

Research Article

Seeking Best-Balanced Patch-Injecting Strategies through Optimal Control Approach

Kaifan Huang ¹, Pengdeng Li,¹ Lu-Xing Yang ²,
Xiaofan Yang ¹ and Yuan Yan Tang ³

¹School of Big Data & Software Engineering, Chongqing University, Chongqing 400044, China

²School of Information Technology, Deakin University, Melbourne, VIC 3125, Australia

³Department of Computer and Information Science, The University of Macau, Macau

Correspondence should be addressed to Xiaofan Yang; xfyang1964@gmail.com

Received 28 February 2019; Revised 4 May 2019; Accepted 22 May 2019; Published 10 June 2019

Guest Editor: Akbar S. Namin

Copyright © 2019 Kaifan Huang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

To restrain escalating computer viruses, new virus patches must be constantly injected into networks. In this scenario, the patch-developing cost should be balanced against the negative impact of virus. This article focuses on seeking best-balanced patch-injecting strategies. First, based on a novel virus-patch interactive model, the original problem is reduced to an optimal control problem, in which (a) each admissible control stands for a feasible patch-injecting strategy and (b) the objective functional measures the balance of a feasible patch-injecting strategy. Second, the solvability of the optimal control problem is proved, and the optimality system for solving the problem is derived. Next, a few best-balanced patch-injecting strategies are presented by solving the corresponding optimality systems. Finally, the effects of some factors on the best balance of a patch-injecting strategy are examined. Our results will be helpful in defending against virus attacks in a cost-effective way.

1. Introduction

Computer networks bring huge convenience to our work and life [1, 2]. Meanwhile, digital viruses can propagate rapidly through computer networks, posing a severe threat to human society. For example, Wanna Decryptor, the notorious ransomware, has recently swept across the globe, leading to massive computer paralysis [3]. Consequently, the problem of how to mitigate the negative impact of computer virus in a cost-effective way has long been a hotspot of research in the field of cyber security [4].

To restrain evolving computer viruses, new virus patches must be constantly injected into networks. In this scenario, there is an obvious conflict between the patch-developing cost and the impact of virus; reducing the former would increase the latter, whereas mitigating the latter would enhance the former. Therefore, the patch-developing cost should be balanced against the impact of virus. We refer to a dynamic patch-injecting strategy that achieves the best balance between the two aspects as a best-balanced

patch-injecting strategy, and we refer to the problem of seeking best-balanced patch-injecting strategies as the *virus-patch tradeoff (VPT) problem*. Solving the VPT problem would be helpful in defending against virus attacks in a cost-effective way.

This article addresses the VPT problem. First, based on a novel virus-patch interactive model, the original problem is reduced to an optimal control problem which we refer to as the VPT control problem, in which (a) each admissible control stands for a feasible patch-injecting strategy and (b) the objective functional measures the balance of a feasible patch-injecting strategy. Second, the solvability of the VPT control problem is shown, and the optimality system for solving the VPT control problem is derived. Next, a few best-balanced patch-injecting strategies are given by solving the corresponding optimality systems. Finally, the effects of some factors on the best balance of a patch-injecting strategy are examined.

The remaining materials are organized in this fashion: Section 2 reviews the related work. Sections 3 and 4 establish

and solve the VPT control problem, respectively. Section 5 illustrates how to solve the VPT control problem, and Section 6 examines the effects of some factors on the best balance. This work is summarized by Section 7.

2. Related Work

In order to solve the VPT problem, the expected total loss of all network users resulting from a patch-injecting strategy must be estimated [5, 6]. As this quantity relies on the expected network states at all times, we need to characterize the evolutionary process of the expected network state. The resulting evolutionary model is essentially a propagation model that captures the interactive propagation of viruses and patches [7, 8]. In the available literature, propagation models of this kind are referred to as Susceptible-Infected-Patched-Susceptible (SIPS) models.

Compartmental propagation models are propagation models in which all nodes of the same state are classified as a class, with the goal of understanding the evolutionary trend of the size or fraction of each class [9]. Compartmental models are suited to capturing propagation phenomena occurring on homogeneously mixed networks but fail to characterize propagation phenomena occurring on highly heterogeneous networks. The compartmental SIPS models proposed in [10–13] take patch forwarding into account but leave patch injection out of consideration. Very recently, [14] proposed a compartmental SIPS model with static patch-injecting mechanism and thereby assessed the effectiveness of patch injection.

Node-level propagation models are propagation models in which each node is regarded as a separate class, with the goal of gaining insight into the evolutionary trend of the expected network state [15, 16]. One striking advantage of node-level propagation models is that they can accurately characterize propagation phenomena occurring on arbitrary networks. With the progress of wireless and mobile communication technologies, most existing computer networks admit an irregular topology [17–19]. As a result, a number of node-level computer virus propagation models have been advised [20–25]. In particular, [26] introduced a node-level SIPS model with no patch injection. Recently, [27] proposed a node-level SIPS model with dynamic patch-injecting mechanism and thereby addressed a problem that is something like the VPT problem through differential game approach. In our opinion, this work has two weaknesses: (i) It is assumed that the network defender is aware of the total attack budget of all relevant cyber malefactors. However, in practice the budget is usually unknown to the defender. (ii) It is assumed that new patches can be injected into any network node. Due to the limited network bandwidth, in practice new patches are typically injected into a small subset of nodes and then forwarded to the unpatched nodes [28].

Optimal control theory [29, 30] provides a powerful tool for studying the problem of how to contain the prevalence of computer virus in a cost-effective way [31–35]. In view of the defects of the research approach used in [27], in this paper we deal with the VPT problem through optimal control

approach. For this purpose, we propose a novel node-level SIPS model with dynamic patch-injecting mechanism, where new patches can be injected into only a small subset of nodes. Thereby, we accurately estimate the expected total loss of all network users. On this basis, we reduce the VPT problem to an optimal control problem and then solve the problem by means of optimal control theory. Our optimal control model is promising, because, by collecting and analyzing the relevant actual data, the model parameters can be estimated quite accurately.

3. The Modeling of the VPT Problem

This section is devoted to the modeling of the VPT problem. First, we introduce basic terms and notations. Second, we establish a node-level SIPS model. Finally, we model the VPT problem as an optimal control problem.

3.1. Terms and Notations. Consider a computer network with N nodes labeled v_1 through v_N . Let $G = (V, E)$ denote the topology of the network, i.e., $V = \{v_1, v_2, \dots, v_N\}$, and each edge stands for a communication link between the two endpoints. Let $\mathbf{A} = (a_{ij})_{N \times N}$ denote the adjacency matrix of G , i.e., $a_{ij} = 1$ or 0 according as $\{v_i, v_j\} \in E$ or not. Suppose new computer viruses can be injected into any node of the network and can propagate over the network, and suppose new virus patches can be injected into only the node subset $U = \{v_1, v_2, \dots, v_M\}$ of the network and can be forwarded to other nodes through the network.

Consider the finite time horizon $[0, T]$. Assume each and every node of the network is in one of three possible states: *susceptible*, *infected*, and *patched*. Susceptible nodes are nodes that are not infected with any virus but have not received the newest patch. This implies these nodes are vulnerable to new viruses. Infected nodes are nodes that are infected with some virus. Patched nodes are nodes that are not infected with any virus and have received the newest patch. This implies that these nodes possess temporary immunity to new viruses. Let $X_i(t) = 0, 1,$ and 2 denote that the node v_i is susceptible, infected, and patched at time t , respectively. Then the state of the network at time t can be characterized by the vector

$$\mathbf{X}(t) = (X_1(t), \dots, X_N(t)). \quad (1)$$

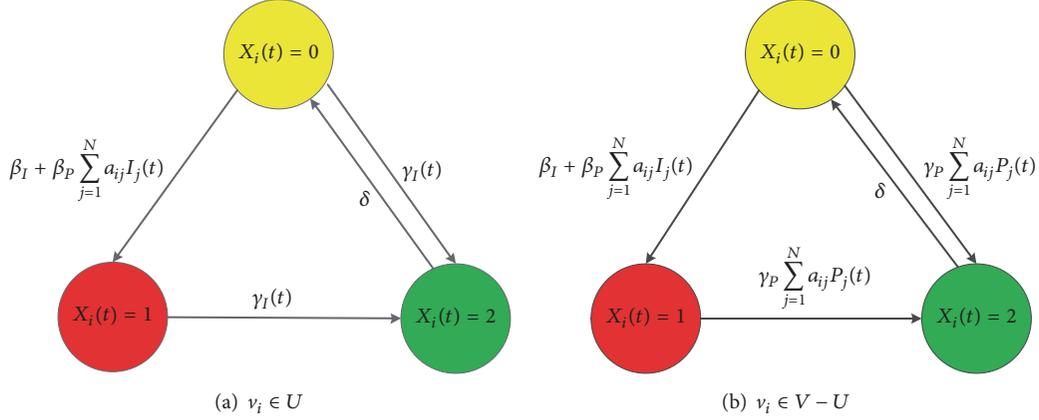
Let $S_i(t), I_i(t),$ and $P_i(t)$ denote the probabilities of the node v_i being susceptible, infected, and patched at time t , respectively.

$$\begin{aligned} S_i(t) &= \Pr \{X_i(t) = 0\}, \\ I_i(t) &= \Pr \{X_i(t) = 1\}, \\ P_i(t) &= \Pr \{X_i(t) = 2\}. \end{aligned} \quad (2)$$

Since $S_i(t) = 1 - I_i(t) - P_i(t)$, the expected state of the network at time t can be characterized by the vector

$$\mathbf{E}(t) = (I_1(t), \dots, I_N(t), P_1(t), \dots, P_N(t)). \quad (3)$$

3.2. A Virus-Patch Interactive Model. In order to establish a virus-patch interactive model, we introduce a set of assumptions as follows.

FIGURE 1: Diagram of the assumptions (A₁)-(A₅).

(A₁) Due to virus injection, each susceptible node gets infected at the average rate β_I which we refer to as the *virus injection rate*.

(A₂) Due to virus propagation, the susceptible node v_i gets infected at time t at the average rate $\beta_P \sum_{j=1}^N a_{ij} I_j(t)$, where β_P is a constant which we refer to as the *virus propagation rate*.

(A₃) Due to patch injection, each unpatched node in U gets patched at time t at the average rate $\gamma_I(t)$ which we refer to as the *patch injection rate* at time t .

(A₄) Due to patch forwarding, the unpatched node $v_i \in V - U$ gets patched at time t at the average rate $\gamma_P \sum_{j=1}^N a_{ij} P_j(t)$, where γ_P is a constant which we refer to as the *patch forwarding rate*.

(A₅) Due to appearance of new viruses, each patched node becomes susceptible at the average rate δ which we refer to as the *patch failure rate*.

Remark 1. The virus injection rate, the virus propagation rate, the patch forwarding rate, and the patch failure rate can be estimated accurately by collecting and analyzing the relevant historical data. All patch injection rates are under control of the network defender.

Figure 1 shows the above assumptions schematically.

Based on the above assumptions, the expected network state evolves over time according to the following differential dynamical system:

$$\frac{dI_i(t)}{dt} = \left[\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j(t) \right] [1 - I_i(t) - P_i(t)]$$

$$- \gamma_I(t) I_i(t), \quad 0 \leq t \leq T, \quad v_i \in U,$$

$$\frac{dP_i(t)}{dt} = \gamma_I(t) [1 - P_i(t)] - \delta P_i(t),$$

$$0 \leq t \leq T, \quad v_i \in U,$$

$$\frac{dI_i(t)}{dt} = \left[\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j(t) \right] [1 - I_i(t) - P_i(t)]$$

$$- \gamma_P I_i(t) \sum_{j=1}^N a_{ij} P_j(t),$$

$$0 \leq t \leq T, \quad v_i \in V - U,$$

$$\frac{dP_i(t)}{dt} = \gamma_P [1 - P_i(t)] \sum_{j=1}^N a_{ij} P_j(t) - \delta P_i(t),$$

$$0 \leq t \leq T, \quad v_i \in V - U,$$

$$\mathbf{E}(0) = \mathbf{E}_0.$$

(4)

This is a novel SIPS model, which can be written in matrix-vector notation as

$$\frac{d\mathbf{E}(t)}{dt} = \mathbf{F}(\mathbf{E}(t), \gamma_I(t)), \quad 0 \leq t \leq T,$$

(5)

$$\mathbf{E}(0) = \mathbf{E}_0.$$

3.3. The Modeling of the VPT Problem. The function γ_I defined by $\gamma_I(t)$, $t \in [0, T]$, is under control of the network defender. We refer to the function as a *patch-injecting strategy*. Let $L[0, T]$ denote the set of all Lebesgue integrable functions defined on the interval $[0, T]$ [36]. Henceforth, we assume the set of all allowable patch-injecting strategies is

$$\Gamma = \{ \gamma_I \in L[0, T] \mid \underline{\gamma}_I \leq \gamma_I(t) \leq \overline{\gamma}_I, \quad 0 \leq t \leq T \}. \quad (6)$$

We refer to $\underline{\gamma}_I$ as the *minimum allowable patch injection rate*, $\overline{\gamma}_I$ as the *maximum allowable patch injection rate*.

Let $C(t)$ denote the cost per unit time at time t for patch developing. Obviously, $C(t)$ is increasing with $\gamma_I(t)$. In this paper we simply assume that $C(t)$ is linearly proportional to $\gamma_I(t)$. That is, $C(t) = c\gamma_I(t)$, where c is a constant which we refer to as the *cost coefficient*. As a result, the total patch-developing cost is $\int_0^T c\gamma_I(t)dt$ units.

Remark 2. In practice, $C(t)$ may be dependent on $\gamma_I(t)$ in a more complex way. For example, $C(t)$ may be proportional to the square of $\gamma_I(t)$. That is, $C(t) = c\gamma_I^2(t)$, where c is a constant. If this is the case, the total patch-developing cost would be $\int_0^T c\gamma_I^2(t)dt$ units. The exact form in which $C(t)$ depends on $\gamma_I(t)$ is yet to be determined through analysis of massive actual data. Nevertheless, our research approach can easily be applied to any other dependence relationship.

On the other hand, we assume that the average loss per unit time caused by the infected node v_i is w_i unit. Then, the expected total loss of all network users is $\int_0^T \sum_{i=1}^N w_i I_i(t) dt$ units. Let $\mathbf{w} = (w_1, \dots, w_N)$. Therefore, we get a measure of the balance of a patch-injecting strategy γ_I as follows.

$$J(\gamma_I) = \int_0^T c\gamma_I(t) dt + \int_0^T \sum_{i=1}^N w_i I_i(t) dt. \quad (7)$$

By combining the above discussions, the VPT problem is reduced to the following optimal control problem:

$$\begin{aligned} & \text{Minimize}_{\gamma_I \in \Gamma} J(\gamma_I) = \int_0^T c\gamma_I(t) dt + \int_0^T \sum_{i=1}^N w_i I_i(t) dt \\ & \text{subject to } \frac{d\mathbf{E}(t)}{dt} = \mathbf{F}(\mathbf{E}(t), \gamma_I(t)), \quad 0 \leq t \leq T, \\ & \mathbf{E}(0) = \mathbf{E}_0. \end{aligned} \quad (8)$$

We refer to the optimal control problem as the *VPT control problem*. In this problem, each admissible control stands for a feasible patch-injecting strategy, and the objective functional measures the balance of a feasible patch-injecting strategy. Each instance of the VPT control problem is given by the 11-tuple

$$\mathcal{M} = (G \mid U, \beta_I, \beta_P, \gamma_P, \delta, \underline{\gamma}_I, \overline{\gamma}_I, c, \mathbf{w}, T, \mathbf{E}_0). \quad (9)$$

4. Theoretical Study of the VPT Control Problem

This section is dedicated to the theoretical study of the VPT control problem. First, we show that the problem is solvable. Second, we present a method for solving this problem.

4.1. Solvability. Let $L(\mathbf{E}, \gamma) = c\gamma_I + \sum_{i=1}^N w_i I_i$. We have the following lemma [30].

Lemma 3. *The VPT game problem (8) admits an optimal control if the following five conditions are met.*

- (C₁) Γ is closed and convex.
- (C₂) There is $\gamma_I \in \Gamma$ such that the differential system $d\mathbf{E}(t)/dt = \mathbf{F}(\mathbf{E}(t), \gamma_I(t))$ ($0 \leq t \leq T$) is solvable.
- (C₃) $\mathbf{F}(\mathbf{E}, \gamma_I)$ is bounded by a linear function in \mathbf{E} .
- (C₄) $L(\mathbf{E}, \gamma_I)$ is concave on Γ .
- (C₅) $L(\mathbf{E}, \gamma_I) \geq c_1 \gamma_I^\rho + c_2$ for some $\rho > 1$, $c_1 > 0$ and c_2 .

The solvability of the VPT control problem is guaranteed by the following theorem.

Theorem 4. *The VPT control problem (8) admits an optimal control.*

Proof. (a) Let γ_I be a limit point of Γ . Then there is a sequence of points in Γ , denoted $\gamma_I^{(1)}, \gamma_I^{(2)}, \dots$, that approaches γ_I . As $L[0, T]$ is complete [36], we get that $\gamma_I \in L[0, T]$. As $\underline{\gamma}_I \leq \gamma_I = \lim_{n \rightarrow \infty} \gamma_I^{(n)} \leq \overline{\gamma}_I$, we get that $\gamma_I \in \Gamma$. So, Γ is closed. (b) Let $\gamma_I^{(1)}, \gamma_I^{(2)} \in \Gamma$, $0 < \alpha < 1$. $\gamma_I = \alpha\gamma_I^{(1)} + (1 - \alpha)\gamma_I^{(2)}$. As $L[0, T]$ is a real vector space [36], we have $\gamma_I \in L[0, T]$. As $\underline{\gamma}_I \leq \gamma_I \leq \overline{\gamma}_I$, we get that $\gamma_I \in \Gamma$. So, Γ is convex. (c) As $\mathbf{F}(\mathbf{E}, \overline{\gamma}_I)$ is continuously differentiable, it follows from Continuation Theorem for Differential Systems [37] that the differential system $d\mathbf{E}(t)/dt = \mathbf{F}(\mathbf{E}(t), \overline{\gamma}_I)$ ($0 \leq t \leq T$) is solvable. (d) Obviously, for $v_i \in U$,

$$\begin{aligned} -\overline{\gamma}_I I_i & \leq \left(\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j \right) (1 - I_i - P_i) - \gamma_I I_i \\ & \leq \beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j, \\ -\delta P_i & \leq \gamma_I (1 - P_i) - \delta P_i \leq \overline{\gamma}_I - \delta P_i, \end{aligned} \quad (10)$$

for $v_i \in V - U$,

$$\begin{aligned} -\gamma_P \sum_{j=1}^N a_{ij} P_j & \leq \left(\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j \right) (1 - I_i - P_i) \\ & - \gamma_P I_i \sum_{j=1}^N a_{ij} P_j \leq \beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j, \\ -\delta P_i & \leq \gamma_P (1 - P_i) \sum_{j=1}^N a_{ij} P_j - \delta P_i \leq \gamma_P \sum_{j=1}^N a_{ij} P_j. \end{aligned} \quad (11)$$

(e) Let $\gamma_I^{(1)}, \gamma_I^{(2)} \in \Gamma$, $0 < \alpha < 1$. As

$$\begin{aligned} L(\mathbf{E}, \alpha\gamma_I^{(1)} + (1 - \alpha)\gamma_I^{(2)}) \\ = \alpha L(\mathbf{E}, \gamma_I^{(1)}) + (1 - \alpha) L(\mathbf{E}, \gamma_I^{(2)}), \end{aligned} \quad (12)$$

we get that $L(\mathbf{E}, \gamma_I)$ is convex with respect to γ_I . (f) Obviously, $L(\mathbf{E}, \gamma_I) \geq c\gamma_I \geq (c/\overline{\gamma}_I)\gamma_I^2$. Hence, the five conditions in Lemma 3 are met. By Lemma 3, the VPT control problem admits an optimal control.

This theorem implies that the VPT problem admits a best-balanced patch-injecting strategy. \square

4.2. *The Optimality System.* According to optimal control theory [29], when the solvability of an optimal control problem is guaranteed, we may solve the problem by solving the optimality system associated with the problem. Now, let us derive the optimality system associated with the VPT control problem (8). The associated Hamiltonian is

$$\begin{aligned}
H(\mathbf{E}, \gamma_I, \mathbf{p}) &= c\gamma_I + \sum_{i=1}^N w_i I_i + \sum_{i=1}^M \mu_i [\gamma_I (1 - P_i) - \delta P_i] \\
&+ \sum_{i=M+1}^N \mu_i \left[\gamma_P (1 - P_i) \sum_{j=1}^N a_{ij} P_j - \delta P_i \right] \\
&+ \sum_{i=1}^M \lambda_i \left[\left(\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j \right) (1 - I_i - P_i) - \gamma_I I_i \right] \quad (13) \\
&+ \sum_{i=M+1}^N \lambda_i \left[\left(\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j \right) (1 - I_i - P_i) \right. \\
&\left. - \gamma_P I_i \sum_{j=1}^N a_{ij} P_j \right],
\end{aligned}$$

where $\mathbf{p} = \mathbf{p}(t) = (\lambda_1(t), \dots, \lambda_N(t), \mu_1(t), \dots, \mu_N(t))$ ($0 \leq t \leq T$) is the adjoint.

The following result is a necessary condition for the optimal control of the VPT control problem.

Theorem 5. *Suppose γ_I is an optimal control for the VPT control problem (8). Let \mathbf{E} be the solution to the differential system (5). Then there exists \mathbf{p} with $\mathbf{p}(T) = \mathbf{0}$ such that*

$$\begin{aligned}
\frac{d\lambda_i(t)}{dt} &= -w_i + \lambda_i(t) \left[\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j(t) + \gamma_I(t) \right] \\
&- \beta_P \sum_{j=1}^N a_{ij} \lambda_j(t) [1 - I_j(t) - P_j(t)], \\
&0 \leq t \leq T, \quad v_i \in U,
\end{aligned}$$

$$\begin{aligned}
\frac{d\lambda_i(t)}{dt} &= -w_i + \lambda_i(t) \left[\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j(t) + \gamma_P \sum_{j=1}^N a_{ij} P_j(t) \right] \\
&- \beta_P \sum_{j=1}^N a_{ij} \lambda_j(t) [1 - I_j(t) - P_j(t)], \\
&0 \leq t \leq T, \quad v_i \in V - U,
\end{aligned}$$

$$\begin{aligned}
\frac{d\mu_i(t)}{dt} &= \mu_i(t) [\delta + \gamma_I(t)] + \lambda_i(t) \left[\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j(t) \right] \\
&+ \gamma_P \sum_{j=M+1}^N a_{ij} \{ I_j(t) \lambda_j(t) + [1 - P_j(t)] \mu_j(t) \}, \\
&0 \leq t \leq T, \quad v_i \in U,
\end{aligned}$$

$$\begin{aligned}
\frac{d\mu_i(t)}{dt} &= \mu_i(t) \left[\delta + \gamma_P \sum_{j=1}^N a_{ij} P_j(t) \right] \\
&+ \lambda_i(t) \left[\beta_I + \beta_P \sum_{j=1}^N a_{ij} I_j(t) \right] \\
&+ \gamma_P \sum_{j=M+1}^N a_{ij} \{ I_j(t) \lambda_j(t) + [1 - P_j(t)] \mu_j(t) \}, \\
&0 \leq t \leq T, \quad v_i \in V - U,
\end{aligned}$$

$$\begin{aligned}
\gamma_I(t) &= \begin{cases} \underline{\gamma}_I & \text{if } c + \sum_{i=1}^M \mu_i(t) [1 - P_i(t)] > \sum_{i=1}^M I_i(t) \lambda_i(t), \\ \overline{\gamma}_I & \text{if } c + \sum_{i=1}^M \mu_i(t) [1 - P_i(t)] < \sum_{i=1}^M I_i(t) \lambda_i(t), \end{cases} \\
&0 \leq t \leq T. \quad (14)
\end{aligned}$$

Proof. According to Pontryagin Minimum Principle [29], there exists \mathbf{p} such that

$$\begin{aligned}
\frac{d\lambda_i(t)}{dt} &= -\frac{\partial H(\mathbf{E}(t), \gamma_I(t), \mathbf{p}(t))}{\partial I_i}, \\
\frac{d\mu_i(t)}{dt} &= -\frac{\partial H(\mathbf{E}(t), \gamma_I(t), \mathbf{p}(t))}{\partial P_i}, \\
&t \in [0, T], \quad 1 \leq i \leq N.
\end{aligned} \quad (15)$$

Thus, the first $2N$ equations in the system (14) follow by direct calculations. As the terminal cost is unspecified and the final state is free, the transversality condition $\mathbf{p}(T) = \mathbf{0}$ holds true. Again by Pontryagin Minimum Principle, we have

$$\gamma_I(t) \in \arg \min_{\gamma_I^* \in \Gamma} H(\mathbf{E}(t), \gamma_I^*(t), \mathbf{p}(t)), \quad 0 \leq t \leq T. \quad (16)$$

The last equation in the system (14) follows by direct calculations.

The optimality system associated with the VPT control problem (8) consists of the system (5), the system (14), and

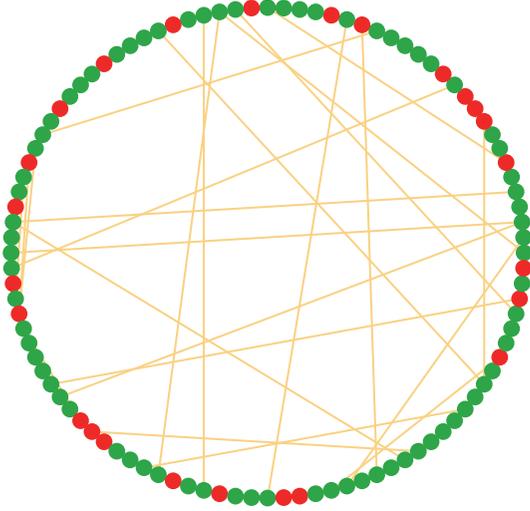


FIGURE 2: A synthetic small-world network G_{SW} , where U_{SW} consists of the red nodes.

$\mathbf{p}(T) = \mathbf{0}$. In practice, we may apply the well-known Forward-Backward Euler Scheme [38] to solve the optimality system. \square

5. Examples of Best-Balanced Patch-Injecting Strategy

In this section, we present a few best-balanced patch-injecting strategies by solving the corresponding instances of the VPT control problem. For comparative purpose, for the VPT control problem (8) and the admissible control γ_I , we define the cumulative balance function as

$$J(\gamma_I, t) = \int_0^t c\gamma_I(s) ds + \int_0^t \sum_{i=1}^N w_i I_i(s) ds, \quad 0 \leq t \leq T. \quad (17)$$

Obviously, $J(\gamma_I, T) = J(\gamma_I)$. For convenience, let $\mathbf{1}$ denote an all-one row vector with appropriate number of dimensions.

Small-world networks are networks with small diameter and high clustering coefficient [39]. By invoking Pajek [40], the well-known social network analysis software, we get a synthetic small-world network G_{SW} , which is plotted in Figure 2, where the patch injection subset U_{SW} consists of the red nodes.

Example 1. Consider the following instance of the VPT control problem:

$$(G_{SW} \mid U_{SW}, 0.1, 0.4, 0.4, 0.1, 0.2, 0.8, 1, \mathbf{1}, 20, 0.1 \times \mathbf{1}). \quad (18)$$

By solving the corresponding optimality system, we get an optimal control, which is depicted in Figure 3(a). Figure 3(b) plots the cumulative balance functions for the optimal control and three static controls, from which it is seen that the optimal control is superior to these static controls in terms of the balance.

Scale-free networks are networks with power-law degree distribution [41]. Again by invoking Pajek, we get a synthetic

scale-free network G_{SF} , which is portrayed in Figure 4, where the patch injection subset U_{SF} consists of the red nodes.

Example 2. Consider the following instance of the VPT control problem:

$$(G_{SF} \mid U_{SF}, 0.1, 0.4, 0.4, 0.1, 0.2, 0.8, 1, \mathbf{1}, 20, 0.1 \times \mathbf{1}). \quad (19)$$

By solving the corresponding optimality system, we get an optimal control, which is exhibited in Figure 5(a). Figure 5(b) plots the cumulative balance functions for the optimal control and three static controls, from which it is seen that the optimal control outperforms these static controls in terms of the balance.

Figure 6 exhibits a real-world email network G_{EM} , which comes from [42]. Here, the patch injection subset U_{EM} consists of the red nodes.

Example 3. Consider the following instance of the VPT control problem:

$$(G_{EM} \mid U_{EM}, 0.1, 0.4, 0.4, 0.1, 0.2, 0.8, 1, \mathbf{1}, 20, 0.1 \times \mathbf{1}). \quad (20)$$

By solving the corresponding optimality system, we get an optimal control, which is shown in Figure 7(a). Figure 7(b) plots the cumulative balance functions for the optimal control and three static controls, from which it is seen that the optimal control overmatches these static controls in terms of the balance.

We conclude from the above examples that a best-balanced patch-injecting strategy first stays at the maximum allowable patch injection rate, then sharply jumps to the minimum allowable patch injection rate, and finally stays at this rate.

6. Further Discussions

In this section, we examine the effects of some factors on the best balance of a patch-injecting strategy. For convenience, let γ_I^{opt} denote a best-balanced patch-injecting strategy, $J^{opt} = J(\gamma_I^{opt})$ the corresponding balance.

6.1. The Effects of the Four Rates. First, we inspect the effect of the four rates, β_I , β_P , γ_P , and δ , on the best balance.

Experiment 6. Consider the following instances of the VPT control problem:

$$(G \mid U, \beta_I, 0.4, 0.4, 0.1, 0.2, 0.8, 1, \mathbf{1}, 20, 0.1 \times \mathbf{1}), \quad (21)$$

where $G \mid U \in \{G_{SW} \mid U_{SW}, G_{SF} \mid U_{SF}, G_{EM} \mid U_{EM}\}$, $\beta_I \in \{0.1, 0.2, \dots, 0.9\}$. Figure 8 exhibits the best balances of these instances.

It is concluded from this experiment that J^{opt} is increasing with β_I . As a result, the best balance can be improved by persuading the network users not to install suspicious software.

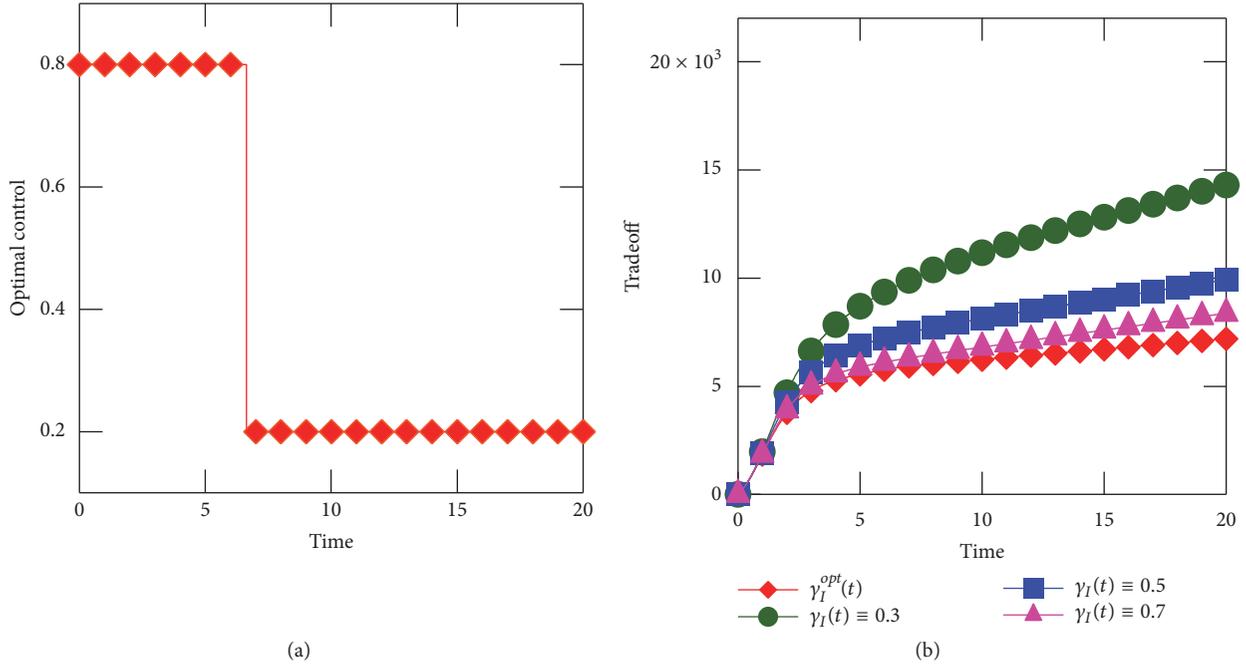


FIGURE 3: Results in Example 1: (a) an optimal control; (b) a comparison between the optimal control and three static controls.

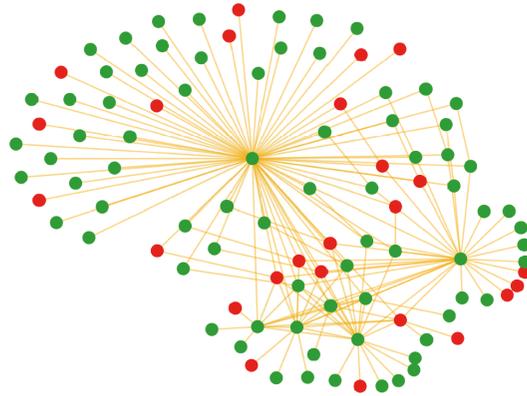


FIGURE 4: A synthetic scale-free network G_{SF} , where U_{SF} consists of the red nodes.

Experiment 7. Consider the following instances of the VPT control problem:

$$(G \mid U, 0.1, \beta_p, 0.4, 0.1, 0.2, 0.8, \mathbf{1}, \mathbf{1}, 20, 0.1 \times \mathbf{1}), \quad (22)$$

where $G \mid U \in \{G_{SW} \mid U_{SW}, G_{SF} \mid U_{SF}, G_{EM} \mid U_{EM}\}$, $\beta_p \in \{0.1, 0.2, \dots, 0.9\}$. Figure 9 displays the best balances of these instances.

It is concluded from this experiment that J^{opt} is increasing with β_p . Again, this conclusion demonstrates that warning the network users not to install suspicious software would improve the best balance.

Experiment 8. Consider the following instances of the VPT control problem:

$$(G \mid U, 0.1, 0.4, \gamma_p, 0.1, 0.2, 0.8, \mathbf{1}, \mathbf{1}, 20, 0.1 \times \mathbf{1}), \quad (23)$$

where $G \mid U \in \{G_{SW} \mid U_{SW}, G_{SF} \mid U_{SF}, G_{EM} \mid U_{EM}\}$, $\gamma_p \in \{0.1, 0.2, \dots, 0.9\}$. Figure 10 exhibits the best balances of these instances.

It is concluded from this experiment that J^{opt} is decreasing with γ_p . Therefore, the best balance can be improved by reminding the network users of timely installing new patches.

Experiment 9. Consider the following instances of the VPT control problem:

$$(G \mid U, 0.1, 0.4, 0.4, \delta, 0.2, 0.8, \mathbf{1}, \mathbf{1}, 20, 0.1 \times \mathbf{1}), \quad (24)$$

where $G \mid U \in \{G_{SW} \mid U_{SW}, G_{SF} \mid U_{SF}, G_{EM} \mid U_{EM}\}$, $\delta \in \{0.1, 0.2, \dots, 0.9\}$. Figure 11 exhibits the best balances of these instances.

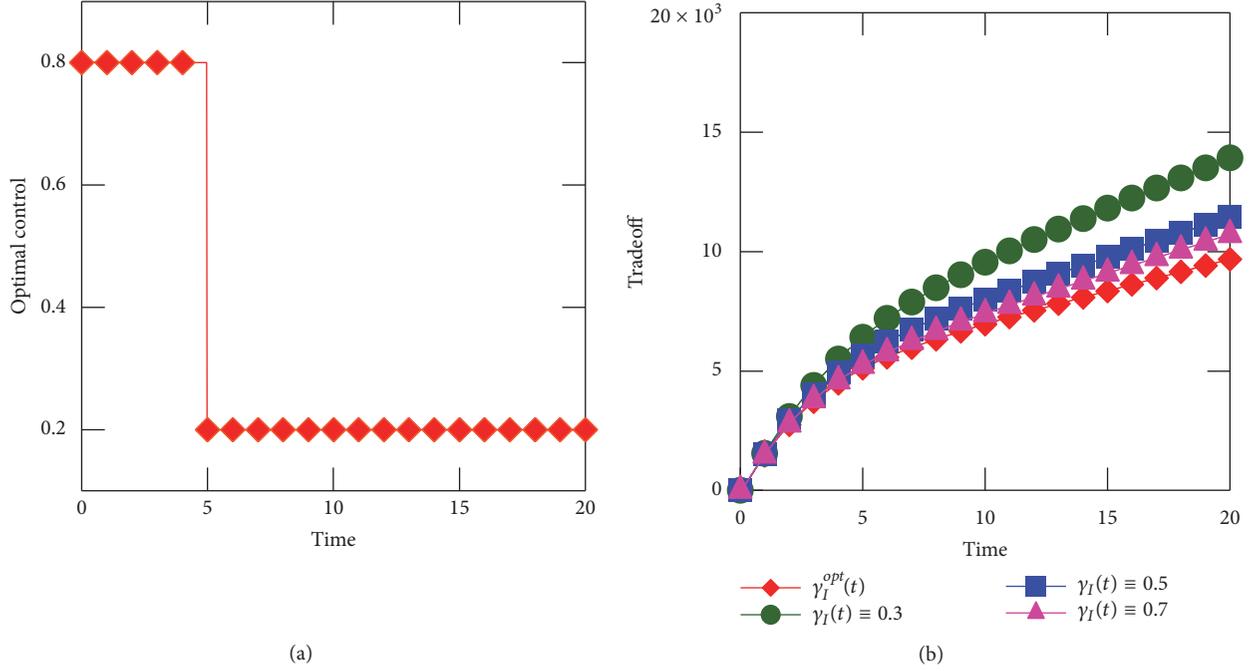


FIGURE 5: Results in Example 2: (a) an optimal control; (b) a comparison between the optimal control and three static controls.

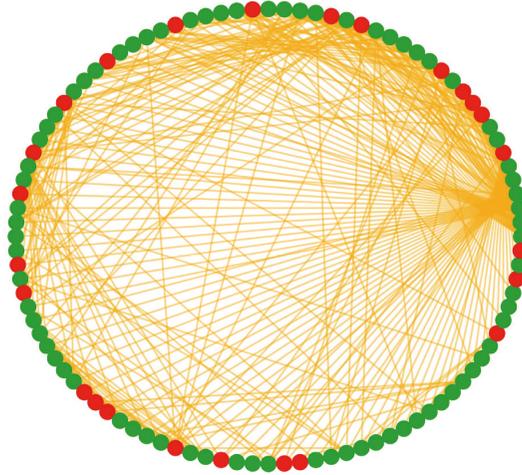


FIGURE 6: An email network G_{EM} , where U_{EM} consists of the red nodes.

It is concluded from this experiment that J^{opt} is increasing with δ . It follows that the best balance can be improved by developing patches that can defend against future viruses.

6.2. The Effects of the Two Bounds. Second, let us investigate the effects of the minimum allowable patch injection rate and the maximum allowable patch injection rate on the best balance.

Experiment 10. Consider the following instances of the VPT control problem:

$$(G | U, \beta_I, 0.1, 0.4, 0.4, 0.1, \underline{\gamma}_I, \overline{\gamma}_I, 1, \mathbf{1}, 20, 0.1 \times \mathbf{1}), \quad (25)$$

where $G | U \in \{G_{SW} | U_{SW}, G_{SF} | U_{SF}, G_{EM} | U_{EM}\}$, $\underline{\gamma}_I, \overline{\gamma}_I \in \{0.1, 0.2, \dots, 0.9\}$. Figure 12 exhibits the best balances of these instances.

It is concluded from this experiment that J^{opt} is increasing with $\underline{\gamma}_I$ and is decreasing with $\overline{\gamma}_I$. In practice, we should reduce the lowest allowable patch injection rate and enhance the highest allowable patch injection rate to achieve a better balance.

7. Concluding Remarks

Virus patches play an important role in restraining computer viruses. This paper has addressed the problem of seeking patch-injecting strategies that achieve the best balance

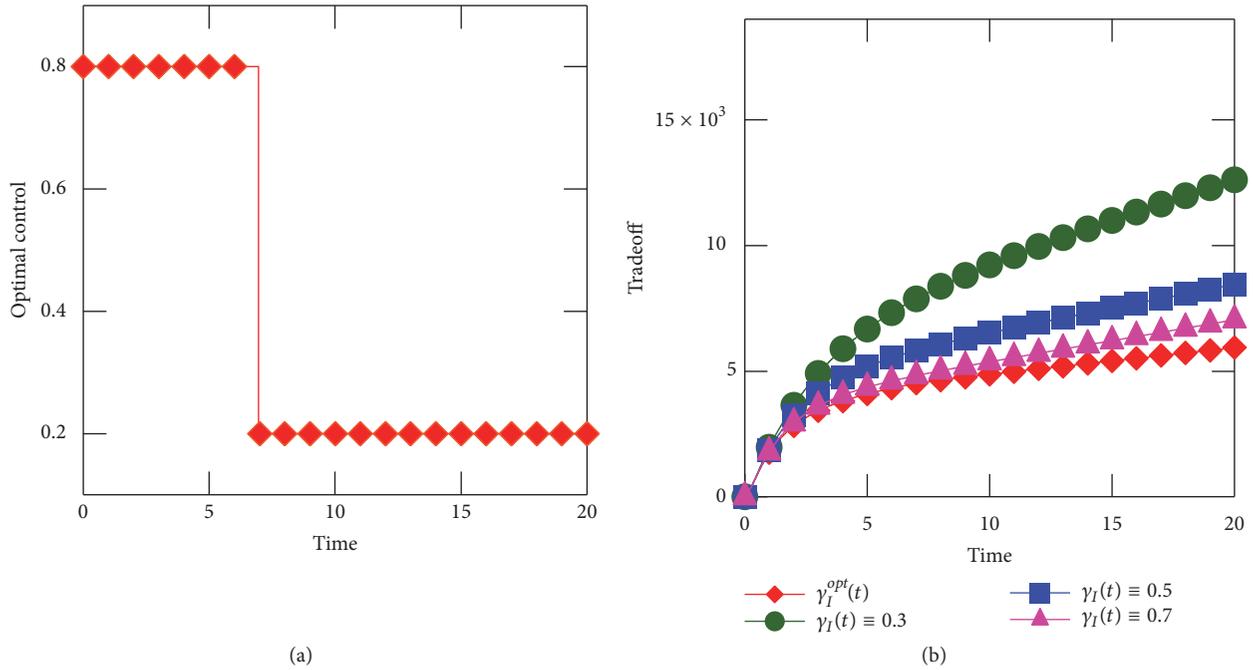


FIGURE 7: Results in Example 3: (a) an optimal control; (b) a comparison between the optimal control and three static controls.

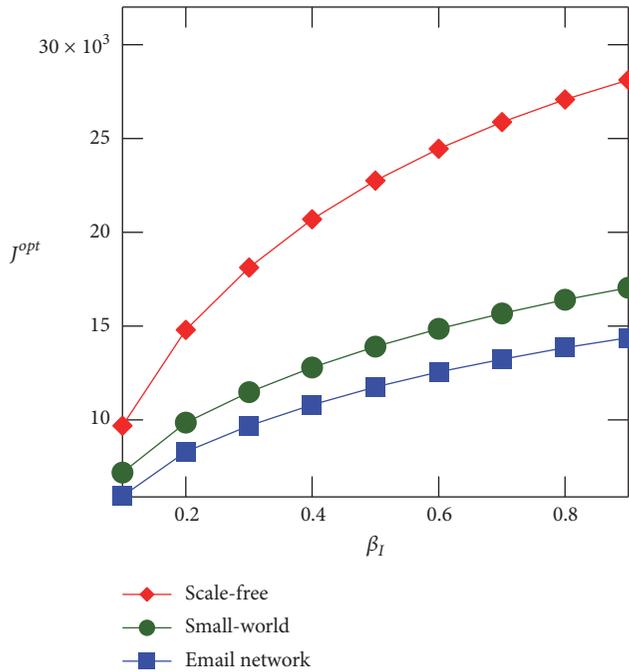


FIGURE 8: The best balances in Experiment 6.

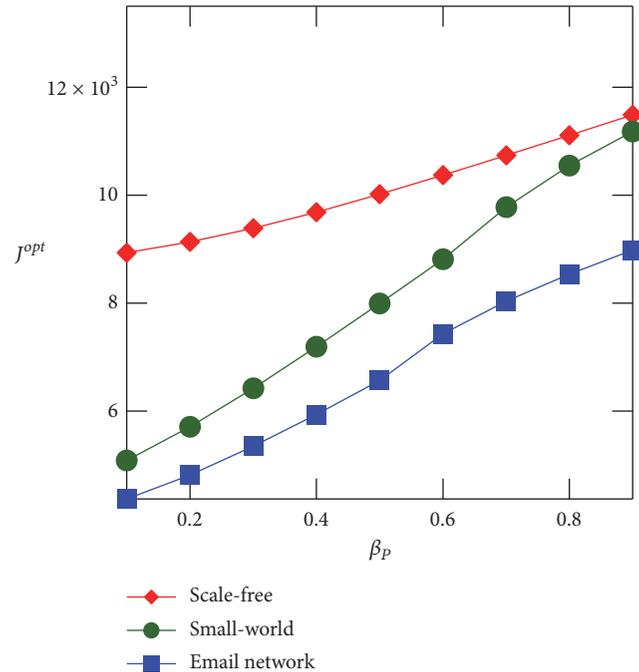


FIGURE 9: The best balances in Experiment 7.

between the patch-developing cost and the impact of virus. The problem has been reduced to an optimal control problem, and a scheme for solving the optimal control problem has been presented. Finally, the effects of some factors on the best balance of a patch-injecting strategy have been examined.

Some relevant problems are yet to be resolved. First, the problem of how to select a given number of patch injection nodes so that the balance is optimized is worth study. Second, in this article it is assumed that the patch propagation rate is fixed. In practice, the network defender may change this rate flexibly through rewriting the communication protocol.

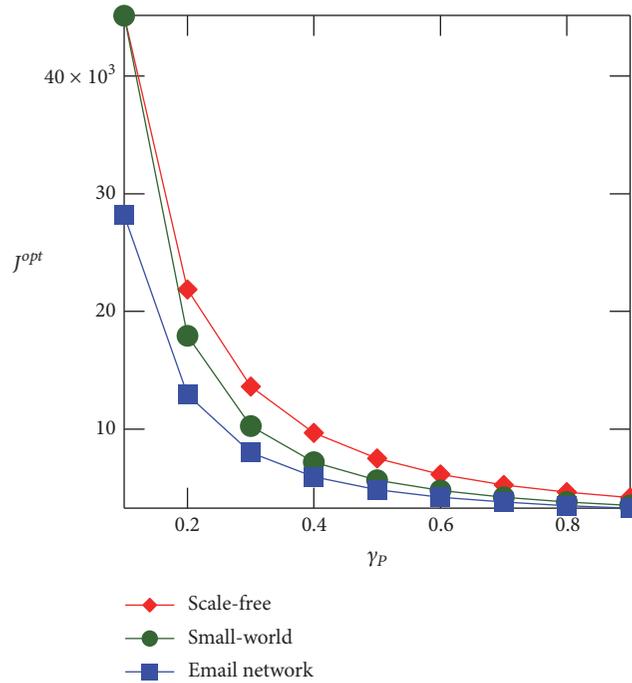


FIGURE 10: The best balances in Experiment 8.

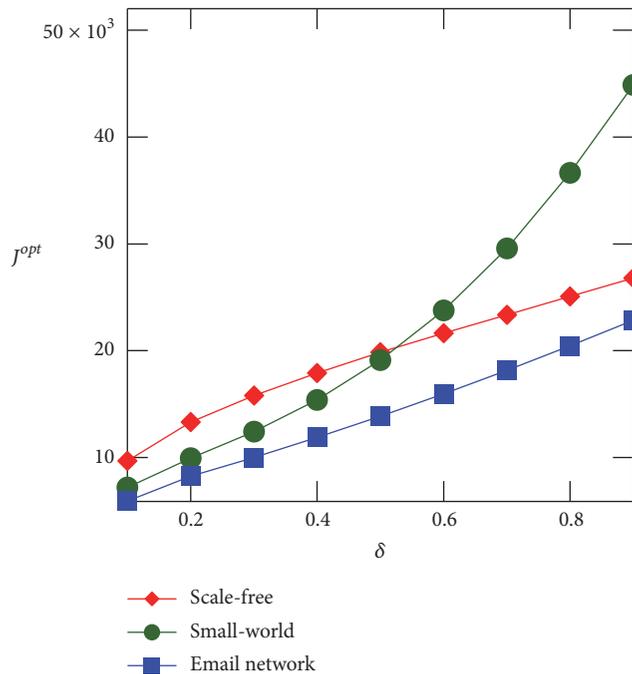


FIGURE 11: The best balances in Experiment 9.

In this situation, we will face a new and more complex balance problem. Next, in this article the virus injection rate is assumed to be fixed. In reality, the virus maker may flexibly change the rate to avoid detection. In this context, it is appropriate to deal with the balance problem through game-theoretic approach [43–46]. Finally, the research approach used in this article may be applied to some other areas

such as cloud security [47, 48] and Internet of Things security [49].

Data Availability

The data used to support the findings of this study are included within the article.

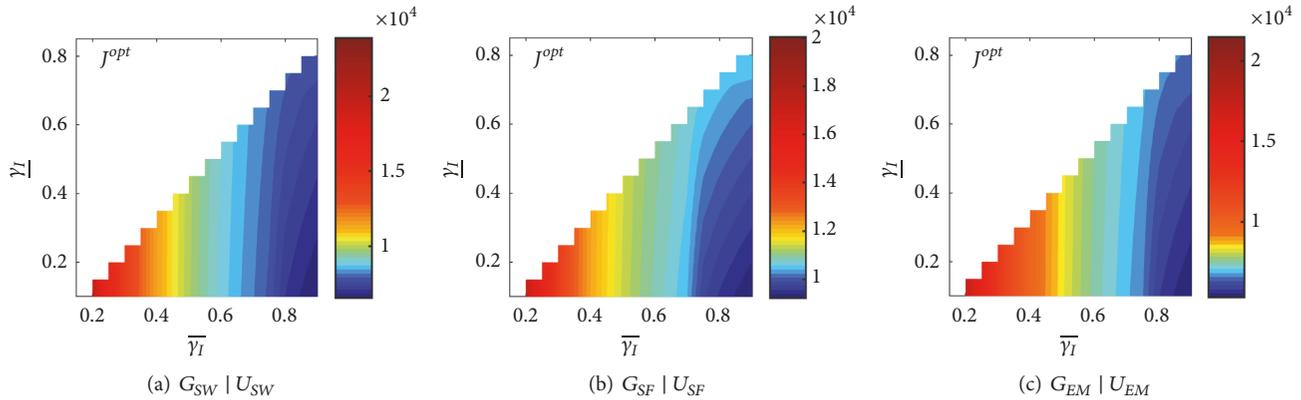


FIGURE 12: The best balances in Experiment 10.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by National Natural Science Foundation of China (Grant No. 61572006), Chongqing Basic Research and Front Exploration Project (Grant No. cstc2018jcyjA3093), and Australian Research Council (Grant No. LP170100458).

References

- [1] T. J. OLeary and L. I. OLeary, "Computing essentials 2014 complete edition, making it work for you," in *Computing Essentials 2014 Complete Edition, Making it Work for You*, McGraw-Hill Education, 2014.
- [2] D. Comer, *Computer Networks and Internets*, Pearson, 6th edition, 2014.
- [3] S. Mohurle and M. Patil, "A brief study of wannacry threat: ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938–1940, 2017.
- [4] P. Szor, *The Art of Computer Virus Research and Defense*, Addison-Wesley Education, 2005.
- [5] J. Freund and J. Jones, *Measuring and Managing Information Risk: A Fair Approach*, Butterworth-Heinemann, 1st edition, 2014.
- [6] D. W. Hubbard and R. Seiersen, *How to Measure Anything in Cybersecurity Risk*, John Wiley & Sons, Inc., Hoboken, NJ, USA, 1st edition, 2016.
- [7] L. C. Chen and K. M. Carley, "The impact of countermeasure propagation on the prevalence of computer viruses," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 34, no. 2, pp. 823–833, 2004.
- [8] J. Goldenberg, Y. Shavitt, E. Shir, and S. Solomon, "Distributive immunization of networks against viruses using the "honeypot" architecture," *Nature Physics*, vol. 1, no. 3, pp. 184–188, 2005.
- [9] N. F. Britton, *Essential Mathematical Biology*, Springer Undergraduate Mathematics Series, Springer, 2003.
- [10] L.-X. Yang and X. Yang, "The effect of infected external computers on the spread of viruses: a compartment modeling study," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 24, pp. 6523–6535, 2013.
- [11] A. K. Misra, M. Verma, and A. Sharma, "Capturing the interplay between malware and anti-malware in a computer network," *Applied Mathematics and Computation*, vol. 229, pp. 340–349, 2014.
- [12] L.-X. Yang and X. Yang, "A novel virus-patch dynamic model," *PLoS ONE*, vol. 10, no. 9, Article ID e0137858, 2015.
- [13] B. Liu and C. Li, "A new virus-antivirus spreading model," in *Proceedings of International Symposium on Neural Networks (ISNN2015)*, pp. 481–488, Springer, 2015.
- [14] D.-W. Huang, L.-X. Yang, X. Yang, Y. Wu, and Y. Y. Tang, "Towards understanding the effectiveness of patch injection," *Physica A: Statistical Mechanics and its Applications*, vol. 526, p. 120956, 2019.
- [15] P. Van Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 1–14, 2009.
- [16] P. Van Mieghem, "The N-intertwined SIS epidemic network model," *Computing*, vol. 93, no. 2, pp. 147–169, 2011.
- [17] I. Stojmenovic, *Handbook of Wireless Networks and Mobile Computing*, John Wiley & Sons, 2002.
- [18] A. Boukerche, *Handbook of Algorithms for Wireless Networking and Mobile Computing*, Taylor & Francis, 2006.
- [19] J. Rodriguez, *Fundamentals of 5G Mobile Networks*, John Wiley & Sons, 2015.
- [20] S. Xu, W. Lu, and Z. Zhan, "A stochastic model of multivirus dynamics," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 30–45, 2012.
- [21] S. Xu, W. Lu, and L. Xu, "Push- and pull-based epidemic spreading in networks: thresholds and deeper insights," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 7, no. 32, 2012.
- [22] S. Xu, W. Lu, L. Xu, and Z. Zhan, "Adaptive epidemic dynamics in networks: Thresholds and control," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 8, no. 4, article no. 19, 2014.
- [23] L.-X. Yang, M. Draief, and X. Yang, "The impact of the network topology on the viral prevalence: a node-based approach," *PLoS ONE*, vol. 10, no. 7, article e0134507, 2015.
- [24] L. X. Yang, M. Draief, and X. Yang, "Heterogeneous virus propagation in networks: a theoretical study," *Mathematical Methods in the Applied Sciences*, vol. 40, pp. 1396–1413, 2016.

- [25] L.-X. Yang, X. Yang, and Y. Yan Tang, "A bi-virus competing spreading model with generic infection rates," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 1, pp. 2–13, 2017.
- [26] L.-X. Yang, X. Yang, and Y. Wu, "The impact of patch forwarding on the prevalence of computer virus: a theoretical assessment approach," *Applied Mathematical Modelling*, vol. 43, pp. 110–125, 2017.
- [27] L. Yang, P. Li, X. Yang, Y. Xiang, and W. Zhou, "A differential game approach to patch injection," *IEEE Access*, vol. 6, pp. 58924–58938, 2018.
- [28] J. Balthrop, S. Forrest, M. E. J. Newman, and M. M. Williamson, "Technological networks and the spread of computer viruses," *Computer Science*, vol. 304, no. 5670, pp. 527–529, 2004.
- [29] E. K. Donald, *Optimal Control Theory: An Introduction*, Dover Publications, 2012.
- [30] D. Liberzon, *Calculus of Variations and Optimal Control Theory: A Concise Introduction*, Princeton University Press, Princeton, NJ, USA, 2012.
- [31] L. Chen, K. Hattaf, and J. T. Sun, "Optimal control of a delayed SLBS computer virus model," *Physica A: Statistical Mechanics and its Applications*, vol. 427, pp. 244–250, 2015.
- [32] L.-X. Yang, M. Draief, and X. Yang, "The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model," *Physica A: Statistical Mechanics and its Applications*, vol. 450, pp. 403–415, 2016.
- [33] Y. Pei, H. Pei, X. Liang, and M. Zhu, "Optimal control of a computer virus model with network attacks," *Communications in Mathematical Biology and Neuroscience*, vol. 2016, Article ID 17, 2016.
- [34] T. Zhang, L.-X. Yang, X. Yang, Y. Wu, and Y. Y. Tang, "Dynamic malware containment under an epidemic model with alert," *Physica A: Statistical Mechanics and its Applications*, vol. 470, pp. 249–260, 2017.
- [35] J. Bi, X. Yang, Y. Wu, Q. Xiong, J. Wen, and Y. Y. Tang, "On the optimal dynamic control strategy of disruptive computer virus," *Discrete Dynamics in Nature and Society*, vol. 2017, Article ID 8390784, 2017.
- [36] E. M. Stein and R. Shakarchi, *Real Analysis: Measure Theory, Integration, Hilbert Spaces*, Princeton University Press, Princeton, NJ, Texas, 2005.
- [37] R. C. Robinson, *An Introduction to Dynamical Systems: Continuous and Discrete*, Prentice Hall, New York, NY, USA, 2004.
- [38] K. E. Atkinson, W. Han, and D. Stewart, *Numerical Solution of Ordinary Differential Equations*, John Wiley & Sons, 2009.
- [39] D. J. Watts and S. H. Strogatz, "Collective dynamics of "small-world" networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.
- [40] W. de Nooy, A. Mrvar, and V. Batagelj, *Exploratory Social Network Analysis with Pajek*, Cambridge University Press, Cambridge, UK, 2005.
- [41] A. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.
- [42] <http://konekt.uni-koblenz.de/networks/arenas-email>.
- [43] M. J. Osborne, *An Introduction to Game Theory*, Oxford University Press, 2003.
- [44] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*, Cambridge University Press, Cambridge, UK, 2010.
- [45] L. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou, "Effective repair strategy against advanced persistent threat: a differential game approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1713–1728, 2019.
- [46] L. Yang, P. Li, X. Yang, and Y. Tang, "A risk management approach to defending against the advanced persistent threat," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2018.
- [47] M. A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11–29, 2016.
- [48] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.
- [49] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: a survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

