatment policy and presents our simulation results. Finally, Section 5 gives our concluding remarks.

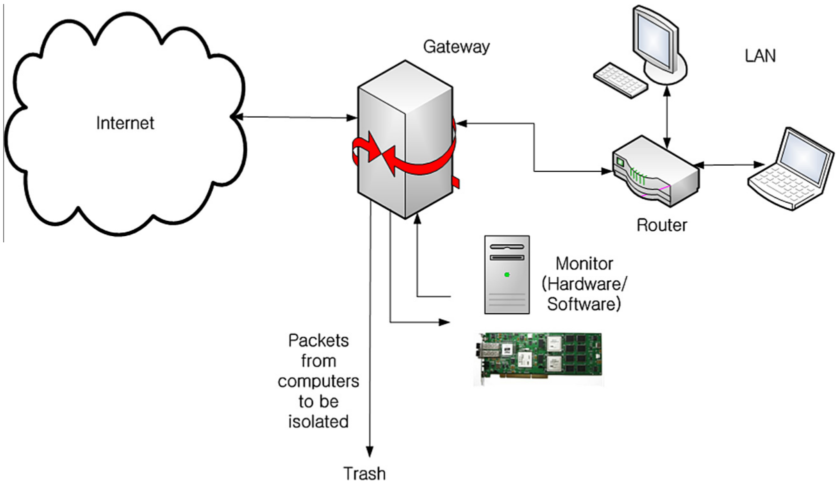
Internet
Gateway
LAN
Router
Monitor (Hardware/ Software)
Packets from computers to be isolated
Trash

Fig. 1. A security gateway. The monitor (hardware or software) is a part of the gateway.

2. The C-SEIRA model

In this section, we describe the C-SEIRA model, an ODE-based model for controlling the propagation of malicious worms in computer networks. The C-SEIRA model is a modification of various ODE-based epidemiological network population models involving S and I (and other) compartments (e.g., [4–9,27,10–25]). In the C-SEIRA model, a total of N computer hosts are partitioned into five compartments, and the five compartment populations are used as the model's state variables: $S(t)$, the number of computer hosts that are susceptible to malicious object attack at time t; $E(t)$, the number of computer hosts that have been exposed to malicious object attack but are not yet actively infectious at time t; $I(t)$, the number of computer hosts that are actively infectious at time t; $R(t)$, the number of computer hosts that have been removed from the network due to death from infection or forced isolation as a result of system treatment effort; $A(t)$, the number of computer hosts that have been restored (from the removed state) and equipped with up-to-date anti-malicious software. The C-SEIRA model considers two kinds of security countermeasures against malicious object attack: the vaccination of computer hosts using anti-malicious software; and the system treatment effort, at the gateway in Fig. 1, of isolating infectious computer hosts from the network.

When vaccination with anti-malicious software is the only security countermeasure available, we can describe the population dynamics of the computer network using the following *basic* SEIRA (susceptible-exposed-infectious-removed-antidotal) model:

$$\begin{aligned}
\dot{S}(t) &= -\beta S(t)I(t)/N - \gamma_S S(t) + \phi A(t)\\
\dot{E}(t) &= \beta S(t)I(t)/N - \alpha E(t) - \gamma_E E(t)\\
\dot{I}(t) &= \alpha E(t) - \gamma_I I(t) - \theta I(t)\\
\dot{R}(t) &= \theta I(t) - \eta R(t)\\
\dot{A}(t) &= \gamma_S S(t) + \gamma_E E(t) + \gamma_I I(t) + \eta R(t) - \phi A(t).
\end{aligned} \tag{2.1}$$

The first equation of (2.1) describes the rate of change of the susceptible compartment population. Its right-hand-side has three terms. The first concerns the transition from the susceptible state to the exposed state due to malicious code infection. This infection is explained by a bilinear incidence law with contact rate β. The second term models the transition from the susceptible state to the antidotal state due to the security countermeasure of vaccination. The third term represents the transition from the antidotal state to the susceptible state, and this transition can be interpreted as a loss of immunity (due to, e.g., the emergence of new computer worms). The behavior of the exposed compartment population, which is modeled by the second equation of (2.1), is also described by a bilinear incidence with contact rate β, combined with a transition into the infectious state after the latent period, and a transition into the antidotal state by acquiring security from vaccination. In the third equation of (2.1), the rate of change of the infectious compartment population is described by three terms. The first represents the transition from the exposed state to the infectious state, which occurs when the latency is over, and the second term describes the transition from the infectious state to the antidotal state due to vaccination. The third term denotes the transition from the infectious state to the removed state due to death from infection. The fourth equation of (2.1) describes the rate of change of the removed compartment population, and its right-hand-side has two terms. The first represents the death of hosts resulting from malicious object attack, and the second term describes the restoration from the removed state into the antidotal state. Finally, the fifth equation of (2.1) represents the rate of change of the antidotal compartment population. The first three terms of its right-hand-side represent the vaccination-based state transitions to the antidotal state from S, E, and I, respectively, and the fourth term denotes restoration from the removed state. The final term of the fifth equation denotes the transition from the antidotal state to the susceptible state due to the loss of immunity. Note that the usual birth and death rates not due to malicious code infection are all omitted in this model. This omission allows us to focus on the core theme of the paper, and consideration of these additional aspects is relatively straightforward. As a result of this omission, we have

$$S(t) + E(t) + I(t) + R(t) + A(t) = N \tag{2.2}$$

throughout the entire time interval. Note also that, when the dead hosts are restored, the model assumes that they are all equipped with up-to-date anti-malicious software and belong to the antidotal state. This assumption seems to be reasonable in many cases, and is used in related studies (e.g., [7]). If it is necessary to consider a more general case (e.g., when antidotal status is not guaranteed and some hosts are still susceptible upon restoration from death), the model can be changed accordingly (e.g., by introducing a new state transition path from the removed state to the susceptible state).

In the C-SEIRA model, we view the system treatment effort of isolating infectious hosts from the network as the action that controls the entire process, and use it as our control action. By incorporating the control action $u(t)$ into our basic SEIRA model (2.1), we obtain the following state equation for C-SEIRA:

$$\begin{aligned}
\dot{S}(t) &= -\beta S(t)I(t)/N - \gamma_S S(t) + \phi A(t)\\
\dot{E}(t) &= \beta S(t)I(t)/N - \alpha E(t) - \gamma_E E(t)\\
\dot{I}(t) &= \alpha E(t) - \gamma_I I(t) - \theta I(t) - I(t)u(t)\\
\dot{R}(t) &= \theta I(t) - \eta R(t) + I(t)u(t)\\
\dot{A}(t) &= \gamma_S S(t) + \gamma_E E(t) + \gamma_I I(t) + \eta R(t) - \phi A(t).
\end{aligned} \tag{2.3}$$

In (2.3), $u(t)$ is the isolation rate of infectious computer hosts provided by the system treatment effort. The equation structure and state transitions of the C-SEIRA model are shown in Figs. 2 and 3, respectively. An explanation of the C-SEIRA parameters is given in Table 1.

3. Stability analysis

In this section, we investigate the asymptotic stability at the infection-free and endemic equilibria of model (2.3). Since $N = S(t) + E(t) + I(t) + R(t) + A(t)$, we may reduce (2.3) to the following equivalent system:

$$\begin{aligned}\dot{S}(t) &= -\beta S(t)I(t)/N - \gamma_S S(t) + \phi(N - S(t) - E(t) - I(t) - R(t))\\ \dot{E}(t) &= \beta S(t)I(t)/N - \alpha E(t) - \gamma_E E(t)\\ \dot{I}(t) &= \alpha E(t) - \gamma_I I(t) - \theta I(t) - I(t)u(t)\\ \dot{R}(t) &= \theta I(t) - \eta R(t) + I(t)u(t)\end{aligned} \tag{3.1}$$

on the closed, positively invariant set

$$\Gamma = \{(S, E, I, R) \in \mathbf{R}^4_+ : S + E + I + R \leqslant N\}.$$

Denote the interior of Γ by $\mathring{\Gamma}$. We define the reproduction rate as

$$R_0 = \frac{\alpha\beta\phi}{(\gamma_S + \phi)(\gamma_I + \theta)(\alpha + \gamma_E)}. \tag{3.2}$$

Besides the trivial solution, (3.1) has the following non-negative equilibria in Γ: the infection-free equilibrium

$$P_0 := \left(\frac{\phi}{\gamma_S + \phi}N, 0, 0, 0\right) \tag{3.3}$$

and a unique positive endemic equilibrium

$$P^* := (S^*, E^*, I^*, R^*) = \left(\frac{(\gamma_I + \phi)(\alpha + \gamma_E)}{\alpha\beta}N, AN, \frac{\alpha}{\gamma_I + \theta}E^*, \frac{\alpha\theta}{\eta(\gamma_I + \theta)}E^*\right), \tag{3.4}$$

if and only if the threshold condition $R_0 > 1$ holds, where

$$A := \frac{\eta(\gamma_I + \theta)[\phi\alpha\beta - (\gamma_S + \phi)(\gamma_I + \theta)(\alpha + \gamma_E)]}{\alpha\beta[\eta(\alpha + \gamma_E + \phi)(\gamma_I + \theta) + \phi\alpha(\eta + \theta)]}. \tag{3.5}$$

First, we determine the local stability of the equilibria of the system. The following result describes the stability of each equilibrium in terms of R_0.

Theorem 3.1.

(i) *The infection-free equilibrium P_0 is locally asymptotically stable if $R_0 < 1$ and unstable if $R_0 > 1$.*
(ii) *If $R_0 > 1$, then the endemic equilibrium P^* is locally asymptotically stable.*

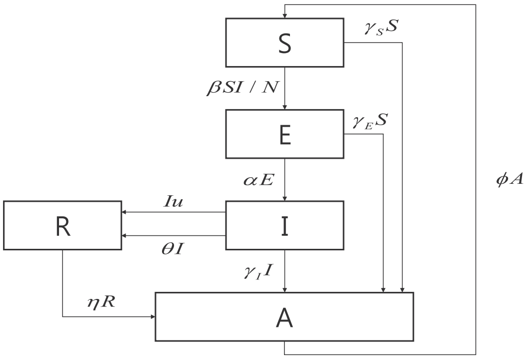

Fig. 2. The C-SEIRA model.

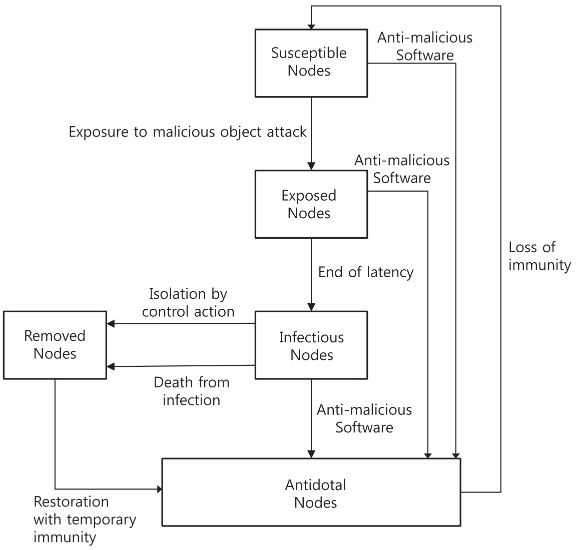

Fig. 3. State transition flow in the C-SEIRA model.

Table 1
Parameters for the C-SEIRA model.

Notation	Meaning
N	Total number of computer hosts
β	Contact rate
α	State transition rate from E to I
γ_S	State transition rate from S to A
γ_E	State transition rate from E to A
γ_I	State transition rate from I to A
ϕ	State transition rate from A to S
θ	Death rate due to malicious code infection
η	Restoration rate from R to A

Proof. We can find the Jacobian matrix, denoted by $J(P_0)$, of the system at P_0:

$$J(P_0)=\begin{pmatrix}-(\gamma_S+\phi) & -\phi & -\frac{\beta\phi}{(\gamma_S+\phi)}-\phi & -\phi\\ 0 & -(\alpha+\gamma_E) & \frac{\beta\phi}{(\gamma_S+\phi)} & 0\\ 0 & \alpha & -(\gamma_I+\theta) & 0\\ 0 & 0 & \theta & -\eta\end{pmatrix}.$$

The characteristic equation of $J(P_0)$ can then be found as

$$[\lambda+(\gamma_S+\phi)](\lambda+\eta)[\lambda^2+(\gamma_I+\theta+\alpha+\gamma_E)\lambda]+\left[(\alpha+\gamma_E)(\gamma_I+\theta)-\frac{\alpha\beta\phi}{\gamma_S+\phi}\right]=0.$$

Thus, $\lambda_1=-(\gamma_S+\phi),\lambda_2=-\eta$ and the other two eigenvalues also are negative, since $(\alpha+\gamma_E)(\gamma_I+\theta)-\frac{\alpha\beta\phi}{\gamma_S+\phi}>0$ by the assumption that $R_0<1$, i.e., all eigenvalues of $J(P_0)$ are negative. Therefore, by the stability theorem, we conclude that the equilibrium point P_0 is locally asymptotically stable.

For the stability of P^*, it is again sufficient to show that all eigenvalues of the Jacobian matrix at the endemic equilibrium are negative. The Jacobian is given by

$$J(P^*)=\begin{pmatrix}-\frac{\alpha\beta}{\gamma_I+\theta}A-(\gamma_S+\phi) & -\phi & -\frac{(\gamma_I+\theta)(\alpha+\gamma_E)}{\alpha}-\phi & -\phi\\ \frac{\alpha\beta}{\gamma_I+\theta}A & -(\alpha+\gamma_E) & \frac{(\gamma_I+\theta)(\alpha+\gamma_E)}{\alpha} & 0\\ 0 & \alpha & -(\gamma_I+\theta) & 0\\ 0 & 0 & \theta & -\eta\end{pmatrix},$$

where A is defined in (3.5). The characteristic equations are then

$$(\lambda+\eta)(a_3\lambda^3+a_2\lambda^2+a_1\lambda+a_0)=0, \tag{3.6}$$

where

$$\begin{aligned}
a_3 &= 1\\
a_2 &= \gamma_I + \theta + \alpha + \gamma_E + \gamma_S + \phi + \frac{\alpha\beta}{\gamma_I+\theta}A,\\
a_1 &= (\gamma_I+\theta)\left(\frac{\alpha\beta}{\gamma_I+\theta}A + \gamma_S + \phi + \alpha + \gamma_E\right),\\
&\quad + (\alpha+\gamma_E)\left(\frac{\alpha\beta}{\gamma_I+\theta}A + (\gamma_S+\phi) + (\gamma_I+\theta)\right) + \frac{\alpha\beta\phi}{\gamma_I+\theta}A,\\
a_0 &= \frac{\alpha^2\beta}{\gamma_I+\theta}A\left(\frac{(\gamma_I+\theta)(\alpha+\gamma_E)}{\alpha} + \phi\right) + 2\frac{\alpha\beta}{\gamma_I+\theta}A(\alpha+\gamma_E)(\gamma_I+\theta),\\
&\quad + 2(\alpha+\gamma_E)(\gamma_I+\theta)(\gamma_S+\phi),
\end{aligned}$$

where A is defined in (3.5). Thus, $\lambda_1 = -\eta$, and the other three eigenvalues are also negative, by the Routh–Hurwitz criterion, because all of the coefficients $a_i, i = 1, 2, 3, 4$, are strictly positive and $a_1 \cdot a_2 > a_0 \cdot a_3$ is satisfied. Therefore, the endemic equilibrium is locally asymptotically stable. □

We now discuss the global stability of the equilibria of the system. The following theorem provides the global stability of the infection-free state.

Theorem 3.2.

(i) *If $R_0 \leqslant 1$, then P_0 is the only equilibrium and is globally stable in Γ.*
(ii) *If $R_0 > 1$, then P_0 is unstable and there exists a unique endemic equilibrium P^*. Moreover, all solutions starting in Γ and sufficiently close to P_0 move away from P_0 if $R_0 > 1$.*

Proof.

(i) Define the function

$$L_0(E, I) = \alpha E + (\alpha + \gamma_E)I.$$

Then,

$$\begin{aligned}
\frac{dL_0}{dt} &= \alpha\left(\beta\frac{SI}{N} - (\alpha+\gamma_E)E\right) + (\alpha+\gamma_E)[\alpha E - (\gamma_I+\theta)I] \leqslant \frac{\alpha\beta\phi}{\gamma_S+\phi}I - \alpha(\alpha+\gamma_E)E + \alpha(\alpha+\gamma_E)E - (\alpha+\gamma_E)(\gamma_I+\theta)I\\
&= I\left(\frac{\alpha\beta\phi}{\gamma_S+\phi} - (\alpha+\gamma_E)(\gamma_I+\theta)\right) = (\alpha+\gamma_E)(\gamma_I+\theta)I\left[\frac{\alpha\beta\phi}{(\alpha+\gamma_E)(\gamma_I+\theta)(\gamma_S+\phi)} - 1\right] \leqslant 0,
\end{aligned}$$

since $R_0 = \frac{\alpha\beta\phi}{(\alpha+\gamma_E)(\gamma_I+\theta)(\gamma_S+\phi)} \leqslant 1$ and $S(t) \leqslant \frac{\phi}{\gamma_S+\phi}N$. Note that $\frac{dL_0}{dt} = 0$ if and only if $E = I = 0$. Thus, L is a Lyapunov function on Γ. Hence, the largest compact invariant subset of Γ satisfying $\frac{dL_0}{dt} = 0$ is the singleton $\{(E, I) = (0, 0)\}$. Thus, by LaSalle's invariance theorem [26],

$$(E, I) \longrightarrow (0, 0)$$

as $t \longrightarrow \infty$. Since $\limsup_{t\to\infty} I = 0$ and $\liminf_{t\to\infty} I = 0$, for sufficiently small $c > 0$, there exists $M > 0$ such that $\limsup_{t\to\infty} I \leqslant c$, for all $t > M$, and so

$$\frac{dR}{dt} \leqslant \theta c - \eta R.$$

By the comparison theorem, $\limsup_{t\to\infty} R \leqslant \frac{\theta c}{\eta}$ and, as $c \to 0$, $\limsup_{t\to\infty} R \leqslant 0$. Similarly, we can show that $\liminf_{t\to\infty} R \geqslant 0$. Thus, $\lim_{t\to\infty} R = 0$. Using a similar argument, it can be shown that

$$\lim_{t\to\infty} S(t) = \frac{\phi N}{\gamma_S + \phi}.$$

Therefore, we conclude that every solution of the model in Γ approaches $\left(\frac{\phi N}{\gamma_S+\phi}, 0, 0, 0\right)$ as $t \to \infty$.

(ii) The claim follows since $\frac{dL_0}{dt} > 0$ if $R_0 > 1$. □

Finally, we obtain the following result, which gives the global stability for the endemic state of the model.

Theorem 3.3. *Assume that $R_0 > 1$. In addition, suppose the following inequalities hold:*

$$min\left\{\alpha + 2\gamma_E - \phi - \frac{\alpha\beta A}{\gamma_I + \theta}, \gamma_I + \frac{1}{2}(\theta - \alpha - \phi), \frac{\alpha\beta A}{\gamma_I + \theta} + 2\gamma_S - \phi\right\} \geqslant \frac{\beta\phi}{\gamma_S + \phi} \tag{3.7}$$

and

$$\eta \geqslant \frac{1}{2}(\phi + \theta), \tag{3.8}$$

where A is defined in (3.5). The unique endemic equilibrium P^* is then globally asymptotically stable in $\mathring{\Gamma}$.

Proof. Define a positive definite function

$$L(S,E,I,R) = \frac{1}{2}(S - S^*)^2 + \frac{1}{2}(E - E^*)^2 + \frac{1}{2}(I - I^*)^2 + \frac{1}{2}(R - R^*)^2.$$

Using the fact that (S^*, E^*, I^*, R^*) satisfies system (3.1), we have

$$\begin{aligned}
\frac{dL}{dt} &= (S-S^*)\frac{dS}{dt} + (E-E^*)\frac{dE}{dt} + (I-I^*)\frac{dI}{dt} + (R-R^*)\frac{dR}{dt} \\
&= (S-S^*)\left(-\beta\frac{SI}{N} + \phi N - (\gamma_S+\phi)S - \phi E - \phi I - \phi R + \beta\frac{S^*I^*}{N} - \phi N + (\gamma_S+\phi)S^* + \phi E^* + \phi I^* + \phi R^*\right) \\
&\quad + (E-E^*)\left(\beta\frac{SI}{N} - (\alpha+\gamma_E)E - \beta\frac{S^*I^*}{N} + (\alpha+\gamma_E)E^*\right) + (I-I^*)(\alpha E - (\gamma_I+\theta)I - \alpha E^* - (\gamma_I+\theta)I^*) + (R-R^*)(\theta I - \eta R - \theta I^* - \eta R^*) \\
&= (S-S^*)\Big\{-\frac{\beta}{N}(S(I-I^*) + I^*(S-S^*)) - (\gamma_S+\theta)(S-S^*) \\
&\quad -\phi(E-E^*) - \phi(I-I^*) - \phi(R-R^*)\Big\} + (E-E^*)\left\{\frac{\beta}{N}[S(I-I^*) + I^*(S-S^*)] - (\alpha+\gamma_E)(E-E^*)\right\} \\
&\quad + (I-I^*)[\alpha(E-E^*) - (\gamma_I+\theta)(I-I^*)] + (R-R^*)[\theta(I-I^*) - \eta(R-R^*)] \\
&= -\left(\frac{\beta}{N}I^* + \gamma_S + \phi\right)(S-S^*)^2 - \frac{\beta}{N}(S-S^*)S(I-I^*) - \phi(S-S^*)(E-E^*) - \phi(S-S^*)(I-I^*) \\
&\quad - \phi(S-S^*)(R-R^*) - (\alpha+\gamma_E)(E-E^*)^2 + \frac{\beta}{N}(E-E^*)[S(I-I^*) + I^*(S-S^*)] + \alpha(I-I^*)(E-E^*) \\
&\quad - (\gamma_I+\theta)(I-I^*)^2 + \theta(R-R^*)(I-I^*) - \eta(R-R^*)^2 \\
&= -\left(\frac{\beta}{N}I^* + \gamma_S + \phi\right)(S-S^*)^2 - (\alpha+\gamma_E)(E-E^*)^2 \\
&\quad - (\gamma_I+\theta)(I-I^*)^2 - \eta(R-R^*)^2 + \left(-\phi + \frac{\beta}{N}I^*\right)(S-S^*)(E-E^*) + \left(-\frac{\beta}{N}S - \phi\right)(S-S^*)(I-I^*) \\
&\quad + \left(\alpha + \frac{\beta}{N}S\right)(E-E^*)(I-I^*) + (-\phi)(R-R^*)(S-S^*) + \theta(R-R^*)(I-I^*) \leqslant -\left(\frac{\beta}{N}I^* + \gamma_S + \phi\right)(S-S^*)^2 \\
&\quad - (\alpha+\gamma_E)(E-E^*)^2 - (\gamma_I+\theta)(I-I^*)^2 - \eta(R-R^*)^2 + \left(\phi + \frac{\beta}{N}I^*\right)|S-S^*||E-E^*| \\
&\quad + \left(\frac{\beta}{N}S + \phi\right)|S-S^*||I-I^*| + \left(\alpha + \frac{\beta S}{N}\right)|E-E^*||I-I^*| + \phi|R-R^*||S-S^*| + \theta|R-R^*||I-I^*| \\
&\leqslant -\left(\frac{\beta}{N}(I^* + \gamma_S + \phi)\right)(S-S^*)^2 - (\alpha+\gamma_E)(E-E^*)^2 - (\gamma_I+\theta)(I-I^*)^2 - \eta(R-R^*)^2 + \frac{1}{2}\left(\phi + \frac{\beta}{N}I^*\right)(S-S^*)^2 \\
&\quad + \frac{1}{2}\left(\phi + \frac{\beta}{N}I^*\right)(E-E^*)^2 + \frac{1}{2}\left(\frac{\beta}{N}S + \phi\right)(S-S^*)^2 + \frac{1}{2}\left(\frac{\beta}{N}S + \phi\right)(I-I^*)^2 + \frac{1}{2}\left(\alpha + \frac{\beta}{N}S\right)(E-E^*)^2 \\
&\quad + \frac{1}{2}\left(\alpha + \frac{\beta}{N}S\right)(I-I^*)^2 + \frac{1}{2}\phi(S-S^*)^2 + \frac{1}{2}\phi(R-R^*)^2 + \frac{1}{2}\theta(R-R^*)^2 + \frac{1}{2}\theta(I-I^*)^2 \\
&\leqslant \left(-\left(\frac{\beta}{N}(I^* + \gamma_S + \phi)\right) + \frac{1}{2}\left(\phi + \frac{\beta}{N}I^*\right) + \frac{1}{2}\left(\frac{\beta}{N}S + \phi\right) + \frac{1}{2}\phi\right)(S-S^*)^2 + \left(-(\alpha+\gamma_E) + \frac{1}{2}\left(\phi + \frac{\beta}{N}I^*\right) + \frac{1}{2}\left(\alpha + \frac{\beta}{N}S\right)\right)(E-E^*)^2 \\
&\quad + \left(-(\gamma_I+\theta) + \frac{1}{2}\left(\frac{\beta}{N}S + \phi\right) + \frac{1}{2}\left(\alpha + \frac{\beta}{N}S\right) + \frac{1}{2}\theta\right)(I-I^*)^2 + \left(-\eta + \frac{1}{2}\phi + \frac{1}{2}\theta\right)(R-R^*)^2 \leqslant 0.
\end{aligned}$$

Here, the last inequality is obtained using assumptions (3.7), (3.8), $I^* = \frac{\alpha}{\gamma_I+\theta}AN$, and $S(t) \leqslant \frac{\phi}{\gamma_S+\phi}N$, as we have

$$\text{(i)}\quad -\left(\frac{\beta}{N}I^* + \gamma_S + \phi\right) + \frac{1}{2}\left(\phi + \frac{\beta}{N}I^*\right) + \frac{1}{2}\left(\frac{\beta}{N}S + \phi\right) + \frac{1}{2}\phi \leqslant -\left(\frac{\beta}{N}\frac{\alpha}{\gamma_I+\theta}AN + \gamma_S + \phi\right)$$
$$+\frac{1}{2}\left(\phi + \frac{\beta}{N}\frac{\alpha}{\gamma_I+\theta}AN\right) + \frac{1}{2}\left(\frac{\beta}{N}\frac{\phi}{\gamma_S+\phi}N + \phi\right) + \frac{1}{2}\phi = -\frac{1}{2}\frac{\alpha\beta}{\gamma_I+\theta}A - (\gamma_S+\phi) + \frac{1}{2}\frac{\beta\phi}{\gamma_S+\phi} + \frac{3}{2}\phi \leqslant 0,$$

$$\text{(ii)}\quad -(\alpha+\gamma_E) + \frac{1}{2}\left(\phi + \frac{\beta}{N}I^*\right) + \frac{1}{2}\left(\alpha + \frac{\beta}{N}S\right) \leqslant -\frac{1}{2}\alpha - \gamma_E + \frac{1}{2}\phi + \frac{1}{2}\frac{\alpha\beta}{\gamma_I+\theta}A + \frac{1}{2}\frac{\beta\phi}{\gamma_S+\phi} \leqslant 0,$$

$$\text{(iii)}\quad -(\gamma_I+\theta) + \frac{1}{2}\left(\frac{\beta}{N}S + \phi\right) + \frac{1}{2}\left(\alpha + \frac{\beta}{N}S\right) + \frac{1}{2}\theta = -\gamma_I + \frac{\beta}{N}S + \frac{1}{2}(\alpha - \theta + \phi) \leqslant -\gamma_I + \frac{\beta}{N}\frac{\phi}{\gamma_S+\phi}N + \frac{1}{2}(\alpha - \theta + \phi)$$
$$= -\gamma_I + \frac{\beta\phi}{\gamma_S+\phi} + \frac{1}{2}(\alpha - \theta + \phi) \leqslant 0.$$

Observe that $\frac{dL}{dt} = 0$ if and only if $S = S^*, E = E^*, I = I^*$, and $R = R^*$. Therefore, L is a Lyapunov function on $\mathring{\Gamma}$. Thus, the largest compact invariant subset of the set satisfying $\frac{dL}{dt}$ is the singleton $\{(S,E,I,R) = (S^*,E^*,I^*,R^*)\}$. By LeSalle's invariance theorem [26], we have that $S(t) \to S^*, E(t) \to E^*, I(t) \to I^*$, and $R(t) \to R^*$ as $t \to \infty$. Therefore, the endemic equilibrium P^* is globally asymptotically stable in $\mathring{\Gamma}$. □

4. Optimal control and simulation results

In order to minimize an objective function comprising the infection cost (i.e., the infectious compartment population) and the system treatment cost for isolating infectious computers from the network, we consider the following optimal control problem:

$$\min_{u(\cdot)} \int_0^{t_f} [c_I I(t) + u(t)^2/2]dt \tag{4.1}$$

subject to the C-SEIRA state Eq. (2.3). Note that, in the cost rate of this problem, c_I is the trade-off constant defining the relative importance of the infection cost over the system treatment cost. In addition, note that the cost rate considers a quadratic cost for the control input, which is a commonly used strategy in related control problems dealing with epidemic-model-based systems (e.g., [6,8,27]). As is well known, the necessary conditions for the optimal solutions of (4.1) can be obtained via the Pontryagin maximum principle [27]. For this, the Hamiltonian H of the optimal control problem (4.1) is defined as

$$H(S,E,I,R,A,p_1,p_2,p_3,p_4,p_5,u) = c_I I + u^2/2 + p_1(-\beta SI/N - \gamma_S S + \phi A) + p_2(\beta SI/N - \alpha E - \gamma_E E) + p_3(\alpha E - \gamma_I I - \theta I$$
$$- Iu) + p_4(\theta I - \eta R + Iu) + p_5(\gamma_S S + \gamma_E E + \gamma_I I + \eta R - \phi A) \tag{4.2}$$

and its costate equations are obtained via

$$\dot{p}_1 = -\frac{\partial H}{\partial S},\quad \dot{p}_2 = -\frac{\partial H}{\partial E},\quad \dot{p}_3 = -\frac{\partial H}{\partial I},\quad \dot{p}_4 = -\frac{\partial H}{\partial R},\quad \dot{p}_5 = -\frac{\partial H}{\partial A},\quad p_1(t_f) = p_2(t_f) = p_3(t_f) = p_4(t_f) = p_5(t_f) = 0. \tag{4.3}$$

From the optimality condition $\frac{\partial H}{\partial u} = 0$, we can also obtain the following condition for optimal control:

$$u(t) = (p_3(t) - p_4(t))I(t). \tag{4.4}$$

Hence, by confining the control input to be nonnegative and subject to a positive upper bound $u_{\max}$, the optimal control of (4.1) can be written in the following form:

$$u(t) = \max(0, \min((p_3(t) - p_4(t))I(t), u_{\max})). \tag{4.5}$$

From the above steps, we can conclude that any solution to the optimal control problem (4.1) must satisfy the following:

$$\dot{S}(t) = -\beta S(t)I(t)/N - \gamma_S S(t) + \phi A(t)$$

$$\dot{E}(t) = \beta S(t)I(t)/N - \alpha E(t) - \gamma_E E(t)$$

$$\dot{I}(t) = \alpha E(t) - \gamma_I I(t) - \theta I(t) - I(t)u(t)$$

$$\dot{R}(t) = \theta I(t) - \eta R(t) + I(t)u(t)$$

$$\dot{A}(t) = \gamma_S S(t) + \gamma_E E(t) + \gamma_I I(t) + \eta R(t) - \phi A(t)$$

$$\begin{aligned}
&\dot{p}_1(t) = -p_1(t)(-\beta I(t)/N - \gamma_S) - p_2(t)\beta I(t)/N - p_5(t)\gamma_S\\
&\dot{p}_2(t) = -p_2(t)(-\alpha - \gamma_E) - p_3(t)\alpha - p_5(t)\gamma_E\\
&\dot{p}_3(t) = -c_I - p_1(t)(-\beta S(t)/N) - p_2(t)\beta S(t)/N\\
&\qquad\quad - p_3(t)(-\gamma_I - \theta - u(t)) - p_4(t)(\theta + u(t)) - p_5(t)\gamma_I\\
&\dot{p}_4(t) = -p_4(t)(-\eta) - p_5(t)\eta\\
&\dot{p}_5(t) = -p_1(t)\phi - p_5(t)(-\phi)\\
&u(t) = \max(0, \min((p_3(t) - p_4(t))I(t), u_{\max}))\\
&S(0) = S_0, \quad E(0) = E_0, \quad I(0) = I_0, \quad R(0) = R_0, \quad A(0) = A_0\\
&p_1(t_f) = p_2(t_f) = p_3(t_f) = p_4(t_f) = p_5(t_f) = 0.
\end{aligned}$$

Note that by solving this boundary value ODE problem, we obtain an optimal control policy for problem (4.1).

In order to illustrate the optimal control policy, we simulate an example of the use of C-SEIRA. The parameters considered for the example are:

Table 2
Initial conditions.

Scenario 1	$S(0) = 70,\ E(0) = 10,\ I(0) = 10,\ R(0) = 0,\ A(0) = 10$
Scenario 2	$S(0) = 10,\ E(0) = 10,\ I(0) = 70,\ R(0) = 0,\ A(0) = 10$

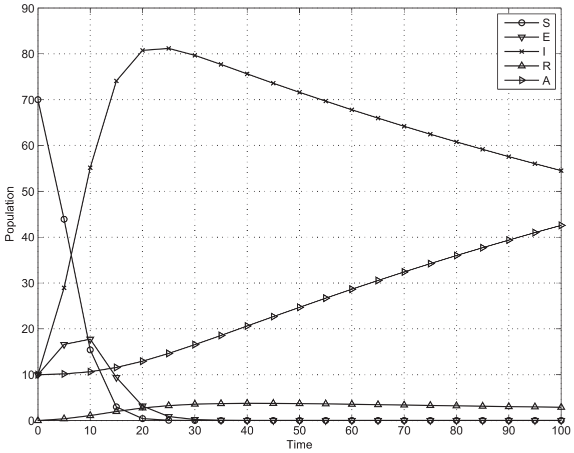

Fig. 4. State trajectories for the uncontrolled case with $S(0) = 70$ (Scenario 1).

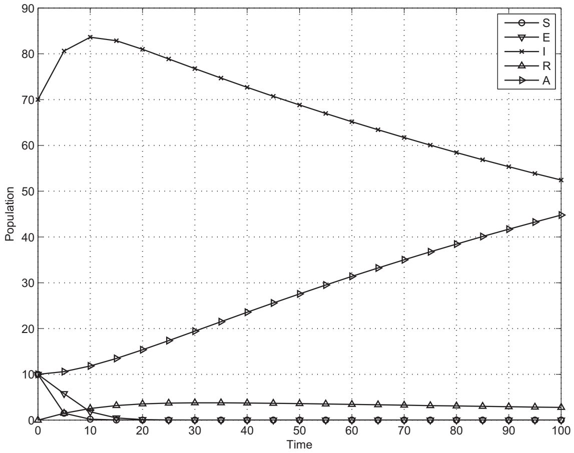

Fig. 5. State trajectories for the uncontrolled case with $I(0) = 70$ (Scenario 2).

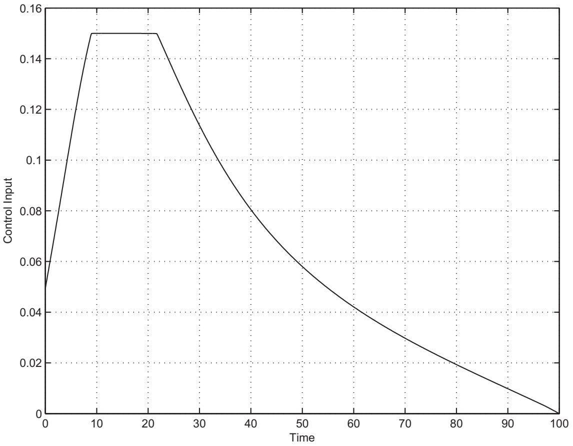

Fig. 6. Control inputs for the case with $S(0) = 70$ (Scenario 1).

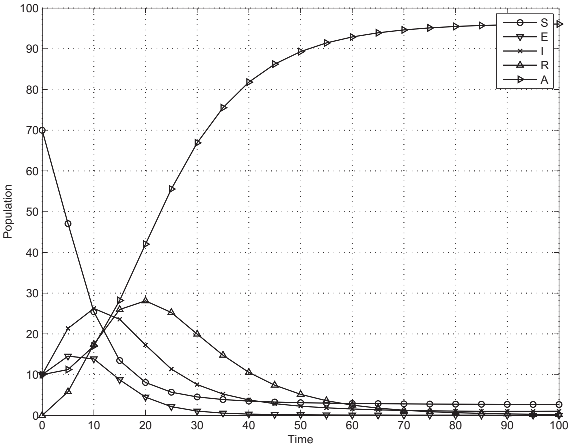

Fig. 7. State trajectories for the case with $S(0) = 70$ (Scenario 1).

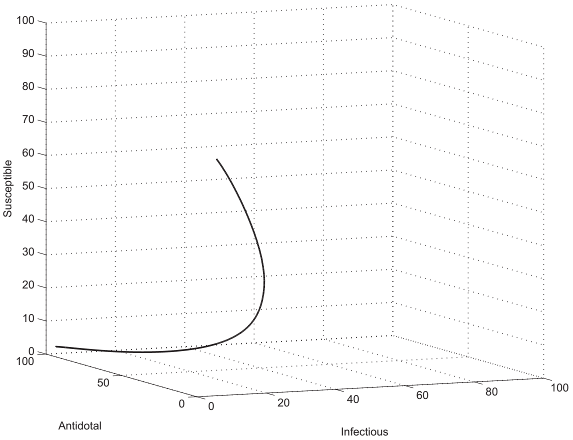

Fig. 8. Three-dimensional trajectory for (I, A, S) (Scenario 1).

$$\alpha = 0.3, \quad \beta = 0.5, \quad \gamma_S = 0.0001, \quad \gamma_E = 0.0001, \quad \gamma_I = 0.0005, \quad N = 100, \quad \phi = 0.0001, \quad \theta = 0.005, \quad \eta = 0.1, \quad c_I = 0.001, \quad u_{\max} = 0.15. \tag{4.7}$$

By $N = 100$, we mean that the total population of computer hosts is expressed as a percentage. Hence, each compartment population in the simulations should be interpreted as a percentage of the total population. With these parameters, we have two equilibrium points, i.e., the infection-free equilibrium point

$$\mathbf{x}_0 = \left(P_0, N - \frac{\phi}{\gamma_S + \phi}N\right) = (50, 0, 0, 0, 50), \tag{4.8}$$

and the endemic equilibrium point

$$\mathbf{x}^* = (P^*, N - S^* - E^* - I^* - R^*) = (1.100, 0.032, 1.744, 0.087, 97.037). \tag{4.9}$$

From the stability results of Section 3, we can see that the C-SEIRA model described by (4.7) has an infection-free equilibrium point that is unstable, whereas its endemic equilibrium point is locally asymptotically stable. The initial conditions used for the simulations are shown in Table 2. The simulations start with two different levels of infection. The first scenario starts from a dominantly susceptible state, with $S(0) = 70$, and the second one starts from a dominantly infectious state, with $I(0) = 70$. Note that the second scenario has a higher infection burden than the first. Figs. 4 and 5 show that, without any system treatment effort of isolating the infectious nodes from the computer network, both scenarios suffer the serious result that their infectious compartment populations dominate the system for a long time. With the goal of keeping the infection level low with a reasonable control effort, we solve the boundary value ODE problem (4.6) for each initial condition set of Table 2.

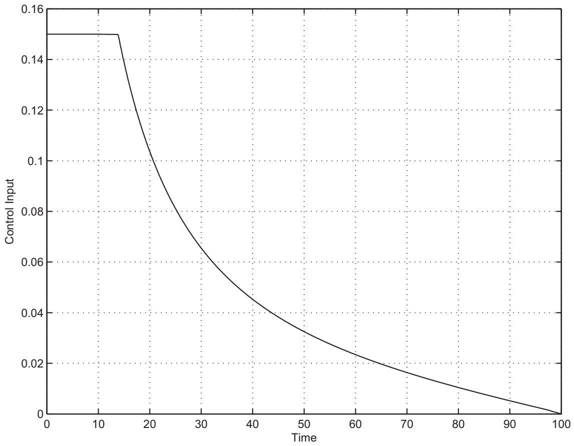

Fig. 9. Control inputs for the case with $I(0) = 70$ (Scenario 2).

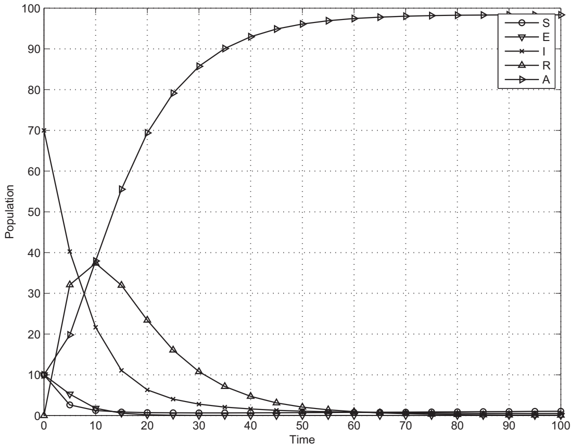

Fig. 10. State trajectories for the case with $I(0) = 70$ (Scenario 2).

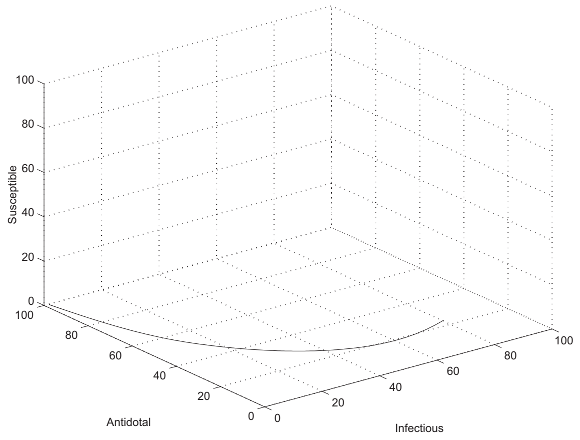

Fig. 11. Three-dimensional trajectory for (I, A, S) (Scenario 2).

Figs. 6–8 show the simulation results for the first scenario. Fig. 6 shows that, under the optimal control strategy, the best method of fighting the infection is to initially increase the system treatment effort from about 0.05 to 0.15, maintain the upper bound at 0.15 for a while, and later reduce it slowly to zero until $t_f = 100$. The resulting state trajectories in Fig. 7 show that, with the optimal control strategy, the infectious compartment population drops to a low level and the antidotal compartment population, which is initially 10, increases more rapidly than in the uncontrolled case. Fig. 8 shows a three-dimensional trajectory for (I, A, S), starting from a dominantly susceptible state $(S(0) = 70)$ and ending at an almost infection-free state at $t_f = 100$.

Simulation results for the second scenario, which deals with the larger infection burden $(I(0) = 70)$, are shown in Figs. 9–11. Fig. 9 shows that, when the infection level is high, the best method of fighting the infection is to apply the full amount of system treatment from the start, and then reduce the effort slowly until the final time $t_f = 100$. The state trajectories resulting from this policy are shown in Fig. 10. Note that the initially high infection level is successfully suppressed in a short time by this policy. Finally, Fig. 11 shows a three-dimensional trajectory for (I, A, S), starting from a dominantly infectious state $(I(0) = 70)$ and ending at a near infection-free state at $t_f = 100$.

5. Concluding remarks

As concern over the burden and damage caused by malicious objects, such as computer worms, increases, the development of a mathematical model of the propagation of malicious objects and the establishment of efficient policies for controlling infection become central issues in the field of computer security. In order to investigate and prepare against malicious worm propagation, we have proposed the C-SEIRA model, in which the state variables are defined as the populations of five compartments (susceptible, exposed, infectious, replaced, and antidotal). We identified infection-free and endemic equilibrium points in the model, and derived their stability conditions. We also applied optimal control theory to the C-SEIRA model, and through some numerical simulations, showed that malicious worm propagation was controlled reasonably well via the optimal control approach. In future work, we will conduct further simulation studies, with the aim of revealing the strengths and weaknesses of the proposed method, and investigate stability and control issues for its extension toward a stochastic approach.

Acknowledgement

This work was supported by a Korea University Grant.

References

[1] J.O. Kephart, S.R. White, D.M. Chess, Computers and epidemiology, IEEE Spectr. 30 (5) (1993) 20–26.
[2] J. Balthrop, S. Forrest, M.E.J. Newman, M.M. Williamson, Technological networks and the spread of computer viruses, Science 304 (2004) 527–529.
[3] M. Draief, A. Ganesh, L. Massouili, Thresholds for virus spread on networks, Ann. Appl. Probab. 18 (2) (2008) 359–378.
[4] J.R.C. Piqueira, V.O. Araujo, A modified epidemiological model for computer viruses, Appl. Math. Comput. 213 (2009) 355–360.
[5] X. Han, Q. Tan, Dynamical behavior of computer virus on Internet, Appl. Math. Comput. 217 (6) (2010) 2520–2526.
[6] J. Kim, S. Radhakrishana, J. Jang, Cost optimization in SIS model of worm infection, ETRI J. 28 (5) (2006) 692–695.
[7] O.A. Toutonji, S.-M. Yoo, M. Park, Stability analysis of VEISV propagation modeling for network worm attack, Appl. Math. Model. 36 (2012) 2751–2761.
[8] C. Zhang, X. Yang, Q. Zhu, W. Liu, Optimal control in a novel computer virus spread model, J. Inf. Comput. Sci. 8 (10) (2011) 1929–1938.
[9] J.D. Murray, Mathematical Biology, third ed., Springer, New York, 2002.
[10] S.H. Sellke, N.B. Shroff, S. Bagchi, Modeling and automated containment of worms, IEEE Trans. Dependable Secure Comput. 5 (2) (2008) 71–86.
[11] S. Dharmapurikar, P. Krishnamurthy, T.S. Sproull, J.W. Lockwood, Deep packet inspection using parallel bloom filters, IEEE Micro 24 (1) (2004) 52–61.

[12] S. Yoon, B. Kim, J. Oh, High-performance stateful intrusion detection system, Proc. Int. Conf. Comput. Intel. Secur. 1 (2006) 574–579.
[13] C.C. Zou, W.B. Gong, D. Towsley, Worm propagation modeling and analysis under dynamic quarantine defense, Proc. ACM CCS Workshop Rapid Malcode (2003) 51–60.
[14] Y. Choi, E.-K. Hong, T.-W. Kim, S.-T. Paek, I.-H. Choi, H.-C. Oh, A traffic pattern matching hardware for a contents security system, J. Inst. Electron. Eng. Korea 46 (CI-1) (2009) 88–95.
[15] Y.H. Cho, W.H. Mangione-Smith, Deep packet filter with dedicated logic and read only memories, Proc. IEEE Symp. Field Program. Custom Comput. Mach. (2004) 125–134.
[16] J.R.C. Piqueira, B.F. Navarro, L.H.A. Monteiro, Epidemiological models applied to viruses in computer networks, J. Comput. Sci. 1 (1) (2005) 31–34.
[17] J.R.C. Piqueira, A.A. de Vasconcelos, C.E.C.J. Gabriel, V.O. Araujo, Dynamic models for computer viruses, Comput. Secur. 27 (7–8) (2008) 355–359.
[18] J.R.C. Piqueira, F.B. Cesar, Dynamical models for computer viruses propagation, Math. Prob. Eng. (2008). Article ID 940526, 11 pages, http://dx.doi.org/10.1155/2008/940526.
[19] B.K. Mishra, G.M. Ansari, Differential epidemic model of virus and worms in computer network, Int. J. Netw. Secur. 14 (3) (2012) 149–155.
[20] B.K. Mishra, D. Saini, Mathematical models on computer viruses, Appl. Math. Comput. 187 (2) (2007) 929–936.
[21] Y. Jin, W. Wang, S. Xiao, An SIRS model with a nonlinear incidence rate, Chaos Solitons Fractals 34 (2007) 1482–1497.
[22] G. Li, J. Zhen, Global stability of an SEI epidemic model with general contact rate, Chaos Solitons Fractals 23 (2004) 997–1004.
[23] X.Z. Li, L.L. Zhou, Global stability of an SEIR epidemic model with vertical transmission and saturating contact rate, Chaos Solitons Fractals 40 (2007) 874–884.
[24] B.K. Mishra, N. Jha, SEIQRS model for the transmission of malicious objects in computer network, Appl. Math. Model. 34 (2009) 1207–1212.
[25] C. Sun, Y. Lin, S. Tang, Global stability for an special SEIR epidemic model with nonlinear incidence rates, Chaos Solitons Fractals 33 (2007) 290–297.
[26] J.P. LaSalle, The Stability of Dynamical Systems, in: CBMS-NSF Regional Conference Series in Applied Mathematics, SIAM, Philadelphia, 1976.
[27] S. Lenhart, J.T. Workman, Optimal Control Applied to Biological Models, Chapman & Hall/CRC, USA, 2007.