Received: 5 October 2018 | Revised: 11 February 2019 | Accepted: 21 March 2019

DOI: 10.1002/oca.2505

RESEARCH ARTICLE

WILEY

Optimal control measures for a susceptible-carrier-infectious-recovered-susceptible malware propagation model

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

[1]ALGORITMI R&D Center, Department of Production and Systems, University of Minho, Braga, Portugal

[2]School of Business Studies, Polytechnic Institute of Viana do Castelo, Valença, Portugal

[3]Center for Research and Development in Mathematics and Applications (CIDMA), University of Aveiro, Aveiro, Portugal

Correspondence

João N.C. Gonçalves, ALGORITMI R&D Center, Department of Production and Systems, University of Minho, 4710-057 Braga, Portugal.

Email: jncostagoncalves@gmail.com

Funding information

Fundação para a Ciência e Tecnologia, Grant/Award Number: UID/MAT/04106/2019 and UID/CEC/00319/2019

Summary

Purposing to lessen malware propagation, this paper proposes optimal control measures for a susceptible-carrier-infectious-recovered-susceptible (SCIRS) epidemiological model formed by a system of ordinary differential equations. By taking advantage of real-world data related to the number of reported cybercrimes in Japan from 2012 to 2017, an optimal control problem is formulated to minimize the number of infected devices in a cost-effective way. The existence and uniqueness of the results related to the optimality system are proved. Overall, numerical simulations show the usefulness of the proposed control strategies in reducing the spread of malware infections.

KEYWORDS

malware propagation, optimal control, optimal control application, SCIRS epidemiological model

1 | INTRODUCTION

Given the usefulness and the fast growth of the Internet and information technologies, social networks are considered to be the main channel for the dissemination of information, as well as a major target for malware attacks.[1] Malware is a common term used to lump together different malicious objects such as worms, viruses, and spyware, which, in fact, are hard to distinguish.[2] Presently, financial motivations lead to the development of new types of malware,[3] which, in turn, are constantly evolving not only in speed and number but also in discrepancy, a concept related to the emergence of new types of malware.[4] Within the technological context, in which the use of mobile devices has increased enormously, Liu and Zhong[3] highlighted the *web-based malware* as an attractive way to attack users, by exploiting vulnerabilities in web pages (eg, via hyperlinks embedded in e-mail messages) or even social engineering.[5] In this regard, ensuring secure networks is a paramount condition to prevent malware propagation,[6] which has become an acute threat to human beings and companies across the world. Hence, in view of the cross-cutting impact of malware on ordinary and everyday tasks, the design of new mathematical models able to simulate the dynamics of malware propagation is of utmost relevance to counteract its prevalence, alongside other preventing mechanisms such as antivirus softwares.[7]

Over time, mathematical epidemiology together with optimal control theory have been increasingly exploited to study viral marketing,[8-10] to model infectious disease dynamics[11,12] or even computer virus propagation.[3,13] In this context, this paper narrows its scope to mathematical modeling approaches applied to malware spreading. Apart from other types of mathematical models to study the dynamic features of malware propagation (see the work of Guillén and del Rey[7] and the references cited therein), compartmental models have been widely used for that purpose since the very first study on epidemiological approaches applied to computer viruses conducted by Kephart et al.[14] Concretely, compartmental extensions of the classical version of the susceptible-infected-recovered epidemic model[15] have been proposed to better understand malware propagation phenomena and to control its prevalence (see, eg, other works[16-21]). At this point, optimal control theory[22] plays a pivotal role in finding optimal ways to control dynamical systems and has been used to propose optimal strategies to minimize the prevalence of malware spreading. Zhu and Zhao[19] proposed a susceptible-infectious-recovered-susceptible model with time delay to assess malware propagation in wireless sensor networks. Additionally, the authors proposed an optimal control strategy to minimize the number of infected nodes and numerical simulations confirmed the effectiveness of the proposed control measure. In the work of Chen et al,[23] a susceptible-latent-breakingout-susceptible computer virus epidemic model was introduced to minimize the number of breaking-out computers with low costs associated with it. By considering delay differential equations and optimal control, the authors showed that the number of breaking-out machines is higher whenever the proposed control measure is not applied. On the other hand, Ahn et al[24] proposed a novel C-SEIRA epidemic model and a control intervention related to isolating infectious computers from the network.

Nevertheless, despite of optimal control theory has been used to model malware propagation, there is a lack of research studies regarding the use of real data in this field. Moreover, with the recent exception of Guillén and del Rey,[7] current mathematical models do not consider devices that can be infected by malware but cannot be harmed by it, a feature that is becoming more commonplace in mobile devices with specific operative systems. Thus, this paper uses real numerical data related to the number of cybercrimes reported to the Japanese police from 2012 to 2017 (see the work of Statista[25]) to propose optimal control strategies for the minimization of the number of infected devices, bearing in mind both the implementation costs and the effectiveness of control measures. For that, the susceptible-carrier-infectious-recovered-susceptible (SCIRS) epidemic model presented in the work of Guillén and del Rey[7] is considered.

The rest of this paper is organized as follows. In Section 2, a short description of the SCIRS model is presented. At this point, the parameters estimation process using real data from Japan cybercrime is also discussed. In Section 3, two control functions are added to the model, as well as two real positive parameters to represent the effectiveness of the proposed control strategies. Furthermore, an optimal control problem is formulated and the existence and uniqueness of the results related to the optimality system are proved. In Section 4, numerical simulations are conducted aiming to compare the theoretical results derived from the application of the control strategies with the Japan cybercrime real data. Finally, concluding remarks are provided in Section 5.

2 | THE SCIRS MODEL

At this stage, we recall the original susceptible-carrier-infectious-recovered-susceptible (SCIRS) epidemic model proposed in the work of Guillén and del Rey[7] and some related features considered to be relevant for subsequent analyses. In this sense, for more details on the model dynamics and formulation, the reader is referred to the original work.

In the SCIRS epidemic model, the number of devices in each compartment varies over time t. Concretely, the total number of devices, N, is subdivided into four compartments: susceptible (S), ie, devices that can be infected by a malware; carriers (C), ie, devices that can be infected and infect susceptible devices but cannot be harmed by malware; infected (I), ie, devices that can infect susceptible devices; and recovered (R), ie, devices that suffered from a malware infection but recovered after proper security interventions, becoming temporarily immune to malware attacks. Hence, by considering that N is constant over time t, ie, $S(t) + C(t) + I(t) + R(t) = N > 0$, the SCIRS model is governed by the following system of ordinary differential equations:

$$\begin{cases} \frac{dS(t)}{dt} = \epsilon R(t) - aS(t)(I(t) + C(t)) - vS(t), \\ \frac{dC(t)}{dt} = a(1-\delta)S(t)(I(t) + C(t)) - b_C C(t), \\ \frac{dI(t)}{dt} = a\delta S(t)(I(t) + C(t)) - b_I I(t), \\ \frac{dR(t)}{dt} = b_C C(t) + b_I I(t) + vS(t) - \epsilon R(t), \end{cases} \tag{1}$$

with nonnegative initial conditions $S(0) = S_0, C(0) = C_0, I(0) = I_0, R(0) = R_0$. Regarding the model parameters, a is the transmission rate, whereby susceptible devices are infected by carriers or infectious ones; δ is the fraction of

TABLE 1 Number of cybercrimes in Japan from 2012 to 2017 (see the work of Statista[25])

Year	2012	2013	2014	2015	2016	2017
Cybercrimes	77 815	84 863	118 100	128 097	131 518	130 011

susceptible devices, which have an operative system vulnerable to the malware attack; ν is the vaccination rate under which susceptible devices can become temporarily immune to malware infections; b_C and b_I are the rates, whereby carriers and infectious devices, respectively, become temporarily immune after the intervention of security countermeasures; and ϵ is the rate under which recovered devices lose their immunity and become susceptible again to new malware attacks.

To validate the numerical results, we consider the SCIRS model in the full form (1) notwithstanding it can be reduced according to the following property:

$$\frac{dS(t)}{dt}+\frac{dC(t)}{dt}+\frac{dI(t)}{dt}+\frac{dR(t)}{dt}=0. \tag{2}$$

The basic reproduction number, $\mathcal{R}_0$, for the model (1) traduces the number of secondary infections induced by a single infected device and is given by

$$\mathcal{R}_0=\frac{aN(b_I+(b_C-b_I)\delta)\epsilon}{b_C b_I(\nu+\epsilon)}. \tag{3}$$

Following the work of Guillén and del Rey,[7] $\mathcal{R}_0 > 1$ is a necessary condition for the existence of an endemic equilibrium solution. The reader is referred to the aforementioned work[7] for the detailed calculations of $\mathcal{R}_0$.

2.1 | Model application to Japan cybercrime data

To give more realism to this work, the SCIRS model previously introduced is now calibrated according to the number of cybercrimes reported to the Japanese police from 2012 to 2017 (see the work of Statista[25]). Hereinafter, it is assumed that one cybercrime reported to the Japanese police corresponds to one, and only one, infected device. Table 1 presents the evolution of the cybercrimes in Japan from 2012 to 2017.

Based on the data presented in Table 1, we adapted the `Matlab` code presented in pages 126 to 130 in the book of Martcheva[26] to estimate the parameters of the SCIRS model. The proposed algorithm takes advantage of the `fminsearch` function from `Matlab` optimization toolbox. This function is based on Nelder-Mead simplex method.[27] Following this numerical procedure, we find that the optimal values of the model parameters are $\epsilon \approx 0.8986, a \approx 7.94 \times 10^{-8}, \nu \approx 1.1261, \delta \approx 0.0008, b_C \approx 0.0412, b_I \approx 0.0485$. From these parameter estimations, it follows that $\mathcal{R}_0 > 1$. Furthermore, according to the number of Internet users in Japan at Internet Live Stats,[28] we assume the total population size, N, as $N = 101,071,581$, and the following initial conditions for the SCIRS model are considered:

$$S(0)=S_0=N-77815, \quad C(0)=C_0=0, \quad I(0)=I_0=77815, \quad R(0)=R_0=0. \tag{4}$$

Due to the lack of real-world data information, the numerical values for $S(0)$, $C(0)$, and $R(0)$ were assumed based on the estimated value of $I(0)$ from.[25] A summary of the model parameters is presented in Table 2.

Under the aforementioned parameters and initial conditions, Figure 1 shows that the SCIRS epidemic model (1) fits well the real data. At this point, it should be noted that $I(0)$ and $I(5)$ correspond to the number of cybercrimes in Japan at 2012 and 2017, respectively.

3 | OPTIMAL CONTROL PROBLEM

This section intends to use optimal control theory to propose control strategies that aim to minimize the number of infected devices over time t, in a cost-effective way. For that, two bounded controls, u_1 and u_2, are added to system (1). The control strategy u_1 is introduced to represent the effort in potentiating the vaccination rate ν (eg, by fostering a deep-seated security culture within internet users via awareness campaigns). On the other hand, the control strategy u_2 traduces the fraction of infected devices in which standard security countermeasures are replaced by high performance and fully updated antimalware software. This replacement is reasonable since better security countermeasures are more able to detect and, eventually, remove malicious objects. In other words, whereas u_1 intends to increase the vaccination rate,

TABLE 2 Summary of the susceptible-carrier-infectious-recovered-susceptible model parameters

Symbol	Description	Value	References
a	Transmission rate	7.94×10^{-8}	Estimated
v	Vaccination rate	1.1261	Estimated
δ	Fraction of susceptible devices with a vulnerable operative system	0.0008	Estimated
b_C	Temporary immunity rate of carrier devices	0.0412	Estimated
b_I	Temporary immunity rate of infectious devices	0.0485	Estimated
ϵ	Loss-of-immunity rate	0.8986	Estimated
N	Total number of devices	101,071,581	Internet Live Stats[28]
$S(0)$	Initial number of susceptible devices	$N - 77815$	Assumed
$C(0)$	Initial number of carrier devices	0	Assumed
$I(0)$	Initial number of infectious devices	77815	Statista[25]
$R(0)$	Initial number of recovered devices	0	Assumed

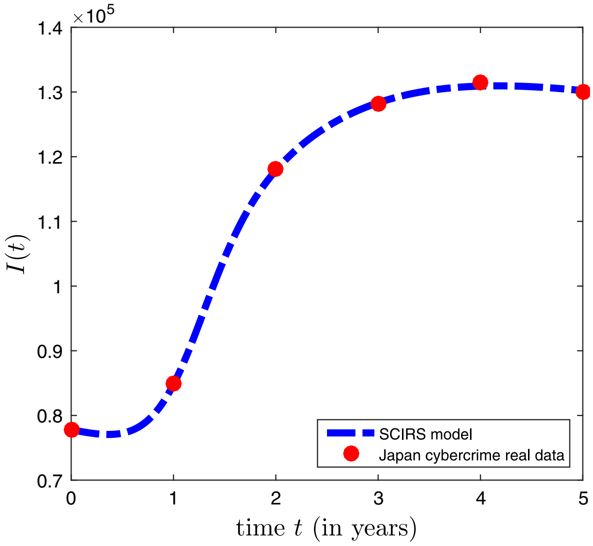


FIGURE 1 Susceptible-carrier-infectious-recovered-susceptible (SCIRS) model adjustment to the real number of cybercrimes in Japan from 2012 to 2017 [Colour figure can be viewed at wileyonlinelibrary.com]

u_2 intends to increase the rate b_I. In addition, two parameters $\alpha_i \in (0,1), i = 1,2$, are also introduced to measure the efficacy of the control strategies $u_i, i = 1,2$, respectively.

Let $[0, T]$ be the time period in which the control strategies act on the SCIRS model (1). Additionally, it is assumed that the admissible set of control functions is

$$\Omega = \left\{(u_1(\cdot), u_2(\cdot)) \in (L^2[0,T])^2 \mid (u_1(t), u_2(t)) \in [0,1] \times [0,1], \forall t \in [0,T]\right\}, \tag{5}$$

where $L^2[0, T]$ represents the set of all Lebesgue square integrable functions on $[0, T]$. Henceforth, based on the real-world data under study, we consider $T = 5$. Note that the magnitude of the control measures is maximum when $u_i = 1, i = 1,2$, and null when $u_i = 0, i = 1,2$. Thus, the SCIRS model (1) can be rewritten into the following controlled system:

$$\begin{cases} \frac{dS(t)}{dt} = \epsilon R(t) - aS(t)(I(t) + C(t)) - (v + \alpha_1 u_1(t))S(t) \\ \frac{dC(t)}{dt} = a(1-\delta)S(t)(I(t) + C(t)) - b_C C(t) \\ \frac{dI(t)}{dt} = a\delta S(t)(I(t) + C(t)) - (b_I + \alpha_2 u_2(t))I(t) \\ \frac{dR(t)}{dt} = b_C C(t) + (b_I + \alpha_2 u_2(t))I(t) + (v + \alpha_1 u_1(t))S(t) - \epsilon R(t), \end{cases} \quad \begin{cases} S(0) = N - 77815 \\ C(0) = 0 \\ I(0) = 77815 \\ R(0) = 0. \end{cases} \tag{6}$$

Due to the fact that the adoption of strategies to mitigate malware propagation is fairly expensive, the number of infected devices should be minimized in a cost-effective way. Hence, we propose an optimal control problem to minimize the following cost functional:

$$J(u_1(\cdot),u_2(\cdot)) = \int_0^T \left[I(t) + \frac{1}{2}\sum_{i=1}^{2} W_i u_i^2(t) \right] dt, \tag{7}$$

subject to (6), where the positive constants $W_i, i = 1, 2$, represent the relative cost of implementing the control strategies $u_i, i = 1, 2$, respectively. All in all, the main objective is to determine $(S^*(\cdot), C^*(\cdot), I^*(\cdot), R^*(\cdot))$, associated to an admissible control pair $(u_1^*(\cdot), u_2^*(\cdot)) \in \Omega$ over $[0, T]$, satisfying the controlled model (6) and minimizing the objective functional (7).

Following the Pontryagin's Maximum Principle,[22] if $(u_1^*(t), u_2^*(t))$ is optimal for the control problem (7) subject to (6), then there exists a nontrivial Lipschitz continuous mapping (the *adjoint vector*) $\lambda : [0, T] \to \mathbb{R}^4$, $\lambda(t) = (\lambda_1(t), \lambda_2(t), \lambda_3(t), \lambda_4(t))$, such that

$$\frac{dS(t)}{dt} = \frac{\partial \mathcal{H}}{\partial \lambda_1}, \quad \frac{dC(t)}{dt} = \frac{\partial \mathcal{H}}{\partial \lambda_2}, \quad \frac{dI(t)}{dt} = \frac{\partial \mathcal{H}}{\partial \lambda_3}, \quad \frac{dR(t)}{dt} = \frac{\partial \mathcal{H}}{\partial \lambda_4}$$

and

$$\frac{d\lambda_1(t)}{dt} = -\frac{\partial \mathcal{H}}{\partial S}, \quad \frac{d\lambda_2(t)}{dt} = -\frac{\partial \mathcal{H}}{\partial C}, \quad \frac{d\lambda_3(t)}{dt} = -\frac{\partial \mathcal{H}}{\partial I}, \quad \frac{d\lambda_4(t)}{dt} = -\frac{\partial \mathcal{H}}{\partial R},$$

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

$$\begin{aligned}\mathcal{H}(S, C, I, R, u_1, u_2, \lambda_1, \lambda_2, \lambda_3, \lambda_4) = {} & I(t) + \frac{1}{2}\sum_{i=1}^{2} W_i u_i^2(t) \\ & + \lambda_1(\epsilon R(t) - aS(t)(I(t) + C(t)) - (\nu + \alpha_1 u_1(t))S(t)) \\ & + \lambda_2(a(1-\delta)S(t)(I(t) + C(t)) - b_C C(t)) \\ & + \lambda_3(a\delta S(t)(I(t) + C(t)) - (b_I + \alpha_2 u_2(t))I(t)) \\ & + \lambda_4(b_C C(t) + (b_I + \alpha_2 u_2(t))I(t) + (\nu + \alpha_1 u_1(t))S(t) - \epsilon R(t))\end{aligned}$$

is called the *Hamiltonian*, and the functions $\lambda_i(t), i = 1, 2, 3, 4$ are the *adjoint functions* to be determined suitably.

Theorem 1 (Existence of optimal controls).
Given the controlled SCIRS model (6) and the objective functional (7), then there exists an optimal control $u_i^* \in \Omega, i = 1, 2$, such that $J(u_1^*(t), u_2^*(t)) = \min_\Omega J(u_1(t), u_2(t))$.

Proof. Firstly, the control functions and state variables of the controlled system (6) are nonnegative. This together with the boundedness of the state variables and coefficients of the controlled system (6) over the finite interval $[0, T]$, make it possible to use the existence result presented in theorem 9.2.1 in the book of Lukes[29] to prove this theorem. Hence, the following conditions should be satisfied (see the works of Fister et al[30] and Xu et al[31] for similar arguments):

(1) The set of solutions of the controlled system (6) and $u_i \in \Omega, i = 1, 2$, is not empty;
(2) The control space Ω is closed and convex;
(3) The right-hand side of the controlled system (6) is continuous, bounded, and can be written as a linear function with respect to the controls with coefficients depending on the states;
(4) The integrand of the objective functional (7) is convex on Ω with respect to $u_i, i = 1, 2$, and there exist constants $\rho > 1, C_1 > 0$, and C_2 such that

$$I(t) + \frac{1}{2}\sum_{i=1}^{2} W_i u_i^2(t) \geqslant C_1 \left(\sum_{i=1}^{2} |u_i(t)|^2 \right)^{\rho/2} - C_2. \tag{8}$$

Attending to the definition of Ω and the nonnegativity of the state variables, the set of solutions of the controlled system with initial conditions (6) and $u_i \in \Omega, i = 1, 2$, is not empty, which proves the Condition 1. The Condition 2 is satisfied since the control set Ω is closed and convex by definition. One could note that system (6) can be rewritten as

$$V(x) \doteq \frac{dx(t)}{dt} = Ax + B(x), \tag{9}$$

where

$$x(t) = \begin{bmatrix} S(t) \\ C(t) \\ I(t) \\ R(t) \end{bmatrix}, \quad A = \begin{bmatrix} -\alpha_1 u_1 - \nu & 0 & 0 & \epsilon \\ 0 & -b_C & 0 & 0 \\ 0 & 0 & -b_I - \alpha_2 u_2 & 0 \\ \alpha_1 u_1 + \nu & b_C & b_I + \alpha_2 u_2 & -\epsilon \end{bmatrix}, \quad B(x) = \begin{bmatrix} -aS(t)(I(t) + C(t)) \\ aS(t)(1-\delta)(I(t) + C(t)) \\ a\delta S(t)(I(t) + C(t)) \\ 0 \end{bmatrix}.$$

Hence, from the Hölder's inequality, the following condition holds:

$$|B(x_1) - B(x_2)| \leqslant M(|S_1 - S_2| + |C_1 - C_2| + |I_1 - I_2|), \tag{10}$$

where M is a positive constant, independent of the state variables. Then, it follows that

$$|V(x_1) - V(x_2)| \leqslant D|x_1 - x_2|, \tag{11}$$

where $D = \max\{M, \|A\|\} < \infty$, which proves that $V(x)$ is uniformly Lipschitz continuous. It is also easy to show that $V(x)$ can be written as a linear function in $u_i, i = 1, 2$, with state variables as coefficients. Therefore, Condition 3 is verified. Lastly, Condition 4 is proved by noting not only that the integrand in the functional (7) is convex on Ω but also that inequality (8) is satisfied by choosing $\rho = 1.5$, $C_1 = \min\{\frac{1}{2}W_i\}, i = 1, 2$, and $C_2 = 1$. Hence, the proof is concluded. □

Theorem 2 (Characterization of the optimal control).
At time t, let S^*, C^*, I^*, and R^* be the optimal state variables. Then, given the optimal control pair $(u_1^*(t), u_2^*(t))$ and the corresponding solution of the control problem (7) subject to (6), there exist adjoint variables $\lambda_i(t), i = 1, 2, 3, 4$ satisfying

$$\begin{cases} \frac{d\lambda_1(t)}{dt} = \lambda_1(t)\left[a(I^*(t) + C^*(t)) + \nu + \alpha_1 u_1^*(t)\right] - \lambda_2(t)a(1-\delta)(I^*(t) + C^*(t)) - \lambda_3(t)a\delta(I^*(t) + C^*(t)) \\ \qquad -\lambda_4(t)\left(\nu + \alpha_1 u_1^*(t)\right) \\ \frac{d\lambda_2(t)}{dt} = \lambda_1(t)aS^*(t) - \lambda_2(t)\left[a(1-\delta)S^*(t) - b_C\right] - \lambda_3(t)a\delta S^*(t) - \lambda_4(t)b_C \\ \frac{d\lambda_3(t)}{dt} = -1 + \lambda_1(t)aS^*(t) - \lambda_2(t)a(1-\delta)S^*(t) - \lambda_3(t)\left[a\delta S^*(t) - b_I - \alpha_2 u_2^*(t)\right] - \lambda_4(t)\left(b_I + \alpha_2 u_2^*(t)\right) \\ \frac{d\lambda_4(t)}{dt} = \epsilon(\lambda_4(t) - \lambda_1(t)), \end{cases} \tag{12}$$

with transversality conditions

$$\lambda_i(T) = 0, \quad i = 1, 2, 3, 4. \tag{13}$$

Furthermore,

$$u_1^*(t) = \min\left\{\max\left\{0, \frac{\alpha_1 S^*(t)(\lambda_1(t) - \lambda_4(t))}{W_1}\right\}, 1\right\}, \tag{14}$$

$$u_2^*(t) = \min\left\{\max\left\{0, \frac{\alpha_2 I^*(t)(\lambda_3(t) - \lambda_4(t))}{W_2}\right\}, 1\right\}. \tag{15}$$

Proof. Following the Pontryagin's Maximum Principle,[22] the adjoint system (12) comes from

$$\begin{cases} \frac{d\lambda_1(t)}{dt} = -\frac{\partial\mathcal{H}(S,C,I,R,u_1,u_2,\lambda_1,\lambda_2,\lambda_3,\lambda_4)}{\partial S}\Big|_{S^*=S,\ C^*=C,\ I^*=I,\ R^*=R,\ u_1^*=u_1,\ u_2^*=u_2} \\ \frac{d\lambda_2(t)}{dt} = -\frac{\partial\mathcal{H}(S,C,I,R,u_1,u_2,\lambda_1,\lambda_2,\lambda_3,\lambda_4)}{\partial C}\Big|_{S^*=S,\ C^*=C,\ I^*=I,\ R^*=R,\ u_1^*=u_1,\ u_2^*=u_2} \\ \frac{d\lambda_3(t)}{dt} = -\frac{\partial\mathcal{H}(S,C,I,R,u_1,u_2,\lambda_1,\lambda_2,\lambda_3,\lambda_4)}{\partial I}\Big|_{S^*=S,\ C^*=C,\ I^*=I,\ R^*=R,\ u_1^*=u_1,\ u_2^*=u_2} \\ \frac{d\lambda_4(t)}{dt} = -\frac{\partial\mathcal{H}(S,C,I,R,u_1,u_2,\lambda_1,\lambda_2,\lambda_3,\lambda_4)}{\partial R}\Big|_{S^*=S,\ C^*=C,\ I^*=I,\ R^*=R,\ u_1^*=u_1,\ u_2^*=u_2}. \end{cases} \tag{16}$$

Finally, by considering the optimality condition, it follows that

$$\frac{\partial\mathcal{H}}{\partial u_1}\Big|_{S^*=S,\ C^*=C,\ I^*=I,\ R^*=R,\ u_1^*=u_1} = W_1 u_1^*(t) - \alpha_1 S^*(t)(\lambda_1(t) - \lambda_4(t)) = 0, \tag{17}$$

$$\frac{\partial\mathcal{H}}{\partial u_2}\Big|_{S^*=S,\ C^*=C,\ I^*=I,\ R^*=R,\ u_2^*=u_2} = W_2 u_2^*(t) - \alpha_2 I^*(t)(\lambda_3(t) - \lambda_4(t)) = 0. \tag{18}$$

Thus, by (17) and (18), and considering the boundedness conditions of $u_i, i = 1, 2$, on Ω, we get

$$\begin{cases} u_1^*(t) = 0, \text{ if } \frac{\alpha_1 S^*(t)(\lambda_1(t)-\lambda_4(t))}{W_1} < 0 \quad, \\ u_1^*(t) = \frac{\alpha_1 S^*(t)(\lambda_1(t)-\lambda_4(t))}{W_1}, \text{ if } 0 \leqslant \frac{\alpha_1 S^*(t)(\lambda_1(t)-\lambda_4(t))}{W_1} \leqslant 1 \quad, \\ u_1^*(t) = 1, \text{ if } \frac{\alpha_1 S^*(t)(\lambda_1(t)-\lambda_4(t))}{W_1} > 1, \end{cases} \tag{19}$$

$$\begin{cases} u_2^*(t) = 0, \quad \text{if } \frac{\alpha_2 I^*(t)(\lambda_3(t)-\lambda_4(t))}{W_2} < 0, \\ u_2^*(t) = \frac{\alpha_2 I^*(t)(\lambda_3(t)-\lambda_4(t))}{W_2}, \quad \text{if } 0 \leqslant \frac{\alpha_2 I^*(t)(\lambda_3(t)-\lambda_4(t))}{W_2} \leqslant 1, \\ u_2^*(t) = 1, \quad \text{if } \frac{\alpha_2 I^*(t)(\lambda_3(t)-\lambda_4(t))}{W_2} > 1, \end{cases} \tag{20}$$

which, in turn, can be rewritten in a compact form as

$$u_1^*(t) = \min\left\{ \max\left\{ 0, \frac{\alpha_1 S^*(t)(\lambda_1(t) - \lambda_4(t))}{W_1} \right\}, 1 \right\}, \tag{21}$$

$$u_2^*(t) = \min\left\{ \max\left\{ 0, \frac{\alpha_2 I^*(t)(\lambda_3(t) - \lambda_4(t))}{W_2} \right\}, 1 \right\}. \tag{22}$$

This completes the proof. □

Based on the foregoing, the optimal control and states can be computed by solving the optimality system, which consists in the state system (6), the adjoint system (12) and the transversality conditions (13) together with the characterizations (14) and (15), ie,

$$\begin{cases} \frac{dS^*(t)}{dt} = \epsilon R^*(t) - aS^*(t)(I^*(t) + C^*(t)) - \left(v + \alpha_1 u_1^*(t)\right) S^*(t) \\ \frac{dC^*(t)}{dt} = a(1-\delta)S^*(t)(I^*(t) + C^*(t)) - b_C C^*(t) \\ \frac{dI^*(t)}{dt} = a\delta S^*(t)(I^*(t) + C^*(t)) - \left(b_I + \alpha_2 u_2^*(t)\right) I^*(t) \\ \frac{dR^*(t)}{dt} = b_C C^*(t) + \left(b_I + \alpha_2 u_2^*(t)\right) I^*(t) + \left(v + \alpha_1 u_1^*(t)\right) S^*(t) - \epsilon R^*(t) \\ \frac{d\lambda_1(t)}{dt} = \lambda_1(t) \left[a(I^*(t) + C^*(t)) + v + \alpha_1 u_1^*(t)\right] - \lambda_2(t)a(1-\delta)(I^*(t) + C^*(t)) - \lambda_3(t)a\delta(I^*(t) + C^*(t)) \\ \qquad -\lambda_4(t)\left(v + \alpha_1 u_1^*(t)\right) \\ \frac{d\lambda_2(t)}{dt} = \lambda_1(t)aS^*(t) - \lambda_2(t)\left[a(1-\delta)S^*(t) - b_C\right] - \lambda_3(t)a\delta S^*(t) - \lambda_4(t)b_C \\ \frac{d\lambda_3(t)}{dt} = -1 + \lambda_1(t)aS^*(t) - \lambda_2(t)a(1-\delta)S^*(t) - \lambda_3(t)\left[a\delta S^*(t) - b_I - \alpha_2 u_2^*(t)\right] - \lambda_4(t)\left(b_I + \alpha_2 u_2^*(t)\right) \\ \frac{d\lambda_4(t)}{dt} = \epsilon(\lambda_4(t) - \lambda_1(t)) \\ u_1^*(t) = \min\left\{ \max\left\{ 0, \frac{\alpha_1 S^*(t)(\lambda_1(t)-\lambda_4(t))}{W_1} \right\}, 1 \right\} \\ u_2^*(t) = \min\left\{ \max\left\{ 0, \frac{\alpha_2 I^*(t)(\lambda_3(t)-\lambda_4(t))}{W_2} \right\}, 1 \right\}, \end{cases} \tag{23}$$

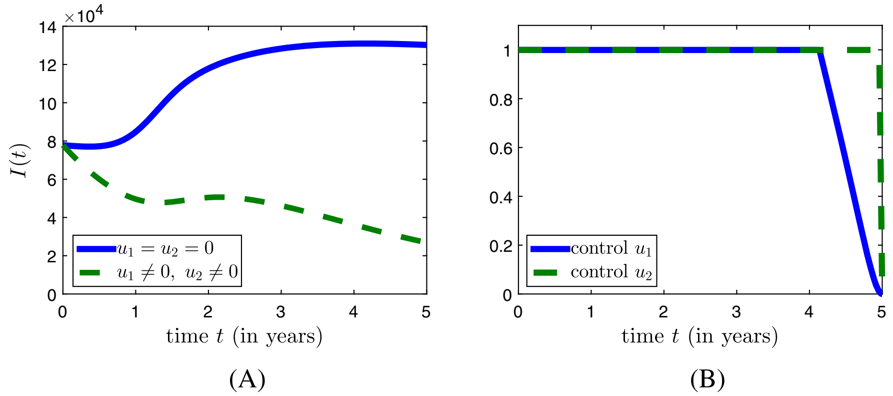
with $S^*(0) = N - 77815, C^*(0) = 0, I^*(0) = 77815, R^*(0) = 0$, and $\lambda_i(T) = 0, i = 1, 2, 3, 4$. Since the state and adjoint functions are bounded over the finite interval $[0, T]$ and systems (6) and (12) preserve the Lipschitz structure, the optimal control pair (u_1^*, u_2^*) is unique for T sufficiently small (see the work of Jung et al[32]). However, the uniqueness of optimality system holds for any value of T since the state system (6) is autonomous.

To derive the optimal controls and states, the system (23) should then be solved using numerical methods.

4 | NUMERICAL SIMULATIONS AND DISCUSSION

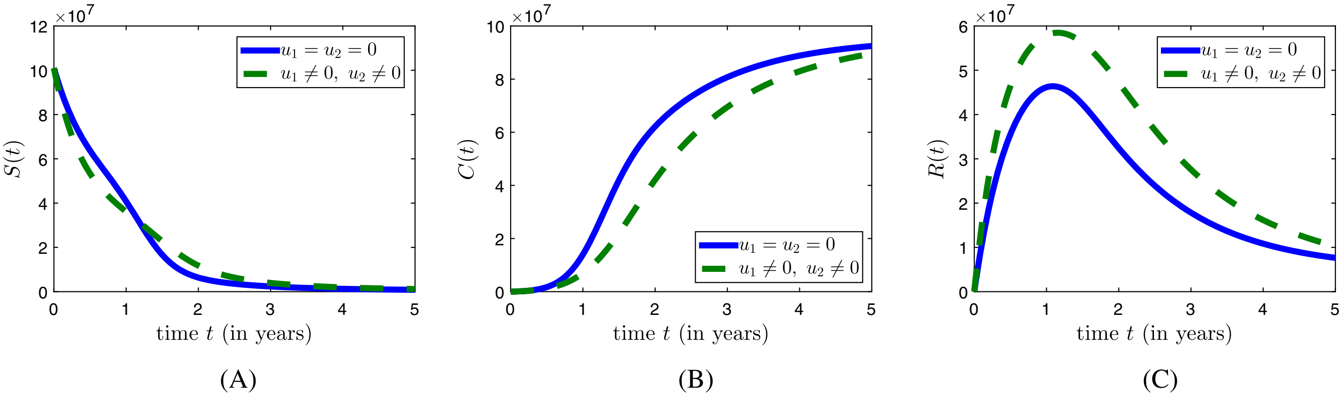
This section intends to present the results of the numerical implementation of the optimality system (23) with cost functional (7). The numerical implementation was conducted in `Matlab` by using the *Forward-Backward Sweep* numerical method,[33] as well as the model parameters presented in Table 2.

Obviously, to decrease malware propagation, it is a common practice to invest in security countermeasures. However, it is not clear that the number of malware infections will be lower the greater the security investment costs. In this sense, it is important to assess whether these investments should increase or decrease to minimize the number of malware infections without incurring significant costs. By looking at the cost functional (7), the parameter $W_i, i = 1, 2$, should be seen as a trade-off factor to minimize the number of malware infections and the costs associated with it. Equally relevant is to analyze how effective the proposed security countermeasures are in reducing the number of malware infections. For these reasons, we investigate the effects of the parameters W_i and $\alpha_i, i = 1, 2$, on the optimal control, as well as on the optimal states, over the time interval $[0, 5]$. Attending to the nature of the control strategies u_1 and u_2, the subsequent



(A) (B)

FIGURE 2 The influence of optimal control on the number of infected devices, for $W_1 = 250$, $W_2 = 550$, $\alpha_1 = \alpha_2 = 0.5$ and parameter values from Table 2. A, $I(t)$ with and without controls; B, Optimal controls u_1 and u_2 [Colour figure can be viewed at wileyonlinelibrary.com]



(A) (B) (C)

FIGURE 3 State variables dynamics with and without controls, for $W_1 = 250$, $W_2 = 550$, $\alpha_1 = \alpha_2 = 0.5$ and parameter values from Table 2. A, $S(t)$; B, $C(t)$; C, $R(t)$ [Colour figure can be viewed at wileyonlinelibrary.com]

analyses assume that the cost of implementing u_1 cannot be greater than the cost of implementing u_2, ie, $W_1 \leqslant W_2$. In Figure 2, the number of infected devices with and without the adoption of control strategies is compared for $W_1 = 250$, $W_2 = 550$ and equally effective controls ($\alpha_1 = \alpha_2 = 0.5$). One could see that the number of infected devices decreases whenever control strategies are adopted (Figure 2A). In addition, Figure 2B suggests that if the goal is to minimize the number of infected devices in a cost-effective way, the control u_1 is at the upper bound until $t = 4$, and then it decreases to the lower bound. On the other hand, the control u_2 is at the upper bound practically throughout the entire time window. Therefore, both control measures are relevant to minimize the objective functional (7).

At this point, it should be stressed that the extra effort on the implementation of both control measures is accommodated through a substantial reduction in the number of infected devices. The benefits derived from the application of the control strategies on the remain state variables are also depicted in Figure 3. Here, a relevant aspect relates to the fact that the number of carrier devices is lower whenever the controls are applied (Figure 3B). This means that the proposed control strategies enable to reduce the number of devices that, in spite of being immune to the malware, can infect susceptible devices over time t. Moreover, the number of recovered individuals is also higher whenever control policies are employed (Figure 3C).

The effects of the variation of the control weight W_2 when W_1 is fixed, for $\alpha_1 = \alpha_2 = 0.5$, are presented in Figure 4. It is then possible to see that the magnitude of the controls u_1, u_2, as well as the number of infected devices, is the same regardless the value of the relative investment cost W_2 over time t. This particularly indicates that the investment in the control strategy u_2, the most expensive one, should be properly assessed since that higher investment costs in the control policy u_2 do not translate into lower levels of malware infections (see Figure 4C).

However, when the investment costs in the control strategies u_1 and u_2 are the same (Figure 5), the magnitude of the control u_1 increases when the value of $W_i, i = 1, 2$, decreases notwithstanding the dynamics of both the control u_2 and the state variable I be the same as in Figure 4. This means that to cope with the minimization of the objective functional (7), the control u_1 should be applied with higher intensity when the related investment cost is low (see Figure 5A), and the

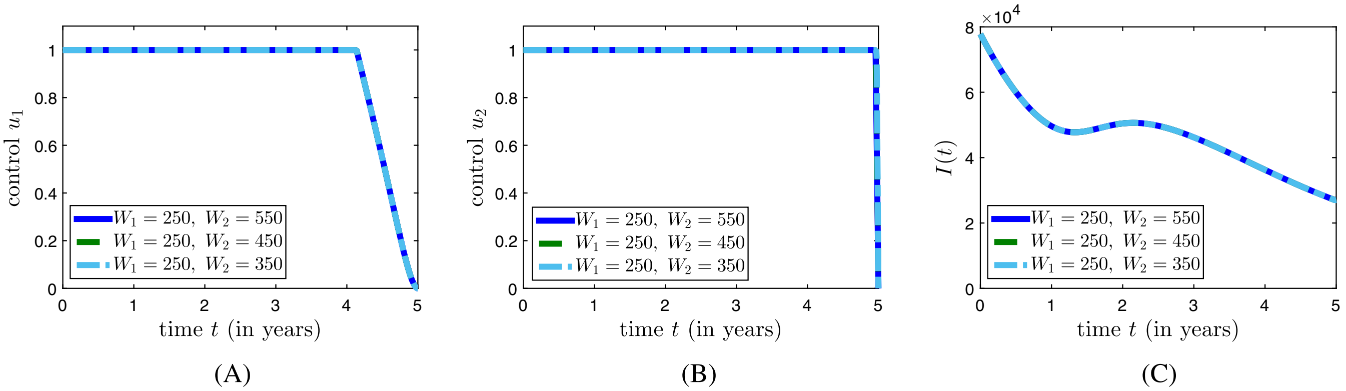


FIGURE 4 Effects of varying the control weight W_2 when $W_1 = 250$, for $\alpha_1 = \alpha_2 = 0.5$ and parameter values from Table 2. A, Control u_1; B, Control u_2; C, $I(t)$ [Colour figure can be viewed at wileyonlinelibrary.com]

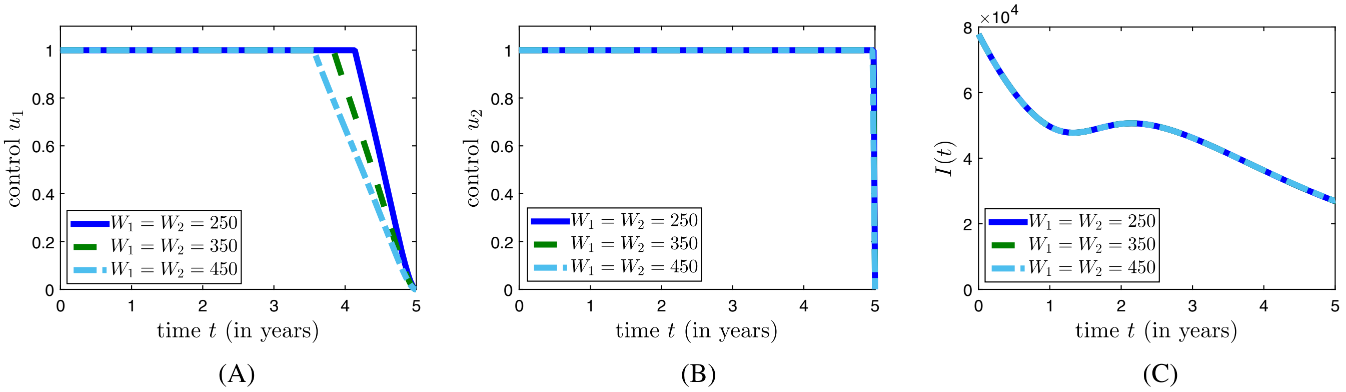


FIGURE 5 Effects of varying the control weights $W_i, i = 1, 2$, for $\alpha_1 = \alpha_2 = 0.5$ and parameter values from Table 2. A, Control u_1; B, Control u_2; C, $I(t)$ [Colour figure can be viewed at wileyonlinelibrary.com]

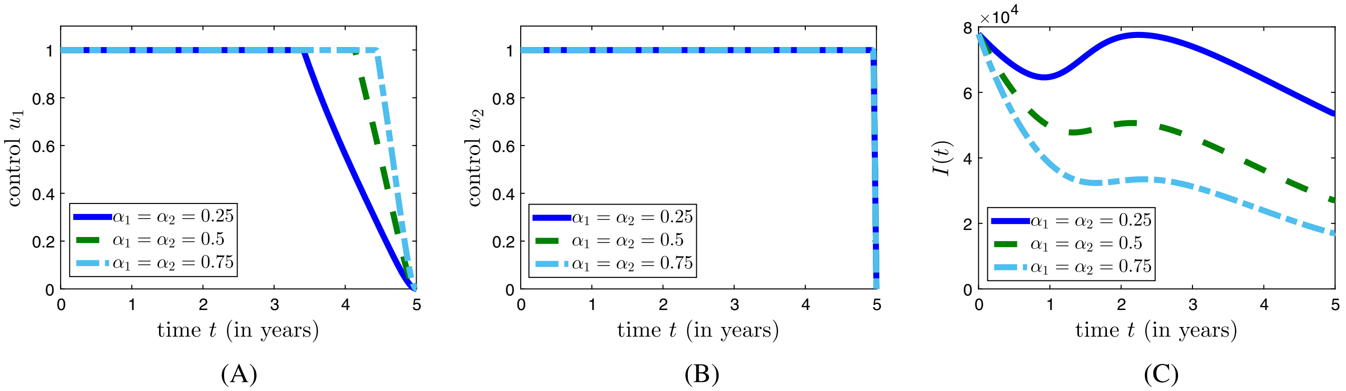
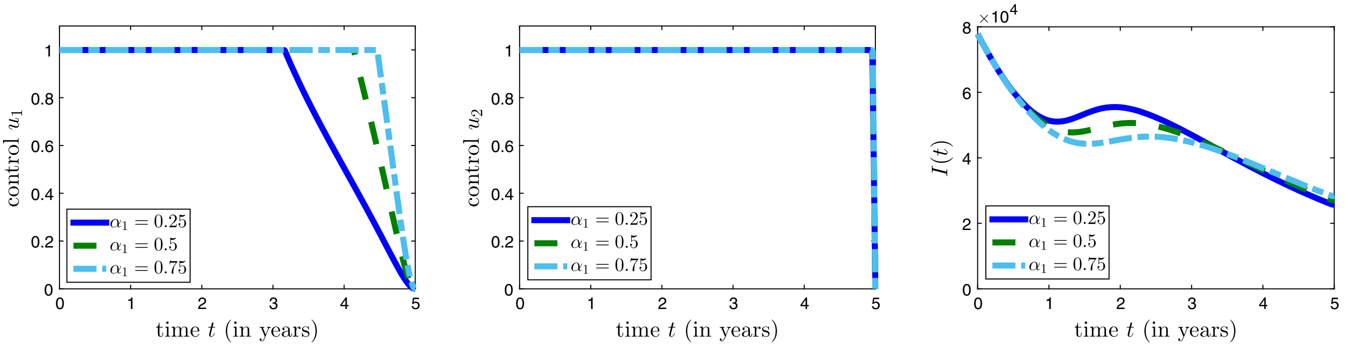


FIGURE 6 Effects of varying the control efficacy parameter $\alpha_i, i = 1, 2$, for $W_1 = 250$, $W_2 = 550$ and parameter values from Table 2. A, Control u_1; B, Control u_2; C, $I(t)$ [Colour figure can be viewed at wileyonlinelibrary.com]

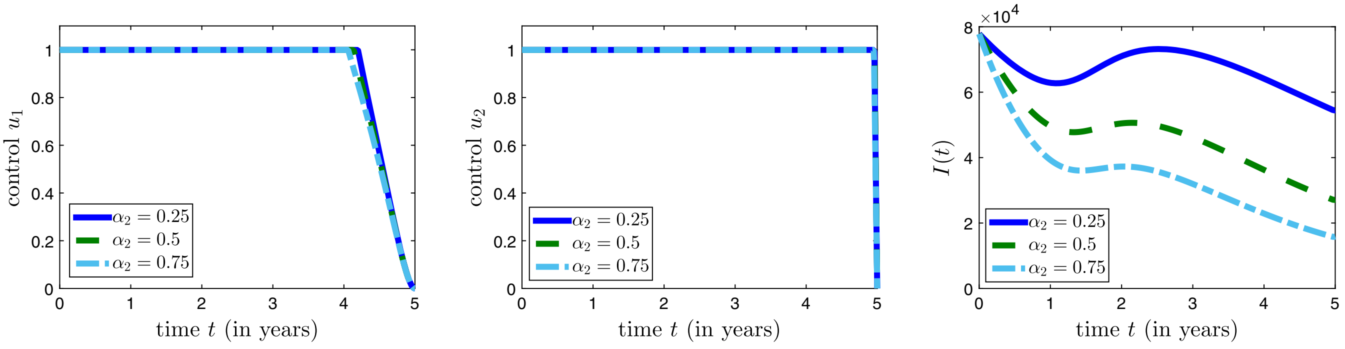
control u_2 is at the upper bound during the entire time horizon. Moreover, in this case, the investment in the control u_2 should be suitably cut down when the costs of new security countermeasures do not confer any advantage to minimize the number of infected devices.

Now, we analyze the implications of varying the control efficacy parameters $\alpha_i, i = 1, 2$, for $W_1 = 250$ and $W_2 = 550$. For that, three scenarios are considered: the scenario 1 (Figure 6), in which the efficacy of both control strategies is the same; the scenario 2 (Figure 7), in which the efficacy of the control strategy u_2 is fixed to 0.5 and the efficacy of the control strategy u_1 increases; and the scenario 3 (Figure 8), in which the efficacy of the control strategy u_1 is fixed to 0.5 and the efficacy of the control strategy u_2 increases.



(A) (B) (C)

FIGURE 7 Effects of varying the control efficacy parameter α_1 when $\alpha_2 = 0.5$, for $W_1 = 250$, $W_2 = 550$ and parameter values from Table 2. A, Control u_1; B, Control u_2; C, $I(t)$ [Colour figure can be viewed at wileyonlinelibrary.com]



(A) (B) (C)

FIGURE 8 Effects of varying the control efficacy parameter α_2 when $\alpha_1 = 0.5$, for $W_1 = 250$, $W_2 = 550$ and parameter values from Table 2. A, Control u_1; B, Control u_2; C, $I(t)$ [Colour figure can be viewed at wileyonlinelibrary.com]

Firstly, whatever the considered scenario, an increasing in the efficacy of the control strategy leads to a decrease in the number of infected devices when compared to the real number of Japanese cybercrimes (see Figures 2A, 6C, 7C, and 8C). Regarding the scenario 1, Figure 6A indicates that the magnitude of the control u_1 increases when $\alpha_i, i = 1, 2$ increases. On the other hand, the control u_2 remains at the upper bound over the time window considered, regardless of the efficacy tested (Figures 6B). In this context, both control strategies are important to minimize the cost functional (7). Analogous dynamics are obtained when α_2 is fixed to 0.5 and α_1 increases (scenario 2) (Figure 7). Nonetheless, this is not the case in scenario 3 (Figure 8). Indeed, whereas the control u_2 remains at the upper bound regardless the value of α_2, the magnitude of u_1 slightly decreases whenever α_2 increases (Figures 8A and 8B). This fact indicates that to meet

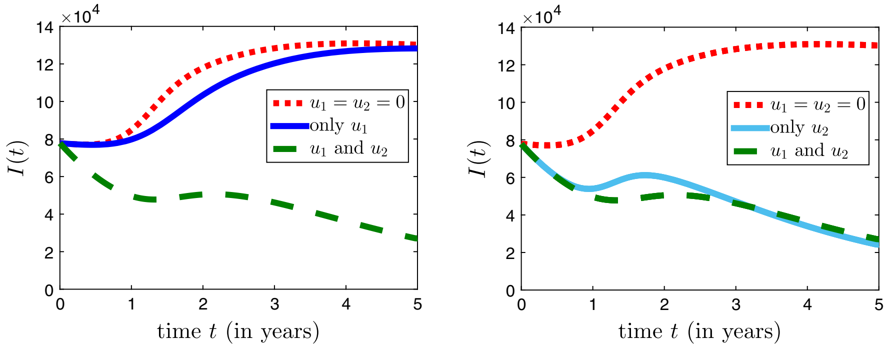


FIGURE 9 The dynamics of infected devices under different control applications, for $\alpha_1 = \alpha_2 = 0.5$, $W_1 = 250$, $W_2 = 550$ and parameter values from Table 2 [Colour figure can be viewed at wileyonlinelibrary.com]

the objective functional (7) when α_2 increases, particularly attention should be given to control strategies related to u_2 in detriment of ones associated with u_1.

Transversally, the number of malware infections is lower whenever optimal control strategies are employed and Figure 2 had already shown this statement. Aiming to understand the role of each control policy in minimizing the number of infected devices, the left of Figure 9 demonstrates that when the control policy u_1 is applied alone the number of malware infections does not decrease over time, albeit the levels of infected devices be smaller than the real infections recorded in that period by the Japanese police. Hence, despite of the control u_1 can in fact contribute for lower levels of malware infections, the right of Figure 9 shows that the best strategy to minimize the cost functional (7) is to apply both control policies concomitantly.

5 | CONCLUDING REMARKS

This paper proposes two control strategies to address the issue of how to soften malware propagation. In this regard, an optimal control problem is formulated to minimize malware propagation in a cost-effective way, under real-world numerical data related to the number of reported cybercrimes in Japan from 2012 to 2017. Under the Pontryagin's Maximum Principle, the necessary conditions for the optimal control problem are derived. The existence and uniqueness of the results associated with the optimality system are proved. Numerical simulations show the usefulness of the proposed approaches in reducing the number of cybercrimes in Japan in that period. It is our understanding that the presented model provides relevant guidelines to control malware propagation in real-world scenarios. Nevertheless, further investigations should be conducted to test different control parameter values. The application of several types of delay, multiobjective optimization, and Bang-Bang controls are also pointed as future research.

ACKNOWLEDGEMENTS

The authors are grateful to the anonymous reviewers for their valuable remarks and comments. This research has been supported by Fundação para a Ciência e Tecnologia (FCT) within the project scopes: UID/MAT/04106/2019 through Center for Research and Development in Mathematics and Applications (CIDMA), and UID/CEC/00319/2019 through ALGORITMI R&D Center.

ORCID

João N.C. Gonçalves https://orcid.org/0000-0002-0933-1995
Helena Sofia Rodrigues https://orcid.org/0000-0002-6319-7782
M. Teresa T. Monteiro https://orcid.org/0000-0001-9499-6811

REFERENCES

1. Hu H, Myers S, Colizza V, Vespignani A. WiFi networks and malware epidemiology. *Proc Natl Acad Sci*. 2009;106(5):1318-1323.
2. Garetto M, Gong W, Towsley D. Modeling malware spreading dynamics. Paper presented at: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Vol. 3; 2003; San Francisco, CA.
3. Liu W, Zhong S. Web malware spread modelling and optimal control strategies. *Scientific Reports*. 2017;7: Article number 42308.
4. Dhammi A, Singh M. Behavior analysis of malware using machine learning. Paper presented at: 2015 Eighth International Conference on Contemporary Computing (IC3); 2015; Noida, India.
5. Peltier TR. Social engineering: concepts and solutions. *Inf Secur J*. 2006;15(5):13-21.
6. Du B, Wang H. Partial differential equation modeling of malware propagation in social networks with mixed delays. *Comput Math Appl*. 2018;75(10):3537-3548.
7. Guillén JH, del Rey A. Modeling malware propagation using a carrier compartment. *Commun Nonlinear Sci Numer Simul*. 2018;56:217-226.
8. Kandhway K, Kuri J. How to run a campaign: optimal control of SIS and SIR information epidemics. *Appl Math Comput*. 2014;231:79-92.
9. Gonçalves J, Rodrigues HS, Monteiro MTT. Optimal control strategies for an advertisement viral diffusion. In: *Operational Research: IO2017, Valença, Portugal, June 28-30*. Cham, Switzerland: Springer International Publishing AG; 2017:135-149.
10. Gonçalves J, Monteiro MTT, Rodrigues HS. On the dynamics of a viral marketing model with optimal control using indirect and direct methods. *Stat Optim Inf Comput*. 2018;6(4):633-644.
11. Silva CJ, Torres DF. Optimal control for a tuberculosis model with reinfection and post-exposure interventions. *Mathematical Biosciences*. 2013;244(2):154-164.

12. Silva CJ, Torres DF. A SICA compartmental model in epidemiology with application to HIV/AIDS in Cape Verde. *Ecological Complexity*. 2017;30:70-75.
13. Zhang C, Huang H. Optimal control strategy for a novel computer virus propagation model on scale-free networks. *Phys A Stat Mech Its Appl*. 2016;451:251-265.
14. Kephart JO, White SR, Chess DM. Computers and epidemiology. *IEEE Spectrum*. 1993;30(5):20-26.
15. Kermack WO, McKendrick AG. Contributions to the mathematical theory of epidemics. ii.–the problem of endemicity. *Proc R Soc Lond A*. 1932;138(834):55-83.
16. Piqueira JR, de Vasconcelos AA, Gabriel CE, Araujo VO. Dynamic models for computer viruses. *Comput Secur*. 2008;27(7-8):355-359.
17. Piqueira JRC, Araujo VO. A modified epidemiological model for computer viruses. *Appl Math Comput*. 2009;213(2):355-360.
18. Toutonji OA, Yoo S-M, Park M. Stability analysis of VEISV propagation modeling for network worm attack. *Appl Math Model*. 2012;36(6):2751-2761.
19. Zhu L, Zhao H. Dynamical analysis and optimal control for a malware propagation model in an information network. *Neurocomputing*. 2015;149:1370-1386.
20. Guillén JH, del Rey AM, Encinas LH. Study of the stability of a SEIRS model for computer worm propagation. *Phys A Stat Mech Its Appl*. 2017;479:411-421.
21. Martín-Vaquero J, del Rey AM, Encinas AH, Guillén JH, Queiruga-Dios A, Sánchez GR. Higher-order nonstandard finite difference schemes for a MSEIR model for a malware propagation. *J Comput Appl Math*. 2017;317:146-156.
22. Pontryagin L, Boltyanskii V, Gramkrelidze R, Mischenko E. *The Mathematical Theory of Optimal Processes*. New York, NY: Wiley Interscience; 1962.
23. Chen L, Hattaf K, Sun J. Optimal control of a delayed SLBS computer virus model. *Phys A Stat Mech Its Appl*. 2015;427:244-250.
24. Ahn I, Oh HC, Park J. Investigation of the C-SEIRA model for controlling malicious code infection in computer networks. *Appl Math Model*. 2015;39(14):4121-4133.
25. Statista. Number of cyber crime related reports in Japan from 2012 to 2017. https://www.statista.com/statistics/746985/japan-number-of-reported-cyber-crimes/. Accessed May 30, 2018.
26. Martcheva M. *An Introduction to Mathematical Epidemiology*. New York, NY: Springer Science+Business Media; 2015. *Texts in Applied Mathematics*; vol. 61.
27. Lagarias JC, Reeds JA, Wright MH, Wright PE. Convergence properties of the Nelder–Mead simplex method in low dimensions. *SIAM J Optim*. 1998;9(1):112-147.
28. Internet Live Stats. Japan Internet users. http://www.internetlivestats.com/internet-users/japan/. Accessed May 26, 2018.
29. Lukes DL. *Differential Equations: Classical to Controlled*. New York, NY: Academic Press; 1982. *Mathematics in Science and Engineering*; vol. 162.
30. Fister KR, Lenhart S, McNally JS. Optimizing chemotherapy in an HIV model. *Electron J Differ Equ*. 1998;1998(32):1-12.
31. Xu D, Xu X, Xie Y, Yang C. Optimal control of an SIVRS epidemic spreading model with virus variation based on complex networks. *Commun Nonlinear Sci Numer Simul*. 2017;48:200-210.
32. Jung E, Lenhart S, Feng Z. Optimal control of treatments in a two-strain tuberculosis model. *Discrete Continuous Dyn Syst Ser B*. 2002;2(4):473-482.
33. Lenhart S, Workman JT. *Optimal Control Applied to Biological Models*. Boca Raton, FL: CRC Press; 2007.

How to cite this article: Gonçalves JNC, Rodrigues HS, Monteiro MTT. Optimal control measures for a susceptible-carrier-infectious-recovered-susceptible malware propagation model. *Optim Control Appl Meth*. 2019;1–12. https://doi.org/10.1002/oca.2505