Research Article

A Virus Propagation Model and Optimal Control Strategy in the Point-to-Group Network to Information Security Investment

Liping Feng ¹, **Ruifeng Han**,¹ **Hongbin Wang**,¹ **Qingshan Zhao**,¹ **Chengli Fu**,¹
and **Qi Han** ²

¹Computer Science Department, Xinzhou Teachers University, Xinzhou, Shanxi 034000, China

²School of Intelligent Technology and Engineering, Chongqing University of Science & Technology, Chongqing 401331, China

Correspondence should be addressed to Qi Han; hanqicq@163.com

Received 7 December 2020; Revised 3 May 2021; Accepted 25 May 2021; Published 3 June 2021

Academic Editor: Luxing Yang

Copyright © 2021 Liping Feng 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.

Epidemiological dynamics is a vital method in studying the spread of computer network viruses. In this paper, an optimal control measure is proposed based on the SEIR virus propagation model in point-to-group information networks. First, considering the need for antivirus measures in reality, an optimal control problem is introduced, and then a controlled computer virus spread model in point-to-group information networks is established. Second, the optimal control measure is formulated by making a tradeoff between control cost and network loss caused by virus intrusion. Third, optimal control strategies are theoretically investigated by Pontryagin's maximum principle and the Hamiltonian function. Finally, through numerical simulations, effective measures for controlling virus spread in point-to-group information networks are proposed.

1. Introduction

Given the situation that critical infrastructures and human daily activities are becoming more and more dependent on information networks, it is vital to understand their weaknesses and uncover potential risks to threaten their security. Network viruses are the main threat that leads to the cyber security. Observing the significant similarities between the propagation of biological epidemics and network viruses, Kephart and White devoted pioneering work research that uses epidemic models to investigate the propagation characteristics of worms and targeted countermeasures [1–3]. After that, some biological epidemic models, such as susceptible-infected-susceptible (SI/SIS) and susceptible-infected-recovered (SIR), have been adapted to capture behaviors of the network virus propagation [4–10]. Based on these classical models, lots of extent models, which have more state transitions among nodes, have also been proposed to investigate the dynamical characteristic of internet worms [11–15]. These previous studies contributed to reveal the dynamical phenomena of internet worms and

provided the effective theoretical instructions for network managers to protect network security.

The optimal control theory has been widely applied to the control of the spread of the epidemic [16–20]; however, to our knowledge, research studies which combine the optimal control theory with models of network viruses are seldom. Zhu et al. [21] established a delayed computer virus model with control, and the existence and uniqueness of an optimal control strategy were proved. Liu et al. [22] proposed a malware dynamical model with the impact of users' security awareness and, furthermore, developed effective prevention strategies with human interventions by optimal control theory. Yang et al. [23] proposed the novel conflicting opinion propagation model based on the differential game theory, which is contributed to the misinformation restraint and competitive viral marketing. These previous studies demonstrate that optimal control strategies are effective to prevent the diffusion of network viruses.

The above existing models suppose that the infection of network viruses is "point to point," i.e., an infected node infects a susceptible node one time. In fact, there is a

situation that an infected node will infect a group of nodes in the information sharing network, such as the popular e-mail system and instant message software. To investigate the effect of optimal control strategies on virus prevalence in the information sharing network, in this paper, an epidemic model with optimal control measures is addressed, which is based on [24].

Our main contributions are as follows: (1) we present a virus propagation model with variable antivirus measures in the point-to-group information sharing network; (2) the optimal control function to adjust antivirus strength is constructed; (3) the existence of the optimized solution is proved theoretically.

This paper is organized as follows. Section 2 formulates the model and corresponding optimal control strategy. The optimal control strategy is studied in Section 3. Section 4 represents some numerical results. Finally, Section 5 concludes the paper.

2. The Model and Optimal Control Strategy

2.1. Model Formulation. An information sharing network is a complex communicating network including a great deal of nodes (computer, terminal, or entity, etc.), in which one node that received the information can send the information to other nodes in the network. We can represent the information sharing network by an undirected network, as shown in Figure 1.

Our model is based on the network virus epidemic model with the point-to-group (P2G) information propagation proposed by Hua Yuan and Guoqing Chen [24]. This model assumes that the individuals in an information network system have four states: susceptible (S), exposed (E), infected (I), and recovered (R). At any time, the node is in one of the four states. And the state of an individual can switch under the action of virus infection and antivirus measures. Consider the following two facts:

The hosts will undergo a latent period (E -state) during the transition from the S -state to the I -state because users do not open the link or e-mail immediately

Users may immunize their hosts with countermeasures in states S , E , and I

These countermeasures can be seen as the strategies of multistate antivirus and may result in the following state transition paths:

$S \rightarrow R$, using countermeasures of real-time immunization

$E \rightarrow R$, cleaning viruses after hosts are infected

$I \rightarrow R$, cleaning viruses after hosts are infected

As a result, the model is formulated as the following ordinary differential equations:

FIGURE 1: An information sharing network.

$$\begin{cases} \frac{dS(t)}{dt} = \mu N - v(t)S(t) - \rho_{SR}S(t) - \mu S(t), \\ \frac{dE(t)}{dt} = v(t)S(t) - \rho_{ER}E(t) - \alpha E(t) - \mu E(t), \\ \frac{dI(t)}{dt} = \alpha E(t) - (\delta + \mu)I(t), \\ \frac{dR(t)}{dt} = \rho_{SR}S(t) + \rho_{ER}E(t) + \delta I(t) - \mu R(t), \end{cases} \quad (1)$$

where μ is the replacement rate of old nodes, α is the transition rate from E to I , δ is the recovery rate from I to R , N is the total number of nodes in the network, ρ_{SR} describes the impact of implementing real-time immunization and ρ_{ER} describes the impact of cleaning the virus and immunizing the nodes in the latent period, $v(t)$ represents the transition rate from S to E , where $v(t) = (\alpha r/N)E(t)$, and r is the average number of neighbor nodes (with various states) that are directly connected with an infected node.

2.2. Optimal Control Strategy. In system (1), parameters ρ_{SR} , ρ_{ER} , and δ mean the strength of antivirus measures. In reality, they should be variable, so in this paper, we will induce a control function to adjust ρ_{SR} , ρ_{ER} , and δ . For our purpose, we want to find the control strategy which can obtain the minimum loss and cost when the accident of cyber security occurs. Let $\Theta = \{\varphi(t), 0 \leq \varphi(t) \leq \bar{\lambda}, t \in [0, T]\}$ indicate an admissible control set. Consider the loss of finance caused by network viruses is relevant to the number of infected nodes. Assume that the average loss caused by a node per unit time is the constant χ . Then, the whole loss caused by all infected nodes in unit time is proportional to the number of infected nodes I , expressed as χI . Define $L_{\text{loss}}(I(t))$ as the loss function; then, during the time interval $[0, T]$, $L_{\text{loss}}(I(t))$ can be calculated as follows:

$$L_{\text{loss}}(I(t)) = \int_0^T \chi I(t) dt. \quad (2)$$

In addition, countermeasures need the investment of enterprises, such as buying antivirus software and users' security education. The famous Gordon–Loeb model shows that the maximum security investment is not necessarily optimal from the view of economics [25]. So, the equilibrium is vital that the loss of the enterprise is the minimum in the condition of minimum investment in information security when a cyber security incident occurs. Let $L_{\text{cost}}(\varphi(t))$ be the cost of deploying security systems during the time interval $[0, T]$. Define

$$L_{\text{cost}}(\varphi(t)) = \int_0^T \frac{\kappa \varphi^2(t)}{2} dt, \quad (3)$$

subject to

$$\begin{cases} \frac{dS(t)}{dt} = \mu N - v(t)S(t) - \mu S(t) - \rho_{\text{SR}}\varphi(t)S(t), \\ \frac{dE(t)}{dt} = v(t)S(t) - \mu E(t) - \alpha E(t) - \rho_{\text{ER}}\varphi(t)E(t), \\ \frac{dI(t)}{dt} = \alpha E(t) - \mu I(t) - \delta\varphi(t)I(t), \\ \frac{dR(t)}{dt} = \rho_{\text{SR}}\varphi(t)S(t) + \rho_{\text{ER}}\varphi(t)E(t) + \delta\varphi(t)I(t) - \mu R(t), \end{cases} \quad (4)$$

where κ is a tradeoff coefficient. Equation (4) is the control system that we will concern. Aiming at equation (4), our aim is to find a control function $\varphi(t)$ to minimize the following objective function:

$$K(\varphi(t)) = \int_0^T \left[\chi I(t) + \frac{\kappa \varphi^2(t)}{2} \right] dt, \quad (5)$$

where $K(\varphi)$ is the sum of loss and investment about cyber security.

For investigating the dynamics of control system (4), we can calculate the basic reproduction number and equilibria by the dynamical theory of differential equations [26]. From equation (4), it is easy to find that the fourth equation will not affect the dynamics of equation (4). So, without loss of generality, we can omit the fourth equation when discussing the dynamics of equation (4). It is easy to get the expression of the basic reproduction number, which is determined by

$$R_0 = \frac{r\mu\alpha}{(\mu + \rho_{\text{SR}}\varphi(t))(\rho_{\text{ER}}\varphi(t) + \alpha + \mu)}. \quad (6)$$

When $R_0 < 1$, equation (4) has the only equilibrium $Q_0 = (S^0, E^0, I^0) = ((\mu/\rho_{\text{SR}}\varphi(t) + \mu), 0, 0)$ which means the network virus will be eliminated completely with the evaluation of time. When $R_0 > 1$, equation (4) has the epidemic equilibrium Q_* besides Q_0 , where Q_* is expressed by

$$Q_* = (S^*, E^*, I^*) = \left(\frac{\alpha + \mu + \rho_{\text{ER}}\varphi(t)}{r\alpha} N, \frac{\mu + \rho_{\text{SR}}\varphi(t)}{r\alpha} N (R_0 - 1), \frac{\alpha}{\delta\varphi(t) + \mu} E^* \right). \quad (7)$$

3. Solving the Optimal Control Strategies

For obtaining the optimal control solution, we need to define the Lagrangian and Hamiltonian function for optimal control problems (4) and (5). In fact, Lagrangian of the optimal problem can be given by

$$L(I, \varphi) = \chi I(t) + \frac{\kappa}{2} \varphi^2(t). \quad (8)$$

Next, we will seek an optimal function φ which satisfies that the integration of equation (8) is minimum. To do so, we define Hamiltonian H as follows:

$$H(S, E, I, \varphi, \lambda_1, \lambda_2, \lambda_3, \lambda_4, t) = L(I, \varphi) + \left[\lambda_1(t) \frac{dS(t)}{dt} + \lambda_2(t) \frac{dE(t)}{dt} + \lambda_3(t) \frac{dI(t)}{dt} + \lambda_4(t) \frac{dR(t)}{dt} \right]. \quad (9)$$

Theorem 1. *There exists an optimal control function φ^* such that $K(\varphi^*(t)) = \min_{\varphi \in \Theta} K(\varphi(t))$.*

Proof. According to the result of Kamien and Schwartz [27], it is easy to confirm the existence of an optimal control function to system (4).

First, the control set and corresponding state variables are not empty. The control set Θ is convex and closed. In the

meanwhile, the right parts of the equations of system (4) are bounded and continuous and can be written a linear function of φ in the state variables. Besides, $L(I, \varphi)$ is convex on Θ , and there exist a constant $\rho > 1$ and two positive numbers ξ_1 and ξ_2 such that $L(I, \varphi) \geq \xi_1 + \xi_2(|\varphi|)^{(\rho/2)}$. Thus, we conclude that there exists an optimal control function.

Next, we will find the optimal solution by means of Pontryagin's maximum principle. $\square$

Theorem 2. Give an optimal control variable $\varphi^*(t)$ and the corresponding solution of system (4), $S^*(t)$, $E^*(t)$, $I^*(t)$, and $R^*(t)$, there exist adjoint variables $\lambda_i (i = 1, 2, 3)$ satisfying

$$\begin{cases} \frac{d\lambda_1}{dt} = (\nu(t) + \mu)\lambda_1(t) + \rho_{SR}\varphi^*(t)\lambda_1(t) - \nu(t)\lambda_2(t) - \rho_{SR}\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_2}{dt} = (\mu + \alpha)\lambda_2(t) + \frac{r\alpha}{N}S^*(t) + \rho_{ER}\varphi^*(t)\lambda_2(t) - \alpha\lambda_3(t) - \rho_{ER}\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_3}{dt} = \mu\lambda_3(t) + \delta\varphi^*(t)\lambda_3(t) - \delta\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_4}{dt} = \mu\lambda_4(t), \end{cases} \quad (10)$$

with boundary conditions $\lambda_i(T) = 0$ ($i = 1, 2, 3$).

Proof. By differentiating Hamiltonian (8) with respect to state variables S , E , I , and R , we obtain the adjoint system as follows:

$$\begin{cases} \frac{d\lambda_1}{dt} = -\frac{\partial H}{\partial S} = (\nu(t) + \mu)\lambda_1(t) + \rho_{SR}\varphi^*(t)\lambda_1(t) - \nu(t)\lambda_2(t) - \rho_{SR}\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_2}{dt} = -\frac{\partial H}{\partial E} = (\mu + \alpha)\lambda_2(t) + \frac{r\alpha}{N}S^*(t) + \rho_{ER}\varphi^*(t)\lambda_2(t) - \alpha\lambda_3(t) - \rho_{ER}\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_3}{dt} = -\frac{\partial H}{\partial I} = \mu\lambda_3(t) + \delta\varphi^*(t)\lambda_3(t) - \delta\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_4}{dt} = -\frac{\partial H}{\partial R} = \mu\lambda_4(t). \end{cases} \quad (11)$$

By using optimality conditions, we have

$$\frac{\partial H}{\partial \varphi(t)}|_{\varphi^*(t)} = \kappa\varphi^*(t) - [(\lambda_1 - \lambda_4)\rho_{SR}S^*(t) + (\lambda_2 - \lambda_4)\rho_{ER}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)] = 0. \quad (12)$$

It follows that

$$\varphi^*(t) = \frac{(\lambda_1 - \lambda_4)\rho_{SR}S^*(t) + (\lambda_2 - \lambda_4)\rho_{ER}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)}{\kappa}. \quad (13)$$

Considering the feature of the feasible region of Θ , we obtain

$$\left\{ \begin{array}{ll} \varphi^*(t) = 0, & \text{if } \frac{(\lambda_1 - \lambda_4)\rho_{\text{SR}}S^*(t) + (\lambda_2 - \lambda_4)\rho_{\text{ER}}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)}{\kappa} \leq 0, \\ \varphi^*(t) = \frac{(\lambda_1 - \lambda_4)\rho_{\text{SR}}S^*(t) + (\lambda_2 - \lambda_4)\rho_{\text{ER}}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)}{\kappa}, & \text{if } \frac{(\lambda_1 - \lambda_4)\rho_{\text{SR}}S^*(t) + (\lambda_2 - \lambda_4)\rho_{\text{ER}}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)}{\kappa} < D, \\ \varphi^*(t) = D, & \text{if } \frac{(\lambda_1 - \lambda_4)\rho_{\text{SR}}S^*(t) + (\lambda_2 - \lambda_4)\rho_{\text{ER}}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)}{\kappa} > D. \end{array} \right. \quad (14)$$

Hence, we can have an optimal control function $\varphi^*(t)$ as follows:

$$\varphi^*(t) = \max \left\{ \min \left\{ \frac{(\lambda_1 - \lambda_4)\rho_{\text{SR}}S^*(t) + (\lambda_2 - \lambda_4)\rho_{\text{ER}}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)}{\kappa}, D \right\}, 0 \right\}. \quad (15)$$

So, we have the following optimal system:

$$\left\{ \begin{array}{l} \frac{dS(t)}{dt} = \mu N - v(t)S(t) - \mu S(t) - \rho_{\text{SR}}\varphi(t)S(t), \\ \frac{dE(t)}{dt} = v(t)S(t) - \mu E(t) - \alpha E(t) - \rho_{\text{ER}}\varphi(t)E(t), \\ \frac{dI(t)}{dt} = \alpha E(t) - \mu I(t) - \delta \varphi(t)I(t), \\ \frac{dR(t)}{dt} = \rho_{\text{SR}}\varphi(t)S(t) + \rho_{\text{ER}}\varphi(t)E(t) + \delta \varphi(t)I(t) - \mu R(t), \\ \frac{d\lambda_1}{dt} = (v(t) + \mu)\lambda_1(t) + \rho_{\text{SR}}\varphi^*(t)\lambda_1(t) - v(t)\lambda_2(t) - \rho_{\text{SR}}\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_2}{dt} = (\mu + \alpha)\lambda_2(t) + \frac{r\alpha}{N}S^*(t)\lambda_2(t) + \rho_{\text{ER}}\varphi^*(t)\lambda_2(t) - \alpha\lambda_3(t) - \rho_{\text{ER}}\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_3}{dt} = \mu\lambda_3(t) + \delta\varphi^*(t)\lambda_3(t) - \delta\varphi^*(t)\lambda_4(t), \\ \frac{d\lambda_4}{dt} = \mu\lambda_4(t), \\ \varphi^*(t) = \max \left\{ \min \left\{ \frac{(\lambda_1 - \lambda_4)\rho_{\text{SR}}S^*(t) + (\lambda_2 - \lambda_4)\rho_{\text{ER}}E^*(t) + (\lambda_3 - \lambda_4)\delta I^*(t)}{\kappa}, 1 \right\}, 0 \right\}. \end{array} \right. \quad (16)$$

4. Numerical Simulations

In this section, numerical simulations will be performed to compare system (1) without optimal control with system

(16) with optimal control, and systems (1) and (16) will be solved with the Runge–Kutta fourth order. As shown in Table 1, the parameter values are taken. Furthermore, we assume that the initial states of the systems are

TABLE 1: Parameters used in experiments.

Parameter	Value
N	10,000
μ	1/4380
r	30
α	1/150
ρ_{SR}	1/200
ρ_{ER}	1/200
δ	1/12- μ
κ	10

FIGURE 2: Evolution of the number of exposed nodes with or without control.

FIGURE 3: Evolution of the number of infected nodes with or without control.

$S(0) = 9999, E(0) = 1, I(0) = 0$, and $R(0) = 0$. Figures 2 and 3 depict the numerical results of $E(t)$ and $I(t)$, respectively.

Figure 2 shows that the growth rate of exposed nodes significantly decreased in the system with optimal control and that the evolution speed from exposed nodes to infected nodes slowed obviously. Hence, taking optimal control

FIGURE 4: Optimal control function for system (16).

measures, network managers can have more time to protect information systems when viruses intrude.

The same as Figure 2, Figure 3 shows that the growth rate of infected nodes with optimal control measures is much slower than that without optimal control measures. Moreover, the scale infected nodes also decreased in the network system with optimal control.

For surveying the evolution of the optimal control strategy with time, Figure 4 is depicted. From Figure 4, one can see that the control strategy keeps a stable state, and then the intensity of control increases with the increase of infected nodes. Subsequently, the intensity of control decreases with a reduction of virus spread.

5. Conclusion

The objective of this work is to model the virus prevalence in point-to-group information sharing networks and then find out certain optimal strategies of controlling the virus propagation. Taking into account the tradeoff of investment and income, the strength of network security defense measures should vary with the severity of the virus damage. So, based on the e-SEIR model [24], we consider the control parameters $\varphi(t)$ that change over time. First, we put forward the objective function and study the optimal control strategy toward the parameter $\varphi(t)$. Second, the existence and uniqueness of the optimal control strategy are proved. Finally, some numerical experiments are performed, which show that the scale and speed of virus prevalence will decrease greatly by taking optimal control strategies. In the future, we need more effort to trace the real data to test our results.

Data Availability

All the data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Research Project supported by the Shanxi Scholarship Council of China (2020-139), Cultivate Scientific Research Excellence Programs of Higher Education Institutions in Shanxi (2020KJ025), Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant nos. KJZD-K201901504 and KJQN201901537), CAS “Light of West China” Program, Humanities and Social Sciences Research of Ministry of Education (19YJCZH047), and Xinzhou Teachers University Academic Leader Project.

References

- [1] J. Kephart and S. White, “Directed-graph epidemiological models of computer viruses,” in *Proceedings of the 1991 IEEE Symposium on Security and Privacy*, pp. 343–359, Oakland, CA, USA, May 1991.
- [2] J. O. Kephart and S. R. White, “Measuring and modeling computer virus prevalence,” in *Proceedings of the IEEE Computer Security Symposium on Research in Security and Privacy*, pp. 2–15, Oakland, CA, USA, May 1993.
- [3] J. O. Kephart, S. R. White, and D. M. Chess, “Computers and epidemiology,” *IEEE Spectrum*, vol. 30, no. 5, pp. 20–26, 1993.
- [4] C. C. Zou, W. B. Gong, D. Towsley, and D. Towsley, “Code red worm propagation modeling and analysis,” *Department of Health Care Services*, vol. 34, pp. 18–22, 2002.
- [5] X. Han and Q. L. Tan, “Dynamical behavior of computer virus on Internet,” *Applied Mathematics and Computation*, vol. 64, no. 7, pp. 1–7, 2010.
- [6] S. Wang, Q. Liu, X. Yu, and Y. Ma, “Bifurcation analysis of a model for network worm propagation with time delay,” *Mathematical and Computer Modelling*, vol. 52, no. 3–4, pp. 435–447, 2010.
- [7] L. P. Feng, X. F. Liao, H. Q. Li, and Q. Han, “Hopf bifurcation analysis of a delayed viral infection model in computer networks,” *Mathematical and Computer Modeling*, vol. 56, no. 7, pp. 167–179, 2012.
- [8] L. Feng, L. Song, Q. Zhao, and H. Wang, “Modeling and stability analysis of worm propagation in wireless sensor network,” *Mathematical Problems in Engineering*, vol. 2015, Article ID 129598, 8 pages, 2015.
- [9] Q. Zhu and C. Cen, “A novel computer virus propagation model under security classification,” *Discrete Dynamics in Nature and Society*, vol. 2017, Article ID 8609082, 11 pages, 2017.
- [10] C. Gan, “Modeling and analysis of the effect of network eigenvalue on viral spread,” *Nonlinear Dynamics*, vol. 84, no. 3, pp. 1727–1733, 2016.
- [11] B. K. Mishra and D. K. Saini, “SEIRS epidemic model with delay for transmission of malicious objects in computer network,” *Applied Mathematics and Computation*, vol. 188, no. 2, pp. 1476–1482, 2007.
- [12] W. P. Liu, C. Liu, X. Y. Liu, S. G. Cui, and Y. Huang, “Modeling the spread of malware with the Influence of heterogeneous immunization,” *Applied Mathematical Modelling*, vol. 40, pp. 269–276, 2016.
- [13] Q. Liu, W. Cai, J. Shen, Z. Fu, X. Liu, and N. Linge, “A speculative approach to spatial-temporal efficiency with multi-objective optimization in a heterogeneous cloud environment,” *Security and Communication Networks*, vol. 9, no. 17, pp. 4002–4012, 2016.
- [14] T. Zhao and D. Bi, “Delay induced hopf bifurcation of an epidemic model with graded infection rates for internet worms,” *Mathematical Problems in Engineering*, vol. 2017, Article ID 9563862, 10 pages, 2017.
- [15] Y. Yao, Q. Fu, W. Yang, Y. Wang, and C. Sheng, “An epidemic model of computer worms with time delay and variable infection rate,” *Security and Communication Networks*, vol. 2018, Article ID 9756982, 11 pages, 2018.
- [16] A. Ali Lashari, “Optimal control of an SIR epidemic model with a saturated treatment,” *Applied Mathematics & Information Sciences*, vol. 10, no. 1, pp. 185–191, 2016.
- [17] L. Chen and J. Sun, “Optimal vaccination and treatment of an epidemic network model,” *Physics Letters A*, vol. 378, no. 41, pp. 3028–3036, 2014.
- [18] G. Zaman, Y. H. Kang, G. Cho, and I. H. Jung, “Optimal strategy of vaccination & treatment in an SIR epidemic model,” *Mathematics and Computers in Simulation*, vol. 136, pp. 63–77, 2017.
- [19] A. Jajarmi, A. Yusuf, D. Baleanu, and M. Inc, “A new fractional HRSV model and its optimal control: a non-singular operator approach,” *Physica A: Statistical Mechanics and Its Applications*, vol. 547, Article ID 123860, 2020.
- [20] I. Ahmad Nasidi, D. Nasidi, and D. Baleanu, “Optimal control model for the transmission of novel COVID-19,” *Computers, Materials & Continuation*, vol. 66, no. 3, pp. 3089–3106, 2021.
- [21] Q. Zhu, X. Yang, L.-X. Yang, and C. Zhang, “Optimal control of computer virus under a delayed model,” *Applied Mathematics and Computation*, vol. 218, no. 23, pp. 11613–11619, 2012.
- [22] W. Liu and S. Zhong, “Web malware spread modelling and optimal control strategies,” *Scientific Reports*, vol. 7, no. 1, Article ID 42308, 2017.
- [23] L.-X. Yang, P. Li, X. Yang, Y. Xiang, and Y. Y. Tang, “Simultaneous benefit maximization of conflicting opinions: modeling and analysis,” *IEEE Systems Journal*, vol. 14, no. 2, pp. 1623–1634, 2020.
- [24] H. Yuan and G. Chen, “Network virus-epidemic model with the point-to-group information propagation,” *Applied Mathematics and Computation*, vol. 206, no. 1, pp. 357–367, 2008.
- [25] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002.
- [26] J. Hale and S. M. Verduyn Lunel, *Introduction to Functional Differential Equations*, Springer, Berlin, Germany, 1993.
- [27] M. I. Kamien and N. L. Schwartz, *Dynamics Optimization: The Calculus of Variations and Optimal Control in Economics and Management*, Elsevier Science, Amsterdam, The Netherlands, 2000.