Volume 9
Issue 2
June 2020

ISSN 2164-6376 (print)
ISSN 2164-6414 (online)

An Interdisciplinary Journal of

Discontinuity, Nonlinearity, and Complexity

L&H

Discontinuity, Nonlinearity, and Complexity

Continued on the inside back cover

An Interdisciplinary Journal of

Discontinuity, Nonlinearity, and Complexity

Volume 9, Issue 2, June 2020

Editors
Xavier Leoncini
Edgardo Ugalde
Dimitry Volchenkov

L&H Scientific Publishing, LLC, USA

Publication Information

Discontinuity, Nonlinearity, and Complexity (ISSN 2164-6376 (print), eISSN 2164-6414 (online)) is published quarterly (March, June, September, and December) by L & H Scientific Publishing, LLC, 25 Glen Ed Professional Park, Glen Carbon, IL62034, USA. Subscription prices are available upon request from the publisher or from this journal website. Subscriptions are accepted on a prepaid basis only and entered on a calendar year basis. Issues are sent by standard mail (Surface in North America, air delivery outside North America). Priority rates are available upon request. Claims for missing issues should be made within six months of the date of dispatch.

Changes of Address

Send address changes to L&H Scientific Publishing, LLC, 25 Glen Ed Professional Park, Glen Carbon, IL62034, USA. Changes of address must be received at L&H Scientific Publishing eight weeks before they are effective.

Authors Inquiries

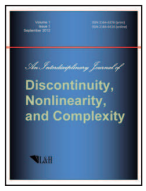
For inquiries relative to the submission including electronic submission where available, please visit journal website or contact journal Editors-in-Chief.

Advertising Information

If you are interested in adverting or other commercial opportunities, please email via lhscientificpublishing@gmail.com and your enquiry will be handled as soon as possible.

Printed in USA on acid-free paper.

Discontinuity, Nonlinearity, and Complexity 9(2) (2020) 187-197



Discontinuity, Nonlinearity, and Complexity

https://lhscientificpublishing.com/Journals/DNC-Default.aspx

Preventing Computer Virus Prevalence using Epidemiological Modeling and Optimal Control

João N.C. Gonçalves[1,2†], Helena Sofia Rodrigues[3,4], M. Teresa T. Monteiro[1,2]

[1] Department of Production and Systems, University of Minho, Portugal
[2] Algoritmi R&D Center, University of Minho, Portugal
[3] Center for Research and Development in Mathematics and Applications (CIDMA), Department of Mathematics, University of Aveiro, Portugal
[4] School of Business Studies, Viana do Castelo Polytechnic Institute, Portugal

Submission Info

Communicated by D. Volchenkov
Received 18 December 2018
Accepted 31 March 2019
Available online 1 July 2020

Keywords

Computer viruses
Optimal control theory
Epidemological models
Network
EpiModel package

Abstract

Computer viruses are a serious threat to the general society, due to their implications for private life and corporative systems. This paper begins to briefly illustrate the dynamics of computer viruses within a network system, by taking advantage of the EpiModel `R` package and using a SIR (Susceptible–Infected–Recovered) epidemic model. However, since devices are not constantly immune to cyberattacks, a SIRS model with an optimal control application is proposed to minimize the levels of infections caused by malicious objects. Additionally, real numerical data related to the number of reported cybercrimes in Japan from 2012 to 2017 are considered. The existence and uniqueness of an optimal control for the proposed control problem are proved. Under proper investment costs, numerical simulations in `Matlab` show the effectiveness of the proposed control strategy in increasing the rate of immunity and decreasing the chances of re–susceptibility to cyberattacks.

1 Introduction

Computer viruses can be defined as computer programs able of replicating themselves and propagate from one computer to another, within a certain network [1], potentially causing massive damages to individuals and corporative systems. Under the premise that the dynamics of computer viruses portray analogies to the propagation of a biological virus [2], the use of mathematical techniques to model the transmission of computer viruses reveals to be of utmost importance [3].

The origin of computer viruses dates back to 1949, in a research article entitled "Theory and Organization of Complicated Automata", by John von Neumann [4]. Following [4], malicious objects are subdivided into four main categories: trojan horses, logic bombs, worms and computer viruses. Additionally, the author described

†Corresponding author.
Email address: jncostagoncalves@gmail.com

ISSN 2164-6376, eISSN 2164-6414/$-see front materials
DOI:10.5890/DNC.2020.06.002

the four main phases that portray the general behavior of computer viruses within a computer system: *Numbness phase*, where the user is unaware of the malware infection in its system; *Propagation phase*, where the malware attempts to attach itself to other files present in the system. Consequently, other hosts that are, somehow, connected to the infected node in the network can also become infected; *Triggering phase*, referring to the moment when the malware is detected by the user; *Damaging phase*, characterized by the stage where the system is totally exposed and compromised by the malware.

Following up the rapid growth of the internet and social networks, computer viruses became more effective and harder to detect and remove [5] (as cited in [6]), raising the potential for damage, loss, and destruction of data within companies and individuals [7]. Thus, purposing to understand the dynamics of Computer Virus Transmission (CVT) and minimize its propagation, mathematical epidemiological models began being intensively explored from the initial work published by J. Kephart and S. White in [8].

In [9], B. Mishra and D. Saini proposed a SEIRS model with latent and temporary immune periods to overcome the drawbacks of the model proposed in [10], namely related with the assumption of a permanent immunization period related to the recovered hosts. The transmission of worms in computer networks was also studied in [11], where the authors formulated an e-epidemic SIRS model for the fuzzy transmission of worms, assessing three epidemic control strategies related to the magnitude of the infection.

Regarding the computer viruses whose life period is associated with latent and disruptive phases (disruptive viruses), Y. Wu et al. [12] proposed a heterogeneous epidemic model to assess the prevalence of disruptive computer viruses in the case that every node in a network has its own virus-related attributes. Besides, some measures containing the prevalence of malicious objects are provided by these authors. Aiming to minimize the damages caused by computer viruses, C. Gan et al. [13] explored the influence of vaccination probability on the diffusion of computer viruses using a novel SIRS model with generalized nonlinear incidence, providing also effective strategies to minimize the prevalence of viruses. From a related perspective, I. Ahn et al. [14] introduced an C-SEIRA epidemic model with optimal control to both minimize the rate of virus infections and the cost of isolating infectious computers from the network, showing that optimal control theory has a positive effect on the control the virus epidemic.

The information above allows to infer that the process of CVT is being increasingly understood, as well as it shows that mathematical epidemiology and optimal control theory reveal to be key tools to model complex problems. Aiming to better understand and model the propagation of computer viruses, in this paper we begin to briefly study the virus dynamics over networks by using an `R` package suitable for that purpose. Then, a SIRS model with an optimal control strategy is proposed to minimize the fraction of infected hosts without considerable financial costs related to its implementation.

The paper is organized as follows. Virus epidemic over networks are studied using the SIR model in Section 2. At this point, the EpiModel package from `R` is explored to briefly illustrate the virus dynamics for a given set of hosts. In Section 3 the standard SIRS model is introduced from a computer network perspective. Then, an optimal control problem is proposed in Section 4, in which we propose a control strategy to minimize the fraction of infected hosts as well as the costs related to its implementation. In Section 5 numerical simulations and discussion of the derived results are presented. Conclusions are carried out in Section 6.

2 Virus epidemic over networks: a SIR model

This section intends to give a general overview on the propagation of computer viruses over networks. Networks and epidemiology theory are intrinsically related [15]. In [16], G. Witten and G. Poulter discussed the spread of infectious diseases on networks, and described several common network models, namely Random, Watts–Strogatz, Lattice, Barabasí–Albert and Scale–free networks. In this regard, let us consider the SIR epidemiological model over homogeneous networks, by treating the spreading of a viral disease as a propagation of a computer virus. For illustration purposes, only the homogeneous case is here presented, notwithstanding heterogenous models can also be defined.

2.1 SIR homogeneous network model

The standard SIR epidemic model is subdivided into mutually–exclusive compartments, namely Susceptible (S), Infected (I) and Recovered (R). The classes S and I represent the number of hosts which are susceptible and infected by a malicious object, respectively. Regarding the model parameters, susceptible hosts move to the class I at a rate β, becoming infected. Then, after the implementation of some kind of anti–malware policies, an infected host recovers (R class), at a rate γ, and cannot become infected again. The total number of the hosts in the network, N, is considered constant over time t.

In the case of SIR homogeneous network model, all hosts have degree very close to $\langle k \rangle$. Thus, by considering that infected hosts have, approximately, $\langle k \rangle$ chances of contagion from neighbours, we can rewrite the standard SIR system as follows.

$$\begin{cases} \dfrac{dS(t)}{dt} = -\dfrac{\beta \langle k \rangle S(t) I(t)}{N} \\ \dfrac{dI(t)}{dt} = \dfrac{\beta \langle k \rangle S(t) I(t)}{N} - \gamma I(t) \\ \dfrac{dR(t)}{dt} = \gamma I(t)\ , \end{cases} \qquad \begin{cases} S(0) = S_0 > 0 \\ I(0) = I_0 > 0 \\ R(0) = 0\ . \end{cases} \tag{1}$$

Considering $S(0) \approx N$, we define $\mathscr{R}_0 = \frac{\beta}{\gamma}$ as the number of secondary infections produced by a single infected host within a computer network system. At this point, it is easy to prove that if $\mathscr{R}_0 \leqslant \frac{1}{\langle k \rangle}$, then an outbreak does not occur. On the contrary, if $\mathscr{R}_0 > \frac{1}{\langle k \rangle}$, an epidemic occurs.

2.2 SIR in EpiModel

Recalling that the dynamics of a virus infection in humans are similar to the propagation of virus in computer network systems, this subsection focuses on network theory to model the propagation of a computer virus infection within a given set of nodes, by using the SIR epidemiological model and exploring a very recent R package for mathematical modeling of infectious diseases over networks (EpiModel).

Throughout this subsection, the networks are considered to be temporal exponential random graph models (ERGMs) (see [17] and the references cited therein for more detailed information). In EpiModel, both the estimation and simulation of the dynamic networks are implemented using Markov Chain Monte Carlo (MCMC) algorithm functions from the *statnet* package [18].

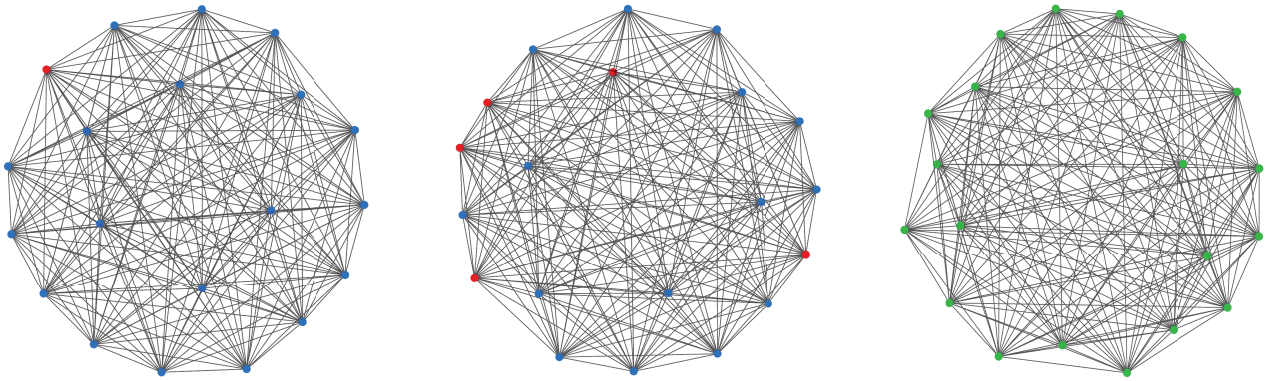
Hereinafter, each host in the network (represented by a node) can develop relationships (represented by edges) with other hosts in its neighborhood in such a way that virus spreads-itself from node to node. At this point, we only consider undirected graphs, which means that given two distinct hosts I_1 and I_2, if I_1 has a relationship with I_2, then the symmetric relationship is also valid. Moreover, the graphs are considered to be complete, meaning that every pair of distinct hosts is connected by a unique edge. Furthermore, based on the assumption that hosts are usually connected to one another, the maximum number of hosts with two or more ties is considered.

In the numerical implementation of the SIR model, the following initial conditions are also assumed:

$$N = 20, \quad S(0) = 19, \quad I(0) = 1, \quad R(0) = 0. \tag{2}$$

Moreover, the numeric values for the model parameters are the following: $\beta = 0.4$ and $\gamma = 0.2$, meaning that the mean infectious period, $\frac{1}{\gamma}$, is 5 (units of time). In the following simulations, let us consider the *blue*, *red* and *green* nodes as susceptible, infected and recovered hosts, respectively. The epidemic behavior on the network is studied by considering different number of time steps to solve the model over ($t = i,\ i = 1, 3, 10$) and 5 simulations to run the MCMC algorithm.

Figure 1(a) illustrates the beginning of the epidemic, where only a single computer system is infected. At $t = 3$ (Fig. 1(b)), attending to the fact that the mean infectious period is 5 (units of time), the number of infected



(a) $t = 1$ (b) $t = 3$ (c) $t = 10$

Fig. 1 Evolution of a computer virus within a network system using a SIR model.

hosts increases. Note that due to the full connections in the computer network, a single infected computer can infect many others. Nonetheless, if anti–malware measures are taken in the long term, then the number of infected hosts decreases and the infected hosts recover from the infection with immunity (Fig. 1(c)). However, considering that a recovered host is permanently immune to new computer virus attacks is not realistic. Hence, in order to try to overcome the drawbacks imposed by the permanent immunity related to the SIR model, the following section introduces the general SIRS model, in which a recovered host can, in fact, become again susceptible to computer virus infections. The novelty here concerns the implementation of a control strategy related to the adoption of anti–malware countermeasures on susceptible hosts.

Remark 1. Although network epidemic models are essential to study the propagation of virus infections, some obstacles arise when high dimensional networks are considered. In the context of challenges for network epidemic models, the reader is referred to [19]. It should also be strengthened that the high dimension of the real networks might be a problem to the use of some softwares to model epidemic phenomena, both in terms of computational performance and accuracy.

3 SIRS model

The standard SIRS epidemic model subdivides the hosts into three mutually–exclusive compartments, similarly to the SIR model. Nevertheless, in the SIRS model, the hosts are not permanent immune and can become susceptible at a rate δ. So, the number of recovered hosts decreases at a rate δ $(-\delta R(t))$, increasing the number of hosts in the class S $(\delta R(t))$. Analogously to the SIR model, the total number of hosts is considered to be constant over time t.

Hence, the deterministic SIRS model is formed by the following system of ordinary differential equations:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta \dfrac{S(t)I(t)}{N} + \delta R(t) \\ \dfrac{dI(t)}{dt} = \beta \dfrac{S(t)I(t)}{N} - \gamma I(t) \\ \dfrac{dR(t)}{dt} = \gamma I(t) - \delta R(t) + \gamma I(t)\,, \end{cases} \qquad \begin{cases} S(0) = S_0 \geqslant 0 \\ I(0) = I_0 \geqslant 0 \\ R(0) = R_0 = 0\,. \end{cases} \tag{3}$$

3.1 Model application to Japan cybercrime data

In this section, the SIRS model previously proposed is calibrated according the number of cybercrimes in Japan from 2012 to 2017 [20], reported to the Japanese police. In Table 1, the number of cybercrimes from 2012 to

Table 1 Number of cybercrimes in Japan from 2012 to 2017 [20].

Year	2012	2013	2014	2015	2016	2017
Cybercrimes	77815	84863	118100	128097	131518	130011

2017 is presented.

According to the data presented in Table 1, we take advantage of the `fminsearch` function from `Matlab` optimization toolbox to estimate the parameters of the proposed model. This function is based on Nelder–Mead method [21]. Thus, we find that the optimal values of the model parameters are $\beta = 10.3626, \gamma = 10.0908, \delta = 0.4307$. We also estimate the total population size, N, as $N = 101071581$, based on the number of Internet users in Japan at 2012 [22]. Furthermore, the following initial conditions for the SIRS model are considered based on [20]:

$$S(0) = S_0 = N - 77815\ , \quad I(0) = I_0 = 77815\ , \quad R(0) = R_0 = 0. \tag{4}$$

Under the above considerations, Figure 2 shows that the model (3) fits well the real data presented in [20]. At this point, note that $I(0)$ and $I(5)$ correspond to the number of cybercrimes in Japan at 2012 and 2017, respectively.

4 Optimal control problem

In this section an optimal control problem is formulated, by adding a control function $u(t)$ to the system (3). Hence, by considering the fractions $s = \frac{S}{N}$, $i = \frac{I}{N}$, $r = \frac{R}{N}$, the resultant model (3) with the control function u is given by

$$\begin{cases} \dfrac{ds(t)}{dt} = -\beta s(t)i(t) + \delta r(t) - u(t)s(t) \\ \dfrac{di(t)}{dt} = \beta s(t)i(t) - \gamma i(t) \\ \dfrac{dr(t)}{dt} = \gamma i(t) - \delta r(t) + u(t)s(t)\ , \end{cases} \qquad \begin{cases} s(0) = \dfrac{S(0)}{N} \\ i(0) = \dfrac{I(0)}{N} \\ r(0) = 0\ . \end{cases} \tag{5}$$

The control function $u(t)$ represents the fraction of susceptible devices in which security countermeasures (e.g. anti–virus software) are installed, aiming to prevent the transition to an infected stage.

The set of admissible control functions is defined as

$$\Omega = \{u(\cdot) \text{ is measurable } \mid 0 \leqslant u(t) \leqslant 1,\ \forall t \in [0,T]\}\ .$$

At this point, note that the implementation of control measures is maximum if $u(t) = 1$ and null if $u(t) = 0$. Therefore, the main objective is to find the optimal value u^* for the control u, in such a way that the state trajectories s, i and r are the solution of the system (5) over $[0,T]$, and minimize the objective functional (6). The optimal control problem consists of minimizing the fraction of infected users and the cost associated to the application of the control policy over $[0,T]$ i.e.,

$$\min_{\Omega} J(u(\cdot)) = \int_0^T [i(t) + \frac{W}{2}u^2(t)]\ dt\ , \tag{6}$$

subject to (5), where the non-negative constant W represents the weight of the investment cost associated to the implementation of the control u.

Under the Pontryagin's Maximum Principle [23], by considering the optimal control problem (5), objective functional (6) and a fixed final time T, if $u^*(\cdot)$ is a control that is optimal for the proposed optimal control

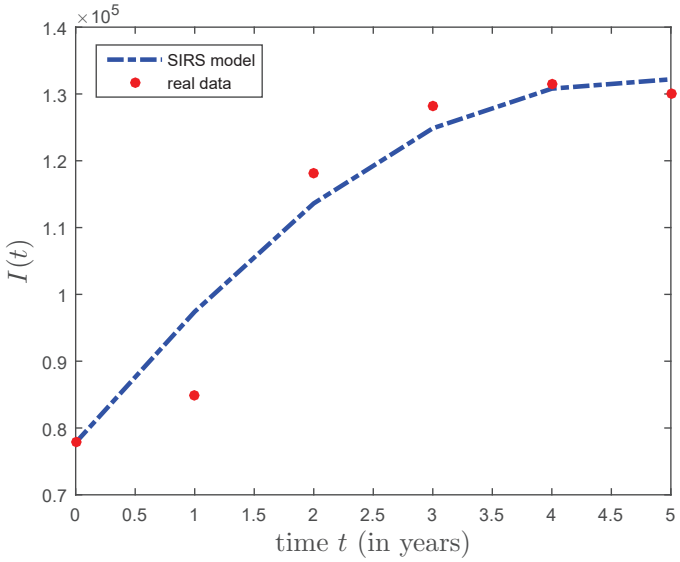


Fig. 2 SIRS model adjustment to the real number of cybercrimes in Japan from 2012 to 2017.

problem, then there exists a nontrivial Lipschitz continuous mapping, called *adjoint vector*, $\lambda : [0,T] \to \mathbb{R}^3$, $\lambda(t) = (\lambda_1(t), \lambda_2(t), \lambda_3(t))$, such that

$$\frac{ds(t)}{dt} = \frac{\partial \mathscr{H}}{\partial \lambda_1}, \quad \frac{di(t)}{dt} = \frac{\partial \mathscr{H}}{\partial \lambda_2}, \quad \frac{dr(t)}{dt} = \frac{\partial \mathscr{H}}{\partial \lambda_3}$$

and

$$\frac{d\lambda_1(t)}{dt} = -\frac{\partial \mathscr{H}}{\partial s}, \quad \frac{d\lambda_2(t)}{dt} = -\frac{\partial \mathscr{H}}{\partial i}, \quad \frac{d\lambda_3(t)}{dt} = -\frac{\partial \mathscr{H}}{\partial r},$$

where the function $\mathscr{H}$ defined by

$$\begin{aligned}\mathscr{H}(s(t), i(t), r(t), u(t), \lambda_1(t), \lambda_2(t), \lambda_3(t)) =& i(t) + \frac{W}{2}u^2(t) \\ &+ \lambda_1(t)\left(-\beta s(t) i(t) + \delta r(t) - u(t)s(t)\right) \\ &+ \lambda_2(t)\left(\beta s(t) i(t) - \gamma i(t)\right) \\ &+ \lambda_3(t)\left(\gamma i(t) - \delta r(t) + u(t)s(t)\right)\end{aligned}$$

is called the *Hamiltonian*, and the functions $\lambda_i(t), i = 1,2,3$, are the *adjoint functions* to be determined suitably.

Theorem 1 (Existence of an optimal control)**.** *For the controlled system (5) with the objective functional (6), there exists an optimal control $u^* \in \Omega$ such that $J(u^*(t)) = \min_{\Omega} J(u(t))$.*

Proof. Due to the boundedness of the state variables and coefficients of the controlled system (5) on the finite time interval considered, the existence result presented in [24] (Theorem 9.2.1) is here invoked to prove this theorem.

First, note that the control set Ω is closed and convex by definition. In addition, also attending to the definition of Ω and the non–negativity of the state solutions, the set of solutions of the controlled system with initial conditions (5) and $u \in \Omega$ is not empty. The right hand side of the system (5) is continuous, bounded above by a sum of the bounded function u and the state variables, and can be written as a linear function in $u(t)$ with

state variables as coefficients. Furthermore, the optimal system is bounded, ensuring the compactness needed for the existence of the optimal control.

Finally, the integrand of the objective functional (6) is convex on Ω and there exist constants $C_0, C_1 > 0$ and $C_2 > 1$ such that $i(t) + \frac{W}{2}u^2(t) \geqslant C_0|u(t)|^{C_2} - C_1$, which concludes the proof.

Theorem 2 (Characterization of the optimal control)**.** *At time t, let s^*, i^* and r^* be the optimal state trajectories associated with the optimal control $u^*(t)$ of the corresponding controlled system (5). Then, there exist adjoint variables $\lambda_i(t), i = 1,2,3$, satisfying*

$$\begin{cases} \dfrac{d\lambda_1(t)}{dt} = \lambda_1(t)\left(\beta i^*(t) + u^*(t)\right) - \lambda_2(t)\beta i^*(t) - \lambda_3(t)u^*(t) \\ \dfrac{d\lambda_2(t)}{dt} = -1 + \lambda_1(t)\beta s^*(t) - \lambda_2(t)\left(\beta s^*(t) - \gamma\right) - \lambda_3(t)\gamma \\ \dfrac{d\lambda_3(t)}{dt} = \delta\left(\lambda_3(t) - \lambda_1(t)\right) \ , \end{cases} \tag{7}$$

with transversality conditions

$$\lambda_i(T) = 0, \ i = 1,2,3 \ . \tag{8}$$

Furthermore,

$$u^*(t) = \min\{1, \max\{\frac{s^*(t)(\lambda_1(t) - \lambda_3(t))}{W}, 0\}\} \ . \tag{9}$$

Proof. Following the Pontryagin's Maximum Principle [23], the adjoint system (7) comes from

$$\begin{cases} \dfrac{d\lambda_1(t)}{dt} = -\dfrac{\partial \mathscr{H}(s(t), i(t), r(t), u(t), \lambda_1(t), \lambda_2(t), \lambda_3(t))}{\partial s}\Big|_{s^*=s,\ i^*=i,\ r^*=r,\ u^*=u} \\ \dfrac{d\lambda_2(t)}{dt} = -\dfrac{\partial \mathscr{H}(s(t), i(t), r(t), u(t), \lambda_1(t), \lambda_2(t), \lambda_3(t))}{\partial i}\Big|_{s^*=s,\ i^*=i,\ r^*=r,\ u^*=u} \\ \dfrac{d\lambda_3(t)}{dt} = -\dfrac{\partial \mathscr{H}(s(t), i(t), r(t), u(t), \lambda_1(t), \lambda_2(t), \lambda_3(t))}{\partial r}\Big|_{s^*=s,\ i^*=i,\ r^*=r,\ u^*=u} \end{cases} \tag{10}$$

Moreover, the optimality condition

$$\frac{\partial \mathscr{H}(s(t), i(t), r(t), u(t), \lambda_1(t), \lambda_2(t), \lambda_3(t))}{\partial u}\Big|_{s^*=s,\ i^*=i,\ r^*=r,\ u^*=u} = Wu^*(t) - s^*(t)(\lambda_1 - \lambda_3) = 0 \ , \tag{11}$$

holds almost everywhere on $[0,T]$. Thus, by (11) and considering the boundedness conditions of u on Ω we derive the characterization (9).

Based on the foregoing, the optimal control and states can be computed by solving the optimality system, which consists in the state system (5), the adjoint system (7) and the transversality conditions (8) together with the characterization (9):

$$
\begin{cases}
\dfrac{ds^*(t)}{dt} = -\beta s^*(t) i^*(t) + \delta r^*(t) - \min\{1, \max\{\dfrac{s^*(t)(\lambda_1(t) - \lambda_3(t))}{W}, 0\}\} s^*(t) \\
\dfrac{di^*(t)}{dt} = \beta s^*(t) i^*(t) - \gamma i^*(t) \\
\dfrac{dr^*(t)}{dt} = \gamma i^*(t) - \delta r^*(t) + \min\{1, \max\{\dfrac{s^*(t)(\lambda_1(t) - \lambda_3(t))}{W}, 0\}\} s^*(t) \\
\dfrac{d\lambda_1(t)}{dt} = \lambda_1(t)(\beta i^*(t) + \min\{1, \max\{\dfrac{s^*(t)(\lambda_1(t) - \lambda_3(t))}{W}, 0\}\}) - \lambda_2(t)\beta i^*(t) \\
\qquad\qquad - \lambda_3(t) \min\{1, \max\{\dfrac{s^*(t)(\lambda_1(t) - \lambda_3(t))}{W}, 0\}\} \\
\dfrac{d\lambda_2(t)}{dt} = -1 + \lambda_1(t)\beta s^*(t) - \lambda_2(t)(\beta s^*(t) - \gamma) - \lambda_3(t)\gamma \\
\dfrac{d\lambda_3(t)}{dt} = \delta(\lambda_3(t) - \lambda_1(t)) \\
\lambda_i(T) = 0, \ i = 1, 2, 3 \\
s^*(0) = 1 - 77815/N\ , \quad i^*(0) = 77815/N\ , \quad r^*(0) = 0.
\end{cases}
\tag{12}
$$

Additionally, since the state and adjoint functions are bounded and the systems (5) and (7) preserve the Lipschitz structure, u^* is unique for T sufficiently small (see [25]). However, the uniqueness of optimality system holds for any value of T since the state system (5) is autonomous.

In order to compute u^* and solve the state system, the optimality system (12) should be solved using numerical methods.

5 Numerical results and discussion

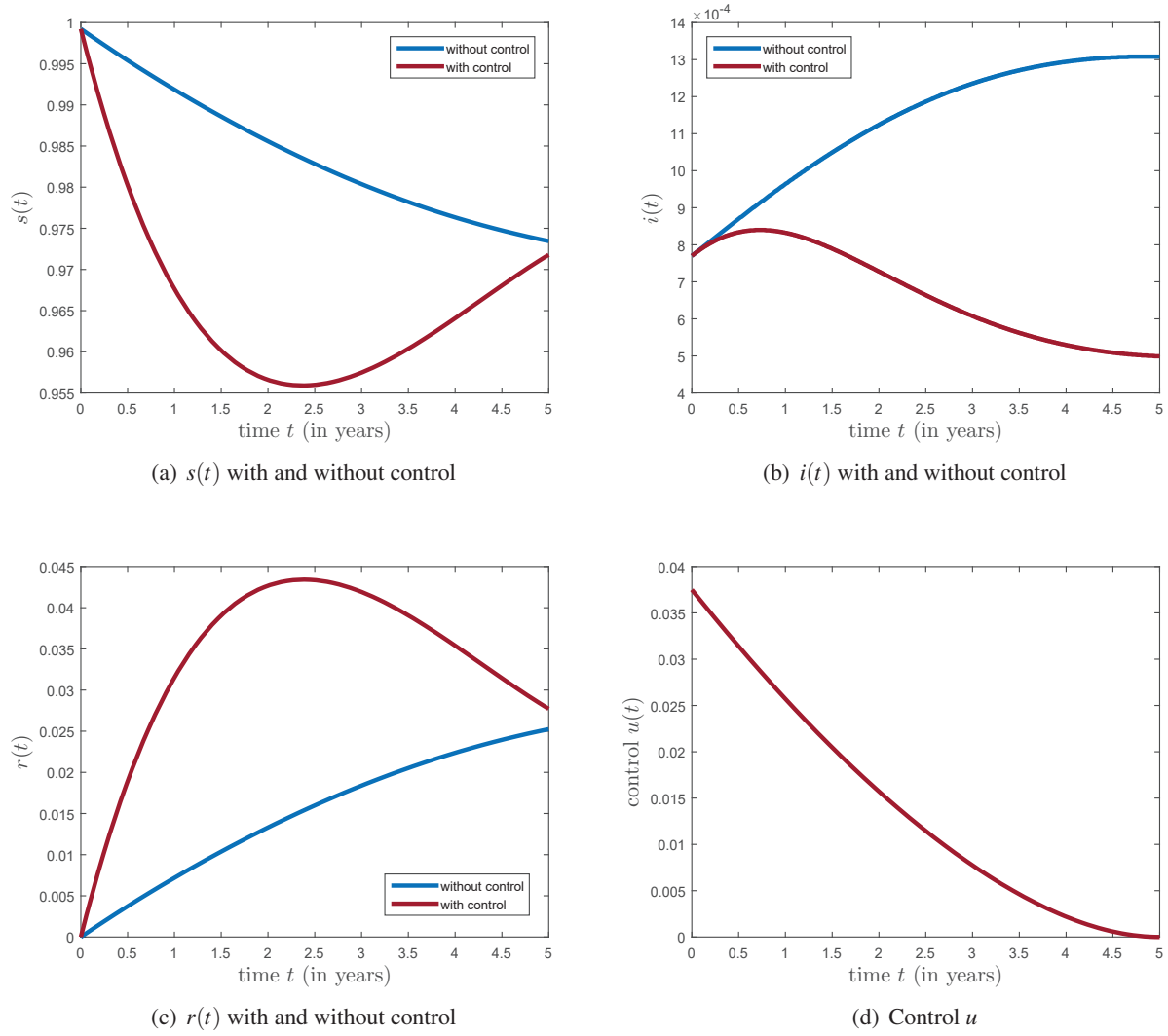
This section intends to present the results of the numerical implementation of the controlled model (5) with objective functional (6). Aiming to analyze the influence of the parameter W, we vary the cost of implementing the control strategy over the time interval $[0, T]$ $(T = 5)$ and infer the associated dynamics on the optimal control, as well as on the optimal states. The numerical implementation was conducted in `Matlab` by using the *Forward-Backward Sweep* numerical method [26].

Firstly, we start by assessing the influence of the control application on the state variables. For that, we consider $W = 1$, initial conditions established in (5) and the aforementioned value parameters, i.e., $\beta = 10.3626, \gamma = 10.0908, \delta = 0.4307$.

In Figure 3, the influence of the control strategy u on the model dynamics is assessed. Note that in spite of the control u never attain the upper bound (Fig. 3(d)), one can conclude that the implementation of the control measure u has a positive effect in terms of the minimization of the fraction of infected hosts over the entire time interval considered (Fig. 3(b)). Hence, a residual application of the control strategy u is sufficient to induce lower levels of cybercrime infections when compared to the real ones recorded.

On the other hand, the fraction of susceptible hosts obtained by using the control measure is always lower than the one obtained without control (Fig. 3(a)). This means that the control measure u is effective in preventing that susceptible hosts become infected. Additionally, the fraction of individuals with temporary immunity is always higher with the application of the control u (Fig. 3(c)), meaning that the control u has a pivotal role in promoting temporary immunity to susceptible hosts.

Finally, since the main objective relates to ensure a lower fraction of infected individuals without heavy initial investments in control measures, Figure 4 presents the dynamics of both the states and the control variable



(a) $s(t)$ with and without control

(b) $i(t)$ with and without control

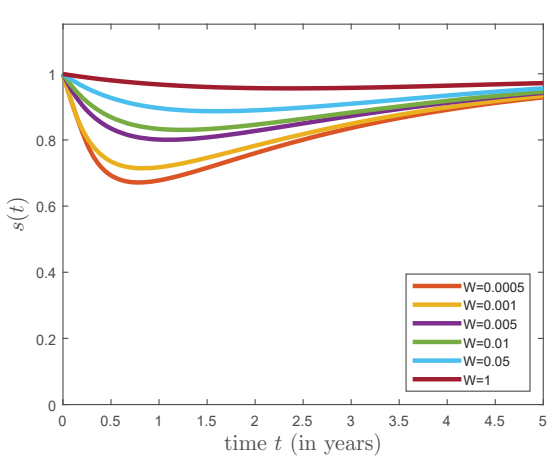
(c) $r(t)$ with and without control

(d) Control u

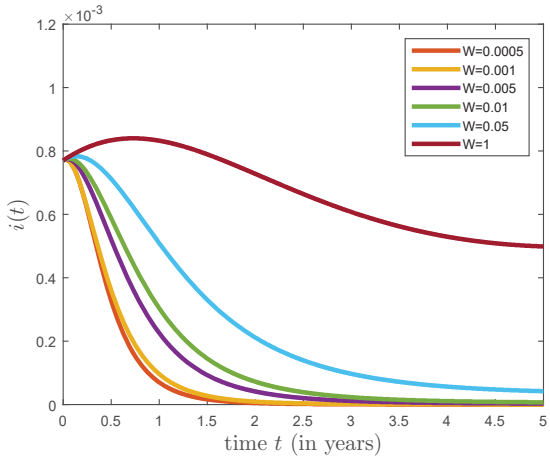
Fig. 3 State variable trajectories with and without controls, for $W = 1$.

by considering the cost W as a variable.

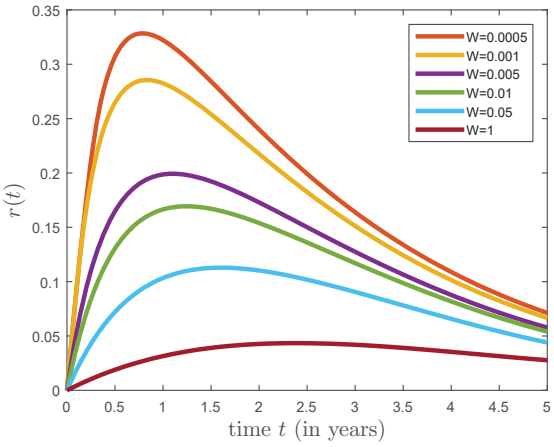
It should first be noted that the fraction of infected hosts (Fig. 4(b)) is always lower when compared to the one derived from the real data (Fig. 3(b)), regardless the value of the cost of implementing the control strategy u. However, the lowest levels of infected hosts are attained for smaller values of W, $\forall t \in [0,5]$. This means that control strategies should not be immeasurably applied if we want to minimize the overall costs of implementing u. In fact, if the goal is to minimize the fraction of infected hosts with a low cost, then the control u is at the upper bound for approximately half a year, when small values of W are considered. Concretely, for $W \in \{0.0005, 0.001\}$, the application of security countermeasures on susceptible hosts during the first half of the first year is the best strategy to massively decrease the fraction of users who suffered cyberattacks (see Figs. 4(d) and 4(b)). Conversely, the greater the investment costs in the control measure u, the greater the levels of infected hosts – notwithstanding those levels be always smaller than the real ones obtained from [20]. Furthermore, the levels of temporary immunity are higher for smaller values of W, meaning not only that the proposed control strategy allows to protect the users from cybercrimes, but also that low investment costs are sufficient to achieve it (see Fig. 4(c)). From a related perspective, high levels of immunity translate into lower levels of susceptibility, meaning that the users are less likely to suffer a new cyberattack (Fig. 4(a)).



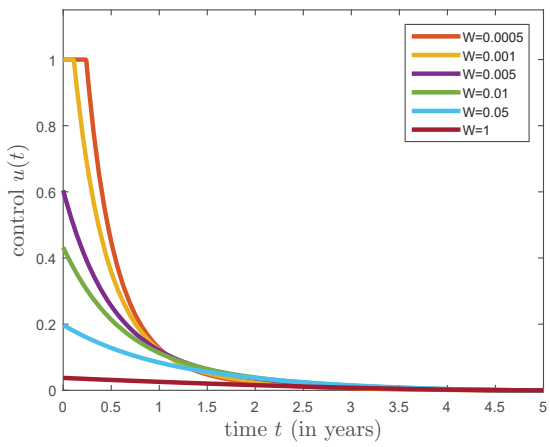
(a) Fraction of susceptible hosts



(b) Fraction of infected hosts



(c) Fraction of recovered hosts



(d) Control u

Fig. 4 Comparison of the effect of W on the controlled model dynamics.

6 Conclusions

In this paper a general overview on the dynamics of computer viruses over networks is provided. Additionally, by using real numerical data related to the number of cybercrimes in Japan from 2012 to 2017, optimal control theory is applied to a SIRS model in order to propose a control strategy to minimize the fraction of infected hosts with a low cost. The existence and uniqueness of an optimal control for the proposed control problem are proved. The characterization of the optimal control is provided by using the Pontryagin's maximum principle.

Numerical simulations show the advantages of the proposed control strategy in minimizing the fraction of infected hosts over the entire time window considered – strengthening the role of optimal control theory. In fact, the fraction of infected hosts is considerably smaller when optimal control theory is applied than without it. By varying the costs of implementing the proposed control strategy, we conclude that the investment in updated security countermeasures should be carefully planned since the fraction of infected hosts does not decrease with the increase of the investment costs in the control. Moreover, the levels of infection decrease at higher rates when the investment cost is low. For lower investment costs in the proposed strategy, a maximum application of the control during the first half of the first year is sufficient to induce higher levels of temporary immunity which, in turn, decreases the chances of a host be susceptible to new cyberattacks.

In further studies, the authors intend to explore additional control measures, as well as to formulate an optimal control problem using delay differential equations. Furthermore, several types of delay and Bang–Bang controls are also interesting topics to be applied.

References

[1] Zhang, C. and Huang, H. (2016), Optimal control strategy for a novel computer virus propagation model on scale-free networks, *Physica A: Statistical Mechanics and its Applications*, **451**, 251-265.

[2] Han, X. and Tan, Q. (2010), Dynamical behavior of computer virus on internet, *Applied Mathematics and Computation*, **217**, 2520-2526.

[3] Guillén, J.H. and del Rey, A.M. (2018), Modeling malware propagation using a carrier compartment, *Communications in Nonlinear Science and Numerical Simulation*, **56**, 217-226.

[4] Brown, D.R. (1992), An introduction to computer viruses. Tech. rep., Oak Ridge National Lab., TN (United States).

[5] Tippett, P.S. (1991), The kinetics of computer virus replication: a theory and preliminary survey, *Safe Computing: Proceedings of the Fourth Annual Computer Virus and Security Conference*, pp. 14-15.

[6] Piqueira, J.R.C. and Araujo, V.O. (2009), A modified epidemiological model for computer viruses, *Applied Mathematics and Computation*, **213**, 355-360.

[7] Cohen, F.B. and Cohen, D.F. (1994), *A short course on computer viruses*. John Wiley & Sons, Inc.

[8] Kephart, J.O. and White, S.R. (1991), Directed-graph epidemiological models of computer viruses. *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*, pp. 343-359, IEEE.

[9] Mishra, B.K. and Saini, D.K. (2007), Seirs epidemic model with delay for transmission of malicious objects in computer network, *Applied Mathematics and Computation*, **188**, 1476-1482.

[10] Yan, P. and Liu, S. (2006), Seir epidemic model with delay, *The ANZIAM Journal*, **48**, 119-134.

[11] Mishra, B.K. and Pandey, S.K. (2010), Fuzzy epidemic model for the transmission of worms in computer network, *Nonlinear Analysis: Real World Applications*, **11**, 4335-4341.

[12] Wu, Y., Li, P., Yang, L.X., Yang, X., and Tang, Y.Y. (2017), A theoretical method for assessing disruptive computer viruses, *Physica A: Statistical Mechanics and its Applications*, **482**, 325-336.

[13] Gan, C., Yang, X., Liu, W., Zhu, Q., and Zhang, X. (2013), An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate, *Applied Mathematics and Computation*, **222**, 265-274.

[14] Ahn, I., Oh, H.C., and Park, J. (2015), Investigation of the c-seira model for controlling malicious code infection in computer networks, *Applied Mathematical Modelling*, **39**, 4121-4133.

[15] Keeling, M.J. and Eames, K.T. (2005) Networks and epidemic models, *Journal of the Royal Society Interface*, **2**, 295-307.

[16] Witten, G. and Poulter, G. (2007), Simulations of infectious diseases on networks, *Computers in Biology and Medicine*, **37**, 195-205.

[17] Jenness, S.M., Goodreau, S.M., and Morris, M. (2018), Epimodel: An r package for mathematical modeling of infectious disease over networks, *Journal of statistical software*, **84**.

[18] Hunter, D.R., Handcock, M.S., Butts, C.T., Goodreau, S.M., and Morris, M. (2008), ergm: A package to fit, simulate and diagnose exponential-family models for networks, *Journal of statistical software*, **24**, 1-29.

[19] Pellis, L., Ball, F., Bansal, S., Eames, K., House, T., Isham, V., and Trapman, P. (2015), Eight challenges for network epidemic models, *Epidemics*, **10**, 58-62.

[20] Statista ((Last checked on 30 May, 2018)), Number of cyber crime related consultations in japan from 2012 to 2017. https://www.statista.com/statistics/746985/japan-number-of-reported-cyber-crimes/.

[21] Lagarias, J.C., Reeds, J.A., Wright, M.H., and Wright, P.E. (1998), Convergence properties of the nelder-mead simplex method in low dimensions, *SIAM Journal on optimization*, **9**, 112-147.

[22] Internet Live Stats ((Last checked on 26 May, 2018)), Japan Internet Users. http://www.internetlivestats.com/internet-users/japan/.

[23] Pontryagin, L., Boltyanskii, V., Gramkrelidze, R., and Mischenko, E. (1962), *The Mathematical Theory of Optimal Processes*, Wiley Interscience.

[24] Lukes, D. (1982), *Differential Equations: Classical to Controlled, Mathematics in Science and Engineering*, vol. 162, Academic Press, New York.

[25] Jung, E., Lenhart, S., and Feng, Z. (2002), Optimal control of treatments in a two-strain tuberculosis model, *Discrete and Continuous Dynamical Systems Series B*, **2**, 473-482.

[26] Lenhart, S. and Workman, J.T. (2007), *Optimal control applied to biological models*., Crc Press.