Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/mbe

MBE, 20(8): 14502–14517.
DOI: 10.3934/mbe.2023649
Received: 31 March 2023
Revised: 25 May 2023
Accepted: 06 June 2023
Published: 04 July 2023

Research article

Optimal control analysis of malware propagation in cloud environments

Liang Tian[1,2], **Fengjun Shang**[1,2] **and Chenquan Gan**[3,*]

[1] School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

[2] Key Lab of Computer Network and Communication Technology, Chongqing Education Commission, Chongqing, China

[3] School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

* **Correspondence:** Email: gcq2010cqu@163.com.

Abstract: Cloud computing has become a widespread technology that delivers a broad range of services across various industries globally. One of the crucial features of cloud infrastructure is virtual machine (VM) migration, which plays a pivotal role in resource allocation flexibility and reducing energy consumption, but it also provides convenience for the fast propagation of malware. To tackle the challenge of curtailing the proliferation of malware in the cloud, this paper proposes an effective strategy based on optimal dynamic immunization using a controlled dynamical model. The objective of the research is to identify the most efficient way of dynamically immunizing the cloud to minimize the spread of malware. To achieve this, we define the control strategy and loss and give the corresponding optimal control problem. The optimal control analysis of the controlled dynamical model is examined theoretically and experimentally. Finally, the theoretical and experimental results both demonstrate that the optimal strategy can minimize the incidence of infections at a reasonable loss.

Keywords: cloud environment; virtual machine; malware; propagation model; optimal control

1. Introduction

Cloud computing has revolutionized the IT industry, bringing benefits such as flexibility, scalability and cost-effectiveness. Virtualization is a crucial technique in cloud computing, enabling the transcendence of temporal and spatial boundaries. By dividing a physical computing resource into multiple same-function virtual machines (VMs), this technique enables the on-demand deployment of computing resources by VM migration [1]. Regrettably, virtualization has introduced new hidden dangers that are increasingly targeted by malware attacks [2]. These vulnerabilities can lead to

significant harm to individuals and organizations, in addition to financial losses, and even pose a potential threat to human life [3]. Therefore, it is crucial to explore effective measures for safeguarding virtual environments against malware attacks in the cloud.

With the rapid development of cloud computing, the problem of malware propagation in cloud environments has become increasingly prominent [4]. Malware in cloud environments usually has the characteristics of large scale, fast propagation speed and being difficult to trace and control. To this end, researchers have proposed many related works for controlling the propagation of malware in cloud environments. These works mainly include malware detection, malware propagation path analysis and malware propagation control.

Malware detection is a crucial technology for controlling the spread of malware in cloud environments. Currently, researchers used feature-based and machine learning-based methods to detect malware [5]. By analyzing the code and behavior characteristics of malware, researchers can effectively detect it [6]. Malware propagation path analysis is another important aspect for understanding the propagation mechanism and rules of malware in cloud environments. Researchers mainly used graph theory-based and data mining-based methods to analyze the propagation path and rules by constructing a malware propagation graph [7–9]. Additionally, malware propagation control is a key technology for controlling the spread of malware in cloud environments. Researchers mainly used network security protocol-based methods for malware propagation control [10]. However, these methods can only play their maximum role after the emergence of malware, with significant lag in development and inability to predict malware propagation in cloud environments.

Noting the attractive analogies between malware and its biological counterparts, some epidemic dynamics of malware, which are devoted to capturing the way that malware spreads over a network so as to contain its diffusion, have been proposed, such as the SEIQR model [11], the SIR_1R_2 model [12], the SE_1E_2IQR model [13], the SIWQ model [14], the SIAR model [15, 16], the SID model [17], the DDSEIR model [18], the SEIR model [19], the SEIRS-V model [20], the SEIRS-Q model [21], the SEIS model [22], the VCQPS model [23], the game model [24–27] and the multi-agent model [28]. However, these models are not specifically designed for cloud environments. On this basis, Abazari et al. [29] explored the effect of anti-malware with infectious nodes in cloud environments and proposed an SPI (susceptible-protected-infected) model, but they assumed that all the machines entering the cloud are susceptible, which does not fit the practical situations. In order to make up for the deficiency and based on the SPI model, a new dynamical model, the susceptible-infected-protected-susceptible (SIPS) model was proposed in [30], but this model cannot describe the cost and effectiveness of malware control.

In reality, it is necessary to consider the input cost and corresponding effects of malware control, and it is impossible to install anti-virus-software-like protection measures for every machine, though every machine must have the same level of protection. Therefore, in this paper, inspired by the above work and discussions, we propose a controlled dynamical model to explore how to effectively contain malware propagation in the cloud by means of optimal dynamic immunization. According to the control strategy and loss definition, we give the optimal control problem of the controlled dynamical model. The optimal analysis is examined theoretically and experimentally. Most importantly, the obtained results indicate the comprehensive effect of the optimal control strategy is the best.

The remaining material of our work is organized as follows: The preliminary knowledge is given in Section 2. Section 3 formulates the controlled dynamical model. The optimal control problem and

theoretical analysis are presented in Section 4. Section 5 gives the experimental analysis. Section 6 summarizes this work.

2. Preliminary knowledge

This section introduces several important lemmas, which are important support for subsequent research work.

Consider the following controlled differential dynamical system

$$\frac{d\mathbf{x}}{dt} = \mathbf{f}(\mathbf{x}, \mathbf{g}), \quad t \in [t_0, t_f], \mathbf{x}(t_0) = \mathbf{x}_0, \mathbf{g} \in \mathscr{G}, \tag{2.1}$$

where t_0 is the initial time, t_f is the terminal time, $\mathbf{x}$ is the system state vector, $\mathbf{x}_0$ is the state at the initial time of the system, $\mathbf{g}$ is the control vector, and $\mathscr{G}$ is the admissible control set.

Given the objective functional $J(\mathbf{g}) = \int_{t_0}^{t_f} L(\mathbf{x}, \mathbf{g})dt$, the optimal control problem of the controlled differential dynamical system (2.1) can be denoted as:

$$\begin{aligned} &\min_{\mathbf{g}\in\mathscr{G}} J(\mathbf{g}) = \int_{t_0}^{t_f} L(\mathbf{x}, \mathbf{g})dt \\ &s.t. \quad \tfrac{d\mathbf{x}}{dt} = \mathbf{f}(\mathbf{x}, \mathbf{g}), \quad t \in [t_0, t_f], \mathbf{x}_0 \in \Psi, \mathbf{g} \in \mathscr{G}, \end{aligned} \tag{2.2}$$

where Ψ is a positive invariant for the system (2.1).

Now, let us introduce the following lemmas, which can be used to prove the solution existence and the optimality system.

Lemma 1. *[31] Consider the optimal control problem* (2.2)*. Then it has optimal control when these six conditions are met.*

(i) *There is* $\mathbf{g} \in \mathscr{G}$ *such that system (2.1) is solvable,*
(ii) $\mathscr{G}$ *is convex,*
(iii) $\mathscr{G}$ *is closed,*
(iv) $\mathbf{f}(\mathbf{x}, \mathbf{g})$ *is bounded by a linear function in* $\mathbf{x}$*,*
(v) $L(\mathbf{x}, \mathbf{g})$ *is convex on* $\mathscr{G}$*, and*
(vi) $L(\mathbf{x}, \mathbf{g}) \geq c_1\|\mathbf{g}\|_2^{\rho} + c_2$ *for some* $\rho > 1$*,* $c_1 > 0$ *and* c_2*.*

Lemma 2. *[31] Suppose that* $\mathbf{g} \in \mathscr{G}$ *is an optimal control of the optimal control problem* (2.2)*,* $\mathbf{x}$ *is a solution of the controlled differential dynamical system* (2.1)*. Then there is* $\mathbf{\Phi}$ *so that*

$$\begin{aligned} &\tfrac{d\mathbf{\Phi}}{dt} = -\nabla_{\mathbf{x}} H(\mathbf{x}, \mathbf{g}, \mathbf{\Phi}), \mathbf{\Phi}(t_f) = \mathbf{0}, \\ &\mathbf{g} = \arg\min_{\tilde{\mathbf{u}}\in\mathscr{G}} H(\mathbf{x}, \tilde{\mathbf{u}}, \mathbf{\Phi}), \end{aligned} \tag{2.3}$$

where $H(\mathbf{x}, \mathbf{g}, \mathbf{\Phi}) = L(\mathbf{x}, \mathbf{g}) + \mathbf{\Phi}^T\mathbf{f}(\mathbf{x}, \mathbf{g})$ *is the Hamilton function of the optimal control problem* (2.2)*.*

The system composed of (2.1) and (2.3) is the "optimality system" of the optimal control problem (2.2). According to this system, we can get some candidate solutions of (2.2). This can narrow the search scope of the optimal solution, thereby accelerating the search effect.

3. The controlled malware propagation model

This section mainly introduces the background and corresponding mathematical model of malware propagation control in cloud environments.

3.1. Background

With the rapid growth of cloud computing in recent years, security concerns surrounding cloud systems have become increasingly important. One of the most significant threats in cloud environments is the propagation of malware, which can be transmitted from one device to another, causing significant damage, data loss, and system downtime. To effectively mitigate the risk of malware propagation in cloud environments, the most effective and direct method is to develop corresponding antivirus software or patches to detect and kill malware. However, with the continuous development of technology, malware has become increasingly high-end and covert, and antivirus software or patches often lag behind the emergence of malware, making it difficult to predict the long-term evolution trend of malware. Therefore, inspired by biological infectious disease models, establishing a malware propagation model is a relatively effective attempt. However, currently available malware propagation models are generally copied from biological infectious disease models and do not take into account the unique conditions of the cloud environment, such as the cost and benefit of actual resource consumption when detecting and killing malware. It is necessary to develop optimized control strategies that can monitor and control the spread of malware [32]. Optimal control is a mathematical optimization technique that seeks to identify the optimal control inputs that can be applied to a system over time. By leveraging this mathematical technique, researchers can find solutions to monitor and control malware in the cloud environment, improving the security and reliability of cloud computing systems.

3.2. Model formulation

To solve the problem of malware propagation between virtual machines and study the key factors affecting the network propagation of malware, a dynamical propagation model was proposed in [30], whose mathematical expression is represented as:

$$\begin{cases} \dfrac{dS(t)}{dt} = \eta_1 + \delta I(t) + \alpha_0 P(t) - \beta\gamma S(t) I(t) - \alpha S(t) - \mu S(t), \\ \dfrac{dI(t)}{dt} = \eta_2 + \beta\gamma S(t) I(t) - \delta I(t) - \mu I(t), \\ \dfrac{dP(t)}{dt} = \eta_3 + \alpha S(t) - \alpha_0 P(t) - \mu P(t), \end{cases} \tag{3.1}$$

where η_1, η_2, and η_3 are the entering rate of infected, susceptible, and protected VMs, respectively; μ and γ are the shutdown rate and the migration rate of each VM, respectively; α and α_0 are the installing rate and the expired rate of antivirus software, respectively; β and δ are the infected rate and the reinstalling system rate, respectively; At time t, $S(t), I(t)$, and $P(t)$ are the proportions of susceptible, infected, and protected VMs, respectively.

Obviously, this dynamical propagation model of malware does not consider dynamic control factors such as immunity. In the real world, immunizations (including treatment and vaccination) are dynamic,

and several security controls can be implemented to protect computer systems from malware infections. These include antivirus software, firewalls, intrusion detection systems (IDS), security updates and patches, and user awareness training. To increase the reality of the developed model, let us take an example of the WannaCry ransomware attack that affected thousands of computers worldwide. This attack exploited a vulnerability in Microsoft Windows operating systems that had been previously patched. Organizations that had not applied the security update were vulnerable to this attack. To prevent such attacks, organizations should ensure that they regularly update their systems with the latest security patches. They should also implement a layered approach to security that includes antivirus software, firewalls, and IDS systems to provide comprehensive protection against malware infections. The scale of malware spread through the network can be controlled by changing the control strategy. To this end, we define two functions (vaccination function and treatment function) with respect to time t, $\alpha(t)$ and $\delta(t)$, to replace the constants α and δ in the model (3.1), respectively. Based on the model (3.1), we can obtain the mathematical representation of the corresponding controlled malware propagation model as follows.

$$\begin{cases} \dfrac{dS(t)}{dt} = \eta_1 + \delta(t)I(t) + \alpha_0 P(t) - \beta\gamma S(t)I(t) - \alpha(t)S(t) - \mu S(t), \\ \dfrac{dI(t)}{dt} = \eta_2 + \beta\gamma S(t)I(t) - \delta(t)I(t) - \mu I(t), \\ \dfrac{dP(t)}{dt} = \eta_3 + \alpha(t)S(t) - \alpha_0 P(t) - \mu P(t), \end{cases} \tag{3.2}$$

with the initial condition $(S(0), I(0), P(0))^T \in \Psi$, where

$$\Psi = \{(S, I, P) \in \mathbb{R}^3_+ : S + I + P = 1\} \tag{3.3}$$

is a positive invariant for the system (3.2). S, I, P are the abbreviations of $S(t), I(t), P(t)$, respectively, and the latter are the same if not specifically declared.

4. Optimal control analysis of the model

In this section, we will perform an optimal control analysis of the controlled malware propagation model to determine the optimal control strategy. Firstly, the control strategy and loss definition will be presented. Next, we will formulate the optimal control problem. Finally, we will analyze the solution existence and optimality system.

4.1. Control strategy and loss definition

From the perspective of controlling the spread of malware, we hope to achieve the best control effect at the minimum control loss by the control strategy such as installing anti-malware software or patch.

Let $\mathbf{g}$ and L denote the control strategy and loss, respectively. From system (3.2), we can adjust vaccination function $\alpha(t)$ and treatment function $\delta(t)$ to implement control of malware propagation. The control loss is related to the control strategy. Specifically, the control loss mainly includes the cost of vaccination and treatment, as well as the losses caused by node infection. Then, the control strategy, at time t, can be described as $\mathbf{g}(t) = (\alpha(t), \delta(t))^T$, and the control loss can be represented as $L(S(t), I(t), P(t), \mathbf{g}(t))$.

Let $\underline{\alpha}$, $\overline{\alpha}$ and $\underline{\delta}$, $\overline{\delta}$ denote the infimum and supremum of $\alpha(t)$ and $\delta(t)$, respectively. Furthermore, $\underline{\alpha}$, $\overline{\alpha}$, $\underline{\delta}$, $\overline{\delta}$ are positive constants, and $0 < \underline{\alpha} < \overline{\alpha} < 1$, $0 < \underline{\delta} < \overline{\delta} < 1$. Let $\mathscr{G}$ represent the feasible control set of $\mathbf{g}$, and then for $t \in [0, T]$,

$$\mathscr{G} = \left\{ \mathbf{g}(t) \in \left(L^2 [0, T] \right)^2 \,\middle|\, \underline{\alpha} \le \alpha(t) \le \overline{\alpha},\ \underline{\delta} \le \delta(t) \le \overline{\delta} \right\}, \tag{4.1}$$

where $L^2 [0, T]$ represents the Lebesgue square integrable function set.

4.2. Optimal control problem formulation

Let $\mathbf{x}(t) = (S(t), I(t), P(t))^T$. Then, $L(S(t), I(t), P(t), \mathbf{g}(t)) = L(\mathbf{x}(t), \mathbf{g}(t))$, and system (3.2) can be represented by a matrix as follows.

$$\frac{d\mathbf{x}(t)}{dt} = \mathbf{f}(\mathbf{x}(t), \mathbf{g}(t)), \quad t \in [0, T], \tag{4.2}$$

where $\mathbf{x}(0) \in \Psi$, $\mathbf{g} \in \mathscr{G}$.

During the time period $[0, T]$, the goal is to find the control strategy $\mathbf{g}(\cdot)$ that minimizes both the scale of malware spread and the total cost for treatment and vaccination. To achieve this goal, we need to solve the optimal control problem as follows.

$$\min_{\mathbf{g} \in \mathscr{G}} J(\mathbf{g}) = \int_0^T L(\mathbf{x}(t), \mathbf{u}(t)) dt \tag{4.3}$$

subject to system (3.2) or (4.2), where

$$L(\mathbf{x}(t), \mathbf{g}(t)) = I + \frac{1}{r} p\alpha(t)^r + \frac{1}{r} q\delta(t)^r, \quad 1 < r \le 2, \tag{4.4}$$

is the Lagrangian, and $p, q > 0$ are tradeoff factors regarding the control goal of the treatment and vaccination.

Remark 1. *Since the control loss mainly includes the cost of vaccination and treatment, as well as the losses caused by node infection, for convenience, we adopt $\alpha(t), \delta(t)$ and I to represent the corresponding costs. In Eq* (4.4)*, the control loss $L(\mathbf{x}(t), \mathbf{g}(t))$ is not limited to quadratic functions [33–35], and the power r $(1 < r \le 2)$ of $L(\mathbf{x}(t), \mathbf{g}(t))$ may be more suitable for the actual situation. Therefore, we take Eq* (4.4) *for the control loss in this paper.*

4.3. Solution existence of optimal control problem

From the preliminary knowledge and Lemma 1, we just need to prove that each condition in Lemma 1 is satisfied. Hence, we can derive the following results.

Lemma 3. *There exists $\mathbf{g} \in \mathscr{G}$ such that the system (3.2) or (4.2) is solvable.*

Proof. By putting $\mathbf{g} \equiv \bar{\mathbf{g}} := \left(\overline{\alpha}, \overline{\delta}\right)^T$ into the system (4.2), the following uncontrolled system can be obtained:

$$\frac{d\mathbf{x}(t)}{dt} = \mathbf{f}(\mathbf{x}(t), \bar{\mathbf{g}}) \tag{4.5}$$

with the initial condition $\mathbf{x}(0) \in \Psi$. Since $\mathbf{f}(\mathbf{x}(t), \bar{\mathbf{g}})$ is continuously differentiable, and Ψ is a positive invariant, it is possible to derive the claim from the continuation theorem [36]. □

Lemma 4. *The feasible control set $\mathscr{G}$ is convex.*

Proof. Define

$$\mathbf{g}_1 = (\alpha_1, \delta_1)^T \in \mathscr{G}, \quad \mathbf{g}_2 = (\alpha_2, \delta_2)^T \in \mathscr{G}, \quad 0 < \xi < 1. \tag{4.6}$$

Since $\left(L^2[0,T]\right)^2$ is a real vector space,

$$(1-\xi)\mathbf{g}_1 + \xi\mathbf{g}_2 \in \left(L^2[0,T]\right)^2. \tag{4.7}$$

Furthermore,

$$\underline{\alpha} \le (1-\xi)\alpha_1 + \xi\alpha_2 \le \overline{\alpha}, \quad \underline{\delta} \le (1-\xi)\delta_1 + \xi\delta_2 \le \overline{\delta}. \tag{4.8}$$

Therefore, the proof is complete. □

Lemma 5. *The feasible control set $\mathscr{G}$ is closed.*

Proof. Let $\mathbf{g} = (\alpha, \delta)^T$ be the limit of $\mathscr{G}$, and $\mathbf{g}_n = (\alpha_n, \delta_n)^T$, $n = 1, 2, \cdots$, which is a sequence of $\mathscr{G}$. Then,

$$\|\mathbf{g}_n - \mathbf{g}\|_2 := \left[\int_0^T |\mathbf{g}_n(t) - \mathbf{g}(t)|^2\, dt\right]^{1/2} < \frac{1}{n}. \tag{4.9}$$

Based on the completeness of $\left(L^2[0,T]\right)^2$, we can get

$$\lim_{n\to\infty} \mathbf{g}_n = \mathbf{g} \in \left(L^2[0,T]\right)^2. \tag{4.10}$$

Note that

$$\underline{\alpha} \le \alpha = \lim_{n\to\infty} \alpha_n \le \overline{\alpha}, \quad \underline{\delta} \le \delta = \lim_{n\to\infty} \delta_n \le \overline{\delta}. \tag{4.11}$$

Hence, the closeness of $\mathscr{G}$ can be followed from the above observations, and the proof is complete. □

Lemma 6. $\mathbf{f}(\mathbf{x}, \mathbf{g})$ *is bounded by a linear function in* $\mathbf{x}$.

Proof. Since

$$\eta_1 - (\overline{\alpha} + \mu)S - \beta\gamma/4 \le \eta_1 + \delta I + \alpha_0 P - \beta\gamma S I - \alpha S - \mu S \le \eta_1 + \overline{\delta} I + \alpha_0 P, \tag{4.12}$$

$$\eta_2 - (\overline{\delta} + \mu)I \le \eta_2 + \beta\gamma S I - \delta I - \mu I \le \eta_2 + \beta\gamma/4, \tag{4.13}$$

$$\eta_3 - (\alpha_0 + \mu)P \le \eta_3 + \alpha S - \alpha_0 P - \mu P \le \eta_3 + \overline{\alpha} S. \tag{4.14}$$

Thus, from the above observations, the proof is complete. □

Lemma 7. $L(\mathbf{x}, \mathbf{g})$ *is convex on* $\mathscr{G}$.

Proof. For $\mathbf{g} \in \mathscr{G}$, we can get the Hessian matrix of $L(\mathbf{x}, \mathbf{g})$ as follows.

$$\mathbf{H}_{\mathbf{g}}(L) = \begin{pmatrix} p(r-1)\alpha^{r-2} & 0 \\ 0 & q(r-1)\delta^{r-2} \end{pmatrix}. \tag{4.15}$$

For any $t \in [0,T]$, we can obtain that $\mathbf{H}_{\mathbf{g}}(L)$ is a real symmetric matrix with all positive eigenvalues. This implies that $\mathbf{H}_{\mathbf{g}}(L)$ is a positive definite matrix. Therefore, from [37], the claimed result follows. □

Lemma 8. *$L(\mathbf{x}, \mathbf{g}) \geq c_1\|\mathbf{g}\|_2^{\rho} + c_2$ for some $\rho > 1$, $c_1 > 0$ and c_2.*

Proof. Note that

$$\begin{aligned} L(\mathbf{x}, \mathbf{g}) &= I + \frac{1}{r}p\alpha^r + \frac{1}{r}q\delta^r \\ &\geq \frac{1}{r}\min\{p, q\}(\alpha^r + \delta^r) \\ &\geq \frac{1}{r}\min\{p, q\}\left(\alpha^2 + \delta^2\right) \\ &= \frac{\min\{p, q\}}{r}\|\mathbf{g}\|_2^2. \end{aligned} \tag{4.16}$$

Thus, the claimed result follows. □

According to Lemmas 3–8, we can derive the following important result.

Theorem 1. *There exists an optimal control for the optimal control problem (4.2)+(4.3).*

Proof. Based on Lemmas 3–8, it can be concluded that all six conditions in Lemma 1 are proven. Therefore, the claimed result can be derived from Lemma 1. □

Remark 2. *Theorem 1 indicates there exists an optimal control strategy, which has important theoretical support and practical guidance for the actual control of malware propagation.*

4.4. Optimality system of optimal control problem

Although we prove the existence of an optimal control strategy through Theorem 1, it is difficult to give an expression of the optimal strategy, which is not conducive to practical applications. Therefore, we are prepared to find an optimal system that meets the optimal solution, in order to narrow down the scope of searching for the optimal strategy, thereby achieving accelerated and practical results. Therefore, we can get the following theorem, which provides a way to find the optimal control of (4.2)+(4.3).

Theorem 2. *Suppose that $\mathbf{g}^*(t)$ is an optimal control of the optimal control problem (4.2)+(4.3), and $(S^*(t), I^*(t), P^*(t))^T$ is a solution to the system (4.2). For $t \in [0, T]$ and $\mathbf{g}(t) = \mathbf{g}^*(t)$, then*

$$\begin{cases} \dfrac{d\theta_1^*(t)}{dt} = \theta_1^*(t)\left(\mu + \alpha^*(t) + \beta\gamma I^*(t)\right) - \beta\gamma I^*(t)\theta_2^*(t) - \alpha^*(t)\theta_3^*(t), \\ \dfrac{d\theta_2^*(t)}{dt} = -1 - \theta_1^*(t)\left(\delta^*(t) - \beta\gamma S^*(t)\right) + \theta_2^*(t)\left(\mu + \delta^*(t) - \beta\gamma S^*(t)\right), \\ \dfrac{d\theta_3^*(t)}{dt} = -\alpha_0\theta_1^*(t) + (\alpha_0 + \mu)\theta_3^*(t), \end{cases} \tag{4.17}$$

where

$$\theta_1^*(T) = \theta_2^*(T) = \theta_3^*(T) = 0. \tag{4.18}$$

In addition, we can get

$$\alpha^*(t) = \max\left\{\min\left\{\left[\frac{S^*(t)}{p}\left(\theta_1^*(t) - \theta_3^*(t)\right)\right]^{\frac{1}{r-1}}, \overline{\alpha}\right\}, \underline{\alpha}\right\}, \quad 0 \leq t \leq T, \tag{4.19}$$

$$\delta^*(t) = \max\left\{\min\left\{\left[\frac{I^*(t)}{q}\left(\theta_2^*(t) - \theta_1^*(t)\right)\right]^{\frac{1}{r-1}}, \overline{\delta}\right\}, \underline{\delta}\right\}, \quad 0 \le t \le T. \tag{4.20}$$

Proof. According to the known conditions in the theorem, we can obtain the corresponding Hamiltonian as follows.

$$H(S, I, P, \theta, \mathbf{g}) = I + \frac{p}{r}\alpha^r + \frac{q}{r}\delta^r + \theta_1\frac{dS}{dt} + \theta_2\frac{dI}{dt} + \theta_3\frac{dP}{dt}, \tag{4.21}$$

where θ_1, θ_2 and θ_3 are undetermined, $\theta = (\theta_1, \theta_2, \theta_3)^T$.

From the Pontryagin Minimum Principle [38] and the Lemma 2, one can get that there exist $\theta_1^*(t)$, $\theta_2^*(t)$ and $\theta_3^*(t)$, such that for $t \in [0, T]$,

$$\begin{cases} \dfrac{d\theta_1^*(t)}{dt} = -\dfrac{\partial H(S^*(t), I^*(t), P^*(t), \theta^*(t), \mathbf{g}^*(t))}{\partial S}, \\ \dfrac{d\theta_2^*(t)}{dt} = -\dfrac{\partial H(S^*(t), I^*(t), P^*(t), \theta^*(t), \mathbf{g}^*(t))}{\partial I}, \\ \dfrac{d\theta_3^*(t)}{dt} = -\dfrac{\partial H(S^*(t), I^*(t), P^*(t), \theta^*(t), \mathbf{g}^*(t))}{\partial P}. \end{cases} \tag{4.22}$$

Therefore, by direct calculations, we can obtain the system (4.17).

The transversality conditions hold because the end cost is not specified, and the end state is free. Thus, noting that

$$H(S^*, I^*, P^*, \theta^*, \mathbf{g}^*) = \min_{\mathbf{g}\in\mathscr{G}} H(S^*, I^*, P^*, \theta^*, \mathbf{g}), \tag{4.23}$$

one can obtain, (i)

$$\frac{\partial H(S^*(t), I^*(t), P^*(t), \theta^*(t), \mathbf{g}^*(t))}{\partial \alpha} = p\left[\alpha^*(t)\right]^{r-1} - \theta_1^*(t)S^*(t) + \theta_3^*(t)S^*(t) = 0, \tag{4.24}$$

or $\alpha^*(t) = \underline{\alpha}$ or $\alpha^*(t) = \overline{\alpha}$, and (ii)

$$\frac{\partial H(S^*(t), I^*(t), P^*(t), \theta^*(t), \mathbf{g}^*(t))}{\partial \delta} = q\left[\delta^*(t)\right]^{r-1} + \theta_1^*(t)I^*(t) - \theta_2^*(t)I^*(t) = 0, \tag{4.25}$$

or $\delta^*(t) = \underline{\delta}$ or $\delta^*(t) = \overline{\delta}$. Hence, the claimed result follows. □

From the preliminary knowledge and the above discussions, the following theorem about the optimality system of (4.2)+(4.3) can be derived.

Theorem 3. *There exists an optimality system of the optimal control problem (4.2)+(4.3).*

$$\begin{cases} \dfrac{dS(t)}{dt} = \eta_1 + \delta(t)I(t) + \alpha_0 P(t) - \beta\gamma S(t)I(t) - \alpha(t)S(t) - \mu S(t), \\ \dfrac{dI(t)}{dt} = \eta_2 + \beta\gamma S(t)I(t) - \delta(t)I(t) - \mu I(t), \\ \dfrac{dP(t)}{dt} = \eta_3 + \alpha(t)S(t) - \alpha_0 P(t) - \mu P(t), \\ \dfrac{d\theta_1(t)}{dt} = \theta_1(t)\left(\mu + \alpha(t) + \beta\gamma I(t)\right) - \beta\gamma I(t)\theta_2(t) - \alpha(t)\theta_3(t), \\ \dfrac{d\theta_2(t)}{dt} = -1 - \theta_1(t)\left(\delta(t) - \beta\gamma S(t)\right) + \theta_2(t)\left(\mu + \delta(t) - \beta\gamma S(t)\right), \\ \dfrac{d\theta_3(t)}{dt} = -\alpha_0\theta_1(t) + (\alpha_0 + \mu)\theta_3(t), \\ \alpha(t) = \max\left\{\min\left\{\left[\dfrac{S(t)}{p}\left(\theta_1(t) - \theta_3(t)\right)\right]^{\frac{1}{r-1}}, \overline{\alpha}\right\}, \underline{\alpha}\right\}, \\ \delta(t) = \max\left\{\min\left\{\left[\dfrac{I(t)}{q}\left(\theta_2(t) - \theta_1(t)\right)\right]^{\frac{1}{r-1}}, \overline{\delta}\right\}, \underline{\delta}\right\}, \end{cases} \tag{4.26}$$

where $t \in [0, T]$ *and* $\theta_1(T) = \theta_2(T) = \theta_3(T) = 0$.

Remark 3. *Theorems 2 and 3 show there exists an optimality system for (4.2)+(4.3), this is also a way to find the optimal control strategy. Through the optimality system, it is possible to accelerate the search for the optimal control strategy.*

5. Experiments

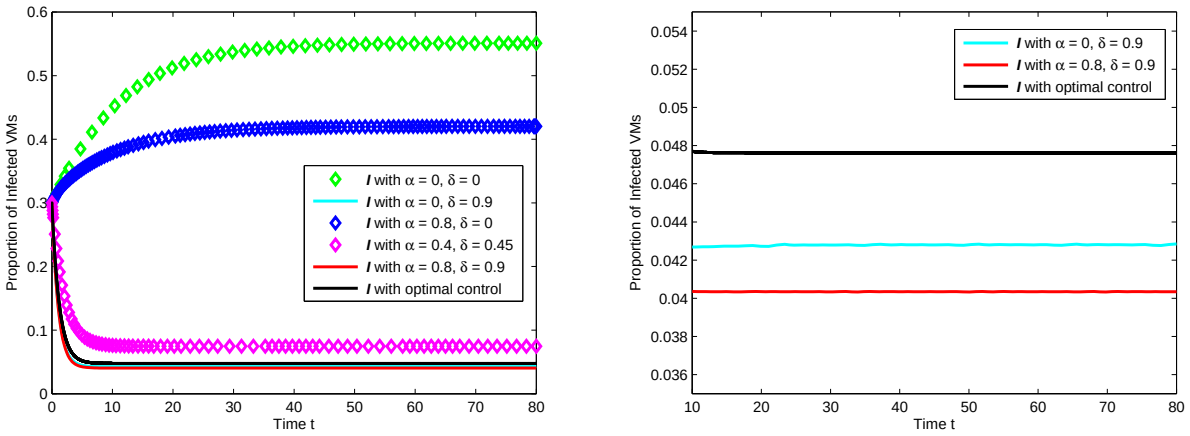
Theoretical analysis and results have been posed in the previous section. In this section, we mainly demonstrate the effectiveness of the optimal control strategy through some numerical simulations. It should be noted that all parameter values presented in the analysis are hypothetical, as real-world data is unavailable.

Firstly, let us introduce the system parameter settings as follows.

Example 1. *Suppose that* $\eta_1 = 0.05$, $\eta_2 = 0.04$, $\eta_3 = 0.01$, $\mu = \eta_1 + \eta_2 + \eta_3$, $\alpha_0 = 0.02$, $\beta = 0.15$, $\gamma = 0.5$, $\underline{\alpha} = 0.05$, $\overline{\alpha} = 0.8$, $\underline{\delta} = 0.05$, $\overline{\delta} = 0.9$, $p = 0.0013$, $q = 0.071$, $r = 1.95$, *and* $T = 80$. *The system of optimality equations (4.26) is numerically solved by calling the backward-forward Runge-Kutta fourth-order scheme, with the initial condition* $(S(0), I(0), P(0)) = (0.5, 0.3, 0.2)$.

All subsequent experiments are conducted in Example 1, and the results are shown in Figures 1–4 and Table 1. Next, we will describe the experimental results in detail.

Figure 1(a) illustrates the changes in the proportion of infected VMs under different control strategies, showing the evolution of the system over time. As I with $\alpha = 0, \delta = 0.9$, I with $\alpha = 0.8, \delta = 0.9$, and I with optimal control cannot be distinguished, they are shown separately in Figure 1(b), which depicts the curves that are very close in Figure 1(a). From Figure 1(a),(b), one can see that there are apparent differences between different control strategies on the eventual scale of



(a) (b)

Figure 1. Evolution of proportion of protected VMs with different control strategies given in Example 1.

malware infection, which also shows the importance of studying control strategies. Specifically, I with $\alpha = 0, \delta = 0$ indicates that no control strategy is adopted, so the scale of malware infection is the largest. On the contrary, the optimal control strategy achieves much better results.

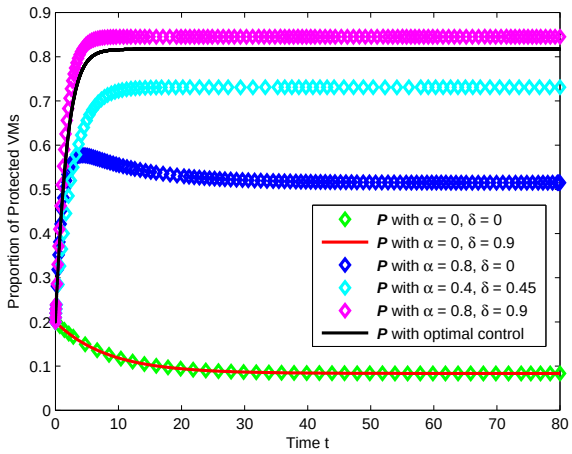


Figure 2. Evolution of proportion of protected VMs with different control strategies given in Example 1.

Figure 2 displays the changes in the proportion of protected VMs under different control strategies, showing the evolution of the system over time. Various control strategies also differ greatly in the final protected VMs scale. P with $\alpha = 0, \delta = 0$ represents that no control strategy is adopted, so the scale of protected VMs is the lowest. On the contrary, the optimal control strategy achieves the best results. This shows the importance of finding the optimal control strategy and also illustrates the significance of the existence of Theorems 2 and 3 from a lateral perspective.

Remark 4. *From Figures 1 and 2, it can be seen that control functions α and δ impose main effects on proportions of protected, and infected VMs, which coincide with the meanings of α and δ, vaccination and treatment, respectively. In addition, it is evident that $\mathbf{g}^*$ is highly effective in curbing the spread of malware. In the experiments, different values of α and δ correspond to different models, but these models are not optimization models, and their effectiveness is significantly inferior to our optimization model.*

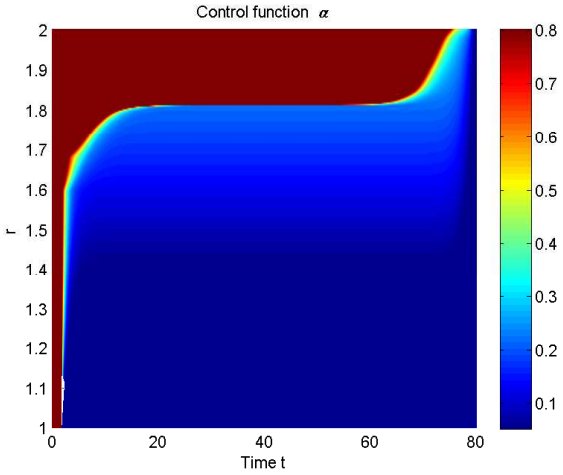


Figure 3. Optimal control function α with varied r for system (4.26) given in Example 1.

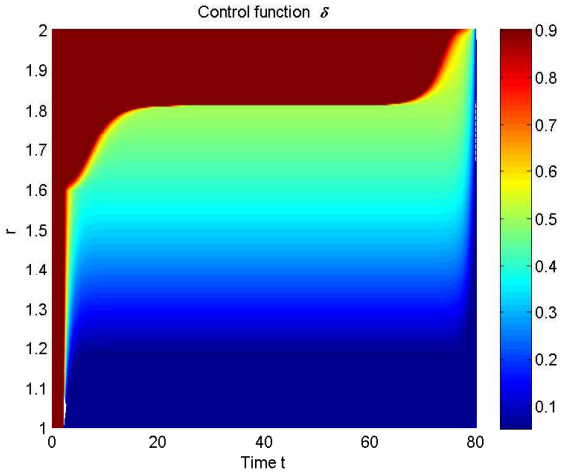


Figure 4. Optimal control function δ with varied r for system (4.26) given in Example 1.

Figures 3 and 4 demonstrate the corresponding optimal control functions α and δ with varied r, respectively. It can be concluded that α and δ are both affected by r, and they increase as r increases. Although the trends of change are similar, δ increased faster, indicating that δ received a greater impact.

Table 1 summarizes the results of different control strategies in terms of the final proportion of infected VMs and their corresponding objective function J values. The table clearly indicates that the optimal control strategy $\mathbf{g}^*$ is the most effective approach in minimizing the objective function J

Table 1. The proportion of infected VMs and their respective objective function J.

	$\mathbf{g} = \mathbf{g}^*$	$\mathbf{g} = (0, 0)$	$\mathbf{g} = (0, 0.9)$	$\mathbf{g} = (0.8, 0)$	$\mathbf{g} = (0.4, 0.45)$	$\mathbf{g} = (0.8, 0.9)$
$I(\mathbf{g})$	0.0476	0.5510	0.0428	0.4204	0.0747	0.0403
$J(\mathbf{g})$	4.9341	40.2648	7.1754	31.1899	8.7248	7.2328

and reducing the prevalence of infected VMs to a significant extent. In addition, Table 1 also further demonstrates the results of the previous figures. It is not only necessary to look at the final control scale but also necessary to consider both the control scale and the control loss. Therefore, our study offers a fresh perspective on tackling the problem of malware diffusion in cloud computing environments.

6. Summary

This paper has presented a novel controlled dynamical model for studying the propagation of malware in cloud computing environments, which integrates dynamic immunization strategies such as treatment and vaccination. The proposed model aims to provide a better understanding of the mechanisms underlying malware diffusion in the cloud. First, we introduce the control strategy and loss definition. Second, we define the optimal control problem. Next, we analyze the solution existence and optimality system of the optimal control problem. Finally, we provide numerical simulations to demonstrate how to determine an optimal immunization strategy. Notably, our results show that the proposed optimal immunization approach can effectively reduce the prevalence of infections at a low loss.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors are grateful to the anonymous reviewers and the editor for their valuable comments and suggestions. This work was supported by the Chongqing Research Program of Basic Research and Frontier Technology (Nos. cstc2017jcyjAX0256 and cstc2021jcyj-msxmX0761), and the Natural Science Foundation of Chongqing, China (No. CSTB2022NSCQ-MSX1130).

Conflict of interest

The authors declare there is no conflict of interest.

References

1. X. Zhu, J. Wang, H. Guo, D. Zhu, L. T. Yang, L. Liu, Fault-tolerant scheduling for real-time scientific workflows with elastic resource provisioning in virtualized clouds, *IEEE Trans. Parallel Distrib. Syst.*, **27** (2016), 3501–3517. https://doi.org/10.1109/TPDS.2016.2543731
2. E. Pluzhnik, E. Nikulchev, Virtual laboratories in cloud infrastructure of educational institutions, in *2014 2nd 2014 2nd International Conference on Emission Electronics (ICEE)*, (2014), 1–3.
3. M. Ali, S. U. Khan, A. V. Vasilakos, Security in cloud computing: Opportunities and challenges, *Inform. Sci.*, **305** (2015), 357–383. https://doi.org/10.1016/j.ins.2015.01.025
4. P. D. Ezhilchelvan, I. Mitrani, Evaluating the probability of malicious co-residency in public clouds, *IEEE Trans. Cloud Comput.*, **5** (2015), 420–427. https://doi.org/10.1109/TCC.2015.2451633
5. H. El Merabet, A. Hajraoui, A survey of malware detection techniques based on machine learning, *Int. J. Adv. Comput. Sci. Appl.*, **10** (2019). https://doi.org/10.14569/IJACSA.2019.0100148
6. K. Lu, J. Cheng, A. Yan, Malware detection based on the feature selection of a correlation information decision matrix, *Mathematics*, **11** (2023), 961. https://doi.org/10.3390/math11040961
7. T. Li, Y. Liu, Q. Liu, W. Xu, Y. Xiao, H. Liu, A malware propagation prediction model based on representation learning and graph convolutional networks, *Digital Commun. Networks*, 2022. https://doi.org/10.3390/math11040961
8. Y. Ye, T. Li, D. Adjeroh, S. S. Iyengar, A survey on malware detection using data mining techniques, *ACM Comput. Surv.*, **50** (2017), 1–40. https://doi.org/10.1145/3073559 .
9. T. Li, Y. Liu, X. Wu, Y. Xiao, C. Sang, Dynamic model of malware propagation based on tripartite graph and spread influence, *Nonlinear Dyn.*, **101** (2020), 2671–2686. https://doi.org/10.1007/s11071-020-05935-6
10. F. Mira, A systematic literature review on malware analysis, in *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, (2021), 1–5. https://doi.org/10.1109/IEMTRONICS52119.2021.9422537
11. Q. Zhu, Y. Liu, X. Luo, K. Cheng, A malware propagation model considering conformity psychology in social networks, *Axioms*, **11** (2022). https://doi.org/10.3390/axioms11110632
12. X. Ye, S. Xie, S. Shen, Sir1r2: Characterizing malware propagation in wsns with second immunization, *IEEE Access*, **9** (2021), 82083–82093. https://doi.org/10.1109/ACCESS.2021.3086531
13. N. P. Dong, H. V. Long, N. T. K. Son, The dynamical behaviors of fractional-order se1e2iqr epidemic model for malware propagation on wireless sensor network, *Commun. Nonlinear Sci. Numerical Simul.*, **111** (2022), 106428. https://doi.org/10.1016/j.cnsns.2022.106428
14. S. M. Al-Tuwairqi, W. S. Bahashwan, The impact of quarantine strategies on malware dynamics in a network with heterogeneous immunity, *Math. Model. Anal.*, **27** (2022), 282–302. https://doi.org/10.3846/mma.2022.14391
15. A. Martin del Rey, G. Hernandez, A. Bustos Tabernero, A. Queiruga Dios, Advanced malware propagation on random complex networks, *Neurocomputing*, **423** (2021), 689–696. https://doi.org/10.1016/j.neucom.2020.03.115

16. J. R. C. Piqueira, M. A. Cabrera, C. M. Batistela, Malware propagation in clustered computer networks, *Phys. A Stat. Mech. Appl.*, **573** (2021), 125958. https://doi.org/10.1016/j.physa.2021.125958

17. W. Zhang, Z. Wang, Z. Zhang, J. Zou, Delay effect on a malware propagation model incorporating user awareness, in *2022 International Conference on Cyber-Physical Social Intelligence (ICCSI)*, (2022), 555–560. https://doi.org/10.1109/ICCSI55536.2022.9970556

18. L. Li, J. Cui, R. Zhang, H. Xia, X. Cheng, Dynamics of complex networks: Malware propagation modeling and analysis in industrial internet of things, *IEEE Access*, **8** (2020), 64184–64192. https://doi.org/10.1109/ACCESS.2020.2984668

19. M. N. Aman, U. Javaid, B. Sikdar, Iot-proctor: A secure and lightweight device patching framework for mitigating malware spread in iot networks, *IEEE Syst. J.*, **16** (2022), 3468–3479. https://doi.org/10.1109/JSYST.2021.3070404

20. S. Hosseini, M. A. Azgomi, Dynamical analysis of a malware propagation model considering the impacts of mobile devices and software diversification, *Phys. A Stat. Mech. Appl.*, **526** (2019), 120925. https://doi.org/10.1016/j.physa.2019.04.161

21. S. Hosseini, Defense against malware propagation in complex heterogeneous networks, *Cluster Comput.*, **24** (2021), 1199–1215. https://doi.org/10.1007/s10586-020-03181-4

22. R. Hassan, S. Rafatirad, H. Homayoun, S. M. P. Dinakarrao, Performance-aware malware epidemic confinement in large-scale iot networks, in *ICC 2021 - IEEE International Conference on Communications*, (2021), 1–6. https://doi.org/10.1109/ICC42927.2021.9500476

23. S. Shen, H. Zhou, S. Feng, J. Liu, H. Zhang, Q. Cao, An epidemiology-based model for disclosing dynamics of malware propagation in heterogeneous and mobile wsns, *IEEE Access*, **8** (2020), 43876–43887. https://doi.org/10.1109/ACCESS.2020.2977966

24. L. Miao, S. Li, Stochastic differential game-based malware propagation in edge computing-based iot, *Secur. Commun. Networks*, **2021** (2021), 1–11. https://doi.org/10.1155/2021/8896715

25. V. S. Varma, Y. Hayel, I. C. Morarescu, A non-cooperative resource utilization game between two competing malware, *IEEE Control Syst. Lett.*, **7** (2023), 67–72. https://doi.org/10.1109/LCSYS.2022.3186620

26. L. Wang, S. S. Iyengar, A. K. Belman, P. Śniatała, V. V. Phoha, C. Wan, Game theory based cyber-insurance to cover potential loss from mobile malware exploitation, *Digital Threats Res. Pract.*, **2** (2021), 1–24. https://doi.org/10.1145/3409959

27. H. Zhou, S. Shen, J. Liu, Malware propagation model in wireless sensor networks under attack-defense confrontation, *Comput. Commun.*, **162** (2020), 51–58. https://doi.org/10.1016/j.comcom.2020.08.009

28. Z. Benomar, C. Ghribi, E. Cali, A. Hinsen, B. Jahnel, Agent-based modeling and simulation for malware spreading in d2d networks, preprint, arXiv: 2201.12230.

29. F. Abazari, M. Analoui, H. Takabi, Effect of anti-malware software on infectious nodes in cloud environment, *Comput. Secur.*, **58** (2016), 139–148. https://doi.org/10.1016/j.cose.2015.12.002

30. C. Gan, Q. Feng, X. Zhang, Z. Zhang, Q. Zhu, Dynamical propagation model of malware for cloud computing security, *IEEE Access*, **8** (2020), 20325–20333. https://doi.org/10.1109/ACCESS.2020.2968916

31. M. I. Kamien, N. L. Schwartz, *Dynamic optimization: the calculus of variations and optimal control in economics and management*, Courier Corporation, 2012.

32. E. Pluzhnik, E. Nikulchev, S. Payain, Optimal control of applications for hybrid cloud services, in *2014 IEEE World Congress on Services*, 2014, 458–461. https://doi.org/10.1109/SERVICES.2014.88

33. Q. Zhu, X. Yang, L. X. Yang, C. Zhang, Optimal control of computer virus under a delayed model, *Appl. Math. Comput.*, **218** (2012), 11613–11619. https://doi.org/10.1016/j.amc.2012.04.092

34. L. Chen, K. Hattaf, J. Sun, Optimal control of a delayed slbs computer virus model, *Phys. A Stat. Mech. Appl.*, **427** (2015), 244–250. https://doi.org/10.1016/j.physa.2015.02.048

35. L. X. Yang, M. Draief, X. Yang, The optimal dynamic immunization under a controlled heterogeneous node-based sirs model, *Phys. A Stat. Mech. Appl.*, **450** (2016), 403–415. https://doi.org/10.1016/j.physa.2016.01.026

36. R. C. Robinson, *An introduction to dynamical systems: Continuous and discrete*, American Mathematical Soc., 2012.

37. J. Stewart, *Multivariable calculus: Concepts and contexts*, Cengage Learning, 2018.

38. D. Liberzon, *Calculus of variations and optimal control theory: A concise introduction*, Princeton university press, 2011.

AIMS Press

© 2023 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)