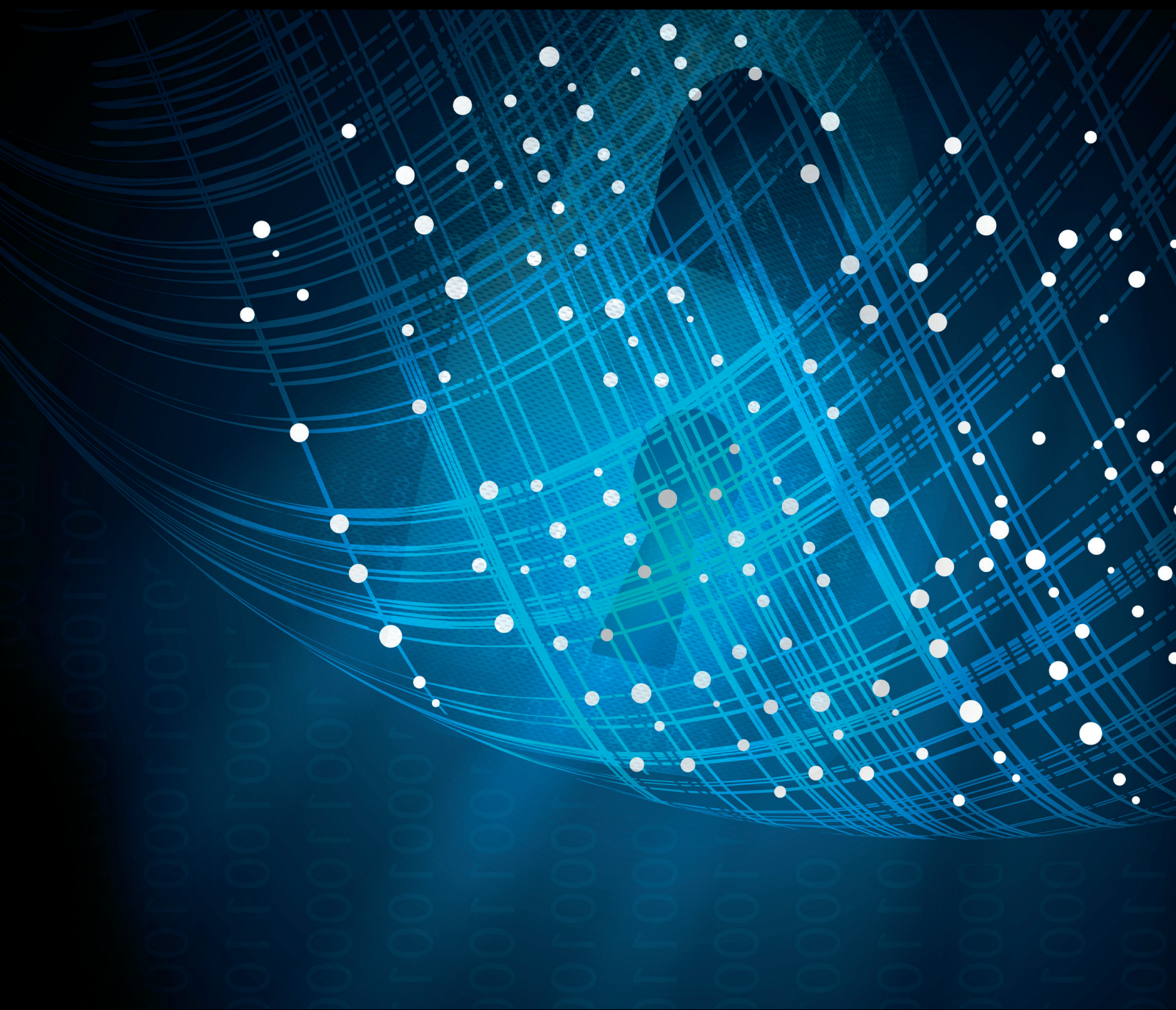
Security and Communication Networks

Mathematical Models for Malware Propagation

Special Issue Editor in Chief: Angel M. Del Rey
Guest Editors: Lu-Xing Yang and Vasileios A. Karyotis



Mathematical Models for Malware Propagation

Security and Communication Networks

Mathematical Models for Malware Propagation

Special Issue Editor in Chief: Angel M. Del Rey
Guest Editors: Lu-Xing Yang and Vasileios A. Karyotis

Editorial Board

Contents

Mathematical Models for Malware Propagation
Ángel Martín del Rey, Lu-Xing Yang, and Vasileios A. Karyotis
Editorial (2 pages), Article ID 6046353, Volume 2019 (2019)

A Novel Load Capacity Model with a Tunable Proportion of Load Redistribution against Cascading Failures
Zhen-Hao Zhang, Yurong Song, Lingling Xia, Yin-Wei Li, Liang Zhang, and Guo-Ping Jiang
Research Article (7 pages), Article ID 6254876, Volume 2018 (2019)

State-Based Switching for Optimal Control of Computer Virus Propagation with External Device Blocking
Qingyi Zhu, Seng W. Loke, and Ye Zhang
Research Article (10 pages), Article ID 4982523, Volume 2018 (2019)

Stability Analysis of an Advanced Persistent Distributed Denial-of-Service Attack Dynamical Model
Chunming Zhang and Jingwei Xiao
Research Article (10 pages), Article ID 5353060, Volume 2018 (2019)

Global Behavior of a Computer Virus Propagation Model on Multilayer Networks
Chunming Zhang
Research Article (9 pages), Article ID 2153195, Volume 2018 (2019)

An Epidemic Model of Computer Worms with Time Delay and Variable Infection Rate
Yu Yao, Qiang Fu, Wei Yang, Ying Wang, and Chuan Sheng
Research Article (11 pages), Article ID 9756982, Volume 2018 (2019)

Defending against the Advanced Persistent Threat: An Optimal Control Approach
Pengdeng Li, Xiaofan Yang, Qingyu Xiong, Junhao Wen, and Yuan Yan Tang
Research Article (14 pages), Article ID 2975376, Volume 2018 (2019)

Hindawi
Security and Communication Networks
Volume 2019, Article ID 6046353, 2 pages
https://doi.org/10.1155/2019/6046353

Editorial

Mathematical Models for Malware Propagation

Ángel Martín del Rey,[1] **Lu-Xing Yang**,[2] **and Vasileios A. Karyotis**[3]

[1] *University of Salamanca, Institute of Fundamental Physics and Mathematics, Department of Applied Mathematics, Salamanca 37007, Spain*
[2] *Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, 2600 GA Delft, Netherlands*
[3] *National Technical University of Athens, School of Electrical and Computer Engineering, Athens 157 80, Greece*

Correspondence should be addressed to Ángel Martín del Rey; delrey@usal.es

Received 19 December 2018; Accepted 20 December 2018; Published 2 January 2019

The dramatic increase of network services through the new paradigms such as cloud computing, Internet of Things, Industry 4.0, and critical infrastructures protection makes it necessary to develop tools and technologies to guarantee the security of digital data, processes, and networks against cyberattacks. These are becoming more and more sophisticated with the advent of advanced persistent threats.

Although the scientific approach to combat malware is mainly focused on the design of efficient methods to detect all types of malware, the design and computational implementation of mathematical models to simulate their spreading are also a very important task. These models allow us not only to predict the behavior of the evolution of malware, but also to study the efficacy of different possible countermeasures. As a consequence, these analytical tools could play a very important role in the forensic computing and cybercrime investigation as new techniques for the security operation centers.

The main goal of this special issue, which had opened for 8 months in the second half of 2017, is to investigate theoretical and practical aspects and design new applications in this research area.

Z.-H. Zhang et al. proposed a novel load capacity model against cascade failures considering clustering. The load redistribution strategy is a kind of nearest-neighbour redistribution methods, where the broken nodes allocate loads to their one-leap neighbours. Moreover, the strength of load redistribution proportion is governed by means of a tunable parameter. The model was simulated and analyzed on artificial and real networks of different type: ER random networks, BS scale-free networks, WS small-world networks, etc. These simulations suggested that networks with large average degree may be robust under the intentional attacks and highly clustered networks with the same degree distribution cannot guarantee the robustness.

Q. Zhu et al. introduced effective control strategies to control the virus spreading among computers and external devices using an optimal control approach: the external device blocking (that is, prohibiting a fraction of connections between external devices and computers) and computer reconstruction (including updating or reinstalling of some infected computers). Furthermore, this work took into account a state-based cost weight index in the objection functional instead of a fixed one and solved the problem by using Pontryagin's minimum principle and a numerical algorithm, respectively.

C. Zhang and J. Xiao proposed a novel dynamical model of an advanced persistent distributed denial-of-service attack (APDDoS) to analyze the behavior of an advanced persistent threat attack. It was a compartmental model where the devices are divided into weak-defensive computers (weak-defensive nodes and attacked devices) and strong-defensive computers (strong-defensive nodes and compromised nodes). The attacked threshold was derived and the global stability of the equilibrium points was studied.

Y. Yao et al. proposed a time-delayed worm propagation model considering variable infection rate. It was a compartmental model where susceptible, infectious, quarantined, vaccinated, and delay host were considered. The basic reproductive number was computed and a qualitative study was performed: the existence conditions and the stability of the unique positive equilibrium are derived by means of the

threshold of Hopf bifurcation. These results were numerically verified.

C. Zhang presented a computer virus propagation model on multilayer networks to understand the mechanism of computer virus spreading. It was a compartmental model where susceptible, latent, breaking out computers are considered. The author found out that the propagation threshold was the maximum eigenvalue of the sum of all the subnetworks on multilayer networks. The global stability of the virus-free equilibrium was studied and the persistence of the system was proved. These results were confirmed by means of extensive experiments.

Finally, P. Li et al. studied the effectiveness of advanced persistent threat (APT) defensive strategy which is quantified by considering a novel individual-level APT attack-defense model. Specifically, the APT defense problem was modeled as an optimal control problem and the existence of an optimal control was proven. The optimality system for the optimal control problem is derived. The influence of some factors on the effectiveness of an optimal control is analyzed through computer numerical simulations.

Conflicts of Interest

The editors declare that they have no conflicts of interest regarding the publication of this special issue.

Acknowledgments

We want to express our deepest gratitude to all authors for their excellent contributions and reviewers for their valuable help and suggestions. We also express our sincere thanks to the Editorial Board of SCN for their approval on this topic and their constant support in successful publication of this special issue. Finally, the Lead Guest Editor would like to show his great appreciation and to thank the two Guest Editors for their dedicated and excellent work.

Ángel Martín Del Rey
Lu-Xing Yang
Vasileios A. Karyotis

Hindawi
Security and Communication Networks
Volume 2018, Article ID 6254876, 7 pages
https://doi.org/10.1155/2018/6254876

Research Article

A Novel Load Capacity Model with a Tunable Proportion of Load Redistribution against Cascading Failures

Zhen-Hao Zhang,[1] **Yurong Song**,[2] **Lingling Xia**,[3] **Yin-Wei Li**,[1] **Liang Zhang**,[3] **and Guo-Ping Jiang**[2]

[1]*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China*
[2]*School of Automation, Nanjing University of Posts and Telecommunications, Nanjing, China*
[3]*Department of Computer Information and Cyber Security, Jiangsu Police Institute, Nanjing, China*

Correspondence should be addressed to Yurong Song; songyr@njupt.edu.cn

Received 10 April 2018; Accepted 13 May 2018; Published 7 June 2018

Academic Editor: Lu-Xing Yang

Defence against cascading failures is of great theoretical and practical significance. A novel load capacity model with a tunable proportion is proposed. We take degree and clustering coefficient into account to redistribute the loads of broken nodes. The redistribution is local, where the loads of broken nodes are allocated to their nearest neighbours. Our model has been applied on artificial networks as well as two real networks. Simulation results show that networks get more vulnerable and sensitive to intentional attacks along with the decrease of average degree. In addition, the critical threshold from collapse to intact states is affected by the tunable parameter. We can adjust the tunable parameter to get the optimal critical threshold and make the systems more robust against cascading failures.

1. Introduction

Cascading failures are ubiquitous phenomena in real life and often occur in many networks such as power grids, Internet, and transportation systems. In 2003, the largest power outage took place in North America, which just resulted from a broken-down power plant in Ohio [1]. Traffic paralysis of south China caused by storm in 2008 and Internet congestions [2] are typical examples of cascading failures as well. These incidents seriously affect people's life and threaten the stability of society. Therefore, more and more researchers come to investigate the issue from different perspectives.

There are several kinds of traditional models on researching cascading failures, respectively, known as the load capacity model [3], the double value impact model [4], the optimal power flow approach model [5], the sand pile model [6], the coupled map lattice model [7], and so on. Load capacity model [3] (ML model) proposed by Motter and Lai shows that, for such networks, where loads can redistribute to other nodes, intentional attacks can lead to a cascade of overload failures, which can in turn cause the entire or a substantial part of the network to collapse. To be more practical and reduce the collapse scale, scholars have put forward many cascading failures model based on ML model. Zhou et al. [8] deem that degrees of nodes in networks can to some extent reflect the processing ability and let nodes with both higher loads and larger degrees acquire more extra capacities. Sun et al. [9] propose a new matching model of capacity by developing a profit function to defence cascading failures on artificially created scale-free networks and the real network structure of the North American power grid. Fang et al. [10] investigate the cascading failures in directed complex networks and make a load redistribution rule of average allocation. Chen et al. [11] propose a nearest neighbours load redistribution model, where load of broken nodes is allocated to nearest neighbours according to their degrees. Wang et al. [12] propose a local load redistribution model. They adopt the initial load of node to be $L_j = \beta k_j^\alpha$ and the load redistribution proportion to be $P_{ji} = \beta k_i^\alpha / \sum_{n\in\Omega_j} \beta k_n^\alpha$, where

Ω_j denotes the neighbors set of broken node j. Wang et al. [13] consider that not all overload nodes will be removed from networks due to some effective measures to protect them and propose a new model with a breakdown probability. Also, they propose a new method considering neighbours' degrees for initiating loads, where the initial load of a node j is $L_j = (k_j \times (\sum_{m\in\Omega_j} k_m))^\alpha$ and the load redistribution proportion is $P_{ji} = (k_i \times (\sum_{m\in\Omega_i} k_m))^\alpha / \sum_{n\in\Omega_j}(k_n \times (\sum_{f\in\Omega_n} k_f))^\alpha$. Peng et al. [14] propose a renewed cascading failures model. In this model, the initial loads are defined as a nonlinear function of the generalized betweenness which is $L_j = (1+q)B_j^\alpha$. The redistribution strategy is $P_{ji} = B_i^\alpha / \sum_{n\in\Omega_j} B_n^\alpha$. The numeric value of betweenness centrality is proportional to that of degree with power exponent [2, 15, 16], so the definition of initial loads is substantially a nonlinear function of degree. Generally, we can conclude that initial loads are all defined as a function of degree. And the load redistribution proportion can be seen as a function of initial loads, where $P_{ji} = f(L_i)/\sum_{n\in\Omega_j} f(L_n)$ and $f(L_i) = L_i$. Actually, the load redistribution proportion [8–14] depends on the initial loads that reflect the load processing ability to some extent. Duan et al. [17, 18] explore the critical thresholds of scale-free networks against cascading failures and spatiotemporal tolerance after a fraction of nodes attacked with a tunable load redistribution model that can tune the load redistribution range and heterogeneity of the broken nodes. The initial load is assumed as $L_j = \rho k_j^\tau$. The redistribution strategy is global. They make l_{ji} denote the distance between broken node j and intact node i. The redistribution proportion is $P_{ji} = l_{ji}^{-\theta} k_i^\beta / \sum_{n\in\Omega_j} l_{jn}^{-\theta} k_n^\beta$. Likewise, the initial loads are defined as a function of degree, and the redistribution proportion can be concluded as a function of $P_{ji} = y(l_{ji}) f(L_i)/\sum_{n\in\Omega_j} y(l_{jn}) f(L_n)$, where $f(*)$ is a function of initial loads with a power exponent β/τ. And $y(*)$ is a function of distance, where $y(x) = x^{-\theta}$. Extending the redistribution range can improve the system robustness against cascading failures undoubtedly. However, this strategy is sometimes unpractical. Long distance load redistribution strategy costs too much in practical application and has high time complexity in computation. Recently, some scholars [19] pay attention to the application of load capacity model in information warfare and propose a cascading failures model for command and control networks with hierarchy structure.

The above scholars are devoted to improving robustness of networks from various points of view and have considered degree, betweenness, path length, and so on. However, scholars have not adopted clustering coefficient [20] into modelling cascading failures. Some researchers have recently investigated the effect of clustering coefficient [20] in the propagation of cascading failures. Zheng et al. [21] find that scale-free networks with larger clustering coefficient are sensitive and are prone to suffering from cascading failures. Ding et al. [22] explore the cascading failures in interconnected weighted networks and draw a conclusion that networks with smaller mean clustering coefficient have stronger ability to resist cascading failures. Eisenberg et al. [23] analyze the topology and resilience of the South Korea power grid. They discover that the power grid has a low efficiency and a high clustering coefficient, implying that highly clustered structure does not necessarily guarantee a functional efficiency of a network. Based on the error and attack tolerance analysis evaluated with efficiency, they find that the South Korea power grid is vulnerable to random or degree-based attacks. Likewise, Monfared et al. [24] investigate the structural properties of power transmission of Iran. The clustering coefficient displayed by Iranian power grid is much larger than that of corresponding random networks. Similarly, after studying the largest connected component of the network, they conclude that the power grid is vulnerable against cascading failures.

In this paper, we propose a novel load capacity model by considering clustering. The load redistribution strategy in our model is a kind of nearest neighbour redistribution methods, where the broken nodes allocate loads to their one-leap neighbours. We introduce a tunable parameter α to govern the strength of load redistribution proportion. By taking the robustness quantified as the critical threshold β_m, where a phase transition takes place from collapse to intact states, we investigate the relation between α and β_m on ER random graph networks [25], BA scale-free networks [26], WS small-world networks [20], North American power grid, and autonomous systems (AS) subnet topology. The simulation of the intentional attacks on a single node shows the nonmonotonic and nonlinear effect between the two parameters. We can control parameter α to adjust the proportion of load redistribution, thus reaching the optimal robustness of networks. Our simulations also suggest that networks with large average degree may be robust under the intentional attacks in our model, and highly clustered networks with the same degree distribution cannot guarantee the robustness. By contrast with another nearest neighbours load redistribution model [14], we verify the better performance of our model. Our model may further the research of controlling and defence against cascading failures in complex networks, which is constructive in designing infrastructure networks, such as power grid, logistics network systems, and communication networks.

2. Cascading Failures Model

For simplicity, we assume that the network is at the static state initially where the initial load of each node is less than its capacity and there are no broken nodes. After removal of one single node caused by intentional attacks, the balance among nodes will be changed. Therefore, the loads of the broken nodes will be redistributed to other nodes. In this paper, these nodes are one-leap neighbours of broken nodes. If some of these nodes do not have enough capacity to handle the extra load from the broken nodes, they will break down afterwards. In turn, these newly generated broken nodes will continue to allocate loads to their normal neighbours, triggering a collapse of partial nodes or even the whole network. This is the process of cascading failures under the frame of load capacity model [3].

Table 1: Relevant parameters of networks. N and M denote the numbers of nodes and links, respectively. $< k >$ denotes the average degree.

Name	N	M	$< k >$	Name	N	M	$< k >$
BA1	1000	2000	4	ER4	1000	5000	10
BA2	1000	3000	6	WS1	1000	2000	4
BA3	1000	4000	8	WS2	1000	3000	6
BA4	1000	5000	10	WS3	1000	4000	8
ER1	1000	2000	4	WS4	1000	5000	10
ER2	1000	3000	6	Power grid	4941	6594	2.67
ER3	1000	4000	8	AS	4158	13422	6.456

Here, we let the initial load of node j be a function of degree. The definition of the initial load of node j is as follows:

$$L_j^0 = \rho \left[k_j \times \left(\sum_{m \in \tau_j} k_m \right) \right], \quad j = 1, 2, \ldots N. \tag{1}$$

N is the number of nodes in the network. k_j is the degree of node j. ρ is a constant parameter that characters the strength of initial loads. τ_j is the set of node j's neighbours. The capacity of a node is the maximal load that the node can manage under the normal operation. The definition is as follows:

$$C_j = (1 + \beta) L_j^0. \tag{2}$$

β ($\beta \geq 0$) is the tolerance parameter. Generally, the tolerance parameter reveals the node's ability of defence against cascading failures. Evidently, the larger it is, the more robust the network is. However, improving the ability of tolerance at all costs is not reasonable. Here, we aim to seek the minimal β that we define as critical threshold β_m to get a balance between costs and robustness. Undoubtedly, reducing the critical threshold as much as possible is our ambition.

Considering that clustering coefficient plays a negative role in the propagation of cascading failures [21–24] and initial loads reflect the load processing ability to some extent [8–14, 17, 18], we make our redistribution strategy as follows:

$$P_{ji} = \frac{\left(g(cc_i) f\left(L_i^0\right) \right)^\alpha}{\sum_{n \in \Omega_j} \left(g(cc_n) f\left(L_n^0\right) \right)^\alpha}. \tag{3}$$

$$L_i \longleftarrow L_i + L_j \times P_{ji}. \tag{4}$$

The term cc_i denotes the clustering coefficient [20] of node i. The definition of clustering coefficient [20] of node i is as follows. E_i denotes the number of links among node i's neighbours. k_i is the degree of node i.

$$cc_i = \frac{2E_i}{k_i (k_i - 1)} \tag{5}$$

Function $f(*)$ is proportional to initial loads and in this paper we adopt the function $f(L_i^0) = L_i^0$ [12–14]. The function $g(cc_i)$ characters the negative effect of clustering coefficient [21–24] and is a decreasing function of clustering coefficient. When a node is broken, the neighbours will be redistributed the loads of the broken node. If the adjacent node has a higher clustering coefficient, it will be redistributed fewer loads from the broken node. We here adopt a simple exponential function, namely, $g(cc_i) = e^{-cc_i}$, a decreasing function of clustering coefficient. Actually, we can apply a more complicated form of $g(cc_i)$. However, a more complicated form of $g(cc_i)$ adds little value to characterize the effect of clustering coefficient but increases the computing complexity. In reality, the results and perspectives of our research are not limited by a specific function of clustering coefficient. Ω_j denotes the set of intact neighbours of node j. Here, node i is an element of the set. When node j breaks down, it will allocate its loads to intact neighbours at the certain proportion of P_{ji}. After getting the extra loads of node j, node i will break down if the updated loads exceed its capacity ($L_i > C_i$). In turn, node i will allocate its loads to intact neighbours, just as (3) and (4). The process will stop until the whole network breaks down or there are no newly generated broken nodes. The parameter α ($\alpha \geq 0$) is tunable. By controlling parameter α, we can adjust the proportion of load redistribution to reach the optimal robustness of networks at the lowest cost.

3. Simulations

In this section, we first investigate the relation between α and β_m on ER random graph networks [25], BA scale-free networks [26], WS small-world networks [20], North American power grid, and autonomous systems (AS) subnet topology. The average degrees of artificial networks are, respectively, four, six, eight, and ten. Fifty networks of the same average degree are generated, and the simulations are implemented in each network. Average results are shown in this paper. Relevant parameters of networks are shown in Table 1.

As triggered by the intentional attacks on a single node, cascading failures may probably spread to a certain scale. We calculate the proportion (see (6)) of broken nodes in the whole network to characterize the scale of cascading failures.

$$P = \frac{n_b}{N} \tag{6}$$

N denotes the number of nodes. n_b denotes the number of broken nodes. There is no doubt that if the tolerance parameter β is equal to zero, the proportion P is always equal to one. In this paper, we intend to attack the nodes of the largest degree and the node of the largest initial load. In

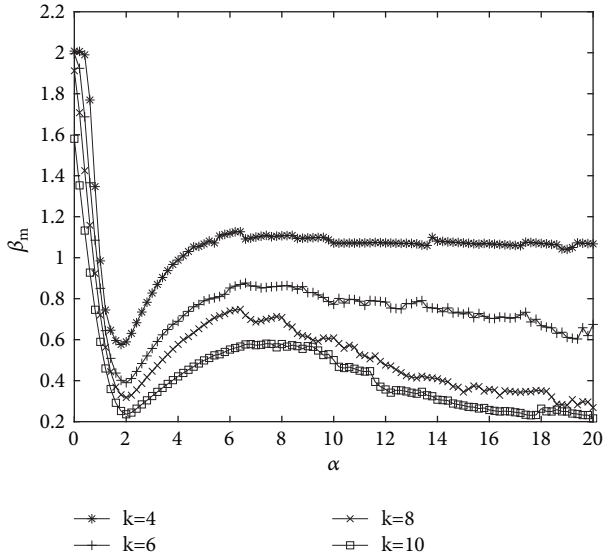


Figure 1: The relation between α and β_m in BA networks.

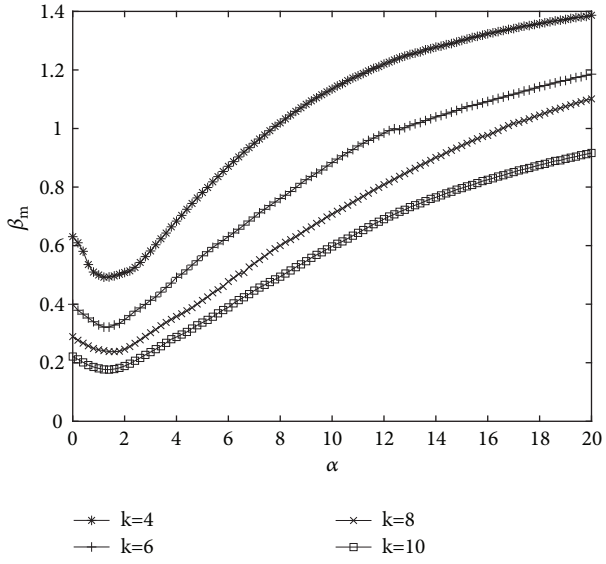


Figure 2: The relation between α and β_m in WS networks.

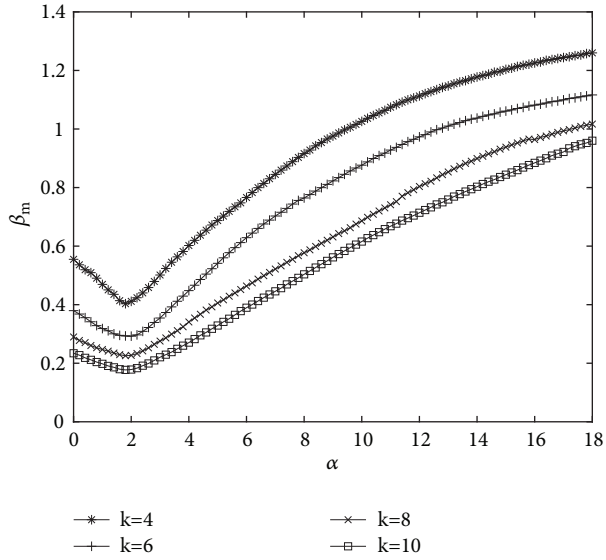


Figure 3: The relation between α and β_m in ER networks.

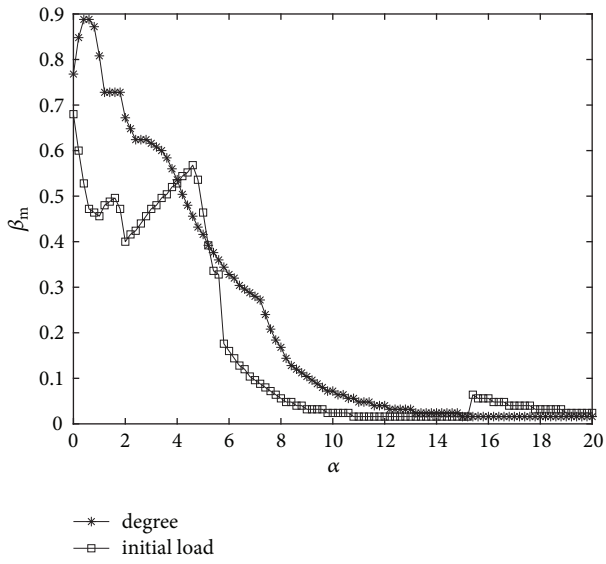


Figure 4: The relation between α and β_m in North American power grid after attacking the nodes of the largest degree and initial loads.

North American power grid, nodes of the largest degree and initial load are, respectively, No. 2554 and No. 4346. In other networks, the node of the largest degree is the same as the node of the largest initial load.

We then attack the above nodes in each network, and the relations between α and β_m are shown in Figures 1–5.

In Figures 1–5, each α corresponds to a critical threshold β_m. It is well known that the larger tolerance parameter β costs more. Therefore, we aim to seek the minimal tolerance parameter under the condition that the network is robust. We can get that optima for four BA networks are around $\alpha = 2$, where the minimum β_m exists. From Figure 1, we can also see that curves tend to be stable when $\alpha > 14$. This is easy to explain. When α is large enough, there is no numerically striking difference among the proportions of redistribution with the change of α, so the curves become stable. When scrutinizing the simulations of BA networks, we discover that β_m (s) are getting smaller with the increase of average degree, indicating that the network is getting robust in our model. If the average degree increases, the scope of load redistribution is actually extended. This situation reduces the probability that neighbours of broken nodes continue to get broken. Hence, the network gets robust with the increase of average degree in our model. When α approaches zero, we can see that β_m (s) of BA networks are evidently larger than those of WS and ER networks. This phenomenon is caused by the heterogeneity of scale-free networks. In BA networks, the heterogeneity of degree distribution makes the initial loads of some nodes large apparently. Therefore, the

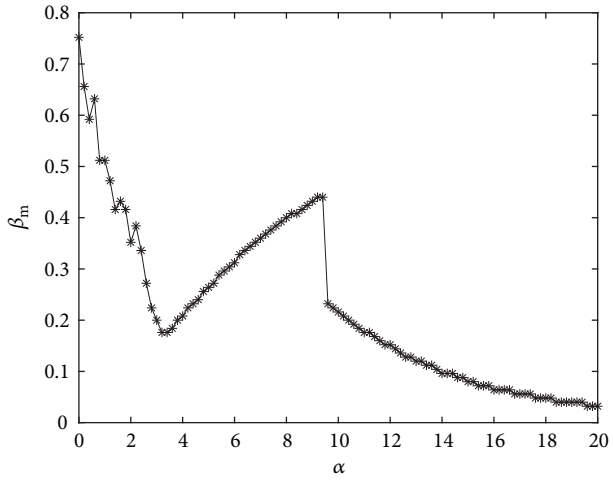


Figure 5: The relation between α and β_m in AS network.

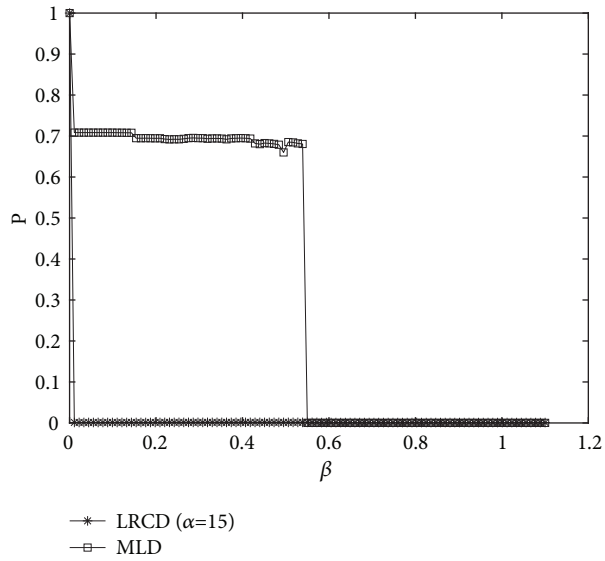


Figure 6: Attacking power grid based on the largest degree and initial load. LRCD (load redistribution based on clustering coefficient and degree) denotes our model. MLD denotes the nearest neighbours load redistribution model [14].

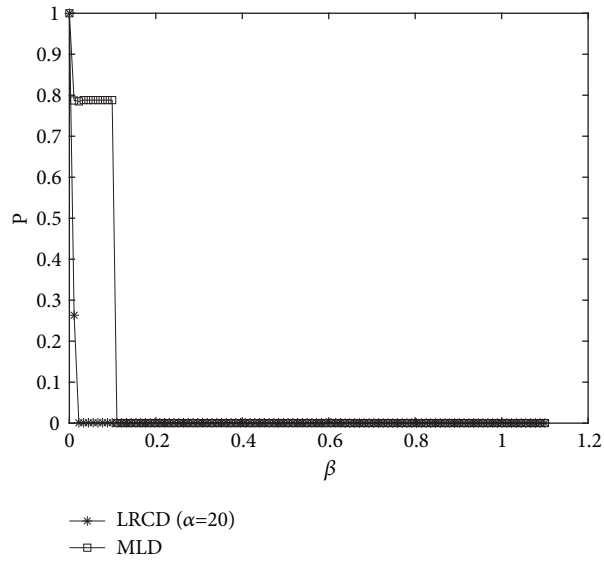


Figure 7: Attacking AS network. LRCD (load redistribution based on clustering coefficient and degree) denotes our model. MLD denotes the nearest neighbours load redistribution model [14].

minimal tolerance parameter β_m ought to be large enough to guarantee the robustness of networks when nodes of the largest degree and the largest initial load are attacked. Compared with critical thresholds of WS and ER networks with the same average degree, β_m of BA networks is smaller at the stable state. Similarly, the heterogeneity of scale-free networks contributes to the phenomenon. The broken nodes of BA networks have more neighbours than those of WS and ER networks, which means that there are more nodes to be redistributed loads from broken nodes. Therefore, the minimal tolerance parameter β_m (s) can be smaller.

The optima for WS networks and ER networks are, respectively, around $\alpha = 1.5$ and $\alpha = 2$. We may also discover a phenomenon that β_m (s) get smaller along with the increase of average degree, indicating that the WS and ER networks are getting robust in our model. Remarkably, the degree distributions of WS and ER networks are both Poisson distribution, and β_m (s) denoting the gentle pieces of curves of WS networks are not strikingly different from those of corresponding ER networks. Even β_m (s) of WS networks are sometimes larger than those of ER networks. Although WS network has the character of high clustering, it cannot guarantee the robustness of networks with the same degree distribution. This finding is coincident with the former research [21–24].

Figures 4-5 indicate that two curves of power grid and that of AS network topology do not have remarkable regularities but all present the declining trends. The optima are around $\alpha = 15$ and $\alpha = 20$, respectively. Figures 4-5 show the simulations on the real networks. Real networks are different from artificial networks, and their statistical characters are sometimes not technically subject to the corresponding network models. Therefore, the simulation curves are sometimes not smooth and sudden change may appear.

The above studies on the relation between α and β_m are from the macro perspective. To verify the better performance of our model, we will next concentrate on the relation between P and β to investigate the propagation process of cascading failures from the microscopic level. We compare our model with another nearest neighbour load redistribution model [14] on American power grid and autonomous systems (AS), using optimal α corresponding to minimal β_m. The simulations are shown in Figures 6-7.

From the simulations, we can see that β_m of our model is smaller, which means that our model decreases the critical threshold and makes it easier to acquire the robustness of networks. Dramatically, when applying our model into real networks, such as North American power grid and

autonomous systems, shown in Figures 6-7, we find that the phase transition from collapse to intact states takes place more quickly. Therefore, our model is more practical in applications and may inspire researchers to design more robust infrastructure systems against cascading failures when faced with the intentional attacks.

4. Conclusions

Nowadays, defence against cascading failures is a vital research, which contributes to operation of power grid, information security, efficiency of logistics networks, and so on. A novel load capacity model by considering clustering is proposed in this paper, aiming to get a smaller critical threshold and improve the robustness of networks. With the help of Monte Carlo simulations, the effectiveness of our model can be verified through comparison with a famous nearest neighbour load redistribution model [14]. The simulations suggest that our model is more practical in applications and may inspire researchers to design more robust infrastructure systems against cascading failures.

Data Availability

The North American power grid and autonomous systems (AS) subnet topology data used to support the findings of this study have been deposited in the website http://snap.stanford.edu/. ER random graph networks, BA scale-free networks, and WS small-world networks used to support the findings of this study are generated by the methods cited in [16, 24, 25].

Conflicts of Interest

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

Acknowledgments

This research has been supported by the National Natural Science Foundation of China (Grants [61672298], [61373136], and [61374180]), the National Social Science Foundation of China (Grant [13BTQ046]), and the High-Level Introduction of Talent Scientific Research Start-up Fund of Jiangsu Police Institute (Grant [JSPI17GKZL403]).

References

[1] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 69, no. 2, Article ID 025103, 2004.

[2] K.-I. Goh, B. Kahng, and D. Kim, "Universal behavior of load distribution in scale-free networks," *Physical Review Letters*, vol. 87, no. 27, Article ID 278701, 2001.

[3] M. E. J. Newman, S. Forrest, and J. Balthrop, "Email networks and the spread of computer viruses," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 66, no. 3, Article ID 035101, 4 pages, 2002.

[4] D. J. Watts, "A simple model of global cascades on random networks," *Proceedings of the National Acadamy of Sciences of the United States of America*, vol. 99, no. 9, pp. 5766–5771, 2002.

[5] I. Dobson, J. Chen, J. S. Thorp, B. A. Carreras, and D. E. Newman, "Examining criticality of blackouts in power system models with cascading events," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS '02)*, vol. 2, p. 63, January 2002.

[6] K. Goh, D. Lee, B. Kahng, and D. Kim, "Sandpile on scale-free networks," *Physical Review Letters*, vol. 91, no. 14, Article ID 148701, 2003.

[7] X. F. Wang and J. Xu, "Cascading failures in coupled map lattices," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 70, no. 5, Article ID 056113, 2004.

[8] P. Li, B.-H. Wang, H. Sun, P. Gao, and T. Zhou, "A limited resource model of fault-tolerant capability against cascading failure of complex network," *The European Physical Journal B*, vol. 62, no. 1, pp. 101–104, 2008.

[9] H. J. Sun, H. Zhao, and J. J. Wu, "A robust matching model of capacity to defense cascading failure on complex networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 387, no. 25, pp. 6431–6435, 2008.

[10] X. Fang, Q. Yang, and W. Yan, "Modeling and analysis of cascading failure in directed complex networks," *Safety Science*, vol. 65, pp. 1–9, 2014.

[11] W. X. Wang and G. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 77, no. 2, Article ID 026101, 2008.

[12] J.-W. Wang and L.-L. Rong, "Cascading failures on complex networks based on the local preferential redistribution rule of the load," *Acta Physica Sinica*, vol. 58, no. 6, pp. 3714–3721, 2009.

[13] J.-W. Wang and L.-L. Rong, "A model for cascading failures in scale-free networks with a breakdown probability," *Physica A: Statistical Mechanics and Its Applications*, vol. 388, no. 7, pp. 1289–1298, 2009.

[14] X. Z. Peng, H. Yao, J. Du, Z. Wang, and C. Ding, "Invulnerability of scale-free network against critical node failures based on a renewed cascading failure model," *Physica A: Statistical Mechanics and Its Applications*, vol. 421, pp. 69–77, 2015.

[15] K. I. Goh, B. Kahng, and D. Kim, "Packet transport and load distribution in scale-free network models," *Physica A: Statistical Mechanics & Its Applications*, vol. 318, no. 1-2, pp. 72–79, 2003.

[16] M. Barthélemy, "Betweenness centrality in large complex networks," *The European Physical Journal B*, vol. 38, no. 2, pp. 163–168, 2004.

[17] D.-L. Duan, X.-D. Ling, X.-Y. Wu, D.-H. Ouyang, and B. Zhong, "Critical thresholds for scale-free networks against cascading failures," *Physica A: Statistical Mechanics and Its Applications*, vol. 416, pp. 252–258, 2014.

[18] C. C. Lv, S. B. Si, and D. L. Duan, "Dynamical robustness of networks against multi-node attacked," *Physica A: Statistical Mechanics & Its Applications*, vol. 471, pp. 837–844, 2017.

[19] X. Gao, D. Zhang, K. Li, and B. Chen, "A cascading failure model for command and control networks with hierarchy structure," *Security and Communication Networks*, vol. 2018, Article ID 6063837, 14 pages, 2018.

[20] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[21] J.-F. Zheng, Z.-Y. Gao, and X.-M. Zhao, "Clustering and congestion effects on cascading failures of scale-free networks,"

Europhysics Letters. EPL, vol. 79, no. 5, Article ID 58002, 5 pages, 2007.

[22] C. Ding, H. Yao, J. Du, X. Peng, Z. Wang, and J. Zhao, "Cascading failure in interconnected weighted networks based on the state of link," *International Journal of Modern Physics C*, vol. 28, no. 3, 2017.

[23] D. H. Kim, D. A. Eisenberg, Y. H. Chun, and J. Park, "Network topology and resilience analysis of South Korean power grid," *Physica A: Statistical Mechanics & Its Applications*, vol. 465, pp. 13–24, 2017.

[24] M. A. S. Monfared, M. Jalili, and Z. Alipour, "Topology and vulnerability of the iranian power grid," *Physica A: Statistical Mechanics and Its Applications*, vol. 406, pp. 24–33, 2014.

[25] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publication of the Mathematical Institute of the Hungarian Academy Ofences*, vol. 38, no. 1, pp. 17–61, 2012.

[26] A.-L. Barabasi and R. Albert, "Emergence of scaling in random networks," *American Association for the Advancement of Science: Science*, vol. 286, no. 5439, pp. 509–512, 1999.

Hindawi
Security and Communication Networks
Volume 2018, Article ID 4982523, 10 pages
https://doi.org/10.1155/2018/4982523

Research Article

State-Based Switching for Optimal Control of Computer Virus Propagation with External Device Blocking

Qingyi Zhu,[1,2] **Seng W. Loke**,[2] **and Ye Zhang**[1]

[1]*School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, China*
[2]*School of Information Technology, Deakin University, Melbourne, VIC, Australia*

Correspondence should be addressed to Qingyi Zhu; zhuqy@cqupt.edu.cn

Received 21 February 2018; Accepted 30 April 2018; Published 30 May 2018

Academic Editor: Vasileios A. Karyotis

The rapid propagation of computer virus is one of the greatest threats to current cybersecurity. This work deals with the optimal control problem of virus propagation among computers and external devices. To formulate this problem, two control strategies are introduced: (a) external device blocking, which means prohibiting a fraction of connections between external devices and computers, and (b) computer reconstruction, which includes updating or reinstalling of some infected computers. Then the combination of both the impact of infection and the cost of controls is minimized. In contrast with previous works, this paper takes into account a state-based cost weight index in the objection function instead of a fixed one. By using Pontryagin's minimum principle and a modified forward-backward difference approximation algorithm, the optimal solution of the system is investigated and numerically solved. Then numerical results show the flexibility of proposed approach compared to the regular optimal control. More numerical results are also given to evaluate the performance of our approach with respect to various weight indexes.

1. Introduction

Computer virus, ranging from Morris worms in 1988 to WannaCry last year, can spread to every corner of our world via Internet in a very short time. The direct and indirect economic losses due to computer virus worldwide amount to as much as several billions and even tens of billions of dollars each year [1]. So a better understanding of the behaviors of virus propagation and predicting its outbreak are of crucial importance to thwart its wide spread. In this scenario, more and more attentions from worldwide scholars have been paid to the dynamical modeling of computer virus propagation through the classical epidemiology approach.

Depending on the topology of propagation networks, all current dynamical models of computer virus fall into two categories: homogeneous models and heterogeneous models [2]. Based on the fact that some virus can infect an arbitrary vulnerable computer through random scanning, the homogeneous models regard the propagation network as fully connected, such as the 1-n-n-1 type D-SEIR malicious propagation model proposed by Mishra et al. [3], SCIR model and SEIRS model proposed by Guillén et al. [4, 5], SLAR model by Dong et al. [6], SIP model proposed by Abazari et al. [7], SVEIR model proposed by Upadhyay et al. [8], and SLBS model proposed by Yang et al. [9, 10]. Instead, the heterogeneous model assumes that the virus could only spread between the direct topological neighbors. The dynamical behaviors of virus spreading over a reduced scale-free network are studied by L.-X. Yang and X. Yang [11] and Keshri et al. [12], respectively. By separating the susceptible compartment into two subcompartments, a heterogeneous WSI model is established and analyzed by Liu et al. [13]. In [14], both the topology of networks and the interaction between computer viruses and honeynet potency are considered. Both homogeneous and heterogeneous models provide significant insights into a detailed and qualitative understanding of how and when computer viruses break out.

The main purpose of modeling virus propagation dynamics is to develop appropriate strategies to suppress its diffusion. One of the most common control strategies is the application of optimal control in virus propagation model. From the perspective of economy, optimal control is used to seek a reasonable tradeoff between cost and benefit. In this context, it has been widely used in the control application of

biological viruses [15–19], rumors [20, 21], and others [22, 23]. Inspired by these, Zhu et al. proposed a delayed SIR model for computer virus propagation [24]. Then optimal control strategy is applied to other computer virus models such as the SLBS model [25] and its delayed form [26], the SIR model [27], and the SICS model on scale-free network [28].

In this paper, we aim to develop some effective strategies to control the virus propagation among computers and external devices using an optimal control approach. To achieve this, a classical model depicting the virus interactive dynamical behaviors between computers and external devices is adopted to formulate the optimal control problem [29]. Moreover, we note that most of current works assume that the weight indexes in their objective function are constant. In fact, the costs of some control strategies will change with the number of infected computers, because the required resources for the control will undoubtedly increase as more computers get infected. So, motivated by this fact and some related work in epidemiology [30], in this paper, we consider a state-based cost weight index in the objection function instead of a fixed one and solve this problem by using Pontryagin's minimum principle and a numerical algorithm, respectively.

The rest of this paper is organized as follows. By using Pontryagin's minimum principle, the optimal control problem is formulated and analyzed in Section 2. In Section 3, the numerical algorithm for the optimal system is given at first. Based on this algorithm, various examples are performed to evaluate the effectiveness of the proposed approach. Finally, this work is outlined in Section 4.

2. Formulation and Analysis of the Problem

In this paper, we take a classic computer virus propagation model [29], which incorporates the interactions between computers and external removable devices, to set our optimal control problem. In the model, all computers are split into the following three classes: susceptible computers (S), infected computers (I), and recovered computers (R), whereas all removable devices are divided into two compartments: susceptible devices (D_S) and infected devices (D_I). Under some reasonable assumptions (see [29]), one can derive the following computer virus propagation model:

$$\begin{aligned}
\dot{S} &= \lambda_1 - \beta_1 SI - \beta_2 S\frac{D_I}{D_N} - \mu_1 S,\\
\dot{I} &= \beta_1 SI + \beta_2 S\frac{D_I}{D_N} - (\mu_1 + \sigma_1) I,\\
\dot{R} &= \sigma_1 I - \mu_1 R,\\
\dot{D}_S &= \lambda_2 - \beta_2 D_S\frac{I}{N} + \sigma_2 D_I\frac{R}{N} - \mu_2 D_S,\\
\dot{D}_I &= \beta_2 D_S\frac{I}{N} - \sigma_2 D_I\frac{R}{N} - \mu_2 D_I.
\end{aligned} \tag{1}$$

And the definitions of notations and parameters are shown in "Definitions of Notations and Parameters in System (1)".

To formulate the optimal control problem of system (1), we introduce two types of countermeasures for inhibiting virus propagation: (a) external device blocking, which means prohibiting a fraction of connections between external devices and computers, and (b) computer reconstruction, which includes updating or reinstalling of some infected computers. Let $u_1(t)$ and $u_2(t)$ denote the control strengths of these two control strategies, respectively. And u_1 and u_2 are in the following two admissible control sets, respectively:

$$\begin{aligned}
u_1 \in U_1 \triangleq \{&u : u \text{ is Lebesgue integrable}, 0 \leqslant u \\
&\leqslant \Delta_1,\ \forall t \in [0, t_f]\},\\
u_2 \in U_2 \triangleq \{&u : u \text{ is Lebesgue integrable}, 0 \leqslant u \\
&\leqslant \Delta_2,\ \forall t \in [0, t_f]\},
\end{aligned} \tag{2}$$

where Δ_1, Δ_2, and t_f are positive constants. More specifically, Δ_1 and Δ_2 are the minimum allowed control strengths of u_1 and u_2, respectively. It is practical to set u_1 and u_2 to be bounded. For u_1, it is unrealistic to quarantine all external devices from computers. For u_2, the control strength is limited by resource capacity of computer reconstruction.

Then, by incorporating the above control variables, the state system corresponding to system (1) can be written as

$$\begin{aligned}
\dot{S} &= \lambda_1 - \beta_1 SI - (1 - u_1)\beta_2 S\frac{D_I}{D_N} - \mu_1 S + u_2 I,\\
\dot{I} &= \beta_1 SI + (1 - u_1)\beta_2 S\frac{D_I}{D_N} - (\mu_1 + \sigma_1) I - u_2 I,\\
\dot{R} &= \sigma_1 I - \mu_1 R,\\
\dot{D}_S &= \lambda_2 - (1 - u_1)\beta_2 D_S\frac{I}{N} + (1 - u_1)\sigma_2 D_I\frac{R}{N}\\
&\quad - \mu_2 D_S,\\
\dot{D}_I &= (1 - u_1)\beta_2 D_S\frac{I}{N} - (1 - u_1)\sigma_2 D_I\frac{R}{N} - \mu_2 D_I.
\end{aligned} \tag{3}$$

Compared to system (1), the infection of computers caused by the infective external devices is reduced to $(1 - u_1)\beta_2 S(D_I/D_N)$ in system (3) due to the introduction of u_1. Meanwhile, the recovered force of infective devices also decreases to $(1 - u_1)\sigma_2 D_I(R/N)$. And here u_2 denotes the fraction of reinstalled computers. Hence, on average, $u_2 I$ is the number of computers whose state changes to susceptible class from infected class per unit time.

Assume further that the control strategies will be applied if and only if the number of infected computers is above a threshold. Denote the threshold as I_m, where $I_m \geqslant 0$. To minimize the number of infected computers and external devices while keeping the cost of control as low as possible, we consider an optimal control problem to minimize the following objective function:

$$J(u_1, u_2, t_0, t_f) = \int_{t_0}^{t_f} g_1(v, t) + g_2(u_1, u_2, v, t)\,\mathrm{d}t, \tag{4}$$

where v is the solution of state system (1) computed at u_1 and u_2. Here $g_1(v,t)$ and $g_2(u_1,u_2,v,t)$ denote the infection index and the cost index, respectively. Furthermore, let w_1 and w_2 be the relative weights of computer and device infection, respectively, where $w_1, w_2 > 0$. Then we have

$$g_1(v,t) = w_1 I + w_2 D_I. \tag{5}$$

Considering the fact that the cost of the first strategy is independent of the infection individuals whereas the second is dependent on the number of infective computers I, we set the cost index $g_2(u_1,u_2,v,t)$ in the following form:

$$g_2(u_1,u_2,v,t) = \frac{1}{\kappa_1} p_1 u_1^{\kappa_1} + \frac{1}{\kappa_2} p_2(I)\, u_2^{\kappa_2}, \tag{6}$$

where both the positive constants κ_1 and κ_2 are set to be 2 in this paper, the positive constant p_1 is the relative cost weight associated with the control measure u_1, and $p_2(I)$ depending on I is the relative cost weight associated with the control measure u_2. For our purpose, we divide the interval $[I_m, +\infty)$ into Z subintervals $[I_i, I_{i+1})$, $i = 1,2,\ldots,Z$, $I_1 = I_m$, and $I_{Z+1} = +\infty$. Then the cost weight $p_2(I)$ can be set as

$$p_2(I) = \alpha_i, \quad \text{if } I \in [I_i, I_{i+1}), \text{ where } \alpha_i > 0,\ i = 1,2,\ldots,Z. \tag{7}$$

Considering the saturation effect that more cost should be paid to get the same result as the number of infected computers increases, we have $\alpha_1 < \alpha_2 < \cdots < \alpha_Z$ and the length of subintervals $I_2 - I_1 < I_3 - I_2 < \cdots < I_{Z+1} - I_Z$.

Here, for given t_0 and t_f, we have the following two cases.

Case 1 ($I(t_0) \geq I_m$). In this case, we find a nonnegative integer j ($j \leq Z$) such that $I(t_0) \in [I_j, I_{j+1})$ always holds for $t \in [t_0, t_1)$, and $t_1 \leq t_f$. Then one can obtain the following sub-objective-function:

$$J_k = \int_{t_k}^{t_{k+1}} w_1 I + w_2 D_I + \frac{1}{2} p_1 u_1^2 + \frac{1}{2} \alpha_j u_2^2 \mathrm{d}t, \quad \text{for } k = 0. \tag{8}$$

Case 2 ($I(t_0) < I_m$). For this case, there is nothing to do until $I(t_1) \geq I_m$ holds for some time t_1. Then go back to Case 1 to seek the optimal control for the minimum J_k for $k = 1$.

In this way, the interval $[t_0, t_f]$ has been divided into multiple subintervals $[t_k, t_{k+1})$. And $I(t_k)$ plays a role as a switch, determining whether the control should be applied. By iterating the above procedure until $t_{k+1} = t_f$ holds for some k, the optimal solution of state system (3) for $[t_0, t_f]$ can be obtained by composing the optimal solutions for all subintervals $[t_k, t_{k+1})$, where $I(t_k) \geq I_m$.

To solve the optimal problem for a subinterval $[t_k, t_{k+1})$, where $I(t_k) \geq I_m$, let η_i for $i = 1,2,\ldots,5$ denote the adjoint variables, let $u_1^*(t)$ and $u_2^*(t)$ denote the optimal control, let S^*, I^*, R^*, D_S^*, D_I^*, and η_i^* for $i = 1,2,\ldots,5$ denote the state and adjoint variables evaluated at $u_1^*(t)$ and $u_2^*(t)$. For applying Pontryagin's minimum principle, one can obtain the following Hamiltonian function:

$$\begin{aligned} H = {} & w_1 I + w_2 D_I + \frac{1}{2} p_1 u_1^2 + \frac{1}{2} \alpha_j u_2^2 + \eta_1 \left(\lambda_1 - \beta_1 SI \right. \\ & \left. - (1-u_1)\beta_2 S \frac{D_I}{D_N} - \mu_1 S + u_2 I \right) + \eta_2 \left(\beta_1 SI \right. \\ & \left. + (1-u_1)\beta_2 S \frac{D_I}{D_N} - (\mu_1 + \sigma_1) I - u_2 I \right) + \eta_3 (\sigma_1 I \\ & - \mu_1 R) + \eta_4 \left(\lambda_2 - (1-u_1)\beta_2 D_S \frac{I}{N} \right. \\ & \left. + (1-u_1)\sigma_2 D_I \frac{R}{N} - \mu_2 D_S \right) + \eta_5 \left((1-u_1)\beta_2 D_S \frac{I}{N} \right. \\ & \left. - (1-u_1)\sigma_2 D_I \frac{R}{N} - \mu_2 D_I \right). \end{aligned} \tag{9}$$

Then the adjoint system can be obtained as

$$\begin{aligned} \dot{\eta}_1^* &= -\left.\frac{\partial H}{\partial S}\right|_{S=S^*, I=I^*, R=R^*, D_S=D_S^*, D_I=D_I^*, u_{1,2}=u_{1,2}^*, \eta_i=\eta_i^*} \\ &= \left(\beta_1 I^* + (1-u_1^*)\beta_2 \frac{D_I^*}{D_N^*} \right)(\eta_1^* - \eta_2^*) + \mu_1 \eta_1^* \\ &\quad + (1-u_1^*)\left(\beta_2 D_S^* \frac{I^*}{N^{*2}} - \sigma_2 D_I^* \frac{R^*}{N^{*2}} \right)(\eta_5^* - \eta_4^*), \\ \dot{\eta}_2^* &= -\left.\frac{\partial H}{\partial I}\right|_{S=S^*, I=I^*, R=R^*, D_S=D_S^*, D_I=D_I^*, u_{1,2}=u_{1,2}^*, \eta_i=\eta_i^*} \\ &= -w_1 + (\beta_1 S^* - u_2^*)(\eta_1^* - \eta_2^*) + (\mu_1 + \sigma_1)\eta_2^* \\ &\quad - \sigma_1 \eta_3^* + (1-u_1^*)\left(\beta_2 D_S^* \frac{S^* + R^*}{N^{*2}} + \sigma_2 D_I^* \frac{R^*}{N^{*2}} \right) \\ &\quad \cdot (\eta_4^* - \eta_5^*), \\ \dot{\eta}_3^* &= -\left.\frac{\partial H}{\partial R}\right|_{S=S^*, I=I^*, R=R^*, D_S=D_S^*, D_I=D_I^*, u_{1,2}=u_{1,2}^*, \eta_i=\eta_i^*} \\ &= \mu_1 \eta_3^* + (1-u_1^*)\left(\beta_2 D_S^* \frac{I^*}{N^{*2}} + \sigma_2 D_I^* \frac{S^* + I^*}{N^{*2}} \right) \\ &\quad \cdot (\eta_5^* - \eta_4^*), \\ \dot{\eta}_4^* &= -\left.\frac{\partial H}{\partial R_S}\right|_{S=S^*, I=I^*, R=R^*, D_S=D_S^*, D_I=D_I^*, u_{1,2}=u_{1,2}^*, \eta_i=\eta_i^*} \\ &= (1-u_1^*)\beta_2 S^* \frac{D_I^*}{D_N^{*2}}(\eta_2^* - \eta_1^*) + \mu_2 \eta_4^* + (1-u_1^*) \\ &\quad \cdot \beta_2 \frac{I^*}{N^*}(\eta_4^* - \eta_5^*), \\ \dot{\eta}_5^* &= -\left.\frac{\partial H}{\partial R_I}\right|_{S=S^*, I=I^*, R=R^*, D_S=D_S^*, D_I=D_I^*, u_{1,2}=u_{1,2}^*, \eta_i=\eta_i^*} \\ &= -w_2 + (1-u_1^*)\beta_2 S^* \frac{D_S^*}{D_N^{*2}}(\eta_1^* - \eta_2^*) + (1-u_1^*) \\ &\quad \cdot \sigma_2 \frac{R^*}{N^*}(\eta_5^* - \eta_4^*) + \mu_2 \eta_5^*. \end{aligned} \tag{10}$$

By the optimal conditions, we have

$$\begin{aligned}
&\left.\frac{\partial H}{\partial u_1}\right|_{S=S^*,I=I^*,R=R^*,D_S=D_S^*,D_I=D_I^*,u_{1,2}=u_{1,2}^*,\eta_i=\eta_i^*} \\
&\quad = p_1 u_1^* + (\eta_1-\eta_2)\beta_2 S^* \frac{D_I^*}{D_N^*} \\
&\qquad + (\eta_4-\eta_5)\left(\beta_2 D_S^* \frac{I^*}{N^*} - \sigma_2 D_I^* \frac{R^*}{N^*}\right) = 0, \\
&\left.\frac{\partial H}{\partial u_2}\right|_{S=S^*,I=I^*,R=R^*,D_S=D_S^*,D_I=D_I^*,u_{1,2}=u_{1,2}^*,\eta_i=\eta_i^*} \\
&\quad = \alpha_j u_2^* + (\eta_1-\eta_2) I^* = 0,
\end{aligned} \tag{11}$$

which implies that

$$\begin{aligned}
u_1^* &= \max\left\{0, \min\left\{\Delta_1, \frac{(\eta_2-\eta_1)\beta_2 S^* D_I^*}{p_1 D_N^*} + \frac{\eta_5-\eta_4}{p_1 N^*}\left(\beta_2 D_S^* I^* - \sigma_2 D_I^* R^*\right)\right\}\right\}, \\
u_2^* &= \max\left\{0, \min\left\{\Delta_2, \frac{(\eta_2-\eta_1) I^*}{\alpha_j}\right\}\right\}.
\end{aligned} \tag{12}$$

Therefore, by combining state system (3), the adjoint system, and the optimal conditions, we have derived the following optimality system:

$$\begin{aligned}
\dot{S}^* &= \lambda_1 - \beta_1 S^* I^* - (1-u_1^*)\beta_2 S^* \frac{D_I^*}{D_N^*} - \mu_1 S^* + u_2^* I^*, \\
\dot{I}^* &= \beta_1 S^* I^* + (1-u_1^*)\beta_2 S \frac{D_I^*}{D_N^*} - (\mu_1+\sigma_1) I^* - u_2^* I^*, \\
\dot{R}^* &= \sigma_1 I^* - \mu_1 R^*, \\
\dot{D}_S^* &= \lambda_2 - (1-u_1^*)\beta_2 D_S^* \frac{I^*}{N^*} + (1-u_1^*)\sigma_2 D_I^* \frac{R^*}{N^*} - \mu_2 D_S^*, \\
\dot{D}_I^* &= (1-u_1^*)\beta_2 D_S^* \frac{I^*}{N^*} - (1-u_1^*)\sigma_2 D_I^* \frac{R^*}{N^*} - \mu_2 D_I^*, \\
\dot{\eta}_1^* &= \left(\beta_1 I^* + (1-u_1^*)\beta_2 \frac{D_I^*}{D_N^*}\right)(\eta_1^*-\eta_2^*) + \mu_1 \eta_1^* \\
&\quad + (1-u_1^*)\left(\beta_2 D_S^* \frac{I^*}{N^{*2}} - \sigma_2 D_I^* \frac{R^*}{N^{*2}}\right)(\eta_5^*-\eta_4^*), \\
\dot{\eta}_2^* &= -w_1 + (\beta_1 S^* - u_2^*)(\eta_1^*-\eta_2^*) + (\mu_1+\sigma_1)\eta_2^* - \sigma_1 \eta_3^* \\
&\quad + (1-u_1^*)\left(\beta_2 D_S^* \frac{S^*+R^*}{N^{*2}} + \sigma_2 D_I^* \frac{R^*}{N^{*2}}\right)(\eta_4^*-\eta_5^*), \\
\dot{\eta}_3^* &= \mu_1 \eta_3^* \\
&\quad + (1-u_1^*)\left(\beta_2 D_S^* \frac{I^*}{N^{*2}} + \sigma_2 D_I^* \frac{S^*+I^*}{N^{*2}}\right)(\eta_5^*-\eta_4^*), \\
\dot{\eta}_4^* &= (1-u_1^*)\beta_2 S^* \frac{D_I^*}{D_N^{*2}}(\eta_2^*-\eta_1^*) + \mu_2 \eta_4^* \\
&\quad + (1-u_1^*)\beta_2 \frac{I^*}{N^*}(\eta_4^*-\eta_5^*), \\
\dot{\eta}_5^* &= -w_2 + (1-u_1^*)\beta_2 S^* \frac{D_S^*}{D_N^{*2}}(\eta_1^*-\eta_2^*) \\
&\quad + (1-u_1^*)\sigma_2 \frac{R^*}{N^*}(\eta_5^*-\eta_4^*) + \mu_2 \eta_5^*, \\
u_1^* &= \begin{cases} 0 & \text{if } I^*(t_k) < I_m \\ a & \text{if } I^*(t_k) \geq I_m, \end{cases} \\
u_2^* &= \begin{cases} 0 & \text{if } I^*(t_k) < I_m \\ \max\left\{0, \min\left\{\Delta_2, \dfrac{(\eta_2-\eta_1) I^*}{\alpha_j}\right\}\right\} & \text{if } I^*(t_k) \geq I_m \end{cases}
\end{aligned} \tag{13}$$

with transversality conditions

$$\eta_i^*(t_{k+1}) = 0 \quad \text{for } i = 1, 2, \ldots, 5 \text{ if } I^*(t_k) \geq I_m, \tag{14}$$

where

$$\begin{aligned}
a = \max\Bigg\{&0, \\
&\min\left\{\Delta_1, \frac{(\eta_2-\eta_1)\beta_2 S^* D_I^*}{p_1 D_N^*} + \frac{\eta_5-\eta_4}{p_1 N^*}\left(\beta_2 D_S^* I^* - \sigma_2 D_I^* R^*\right)\right\}\Bigg\}.
\end{aligned} \tag{15}$$

3. Numerical Results and Discussion

In this section, some numerical results of the proposed optimal control strategies are evaluated. By using a modified forward and backward difference approximation algorithm shown in Algorithm 1, the optimality system can be solved numerically. For the sake of simplicity, the final number of all removable devices is normalized to unity, whereas the final number of all computers is normalized to ten as the assumption in [29]. For our purpose, some parameter values of the system used in the simulations are fixed in Table 1. And the initial conditions of the state system at t_0 are chosen as $S(0) = 5$, $I(0) = 1$, $R(0) = 0$, $R_S(0) = 0.5$, and $R_I(0) = 0.1$. In the first subsection, the performance of proposed optimal control strategies is evaluated by comparison with both regular optimal control and no control. And the effect of objective function weight indexes is evaluated in the second subsection.

Input: $S(t_0)$, $I(t_0)$, $R(t_0)$, $D_S(t_0)$, $D_I(t_0)$, w_1, w_2, p_1, ϵ, L, α_i and I_i
Output: u_1^* and u_2^*
Divide the $[t_0, t_f]$ into M subintervals $[t_k, t_{k+1})$ for $k = 0, 1, \ldots, M-1$.
for $k = 0$ **to** $M-1$ **do**
  $u_1^*, u_2^* \leftarrow 0, \forall t \in [t_k, t_{k+1})$
  if $I(t_k) < I_1$
    break
  else
    for $j = 1$ **to** Z **do** % *find index* j *of* α_j *for* $[t_k, t_{k+1})$
      if $I_j \le I(t_k)$ **and** $I_{j+1} \ge I(t_k)$
        $index \leftarrow j$
        break
      end if
    end for
    $\eta_i(t_{k+1}) \leftarrow 0$ for $i = 1, 2, \ldots, 5$
    $loop \leftarrow 0$
    do
      $\widetilde{u}_1 \leftarrow u_1^*, \widetilde{u}_2 \leftarrow u_2^*$
      $loop \leftarrow loop + 1$
      Calculate $S^*, I^*, R^*, D_S^*, D_I^*$ with $\widetilde{u}_1$ and $\widetilde{u}_2$ % *forward*
      Calculate η_i^* with $\eta_i(t_{k+1}) = 0$ for $i = 1, 2, \ldots, 5$ % *backward*
      Calculate u_1^*, u_2^* with α_{index}
    until $\sqrt{(u_1^* - \widetilde{u}_1)^2 + (u_2^* - \widetilde{u}_2)^2} < \epsilon$ **or** $loop > L$
    % ϵ *is a given sufficiently small positive constant*
    % L *is the maximum number of iterations*
  end if
end for

Algorithm 1: Algorithm of the optimal control.

3.1. Performance of Proposed Optimal Control. According to the problem formulation in Section 2, a simple form of piecewise weight index $p_2(I)$ is considered as follows:

$$p_2(I) = \begin{cases} \alpha_1 = 3000 & \text{for } I \in [y_1, y_2) = [2, 4), \\ \alpha_2 = 5000 & \text{for } I \in [y_2, +\infty) = [4, +\infty). \end{cases} \quad (16)$$

That is, no action is required in the slight infection phase with the infection number of computers less than the control threshold. Here the control threshold is set to be 2 (i.e., 20% in proportion). With the increase of the infected computers I, a more serious phase is reached, and the optimal control is employed with $p_2(I) = 3000$. When I is greater or equal to 4 (i.e., 40% in proportion), the most serious phase is reached; the optimal control is employed with $p_2(I) = 5000$. Moreover, other weight indexes are chosen as $w_1 = 10$, $w_2 = 5$, and $p_1 = 500$, and the control period is set as $t_0 = 0$ and $t_f = 60$.

In Figure 1, the evolution of both the optimal control and the infective proportion of computers is depicted. Obviously, the shape of the control signal u_2 is divided into 3 segments by switching based on the infection proportion of computers, which is defined in (16). And the shape of the control signal u_1 is divided into 2 segments as the device blocking control strategy is deployed with constant weight index if I exceeds the control threshold. Correspondingly, the controlled evolution of infective proportion of computers is split into 3 segments by 2 inflection points: the first segment performs exactly the same as the one without control, whereas the following two segments significantly lie below the one without control.

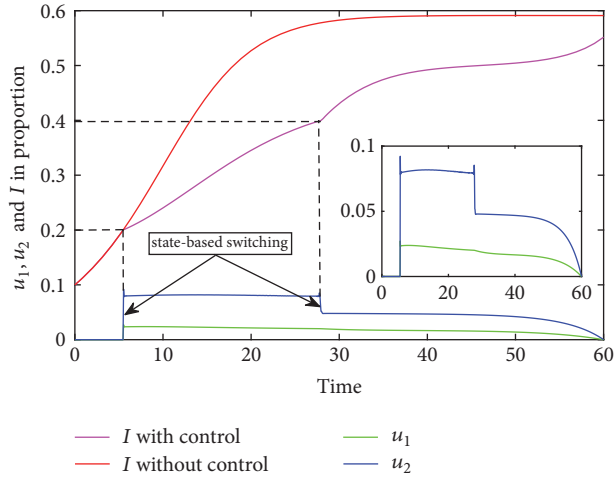


Figure 1: Optimal control with respect to I in proportion.

In order to examine the performance of proposed state-based switching control with respect to the regular optimal control, two solutions of regular optimal control with constant cost weight indexes $p_2 = 3000$ and $p_2 = 5000$ are considered, respectively, in Figures 2–5, while maintaining all other parameters the same as Figure 1.

Table 1: Parameter values used in the simulation.

Parameter	λ_1	λ_2	β_1	β_2	σ_1	σ_2	μ_1	μ_2	Δ_1	Δ_2
Values	1	0.1	0.035	0.1	0.02	0.005	0.1	0.1	0.1	0.1

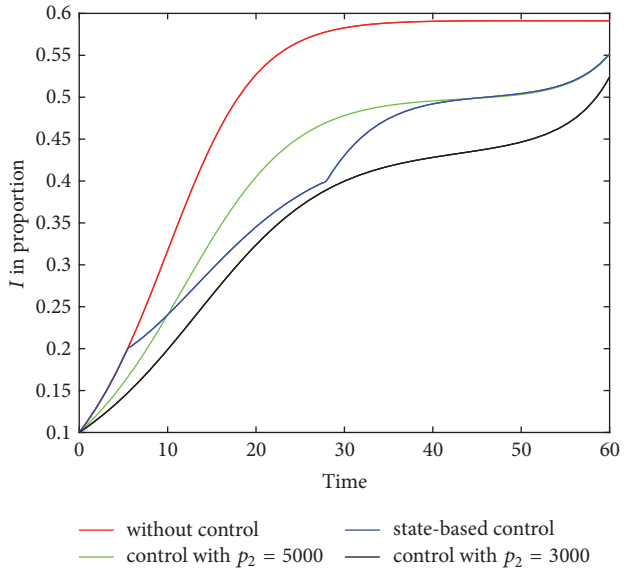


Figure 2: Comparison of I in proportion with different control approaches.

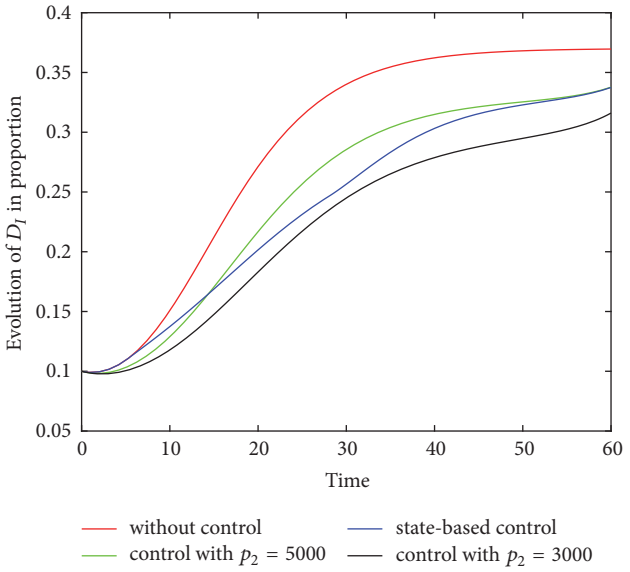


Figure 3: Comparison of D_I in proportion with different control approaches.

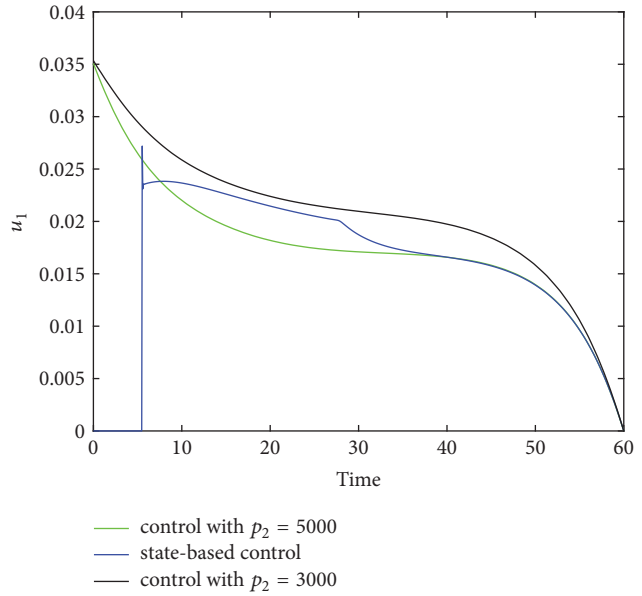


Figure 4: Comparison of u_1 with different control approaches.

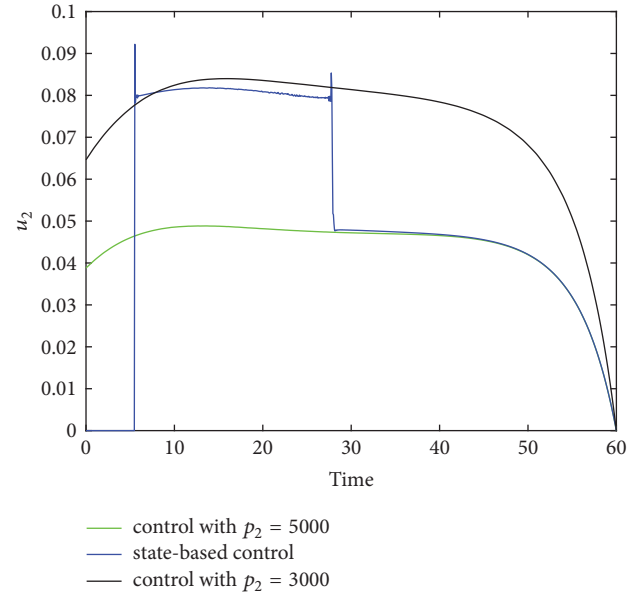


Figure 5: Comparison of u_2 with different control approaches.

Obviously, a lower cost weight index implies a heavier strength control force, which leads to a lower infective proportion. Hence, as shown in Figures 2 and 3, the infective proportions of both computers and devices with $p_2 = 3000$ always lie below the ones with $p_5 = 3000$. The evolution shapes of both computers and devices infective proportion with switching control are located above the other two shapes, respectively, in the initial period of time, because the control is not deployed when the infection proportion is small. Then, in the middle period of time, the evolution curve of the proportion of infected computers with switching control lies between the other two curves with $p_2 = 3000$ and $p_2 = 5000$. Similar observation for the evolution of the proportion of infected devices can be made in Figure 3. Instead, in the final

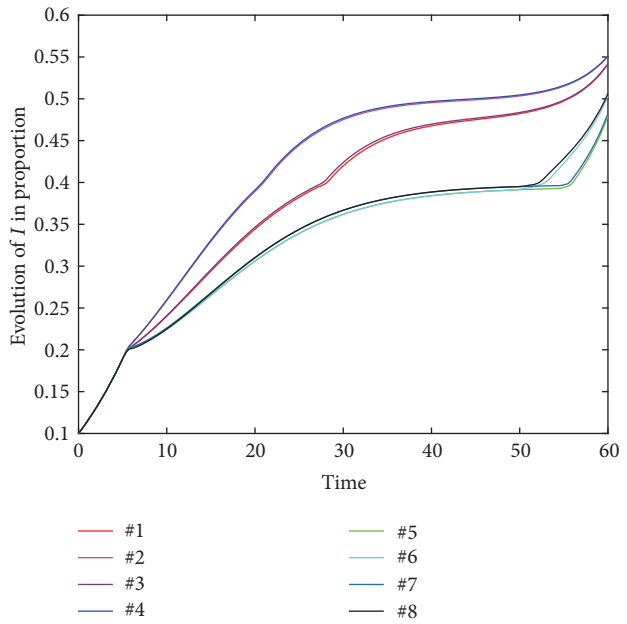


Figure 6: Comparison of I in proportion with different groups of weight indexes.

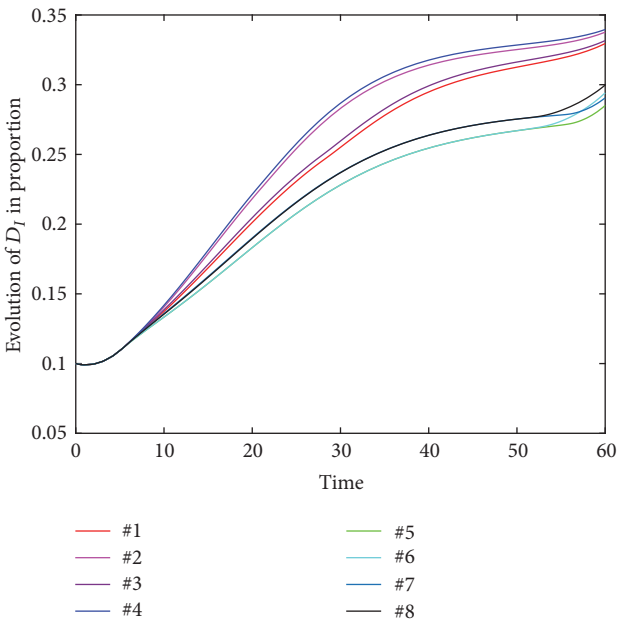


Figure 7: Comparison of D_I in proportion with different groups of weight indexes.

period of time, the evolution seems to act the same as the one with $p_5 = 3000$ due to the same weight index used in these two cases. The similar characteristics of evolution behaviors of both u_1 and u_2 can be observed from Figures 4 and 5.

In reality, when performing the same control force, more cost should be paid with the increase of the number of infection computers. So in the application of optimal control it is reasonable to assume that the cost weight index needs to be adjusted dynamically along with the evolution of infection nodes. The proposed optimal control approach provides a flexible solution to this kind of situation: the control is required if and only if the one infected is above the control threshold and a lower cost weight index should be applied with the further increase of infection. Also note that by setting $I_0 = 0$ and $I_1 = +\infty$ the proposed approach can be translated into the regular one. As a result, the proposed control strategies perform more reasonably and flexibly than regular optimal control with constant cost weight index.

3.2. Performance of Different Groups of Weight Indexes. In this subsection, 8 groups of numerical experiments are carried out to show the impacts of weight indexes on the solution of optimal control. The parameter values used here can be found in Table 1, and the weight indexes are shown in Table 2, where p_2 is of the same form as (16). All experimental results are shown in Figures 6–9. Then the following visually results can be obtained:

(1) The change of cost weight index p_1 has little effect upon the infection reduction, as the shapes of #1, #2, #5, and #6 are, respectively, close to shapes of #3, #4, #7, and #8 shown in Figures 6 and 7.

(2) Both the increase of index p_2 and the decrease of w_1 and w_2 have a remarkable effect on obtaining lower infection solution.

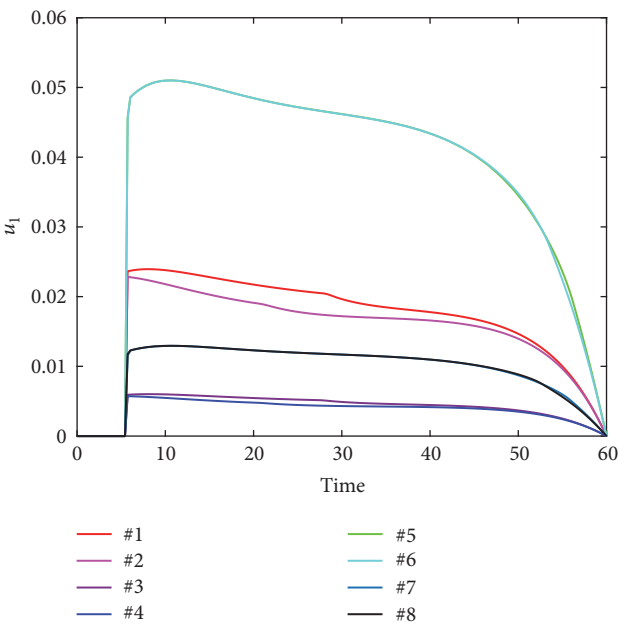


Figure 8: Comparison of u_1 in proportion with different groups of weight indexes.

(3) As shown in Figures 8 and 9, higher indexes p_1 and p_2 mean that weaker optimal controls of u_1 and u_2 will be applied, respectively.

Moreover, to further show the flexibility of the proposed approach, comparison experiments of various forms of p_2 are carried out as shown in Figures 10 and 11. Here, the forms of

Table 2: Combinations of different weight indexes.

Index	Cases							
	#1	#2	#3	#4	#5	#6	#7	#8
w_1	10	10	10	10	20	20	20	20
w_2	5	5	5	5	10	10	10	10
p_1	500	500	1000	1000	500	500	1000	1000
p_2								
α_1	3000	4000	3000	4000	3000	4000	3000	4000
α_2	4000	5000	4000	5000	4000	5000	4000	5000

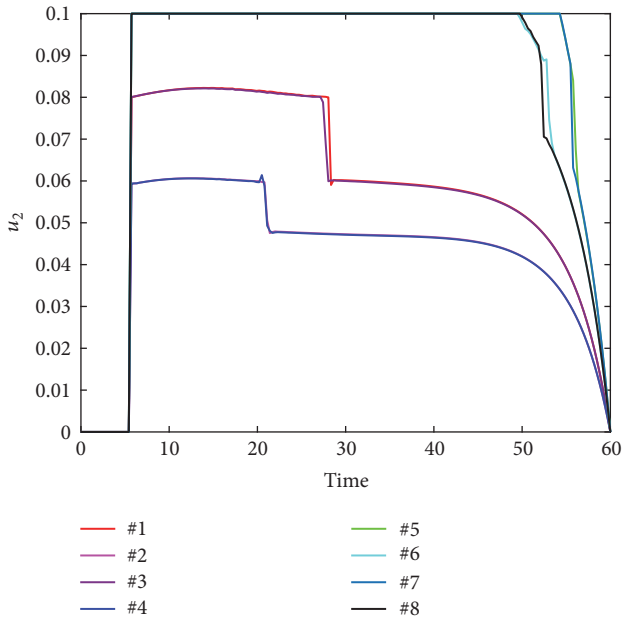


Figure 9: Comparison of u_2 in proportion with different groups of weight indexes.

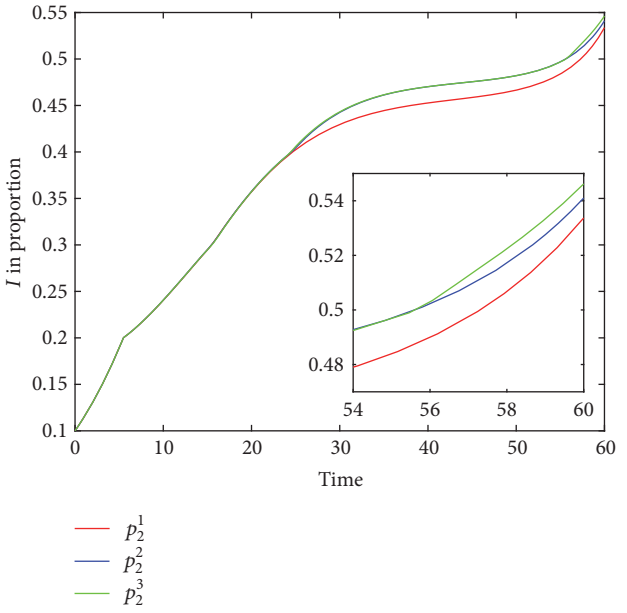


Figure 10: Comparison of I in proportion with different forms of p_2.

p_2 are chosen as follows, and other weight indexes are chosen as $w_1 = 10$, $w_2 = 5$, and $p_1 = 500$:

$$p_2^1(I) = \begin{cases} \alpha_1 = 3000 & \text{for } I \in [y_1, y_2) = [2, 3), \\ \alpha_2 = 3500 & \text{for } I \in [y_2, +\infty) = [3, +\infty), \end{cases}$$

$$p_2^2(I) = \begin{cases} \alpha_1 = 3000 & \text{for } I \in [y_1, y_2) = [2, 3), \\ \alpha_2 = 3500 & \text{for } I \in [y_2, y_3) = [3, 4), \\ \alpha_3 = 4000 & \text{for } I \in [y_3, +\infty) = [4, +\infty), \end{cases} \quad (17)$$

$$p_2^3(I) = \begin{cases} \alpha_1 = 3000 & \text{for } I \in [y_1, y_2) = [2, 3), \\ \alpha_2 = 3500 & \text{for } I \in [y_2, y_3) = [3, 4), \\ \alpha_3 = 4000 & \text{for } I \in [y_3, y_4) = [4, 5), \\ \alpha_4 = 5000 & \text{for } I \in [y_5, +\infty) = [5, +\infty). \end{cases}$$

3.3. Further Discussion. From the above experiments, we can conclude that (1) the proposed state-based optimal control

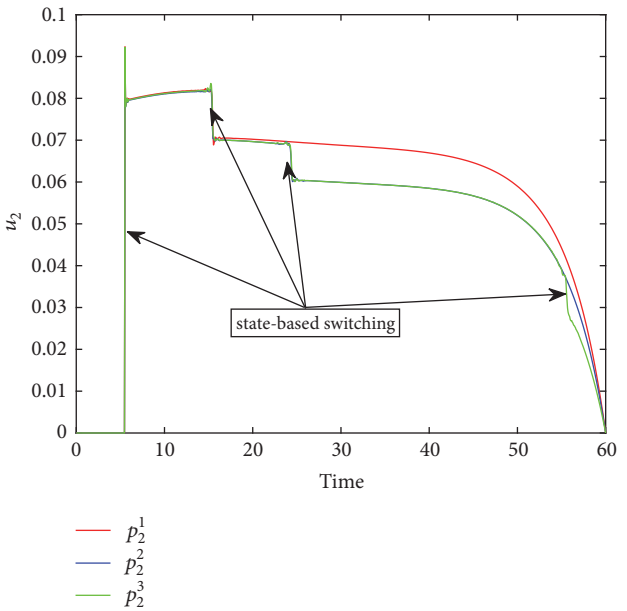


Figure 11: Comparison of u_2 with different forms of p_2.

approach can be applied to contain the spread of virus among computers and external devices; (2) the approach also performs more reasonably and flexibly compared to the conventional optimal control with constant coast weight index. We also note that the original model considered in this paper regards the propagation network as fully connected. However, as mentioned in Introduction, there are an increasing number of heterogeneous models that incorporate the impact of topology. Considering the similarity of applications of optimal control in heterogeneous models [31, 32], we can conclude that our proposed approach is also suitable for these models. In addition, this approach may provide some insights for other related fields such as rumor propagation [33] and marketing [34].

Although the efficiency of the proposed model has been verified by simulation, several issues still need to be settled when it is applied in reality. The first issue is how to determine the precise value of I_m. It may be a good way to obtain it from extensive simulation experiments.

4. Conclusion

In this work, we have formulated an optimal control problem to minimize the tradeoff between spread of virus and costs of control. Instead of a fixed cost weight index used in previous work, we adopted an infection state-based index. By using Pontryagin's minimum principle, the optimal control problem is analyzed. We also develop a modified forward-backward algorithm to calculate the optimal solution numerically. Finally, the flexibility and effectiveness of our proposed approach are verified by simulations. We will also consider exploring the ideas in strategic networks, with different topologies, and consider how to practically apply the ideas here.

Definitions of Notations and Parameters in System (1)

λ_1: The rate at which computers are connected to network
λ_2: The recruitment of external devices
β_1: The contact infective force between susceptible and infected computers
β_2: The contact infective force between computers and external devices
σ_1: The recovery rates of infective computers
σ_2: The recovery rates of external devices
μ_1: The rate at which networked computers are disconnected from network
μ_2: The rate at which removable devices break down
S: Short for $S(t)$, the number of susceptible computers at time t
I: Short for $I(t)$, the number of infected computers at time t
R: Short for $R(t)$, the number of recovered computers at time t
N: Short for $N(t)$, the total number of computers at time t, i.e., $N \equiv S + I + R$
D_S: Short for $D_S(t)$, the number of susceptible external devices at time t
D_I: Short for $D_I(t)$, the number of infective external devices at time t
D_N: Short for $D_N(t)$, the total number of external devices at time t, i.e., $D_N \equiv D_S + D_I$.

Data Availability

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 is supported by the National Natural Science Foundation of China (nos. 11747125, 61702066, and 61672004), Scientific and Technological Research Program of Chongqing Municipal Education Commission (no. KJ1500434), the Foundation from China Scholarship Council (201707845012), and Chongqing Engineering Research Center of Mobile Internet Data Application.

References

[1] Y. Wang, S. Wen, Y. Xiang, and W. Zhou, "Modeling the propagation of worms in networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 942–960, 2014.

[2] 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.

[3] B. K. Mishra, K. Haldar, and D. N. Sinha, "Impact of information based classification on network epidemics," *Scientific Reports*, vol. 6, Article ID 28289, 2016.

[4] J. D. H. Guillén, A. M. del Rey, and L. H. Encinas, "Study of the stability of a SEIRS model for computer worm propagation," *Physica A: Statistical Mechanics and its Applications*, vol. 479, pp. 411–421, 2017.

[5] J. D. Guillén and A. M. del Rey, "Modeling malware propagation using a carrier compartment," *Communications in Nonlinear Science and Numerical Simulation*, vol. 56, pp. 217–226, 2018.

[6] T. Dong, A. Wang, and X. Liao, "Impact of discontinuous antivirus strategy in a computer virus model with the point to group," *Applied Mathematical Modelling: Simulation and Computation for Engineering and Environmental Systems*, vol. 40, no. 4, pp. 3400–3409, 2016.

[7] F. Abazari, M. Analoui, and H. Takabi, "Effect of anti-malware software on infectious nodes in cloud environment," *Computers & Security*, vol. 58, pp. 139–148, 2016.

[8] R. K. Upadhyay, S. Kumari, and A. K. Misra, "Modeling the virus dynamics in computer network with SVEIR model and nonlinear incident rate," *Applied Mathematics and Computation*, vol. 54, no. 1-2, pp. 485–509, 2017.

[9] L.-X. Yang, X. Yang, L. Wen, and J. Liu, "A novel computer virus propagation model and its dynamics," *International Journal of Computer Mathematics*, vol. 89, no. 17, pp. 2307–2314, 2012.

[10] L.-X. Yang, X. Yang, Q. Zhu, and L. Wen, "A computer virus model with graded cure rates," *Nonlinear Analysis: Real World Applications*, vol. 14, no. 1, pp. 414–422, 2013.

[11] L.-X. Yang and X. Yang, "The spread of computer viruses over a reduced scale-free network," *Physica A: Statistical Mechanics and its Applications*, vol. 396, pp. 173–184, 2014.

[12] N. Keshri, A. Gupta, and B. K. Mishra, "Impact of reduced scale free network on wireless sensor network," *Physica A: Statistical Mechanics and its Applications*, vol. 463, pp. 236–245, 2016.

[13] W. Liu, C. Liu, X. Liu, S. Cui, and X. Huang, "Modeling the spread of malware with the influence of heterogeneous immunization," *Applied Mathematical Modelling: Simulation and Computation for Engineering and Environmental Systems*, vol. 40, no. 4, pp. 3141–3152, 2016.

[14] J. Ren and Y. Xu, "A compartmental model to explore the interplay between virus epidemics and honeynet potency," *Applied Mathematical Modelling: Simulation and Computation for Engineering and Environmental Systems*, vol. 59, pp. 86–99, 2018.

[15] S. Sharma, A. Mondal, A. K. Pal, and G. P. Samanta, "Stability analysis and optimal control of avian influenza virus A with time delays," *International Journal of Dynamics and Control*, pp. 1–16, 2017.

[16] D. P. Moualeu, M. Weiser, R. Ehrig, and P. Deuflhard, "Optimal control for a tuberculosis model with undetected cases in Cameroon," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 3, pp. 986–1003, 2015.

[17] K. O. Okosun and O. D. Makinde, "Optimal control analysis of hepatitis C virus with acute and chronic stages in the presence of treatment and infected immigrants," *International Journal of Biomathematics*, vol. 7, no. 2, Article ID 1450019, pp. 1–23, 2014.

[18] H. S. Rodrigues, M. T. Monteiro, and D. F. Torres, "Vaccination models and optimal control strategies to dengue," *Mathematical Biosciences*, vol. 247, pp. 1–12, 2014.

[19] A. Mojaver and H. Kheiri, "Dynamical analysis of a class of hepatitis C virus infection models with application of optimal control," *International Journal of Biomathematics*, vol. 9, no. 3, Article ID 1650038, pp. 1–23, 2016.

[20] K. Kandhway and J. Kuri, "Optimal control of information epidemics modeled as Maki Thompson rumors," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 12, pp. 4135–4147, 2014.

[21] L. Huo, T. Lin, C. Fan, C. Liu, and J. Zhao, "Optimal control of a rumor propagation model with latent period in emergency event," *Advances in Difference Equations*, vol. 54, no. 1, 2015.

[22] K. Kandhway and J. Kuri, "How to run a campaign: optimal control of SIS and SIR information epidemics," *Applied Mathematics and Computation*, vol. 231, pp. 79–92, 2014.

[23] P.-Y. Chen, S.-M. Cheng, and K.-G. Chen, "Optimal control of epidemic information dissemination over networks," *IEEE Transactions on Cybernetics*, vol. 44, no. 12, pp. 2316–2328, 2014.

[24] 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.

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

[26] L. Chen, K. Hattaf, and J. Sun, "Optimal control of a delayed SLBS computer virus model," *Physica A: Statistical Mechanics and its Applications*, vol. 427, pp. 244–250, 2015.

[27] L. H. Zhu and H. Y. Zhao, "Dynamical analysis and optimal control for a malware propagation model in an information network," *Neurocomputing*, vol. 149, pp. 1370–1386, 2015.

[28] X. Zhang and C. Gan, "Global attractivity and optimal dynamic countermeasure of a virus propagation model in complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 490, pp. 1004–1018, 2018.

[29] Q. Zhu, X. Yang, and J. Ren, "Modeling and analysis of the spread of computer virus," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 5117–5124, 2012.

[30] P. Di Giamberardino and D. Iacoviello, "Optimal control of SIR epidemic model with state dependent switching cost index," *Biomedical Signal Processing and Control*, vol. 31, pp. 377–380, 2017.

[31] 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.

[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] C. Pan, L.-X. Yang, X. Yang, Y. Wu, and Y. Y. Tang, "An effective rumor-containing strategy," *Physica A: Statistical Mechanics and its Applications*, vol. 500, pp. 80–91, 2018.

[34] P. Li, X. Yang, L.-X. Yang, Q. Xiong, Y. Wu, and Y. Y. Tang, "The modeling and analysis of the word-of-mouth marketing," *Physica A: Statistical Mechanics and its Applications*, vol. 493, pp. 1–16, 2018.

Hindawi
Security and Communication Networks
Volume 2018, Article ID 5353060, 10 pages
https://doi.org/10.1155/2018/5353060

Research Article

Stability Analysis of an Advanced Persistent Distributed Denial-of-Service Attack Dynamical Model

Chunming Zhang and Jingwei Xiao

School of Information Engineering, Guangdong Medical University, Dongguan 523808, China

Correspondence should be addressed to Chunming Zhang; chunfei2002@163.com

Received 27 December 2017; Accepted 22 April 2018; Published 24 May 2018

Academic Editor: Angel M. Del Rey

The advanced persistent distributed denial-of-service (APDDoS) attack is a fairly significant threat to cybersecurity. Formulating a mathematical model for accurate prediction of APDDoS attack is important. However, the dynamical model of APDDoS attack has barely been reported. This paper first proposes a novel dynamical model of APDDoS attack to understand the mechanisms of APDDoS attack. Then, the attacked threshold of this model is calculated. The global stability of attack-free and attacked equilibrium are both proved. The influences of the model's parameters on attacked equilibrium are discussed. Eventually, the main conclusions of the theoretical analysis are examined through computer simulations.

1. Introduction

Cyberattack has already become one of the greatest threats to cybersecurity [1–4]. With the rapid development of information technologies, a considerable number of cyberattack methods have been emerging in the past few decades, such as SQL injection (SQLi) attack, distributed denial-of-service (DDos) attack, targeted attack, and account hijackings [5]. In particular, DDoS attack has become one of the most popular methods of hackers due to its strong covertness and low cost. Recently, several cases have been widely reported; for instance, in November, 2016, five Russian banks have suffered a persistent DDoS attack for almost 12 hours, which caused unnumbered economic losses and social turbulence [6]. What is more, in August, 2017, Ukraine's national postal service has been hit by a two-day-long cyberattack [7].

Denial-of-service attack (DoS attack) is a cyberattack, where the attackers attempt to disrupt the servers which are going to respond to the requests. When these attacks of DoS attack originate from many different computers and networks, this attack mode can be referred to as distributed denial-of-service attack (DDoS attack). On the other hand, the dynamical models of advanced persistent threats (APTs) have already attracted the attention of researchers [8–12]. An advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity [13]. The computers with defensive ability in network cannot be successfully attacked easily by a standard DDoS attack (only DDoS attack once), which means that a standard DDoS attack does little harm to the network. But nowadays, there are numerous hackers with clear aim, well resource, and exceptional skills. Therefore, they are able to launch continuous and long-term attack, which is also called APDDoS attack in this paper. In this way, attackers of APDDoS attack would cause a bigger threat to cybersecurity [14].

Although the APDDoS attack has been mentioned in numerous papers [15–18], the dynamical models of APDDoS attack have rarely been reported yet. In this context, this paper proposes a dynamical model of APDDoS attack, which can help to figure out the mechanism of APDDoS attack.

In reality, different computer has different defensive ability. For example, the computer with low level of defensive ability is more likely to be attacked, while the high level of defensive ability makes the computer not be totally affected easily, so that the flooding attack is the only one way to attack the high-defensive computer. Hence, this paper divides the computers into two parts which are weak-defensive

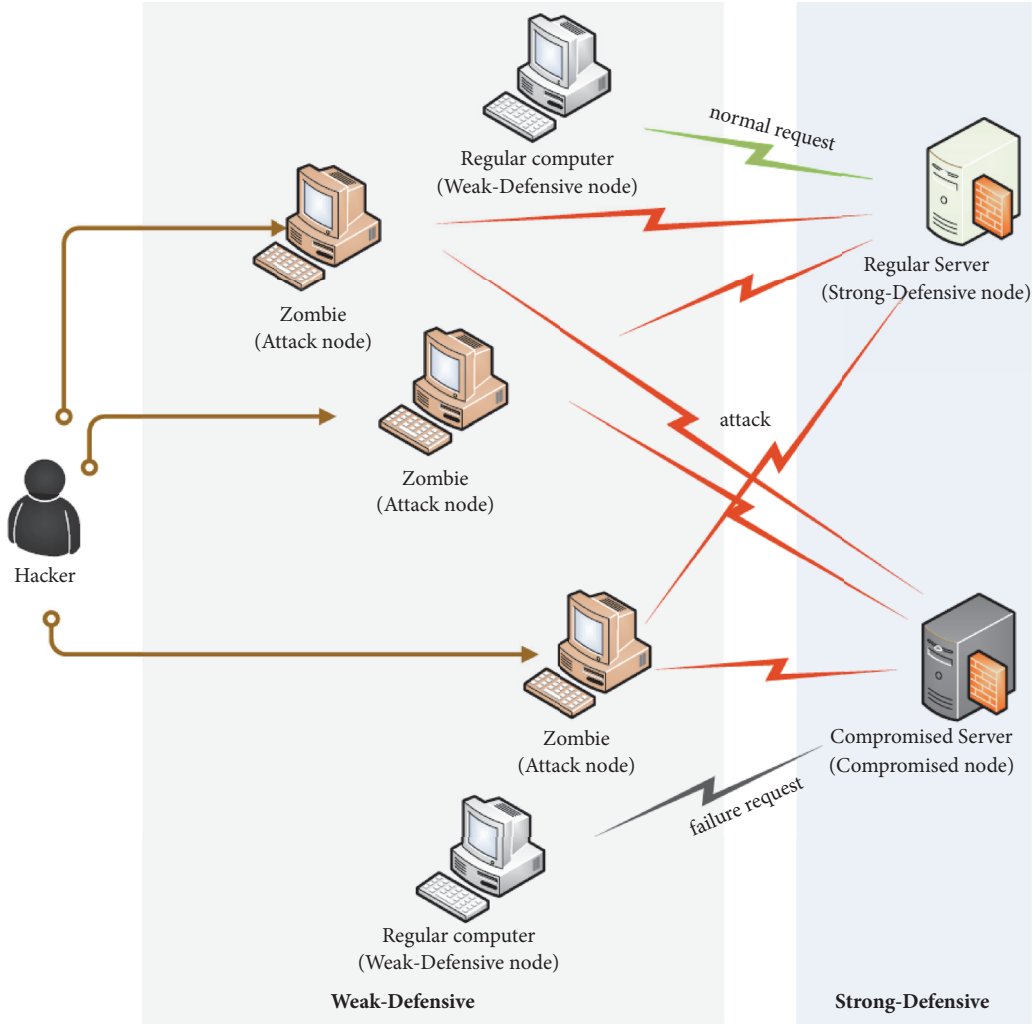


Figure 1: Schematic diagram of APDDoS attack.

computers and strong-defensive computers. Meanwhile, the procedures of APDDoS attack can be typically classified into two phases, including spreading computer worms and launching flooding attacks (see Figure 1).

(1) Spreading Computer Worms. As to infect more computers with low level of defensive ability, hackers are attempting to spread more computer worms on networks (such as Internet and WWW) by sending fake and malicious emails or links, which are going to lure people to click on them and thus lead them to visit virus websites and then download malware unconsciously. So, zombie in here is used to denote the infected computer or an infectious local network. Then, worms can also be diffused through the zombie to its neighbors under the control of the hackers.

(2) Launching Flooding Attacks. After successfully intruding the computer and gaining the control of zombies, the hackers will send instructions to the zombies so as to launch APDDoS attacks to computers with extraordinary high-defensive levels. Owing to the strong disruptive power of APDDoS attacks, some high-defensive computers will still be intruded and broken down. So, compromised computer is utilizing to represent the high-defensive computer, which has been broken down.

The rest of this paper is organized as follows. In Section 2, a dynamical model of APDDoS attack is proposed; then the model is analyzed in Section 3; some further discussions are provided in Section 4; finally, the summary of this paper is given in Section 5.

2. Model Description

This paper makes the hypothesis that computers can be classified into two parts: weak-defensive computers and strong-defensive computers.

The weak-defensive computers consist of two groups, weak-defensive nodes (not infected yet) and attacked nodes.

(i) Weak-defensive node, which has not been infected by worms or malwares yet, lacks in defending the malicious attacks, for existing some system vulnerabilities and device

defects or being without the defense of antivirus software. It is also called W node for short.

(ii) Attack node, the zombie that can infect other W nodes and launch attacks controlled by hackers, can be also represented by A node briefly.

The strong-defensive computers also can be divided into two groups, strong-defensive nodes (not compromised yet) and compromised nodes.

(i) Strong-defensive node, which provides considerable power of filtering and self-defensive ability, represents the computer with firewall equipped. In general, strong-defensive node acts as server in the network, and it is also called S node in this paper.

(ii) Compromised node, which denotes the state that S node becomes compromised and cannot respond to the requests after the attacks, is called C node in this paper.

Based on the above facts, the following assumptions can be obtained.

($H1$) The system is closed; the total number of systems is constant. Hence, $W(t) + A(t) + S(t) + C(t) \equiv 1$.

($H2$) Due to opening the phishing emails or text or performing some operations which would damage system security, W node is infected with the probability of β.

($H3$) Due to executing some positive measures, like reinstalling operation system, A node recovers with the probability of γ.

($H4$) Due to the APDDoS attacks, S node is compromised with the probability of α.

($H5$) With the assistance of firewall, p, used to describe the self-protection ability of S node, represents the ability of resisting attack of APDDoS. And $1/p$ should be proportional to the rate that S node compromised. Besides, p must be greater than 1.

($H6$) Due to some positive measures, like restarting the computer, C node turns to an S node with the probability of η.

($H7$) As the system is divided into two separated parts, the parameters ϕ and $1 - \phi$ are used to, respectively, denote the rate of the weak part and the strong part. So the following equations hold, $\phi = W(t) + A(t)$ and $1 - \phi = S(t) + C(t)$.

According to ($H1$)–($H7$), the following dynamical system is got (see Figure 2).

$$\begin{aligned}
\frac{dW(t)}{dt} &= -\beta W(t) A(t) + \gamma A(t), \\
\frac{dA(t)}{dt} &= \beta W A(t) - \gamma A(t), \\
\frac{dS(t)}{dt} &= -\frac{\alpha S(t) A(t)}{p} + \eta C(t), \\
\frac{dC(t)}{dt} &= \frac{\alpha S(t) A(t)}{p} - \eta C(t),
\end{aligned} \tag{1}$$

where $0 \le W(t), A(t) \le \phi$, $0 \le S(t), C(t) \le 1 - \phi$, and $0 \le \alpha, \beta, \gamma, \eta, \phi \le 1$.

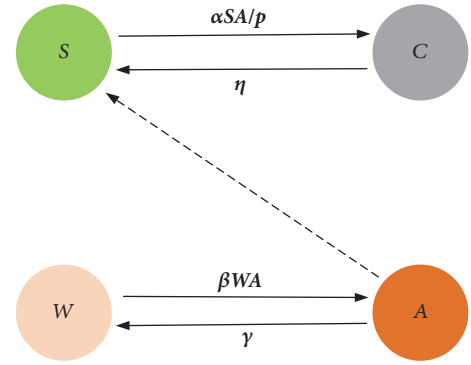


Figure 2: Status transition graph of the basic model (the dashed line on the graph means the attack from A node to S node).

3. Theoretical Analysis of the Dynamical Model

This section focuses on the mathematical properties of the dynamical model, such as equilibriums, threshold, and the local and global stability of system (1).

As $W(t) + A(t) = \phi$ and $S(t) + C(t) = 1 - \phi$, the equations of system (1) can be deduced into a two-dimensional system as follows:

$$\begin{aligned}
\frac{dA(t)}{dt} &= \beta(\phi - A(t)) A(t) - \gamma A(t), \\
\frac{dC(t)}{dt} &= \frac{\alpha(1 - \phi - C(t)) A(t)}{p} - \eta C(t),
\end{aligned} \tag{2}$$

where $0 \le A(t) \le \phi \le 1$ and $0 \le C(t) \le 1 - \phi \le 1$. The simply connected compact set can be obtained that $\Omega = \{(A(t), C(t)) \in R_+^2 : A(t) \in [0, \phi],\ C(t) \in [0, 1 - \phi]\}$.

Since system (1) and system (2) are equivalent, we are going to examine the properties of system (2).

3.1. Equilibriums

Theorem 1. *System (2) has a unique attack-free equilibrium E_0.*

Proof. Letting $A(t) = A_0 = 0$ and $C(t) = C_0 = 0$, then the unique attack-free equilibrium E_0 is shown as follows:

$$E_0 = (A_0, C_0)^T = (0, 0)^T. \tag{3}$$

□

Theorem 2. *System (2) has a unique attack-free equilibrium:*

$$E^* = (A^*, C^*) = \left(\phi - \frac{\gamma}{\beta}, \frac{\alpha(1 - \phi)(\beta\phi - \gamma)}{p\beta\eta + \alpha(\beta\phi - \gamma)}\right). \tag{4}$$

It is easy to prove, so the proof has been omitted here.

3.2. Attacked Threshold. In this paper, propagation threshold is a vital indicator that determines whether system will suffer APDDoS attack.

According to method described in Appendix, there are four statuses in system (1), so let

$$x = \left(x_1, x_2, x_3, x_4\right)^T = \left(A\left(t\right), C\left(t\right), W\left(t\right), S\left(t\right)\right)^T, \quad (5)$$

and the following vectors can be obtained that

$$F\left(x\right) = \begin{bmatrix} \beta x_1 x_3 \\ \dfrac{\alpha}{p} x_1 x_4 \\ 0 \\ 0 \end{bmatrix},$$

$$V^- = \begin{bmatrix} \gamma x_1 \\ \eta x_2 \\ \beta x_1 x_3 \\ \dfrac{\alpha}{p} x_1 x_4 \end{bmatrix}, \quad (6)$$

$$V^+ = \begin{bmatrix} 0 \\ 0 \\ \gamma x_1 \\ \eta x_2 \end{bmatrix},$$

which satisfies E_0 where ${x_1}^* = 0$, ${x_2}^* = 0$, ${x_3}^* = \phi$, ${x_4}^* = 1 - \phi$. So

$$\mathbf{F} = \begin{pmatrix} \beta x_3 & 0 \\ \dfrac{\alpha}{p} x_4 & 0 \end{pmatrix}, \quad (7)$$

$$\mathbf{V} = \begin{pmatrix} \gamma & 0 \\ 0 & \eta \end{pmatrix}.$$

Then $R_0 = \rho(\mathbf{F}\mathbf{V}^{-1}) = \phi\beta/\gamma$, where R_0 is strictly increasing with respect to the parameters ϕ and β and strictly decreasing with respect to γ.

Example 3. Fixing $\gamma = 0.3$ and changing the parameters β and ϕ, the value of R_0 is shown in Figure 3.

Example 4. Fixing the $\beta = 0.3$ and varying the parameters γ and ϕ, the value of R_0 is shown in Figure 4.

3.3. The Global Stability of Attack-Free Equilibrium

Theorem 5. *E_0 is globally asymptotically stable when $R_0 < 1$.*

Proof. Consider the following Lyapunov function with an undermined coefficient

$$V\left(A\left(t\right), C\left(t\right)\right) = A\left(t\right) + \frac{1}{2}\kappa C\left(t\right)^2, \quad (8)$$

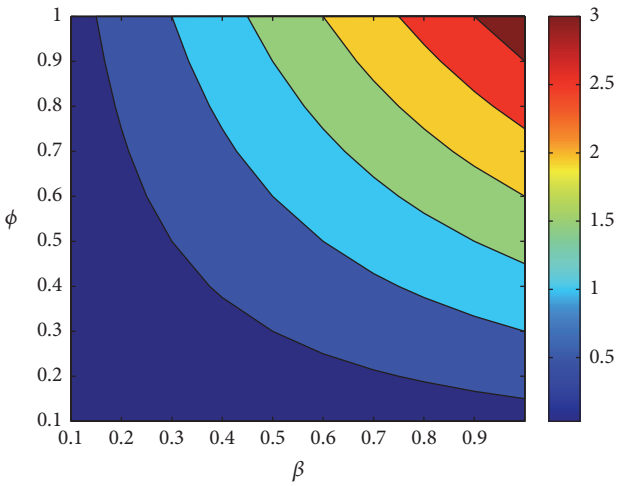


Figure 3: Example 3.

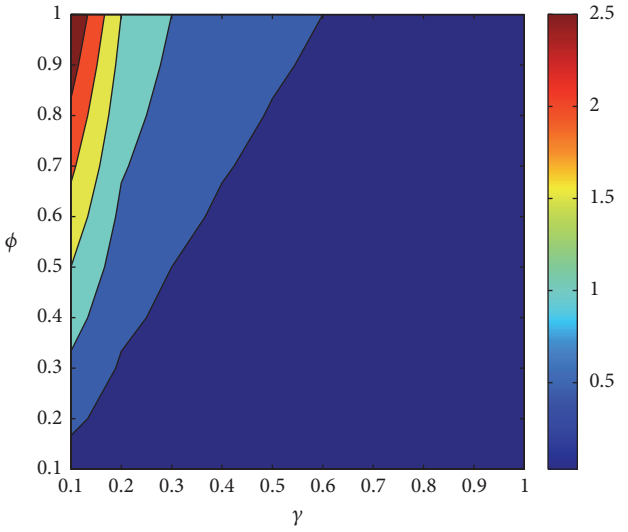
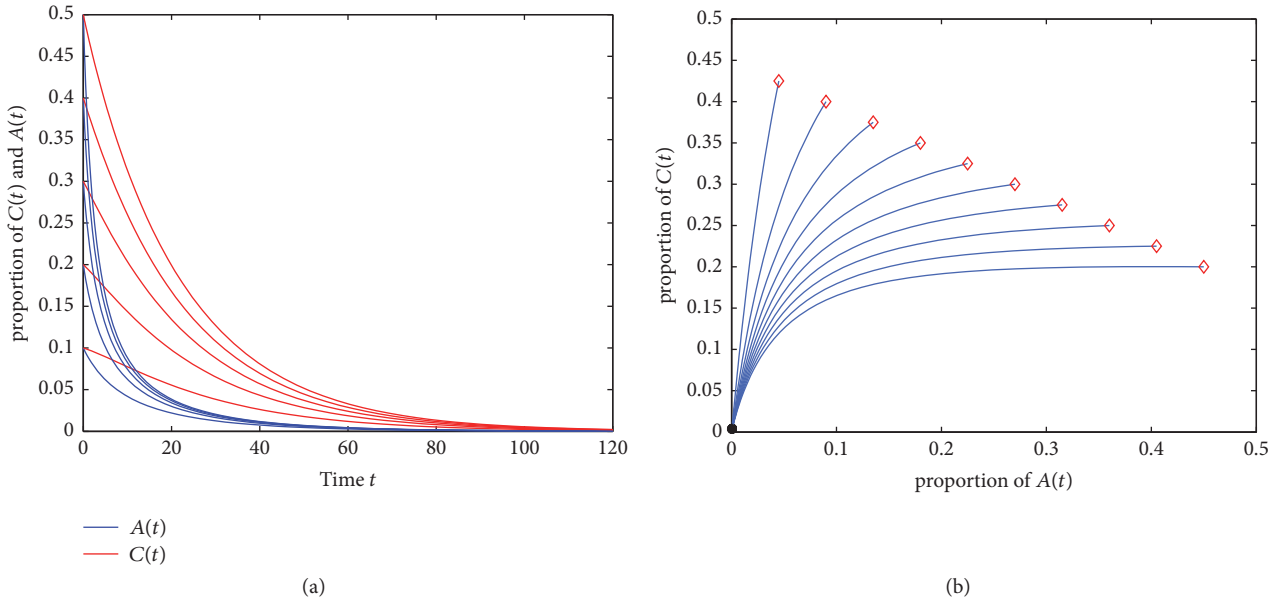


Figure 4: Example 4.

where κ is a positive constant to be determined. Besides, $A(t) \geq 0$ and $C(t) \geq 0$, so V is nonnegative.

The time derivative of V along an orbit of system (2) is

$$\begin{aligned} \frac{\mathrm{d}V}{\mathrm{d}t} &= A' + \kappa CC' \\ &= \beta\left(\phi - A\right)A - \gamma A \\ &\quad + \kappa C\left[\frac{\alpha\left(1 - \phi - C\right)}{p}A - \eta C\right] \\ &= \left(\beta\phi - \gamma\right)A - \beta\left[A^2 - \kappa\frac{\alpha\left(1 - \phi\right)}{p\beta}CA + \frac{\kappa\eta}{\beta}C^2\right] \\ &\quad - \frac{\alpha\kappa}{p}AC^2. \end{aligned} \quad (9)$$



(a) (b)

FIGURE 5: (a) and (b) represent the variety of the proportion of $C(t)$ and $A(t)$ in different initial conditions by time-varying diagram and phase diagram, respectively.

As $R_0 = \phi\beta/\gamma < 1$, then $\beta\phi - \gamma < 0$ and $(\beta\phi - \gamma)A(t) \leq 0$ are obtained. And another part, $\beta[A^2 - \kappa(\alpha(1-\phi)/p\beta)CA + (\kappa\eta/\beta)C^2]$, can be deduced into

$$\beta\left(A - \frac{\kappa\alpha(1-\phi)}{2p\beta}C\right)^2 - \beta\left[\left(\frac{\kappa\alpha(1-\phi)}{2p\beta}\right)^2 - \frac{\kappa\eta}{\beta}\right]C^2. \tag{10}$$

Obviously, $\beta(A - (\kappa\alpha(1-\phi)/2p\beta)C)^2 \geq 0$. When

$$\left(\frac{\kappa\alpha(1-\phi)}{2p\beta}\right)^2 - \frac{\kappa\eta}{\beta} \leq 0, \tag{11}$$

then the inequality $\beta[A^2 - \kappa(\alpha(1-\phi)/p\beta)CA + (\kappa\eta/\beta)C^2] \geq 0$ holds.

Considering inequality (11), let $\kappa = 4\eta p^2/\alpha^2(1-\phi)^2 > 0$, so $(\kappa\alpha(1-\phi)/2p\beta)^2 - \kappa\eta/\beta = 0$. Finally, the remaining part, $(\alpha\kappa/p)AC^2$, is nonnegative, for $\kappa > 0$. Hence, only if $A(t) = C(t) = 0$, that $(A(t), C(t))^T \in E_0$, $dV/dt = 0$. $dV/dt < 0$, when $(A(t), C(t))^T \in \Omega - E_0$. The result confirms the stability principle in [19].

The proof is completed. □

Example 6. In system (2) with $\alpha = 0.1$, $\gamma = 0.37$, $\eta = 0.05$, $\beta = 0.65$, $\phi = 0.5$, $p = 1.2$, where $R_0 = 0.8784 < 1$, computers will not suffer from APDDoS attacks and the attack-free equilibrium is globally asymptotically stable (see Figure 5).

3.4. The Global Stability of Attacked Equilibrium. Firstly, the local stability of attacked equilibrium of system (2) will be demonstrated.

Lemma 7. *E^* is locally asymptotically stable when $R_0 > 1$.*

Proof. The Jacobian of the linearized system (2) evaluated at E^* is as follows:

$$J = \begin{pmatrix} \beta\phi - 2\beta A^* - \gamma & 0 \\ -\dfrac{\alpha(1-\phi-C^*)}{p} & -\left(\dfrac{\alpha A^*}{p} + \eta\right) \end{pmatrix}, \tag{12}$$

and the corresponding characteristic equation is

$$[\lambda - (\beta\phi - 2\beta A^* - \gamma)]\left[\lambda + \left(\frac{\alpha A^*}{p} + \eta\right)\right] = 0. \tag{13}$$

Clearly, two roots of (13) are $\lambda_1 = -\alpha A^*/p - \eta$ and $\lambda_2 = \beta\phi - 2\beta A^* - \gamma$, so the possibility of these two roots will be discussed next. As $A^* = \phi - \gamma/\beta > 0$, it is easy to get that $\lambda_1 < 0$. Besides, the equation of λ_2 can be rewritten into $\lambda_2 = -\beta\phi + \gamma$ and $\lambda_2 < -1 < 0$, for $R_0 = \beta\phi - \gamma > 1$. Hence, the two roots of (13) both have negative real parts. Further, the conclusion of this result follows by the Lyapunov theorem, conforming to the Hurwitz criterion [19].

The proof is completed. □

Second, the global behaviors of the equilibrium of E^* will be examined.

Lemma 8. *The simplified system admits no periodic orbit in the interior of Ω [20].*

Proof. Let

$$f_1(x) = \beta(\phi - A(t))A(t) - \gamma A(t),$$
$$f_2(x) = \frac{\alpha(1-\phi-C(t))}{p}A(t) - \eta C(t). \tag{14}$$

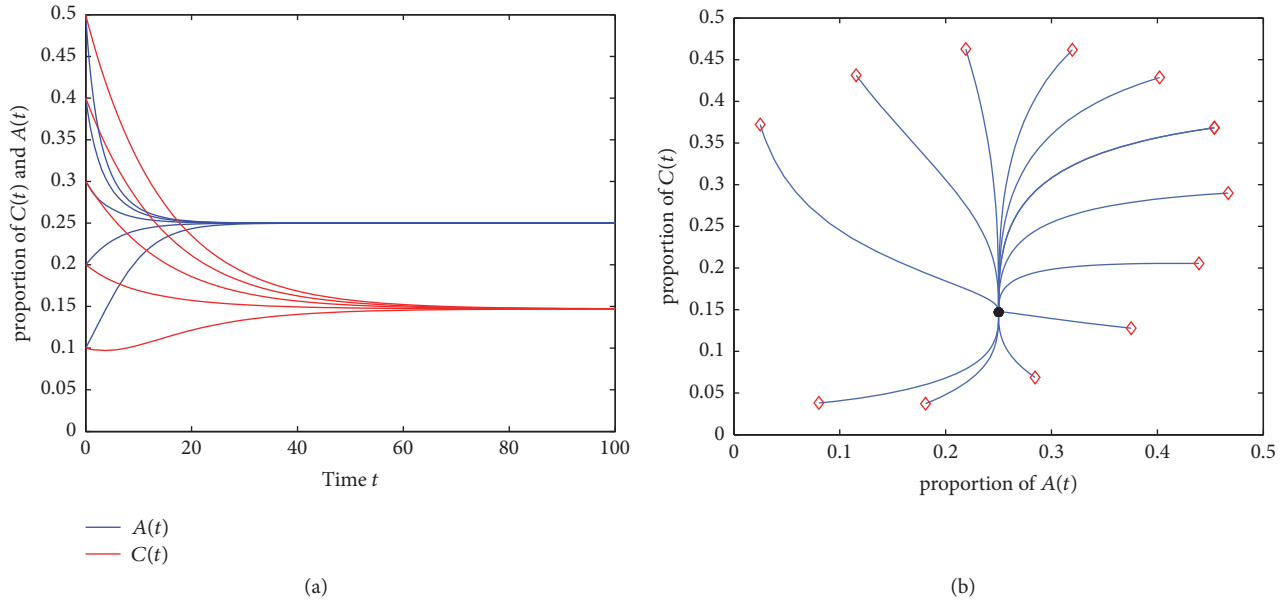


FIGURE 6: (a) and (b) represent the variety of proportion of $C(t)$ and $A(t)$ in different initial conditions by time-varying diagram and phase diagram, respectively.

Define $D(A, C) = 1/A$; then

$$\frac{\partial (Df_1)}{\partial L} + \frac{\partial (Df_2)}{\partial A} = -\beta - \frac{\alpha}{p} - \frac{\eta}{A} < 0. \tag{15}$$

The result follows the Bendixson–Dulac criterion [20]. □

Lemma 9. *System (2) admits no periodic orbit that passes through a point on $\partial\Omega$, that is the boundary of Ω.*

Proof. As for the smoothness of all orbits of system (2), all conditions can be enumerated as follows.

(a) There is no periodic orbit that passes through a corner of Ω, i.e., either $(0, 0)$ or $(\phi, 0)$ or $(0, 1-\phi)$, or $(\phi, 1-\phi)$.

(b) If there is a periodic orbit passes through a noncorner point on $\partial\Omega$, then this orbit must be tangent to $\partial\Omega$ at this point. □

On the contrary, suppose that there is a periodic orbit Γ that passes through a noncorner point $(\overline{A}, \overline{C})$ on $\partial\Omega$; then there are four possibilities.

Case 1. $0 < \overline{A} < \phi, \overline{C} = 0$. Then $\mathrm{d}C/\mathrm{d}t|_{(\overline{A},\overline{C})} = (\alpha(1-\phi)/p)\overline{A} > 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which leads to a contradiction.

Case 2. $0 < \overline{C} < 1-\phi, \overline{A} = 0$. Then $\mathrm{d}A/\mathrm{d}t|_{(\overline{A},\overline{C})} = 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which is self-contradictory.

Case 3. $0 < \overline{A} < \phi, \overline{C} = 1-\phi$. Then $\mathrm{d}C/\mathrm{d}t|_{(\overline{A},\overline{C})} = -\eta(1-\phi) < 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which leads to a contradiction.

Case 4. $0 < \overline{C} < 1-\phi, \overline{A} = \phi$. Then $\mathrm{d}A/\mathrm{d}t|_{(\overline{A},\overline{C})} = -\phi\gamma < 0$, implying that Γ is not tangent to $\partial\Omega$ at this point, which is also a contradiction.

Theorem 10. *E^* is globally asymptotically stable when $R_0 > 1$.*

Proof. The claimed result follows by combining Lemmas 7–9 with the generalized Poincaré–Bendixson theorem [20]. □

Example 11. Under system (2) with $\alpha = 0.1, \gamma = 0.2, \eta = 0.05, \beta = 0.8, \phi = 0.5, p = 1.2$, where $R_0 = 2.0$, computers in this situation will under the attack of APDDoS, and thus the attacked equilibrium E^* is globally asymptotically stable (see Figure 6).

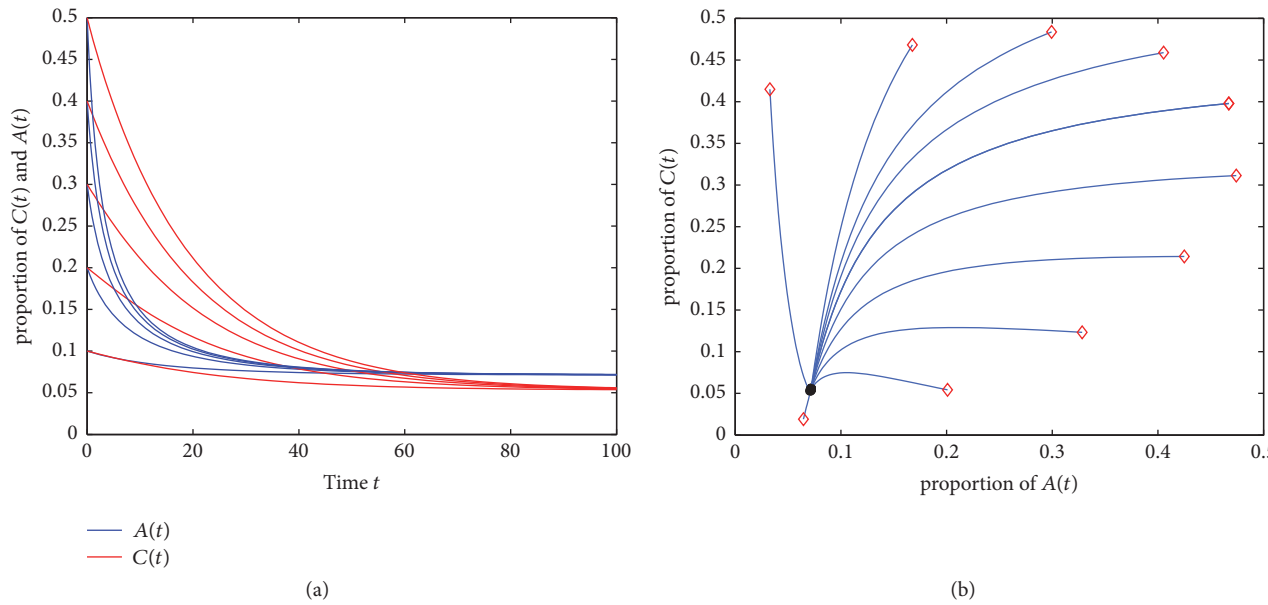
Example 12. Under system (2) with $\alpha = 0.1, \gamma = 0.3, \eta = 0.05, \beta = 0.7, \phi = 0.5, p = 1.2$ that $R_0 = 1.1667$, computers will suffer APDDoS attack, also the attacked equilibrium E^* is globally asymptotically stable (see Figure 7).

4. Further Discussion

In this section, the impact of parameters on the attacked equilibrium E^* of system (2) will be discussed.

In Section 3, the attacked equilibrium E^* can be rewritten into

$$\begin{aligned} E^* = (A^*, C^*) &= \left(\frac{\gamma}{\beta}(R_0 - 1), \frac{\alpha\gamma(1-\phi)(R_0-1)}{p\beta\eta + \alpha\gamma(R_0-1)} \right) \\ &= \left(\phi - \frac{\gamma}{\beta}, \frac{\alpha(1-\phi)(\beta\phi - \gamma)}{p\beta\eta + \alpha(\beta\phi - \gamma)} \right). \end{aligned} \tag{16}$$



(a) (b)

FIGURE 7: (a) and (b) represent the variety of proportion of $C(t)$ and $A(t)$ in different initial conditions by time-varying diagram and phase diagram, respectively.

By calculation,

$$C^* = \frac{\alpha\gamma(1-\phi)(R_0-1)}{p\beta\eta+\alpha\gamma(R_0-1)} = \frac{\alpha(1-\phi)(\beta\phi-\gamma)}{p\beta\eta+\alpha(\beta\phi-\gamma)} = \frac{(1-\phi)}{p\beta\eta/\alpha(\beta\phi-\gamma)+1}. \tag{17}$$

So, it is easy to get the following conclusions:

(1) A^* is strictly increasing with respect to parameters ϕ and β.

(2) C^* is strictly increasing with respect to parameter α, and C^* is strictly decreasing with respect to parameters p and η.

(3) Both of A^* and C^* are strictly decreasing with respect to parameter γ.

Now, let us consider the influence of ϕ and β on the proportion of C^*. The following relations can be gained:

$$\frac{\partial C^*}{\partial\beta} = \alpha\frac{[\alpha(\beta\phi-\gamma)+p\beta\eta]\phi(1-\phi)-(\alpha\phi+p\eta)(1-\phi)(\beta\phi-\gamma)}{[\alpha(\beta\phi-\gamma)+p\beta\eta]^2} = \frac{\alpha p\eta\gamma}{[\alpha(\beta\phi-\gamma)+p\beta\eta]^2} > 0. \tag{18}$$

Hence, C^* is strictly increasing with respect to the parameters β.

Then, focusing on the influence of ϕ, the relation between C^* and ϕ is shown as follows:

$$\frac{\partial C^*}{\partial\phi} = \frac{[\alpha(\beta\phi-\gamma)+p\beta\eta]\alpha[\beta(1-\phi)-(\beta\phi-\gamma)]-\alpha^2\beta(1-\phi)(\beta\phi-\gamma)}{[\alpha(\beta\phi-\gamma)+p\beta\eta]^2}. \tag{19}$$

So the following function has been constructed:

$$f(\phi) = -\alpha\beta^2\phi^2+2(\alpha\beta\gamma-p\beta^2\eta)\phi+p\beta\eta(\beta+\gamma)-\alpha\gamma^2, \tag{20}$$

when ϕ is the positive root of function (20) and C^* will get its maximum or minimum.

Finally the discussion of the value of ϕ will be shown as follows.

Let Δ represent the discriminant which determines whether the function $f(\phi)$ has real root and how many it has. By definition, it is easy to get $\Delta = 4p\beta^3\eta\Lambda$, where $\Lambda = p\beta\eta+\alpha\beta-\alpha\gamma$. $f(\phi)$ exists in two real roots if $\Lambda > 0$. Let ϕ_1 and ϕ_2 ($\phi_1 \le x_2$) denote the two real roots of $f(\phi)$ if $\Delta \ge 0$. Also the axis of symmetry of the function $f(\phi)$, $\gamma/\beta - p\eta/\alpha$, can be obtained easily.

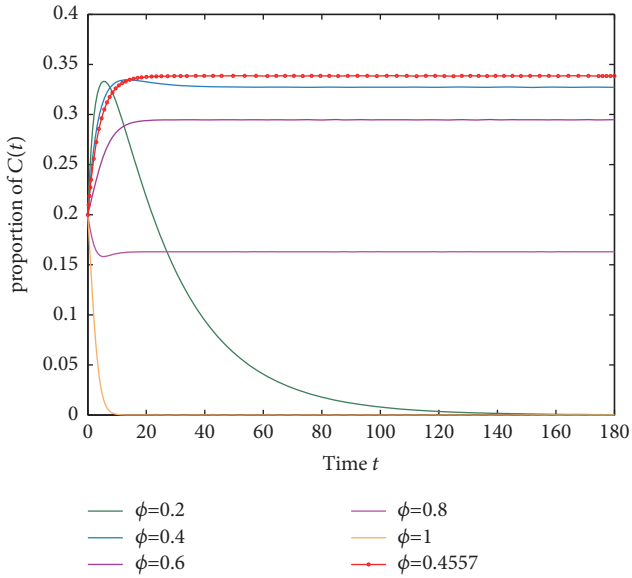


Figure 8: Example 13.

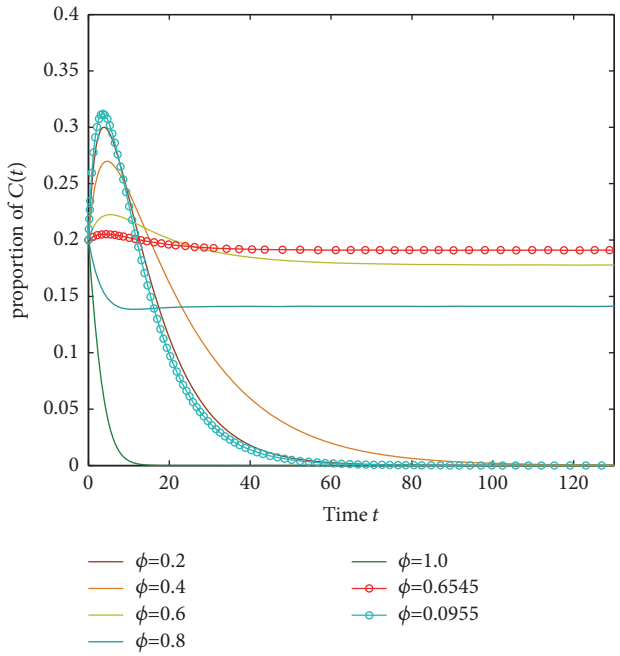


Figure 9: Example 14.

Case 1. $\Lambda \leq 0$, which also means $p\beta\eta + \alpha\beta - \alpha\gamma < 0$, the inequality can be derived as

$$\begin{aligned} p\beta\eta + \alpha\beta - \alpha\gamma &> \beta\eta + \alpha\beta - \alpha\gamma \\ &= \beta\left(\eta + \alpha\left(1 - \frac{\gamma}{\beta}\right)\right). \end{aligned} \tag{21}$$

$\phi \in (0,1)$ and $\phi > \gamma/\beta$ ($R_0 > 1$) infer that $\gamma/\beta < 1$, which means $\beta(\eta + \alpha(1 - \gamma/\beta)) > 0$; thus, that contradicts $p\beta\eta + \alpha\beta - \alpha\gamma < 0$. Therefore, the attacked equilibrium does not exist, and this condition is not satisfied when $R_0 > 1$.

Case 2. $\Lambda > 0$, and $\phi_1 < 0$, $\phi_2 \in (0,1)$. Considering the positive value ϕ_2, C^* increases with respect to ϕ when $\phi \in (0, \phi_2]$, and C^* decreases with respect to ϕ when $\phi \in (\phi_2, 1)$. So $C^*|_{\phi=\phi_2}$ is the local maximum of C^* (see Figure 8).

Case 3. $\Lambda > 0$, and $\phi_1, \phi_2 \in (0,1)$. When $\phi \leq \phi_1$, the attacked equilibrium does not exist because $\phi_1 < \gamma/\beta - p\eta/\alpha < \gamma/\beta$ and $R_0 < 1$. Hence, C^* increases with respect to ϕ when $\phi \in (\phi_1, \phi_2]$, and C^* decreases with respect to ϕ when $\phi \in (\phi_2, 1)$. Here the only concern about the condition is that $\phi = \phi_2$, where $C^*|_{\phi=\phi_2}$ is the local maximum of C^*, respectively (see Figure 9).

Case 4. $\Lambda > 0$, and $\phi_1 < 0$, $\phi_2 > 1$. If $\phi_1 < 0$, $\phi_2 > 1$, then

$$\begin{aligned} \phi_1 &= \frac{-2\left(\alpha\beta\gamma - p\beta^2\eta\right) - \sqrt{\Delta}}{-2\alpha\beta^2} < 0, \\ \phi_2 &= \frac{-2\left(\alpha\beta\gamma - p\beta^2\eta\right) + \sqrt{\Delta}}{-2\alpha\beta^2} > 1; \end{aligned} \tag{22}$$

these two inequalities can be further derived as

$$\begin{aligned} p\beta\eta - \alpha\gamma &> \sqrt{\Delta} > 0, \\ -\alpha\beta - \left(p\beta\eta - \alpha\gamma\right) &> \sqrt{\Delta}; \end{aligned} \tag{23}$$

however, these two formulas are contradictory. Hence, this condition does not hold.

Case 5. $\Lambda > 0$, and $\phi_1, \phi_2 > 1$. Then $\gamma/\beta - p\eta/\alpha > 1$; the axis of symmetry of the function $f(\phi)$ is on the right side of $\phi = 1$, which means $\gamma/\beta > 1 > \phi$. So this condition does not hold.

According to the above discussion, only Cases 2 and 3 may have attacked equilibrium.

(4) When the attacked equilibrium exists, C^* will increase at first, and then C^* will decrease.

Example 13. Fixing $\alpha = 0.8$, $\gamma = 0.2$, $\eta = 0.1$, $\beta = 0.8$, $p = 1.0$, and varying ϕ, the change of $C(t)$ in system (2) is shown in Figure 8. By calculation, $\phi_1 = -0.2057$ (has been ignored because of $\phi = \phi_1 < 0$), $\phi_2 = 0.4557$ (see Figure 8).

Example 14. Fixing $\alpha = 0.8$, $\gamma = 0.3$, $\eta = 0.1$, $\beta = 0.6$, $p = 1.0$, and varying ϕ, the proportion of $C(t)$ in system (2) is shown in Figure 9. By calculation, $\phi_1 = 0.0955$, $\phi_2 = 0.6545$, so C^* exists as a maximum (see Figure 9).

According to above conclusion, there are some suggestions as follows.

(1) Regular antivirus and strengthening the precaution of malwares will help to reduce β and enlarge γ and can decrease A node.

(2) Also strengthening the precaution of malwares, which will enlarge γ, can help to decrease C nodes.

(3) Enhancing the firewall's abilities, like filter and information processing, helps to increase p and prevent S nodes from becoming C nodes.

(4) Reinstalling operation system or changing the hardware of computer, which also means to enlarge η or γ, will be useful to turn C nodes to S nodes or make A nodes become W nodes.

(5) Practically, it is hard to reduce α by controlling or decreasing the destructive power of malware, but it is available to inhibit the propagation of malware by enhancing the firewall's abilities of spying and controlling.

(6) By taking some special strategies, it is feasible to change the structure of the network, which also means to change ϕ, like installing firewall. Besides, according to the discussion of the parameter of ϕ, it must be regarded that the proportion of C nodes will get its maximum in special ϕ, which will cause enormous damage.

5. Conclusion

This paper aims at modelling a dynamical APDDoS attack model. And some properties of this novel model have been deeply researched, like threshold, equilibriums, and stability. The numerical simulations have been got at the same time. Finally, by analyzing the respective influences of system parameters, some suggestions are proposed to reduce the harm of DDoS attacks

Appendix

Referring to the method of calculating the propagation threshold in [21], the calculation process is shown as follows.

In an n-dimensional system, let $x = (x_1, x_2, \ldots, x_n)^T$ denote the number of individuals in each compartment with $x_i \geq 0$. And let $X = \{x \geq 0 \mid x_i = 0,\ i = 1, \ldots, m\}$ denote the set of disease states. Also let $F_i(x)$ be the rate of appearance of new infections in compartment i, V_i^+ be the rate of transfer of individuals into compartment i, and V_i^- be the rate of transfer of individuals out of compartment i.

Then the above model consists of nonnegative initial condition together with the following system of equations:

$$\dot{x}_i = f_i(x) = F_i(x) - V_i(x), \quad i = 1, \ldots, n, \tag{A.1}$$

where $V_i(x) = V_i^-(x) - V_i^+(x)$ and the functions satisfy the following 5 assumptions:

($A1$) If $x \geq 0$, then $F_i, V_i^+, V_i^- \geq 0$ for $i = 1, \ldots, n$.

($A2$) If $x_i = 0$, then $V_i^- = 0$. In particular, if $x \in X$, then $V_i^- = 0$ for $i = 1, \ldots, m$.

($A3$) $F_i(x) = 0$ if $i > m$.

($A4$) If $x \in X$ then $F_i(x) = 0$ and $V_i^+(x) = 0$ for $i = 1, \ldots, m$.

($A5$) If $F(x)$ is a set of zeros, then all eigenvalues of $Df(x_0)$, which is the derivative $[\partial f_i / \partial x_i]$ evaluated at the equilibrium, x_0, have negative real parts.

And then, the derivatives $DF(x_0)$ and $DV(x_0)$ are partitioned as

$$DF(x_0) = \begin{pmatrix} \mathbf{F} & 0 \\ 0 & 0 \end{pmatrix}, \qquad DV(x_0) = \begin{pmatrix} \mathbf{V} & 0 \\ J_3 & J_4 \end{pmatrix}, \tag{A.2}$$

where $\mathbf{F}$ and $\mathbf{V}$ are the $m \times m$ matrices defined by

$$\mathbf{F} = \left[\frac{\partial F_i}{\partial x_j}(x_0) \right], \qquad \mathbf{V} = \left[\frac{\partial V_i}{\partial x_j}(x_0) \right], \quad \text{with } 0 \leq i,\ j \leq m. \tag{A.3}$$

Further, $\mathbf{F}$ is nonnegative, $\mathbf{V}$ is a matrix, and all eigenvalues of J_4 have positive real part. $\rho(\mathbf{FV}^{-1})$, the spectral radius of $\mathbf{FV}^{-1}$, is a threshold parameter.

Conflicts of Interest

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

Acknowledgments

This work is supported by the Natural Science Foundation of Guangdong Province, China (no. 2014A030310239).

References

[1] R. Zheng, W. Lu, and S. Xu, "Active cyber defense dynamics exhibiting rich phenomena," in *Proceedings of the Symposium and Bootcamp on the Science of Security, HotSoS '15*, p. 2, ACM, 2015.

[2] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 40, no. 4, pp. 853–865, 2010.

[3] S. Xu, "Emergent behavior in cybersecurity," in *Proceedings of the the 2014 Symposium and Bootcamp*, pp. 1-2, Raleigh, North Carolina, April 2014.

[4] 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: Simulation and Computation for Engineering and Environmental Systems*, vol. 43, pp. 110–125, 2017.

[5] http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics.

[6] http://www.bbc.com/news/technology-37941216.

[7] http://www.bbc.com/news/technology-40886418.

[8] C. Tankard, "Advanced Persistent threats and how to monitor and deter them," *Network Security*, vol. 2011, no. 8, pp. 16–19, 2011.

[9] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," *PLoS ONE*, vol. 12, no. 1, Article ID e0168675, 2017.

[10] B. Schneier, "Attack trees," *Doctor Dobbs Journal*, vol. 24, no. 12, pp. 21–29, 1999.

[11] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: a superset of advanced persistent threats," *IEEE Security and Privacy*, vol. 11, no. 1, pp. 54–61, 2013.

[12] L.-X. Yang, P. Li, X. Yang, and Y. Y. Tang, "Security evaluation of the cyber networks under advanced persistent threats," *IEEE Access*, vol. 5, pp. 20111–20123, 2017.

[13] https://en.wikipedia.org/wiki/Advanced_persistent_threat.

[14] W. Liu and S. Zhong, "Web malware spread modelling and optimal control strategies," *Scientific Reports*, vol. 7, Article ID 42308, 2017.

[15] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," *IEEE International Conference on Network Protocols IEEE Computer Society*, vol. 154, no. 3-4, pp. 312–321, 2002.

[16] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking," *Computer Networks*, vol. 81, pp. 308–319, 2015.

[17] Q. Yan, F. R. Yu, Q. X. Gong, and J. Q. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[18] L. X. Yang, X. Yang, and Y. Y. Tang, "A bi-virus competing spreading model with generic infection rates," *IEEE Network Science and Engineering*, vol. 5, no. 1, pp. 2–13, 2018.

[19] J. P. LaSalle, "The stability of dynamical systems," *SIAM Journal on Mathematical Analysis*, vol. 25, 1976.

[20] R. C. Robinson, "An introduction to dynamical systems: continuous and discrete," *American Mathematical Society*, vol. 19, 2012.

[21] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Mathematical Biosciences*, vol. 180, no. 1-2, pp. 29–48, 2002.

Hindawi
Security and Communication Networks
Volume 2018, Article ID 2153195, 9 pages
https://doi.org/10.1155/2018/2153195

Research Article

Global Behavior of a Computer Virus Propagation Model on Multilayer Networks

Chunming Zhang

School of Information Engineering, Guangdong Medical University, Dongguan 523808, China

Correspondence should be addressed to Chunming Zhang; chunfei2002@163.com

Received 10 October 2017; Revised 2 February 2018; Accepted 4 March 2018; Published 12 April 2018

Academic Editor: Vasileios A. Karyotis

This paper presents a new linear computer viruses propagation model on multilayer networks to explore the mechanism of computer virus propagation. Theoretical analysis demonstrates that the maximum eigenvalue of the sum of all the subnetworks is a vital factor in determining the viral prevalence. And then, a new sufficient condition for the global stability of virus-free equilibrium has been obtained. The persistence of computer virus propagation system has also been proved. Eventually, some numerical simulation results verify the main conclusions of the theoretical analysis.

1. Introduction

In 1987, the first computer viruses propagation model was proposed by Cohen [1]. Since then, numbers of typical computer viruses propagation models had been proposed, for instance, susceptible–infected–susceptible (SIS) models [2], susceptible–infected–removed (SIR) models [3, 4], susceptible–infected–recovered–susceptible (SIRS) models [5], susceptible–exposed–infected–removed–susceptible (SEIRS) models [6], susceptible–infected–patched–susceptible (SIPS) models [7], and susceptible–infected–external–susceptible (SIES) [8]. However, some of these models simply ignore the fact that the dominating majority of computer viruses have a quite long propagation period before breaking out which can vividly express the node with high infectious ability, while some other models assume that, during its latency, an infected computer just infected recently that has low infectious ability compared with breaking out nodes, also known as an E computer, has no infectivity. This, however, is inconsistent with the fact that, in general, an infected computer does possess infectivity [9]. To overcome these deficiencies, Yang et al. proposed a novel computer virus propagation model, called Susceptible–Latent–Breaking–Susceptible (SLBS) model, in which all the computers connected to the Internet are divided into three groups: virus-free computers, known as susceptive computer (S computer), infected computers that are latent (L computer), and infected computers in which the viruses are breaking out that means the computer with a high infectious level (B computer). One remarkable distinction between the SLBS model and the classical SEIS model is that a latent computer possesses infecting capability [9].

While the mechanism of computer virus propagation on networks is an important research area, lots of network-based computer viruses propagation models ranging from susceptible–infected (SI) models [2, 10] and SIS models [3–5, 8, 11–14] to SIR models [5, 6, 13, 15, 16] and SLBS models [14] and SIPS models [7] have also been inspected. However, these studies mainly focus on single layer networks [11–13, 15, 17–24]. In reality, computer viruses can spread not only through single layer networks but also through multilayer networks; for example, mobile phone viruses (a type of computer virus) can utilize 3G network, 4G network, Wi-Fi network, and even Bluetooth network as their communication network.

On the other hand, from the point of view of research methods, Markov chain method, which is proposed by Van Mieghem et al. [10, 25], can exactly describe computer viruses propagation process with constant transition rates between compartments on any networks. Nevertheless, this method is complex in mathematical analysis. For the purpose of overcoming this deficiency, several approximate methods of researching computer viruses propagation on networks are also proposed in recent years. For example, based on

the assumption that the dynamic state of every node is statistically independent of the state of its nearest neighbors, Wang et al. [26], Youssef and Scoglio [27], and Yang et al. [14] proposed the so-called Individual-based mean-field theory (IBMF); based on the assumption that all nodes of degree k are statistically equivalent, Pastor-Satorras and Vespignani [28, 29] and Barthélemy et al. [30] proposed the so-called degree-based mean-field theory (DBMF), and so on.

For the purpose of more accurately understanding the propagation mechanism of computer viruses on multilayer networks, in this paper, we propose a novel SLBS computer virus propagation model on multilayer network. Highlights of this paper are as follows.

(1) Based on the assumption of multilayer network, by applying the IBMF to the existing SLBS model, a high-dimensional computer virus propagation dynamic model, which is known as the individual-based SLBS model, is formulated. This model forms the foundation of this work. To our knowledge, there is no report about the spread of computer viruses on multilayer networks.

(2) To find out the influence of multilayer networks topology on computer virus spreading, by means of mathematical analysis, I find out that the propagation threshold is the maximum eigenvalue of the sum of all the subnetworks on multilayer networks. Then, the global stability of the virus-free equilibrium has been analyzed. The persistence of system has been proved. Extensive experiments confirmed the conclusions of the mathematical analysis.

The subsequent materials of this paper are organized as follows. In Section 2, we present the multilayer networks and computer viruses propagation model in detail; and then in Section 3 the model is analyzed comprehensively; numerical simulation results are given in Section 4; eventually, in Section 5, we outline this work.

2. Assumptions and Modeling

For the purpose of describing the model in detail, the following notations are proposed:

(i) $G = (V, E)$: the multilayer network, which consists of n subnetworks

(ii) $G_s = (V_s, E_s)$ $(s = 1, 2, \ldots, n)$: the sth layer subnetwork; each subnetwork G_s has N nodes

(iii) V_s: the set of nodes contained in G_s

(iv) E_s: the set of edges contained in G_s

(v) a_{ij}^s: the link from node i to node j in G_s, $a_{ij}^s \in \{0, 1\}$

(vi) $A_s = [a_{ij}^s]_{N\times N}$: the corresponding parameterized adjacency matrix of graph G_s.

In addition, a dynamic switching network $G = (V, E)$ also must satisfy the following conditions:

(I) $V = V_1 = V_2 = \cdots V_n$.

(II) $E = \bigcup_{s=1}^{n} E_s$ and $E_{s_1} \cap E_{s_2} = \varnothing$ for all $s_1 \neq s_2$.

Condition (I) presents that nodes in all subnetworks are identical. Condition (II) shows that the edges of any two subnetworks are different.

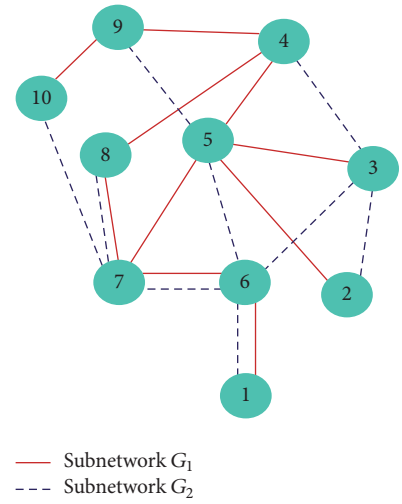


Figure 1: Multilayer network.

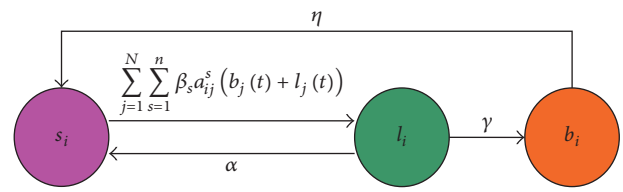


Figure 2: State diagram of SLBS model in multilayer networks.

A simple example of a multilayer network is shown in Figure 1.

As discussed above in the paper, the traditional SLBS model can divide the node into three parts: susceptive node (S node) used to be known as health node and uninfected node, latent node (L node) representing the node which is infected but only showing a low infectious ability, and breaking out node (B node). Compared with L node, B node has significant high infectious power. Let $\xi_i(t) = 0$ (1, 2) stand for the state of the node which is susceptible (latent, breaking out) at time t. Then the state of the multilayer network at time t can be expressed as follows:

$$\xi(t) = \left(\xi_1(t), \ldots, \xi_n(t)\right) \in \{0, 1, 2\}^n. \tag{1}$$

Let $s_i(t)$ $(l_i(t), b_i(t))$ represent the probability that node i is S node (L node, B node) at time t:

$$\begin{aligned} s_i(t) &= \Pr\left(\xi_i(t) = 0\right), \\ l_i(t) &= \Pr\left(\xi_i(t) = 1\right), \\ b_i(t) &= \Pr\left(\xi_i(t) = 2\right). \end{aligned} \tag{2}$$

Then, the following assumptions are given (see Figure 2):

($H1$) In the sth layer subnetwork G_s, the probability that a susceptible node i is infected by a viral (including latent and breaking out) neighbor j is $\beta_s a_{ij}^s (b_j(t) + l_j(t))$, where β_s denotes the infection rate in the sth layer subnetwork G_s. The probability that a susceptible node i is infected by a viral

neighbor j in all layer subnetworks is $\sum_{s=1}^{n} \beta_s a_{ij}^s (b_j(t) + l_j(t))$. Then, the probability that a susceptible node i is infected by all viral neighbors in all subnetworks is $\sum_{j=1}^{N} \sum_{s=1}^{n} \beta_s a_{ij}^s (b_j(t) + l_j(t))$.

($H2$) The probability that a latent node becomes a breaking out node is γ.

($H3$) The probability that a breaking out node becomes a susceptible node is η.

($H4$) The probability that a latent node becomes a susceptible node is α.

Let Δt denote a short time interval. According to the total probability theorem, several formulas can be given from the above assumptions as follows (see Figure 2):

$$\begin{aligned} s_i(t+\Delta t) &= s_i(t) \Pr(\xi_i(t+\Delta t) = 0 \mid \xi_i(t) = 0) \\ &\quad + l_i(t) \Pr(\xi_i(t+\Delta t) = 0 \mid \xi_i(t) = 1) \\ &\quad + b_i(t) \Pr(\xi_i(t+\Delta t) = 0 \mid \xi_i(t) = 2), \\ l_i(t+\Delta t) &= s_i(t) \Pr(\xi_i(t+\Delta t) = 1 \mid \xi_i(t) = 0) \\ &\quad + l_i(t) \Pr(\xi_i(t+\Delta t) = 1 \mid \xi_i(t) = 1) \\ &\quad + b_i(t) \Pr(\xi_i(t+\Delta t) = 1 \mid \xi_i(t) = 2), \\ b_i(t+\Delta t) &= s_i(t) \Pr(\xi_i(t+\Delta t) = 2 \mid \xi_i(t) = 0) \\ &\quad + l_i(t) \Pr(\xi_i(t+\Delta t) = 2 \mid \xi_i(t) = 1) \\ &\quad + b_i(t) \Pr(\xi_i(t+\Delta t) = 2 \mid \xi_i(t) = 2). \end{aligned} \tag{3}$$

Here $o(\Delta t)$ represents time t higher-order infinitesimal. According to ($H1$)–($H4$) and (3), we can derive the following equations:

$$\begin{aligned} &\Pr(\xi_i(t+\Delta t) = 0 \mid \xi_i(t) = 0) \\ &\quad = 1 - \left(\sum_{j=1}^{N} \sum_{s=1}^{n} \beta_s a_{ij}^s (b_j(t) + l_j(t)) \right) \Delta t + o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 1 \mid \xi_i(t) = 0) \\ &\quad = \left(\sum_{j=1}^{N} \sum_{s=1}^{n} \beta_s a_{ij}^s (b_j(t) + l_j(t)) \right) \Delta t + o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 2 \mid \xi_i(t) = 0) = o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 0 \mid \xi_i(t) = 1) = \alpha \Delta t + o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 1 \mid \xi_i(t) = 1) \\ &\quad = 1 - \alpha \Delta t - \gamma \Delta t + o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 2 \mid \xi_i(t) = 1) = \gamma \Delta t + o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 0 \mid \xi_i(t) = 2) = \eta \Delta t + o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 1 \mid \xi_i(t) = 2) = o(\Delta t), \\ &\Pr(\xi_i(t+\Delta t) = 2 \mid \xi_i(t) = 2) = 1 - \eta \Delta t + o(\Delta t). \end{aligned} \tag{4}$$

Substituting (4) into the above formulas and letting $\Delta t \to 0$, we deduce the $3N$-dimensional differential system as follows:

$$\begin{aligned} \frac{ds_i(t)}{dt} &= -\left(\sum_{j=1}^{N} \sum_{s=1}^{n} \beta_s a_{ij}^s (b_j(t) + l_j(t)) \right) s_i(t) + \alpha l_i(t) \\ &\quad + \eta b_i(t), \\ \frac{dl_i(t)}{dt} &= \left(\sum_{j=1}^{N} \sum_{s=1}^{n} \beta_s a_{ij}^s (b_j(t) + l_j(t)) \right) s_i(t) - \alpha l_i(t) \\ &\quad - \gamma l_i(t), \\ \frac{db_i(t)}{dt} &= \gamma l_i(t) - \eta b_i(t). \end{aligned} \tag{5}$$

Because $s_i(t) + l_i(t) + b_i(t) \equiv 1$, $s_i(t)$ can be expressed by the following equation: $s_i(t) = 1 - l_i(t) - b_i(t)$. Then, the following $2N$-dimensional subsystem can be derived:

$$\begin{aligned} &\frac{dl_i(t)}{dt} \\ &\quad = \left(\sum_{j=1}^{N} \sum_{s=1}^{n} \beta_s a_{ij}^s (b_j(t) + l_j(t)) \right) (1 - l_i(t) - b_i(t)) \\ &\qquad - \alpha l_i(t) - \gamma l_i(t), \\ &\frac{db_i(t)}{dt} = \gamma l_i(t) - \eta b_i(t), \\ &\qquad\qquad 1 \le i \le N. \end{aligned} \tag{6}$$

Without loss of generality, we introduce an infection matrix $H = (h_{ij}) \in R^{N \times N}$, where $h_{ij} = \beta_1 a_{ij}^1 + \beta_2 a_{ij}^2 + \cdots + \beta_n a_{ij}^n = \sum_{s=1}^{n} \beta_s a_{ij}^s$ (or $H = \beta_1 A_1 + \beta_2 A_2 + \cdots + \beta_n A_n$). We assume $\lambda_{\max}$ represents the maximum eigenvalue of matrix H.

Then, system (6) can be expressed as follows:

$$\begin{aligned} \frac{dl_i(t)}{dt} &= \left(\sum_{j=1}^{N} h_{ij} (b_j(t) + l_j(t)) \right) (1 - l_i(t) - b_i(t)) \\ &\quad - \alpha l_i(t) - \gamma l_i(t), \\ \frac{db_i(t)}{dt} &= \gamma l_i(t) - \eta b_i(t), \\ &\qquad 1 \le i \le N. \end{aligned} \tag{7}$$

3. Theoretical Analysis

System (7) obviously has a unique virus-free equilibrium $E_0 = (0, 0, \ldots, 0)^T{}_{2N \times 1}$. This section concentrates on the stability of the virus-free equilibrium and persistence of system (7).

First, consider properties of the virus-free equilibrium of system (7).

Let

$$\Omega = \left\{X = \left(x_1, x_2, \ldots, x_{2N}\right)^T \in \Re_+^{2N} \mid x_i + x_{i+N} \le 1,\ i = 1, 2, \ldots, N\right\}. \tag{8}$$

Let

$$x(t) = \left(l_1(t), \ldots, l_N(t), b_1(t), \ldots, b_N(t)\right)^T. \tag{9}$$

Then, system (7) can be expressed in the form of a matrix as follows:

$$\frac{dx(t)}{dt} = Wx(t) + Y(x(t)), \tag{10}$$

with initial condition $x(0) \in \Omega$, where

$$W_{2N\times 2N} = \begin{bmatrix} -\alpha I - \gamma I + H & H \\ \gamma I & -\eta I \end{bmatrix}, \tag{11}$$

$$Y(x(t))_{2N\times 1} = \Bigg[-\left(l_1(t) + b_1(t)\right) \cdot \sum_j h_{1j}\left(l_j(t) + b_j(t)\right), \ldots, -\left(l_N(t) + b_N(t)\right) \cdot \sum_j h_{Nj}\left(l_j(t) + b_j(t)\right), \overbrace{0, \ldots, 0}^{N} \Bigg]^T. \tag{12}$$

Let

$$R_0 = \frac{\eta(\alpha + \gamma)}{\eta + \gamma}. \tag{13}$$

Theorem 1. *Consider linear system (7):*

(a) *The virus-free equilibrium* $E_0 = (0, 0, \ldots, 0)^T_{2N\times 1}$ *is asymptotically stable if* $\lambda_{max} < R_0$.

(b) *The virus-free equilibrium* $E_0 = (0, 0, \ldots, 0)^T_{2N\times 1}$ *is unstable if* $\lambda_{max} > R_0$.

Proof. The characteristic equation of the Jacobian matrix of system (7) at E_0 is

$$\begin{aligned} &\det(\lambda I - W) \\ &= \det\begin{pmatrix} (\lambda + \alpha + \gamma) I - H & -H \\ -\gamma I & (\lambda + \eta) I \end{pmatrix}_{2N\times 2N} \\ &= \det\left((\lambda + \alpha + \gamma)(\lambda + \eta) I - ((\lambda + \gamma + \eta) H)\right) \\ &= 0. \end{aligned} \tag{14}$$

Equation (14) has two possible cases.

Case 1 ($\alpha = \eta$). $R_0 = \eta$, and (14) is derived into

$$(\lambda + \eta + \gamma)^N \det\left((\lambda + \eta) I - H\right) = 0. \tag{15}$$

This equation has a negative root $-\eta - \gamma$ with multiplicity N; and the remaining N roots of the equation are $\lambda_k - \eta$, $1 \le k \le N$. If $\lambda_{\max} < R_0$, then $\lambda_k - \eta \le \lambda_{\max} - \eta < 0$ for all k. Hence, all the roots of (14) are negative. So, the virus-free equilibrium of system (7) is asymptotically stable. On the contrary, if $\lambda_{\max} > R_0$, then $\lambda_{\max} - \eta > 0$. So, (14) has a positive root. As a result, the virus-free equilibrium is unstable.

Case 2 ($\alpha \ne \eta$). $-\eta - \gamma$ is not a root of (14). Thus,

$$\det\left(\frac{(\lambda + \alpha + \gamma)(\lambda + \eta)}{(\lambda + \gamma + \eta)} I - H\right) = 0. \tag{16}$$

This means that λ is a root of (14) if and only if λ is a root of

$$\lambda^2 + a_k \lambda + b_k = 0, \tag{17}$$

where

$$\begin{aligned} a_k &= \alpha + \gamma + \eta - \lambda_k, \\ b_k &= (\alpha + \gamma)\eta - \lambda_k(\gamma + \eta). \end{aligned} \tag{18}$$

If $\lambda_{\max} < R_0$, we have $a_k > 0$ and $b_k > 0$. According to the Hurwitz criterion, the two roots of (17) both have negative real parts. So, all roots of (14) have negative real parts. Hence, the virus-free equilibrium is asymptotically stable. Otherwise, if $\lambda_{\max} > R_0$, then

$$\lambda^2 + a_k \lambda + b_k = 0 \tag{19}$$

has a root with positive real part. As a result, (14) has a root with positive real part. Hence, the virus-free equilibrium is unstable.

The proof is complete. □

Then, we consider the global stability of the virus-free equilibrium of system (7).

Lemma 2 (see [31]). *Consider a system* $dx/dt = f(x)$ *that is defined at least in a compact set C. Then, C is invariant if, for every point y on* ∂C, *the vector* $f(y)$ *is tangent to or pointing to C.*

Lemma 3. *The set* Ω *is positively invariant for system (7). That is,* $x(0) \in \Omega$ *implies* $x(t) \in \Omega$ *for all* $t > 0$.

Proof. $\partial\Omega$ consists of the following $3N$ hyperplanes:

$$\begin{aligned} S_i &= \{x \in \Omega \mid x_i = 0\}, \\ T_i &= \{x \in \Omega \mid x_{i+N} = 0\}, \\ U_i &= \{x \in \Omega \mid x_i + x_{i+N} = 1\}, \end{aligned} \tag{20}$$

which have

$$\begin{aligned} \varphi_i &= \left(0, \ldots, 0, \overset{i}{-1}, 0, \ldots, 0\right), \\ \psi_i &= \left(0, \ldots, 0, \overset{i+N}{-1}, 0, \ldots, 0\right), \\ \xi_i &= \left(0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0, \overset{i+N}{1}, 0, \ldots, 0\right) \end{aligned} \tag{21}$$

as their respective outer normal vectors. For $1 \le i \le N$, we have

$$\begin{aligned}\left(\left.\frac{dx}{dt}\right|_{x\in S_i}\cdot\varphi_i\right) &= -\left(1-x_{i+N}\right)\sum_{j=1}^{N}h_{ij}\left(x_j+x_{j+N}\right)\\ &< 0,\\ \left(\left.\frac{dx}{dt}\right|_{x\in T_i}\cdot\psi_i\right) &= -\gamma x_i < 0,\\ \left(\left.\frac{dx}{dt}\right|_{x\in U_i}\cdot\xi_i\right) &= -\alpha x_i-\eta\left(1-x_i\right) < 0.\end{aligned} \tag{22}$$

Thus, the claimed result follows from Lemma 2. □

Lemma 4 (see [31]). *Consider an n-dimensional autonomous system*

$$\frac{dz(t)}{dt} = Az(t) + Q(z(t)), \quad z \in D, \tag{23}$$

where A is an irreducible $n\times n$ matrix, D is a region containing the origin, $Q(z) \in C$, and $\lim_{x\to 0}\|Q(z)\|/\|z\| = 0$. We assume that there exists a positively invariant compact convex set [16] $C \subset D$ containing the origin, a positive number r, and a real eigenvector ω of A^T such that

(C1) $\langle z, \omega\rangle \ge r\|z\|$ *for all* $z \in C$,

(C2) $\langle Q(z), \omega\rangle \le 0$ *for all* $z \in C$,

(C3) *the origin forms the largest positively invariant set [16] included in* $N = \{z \in C \mid \langle Q(z), \omega\rangle = 0\}$.

Then, we have the following:

(1) $\omega < 0$ *implies that the origin is globally asymptotically stable in* C.

(2) $\omega > 0$ *implies that there exists* $m > 0$ *such that, for each* $z_0 \in C - \{0\}$, *the solution* $\phi(t, z_0)$ *to system (7) satisfies* $\lim_{t\to\infty}\inf\|\phi(t, z_0)\| \ge m$.

Theorem 5. *Consider system (7). The virus-free equilibrium* $E_0 = (0, 0, \ldots, 0)^T_{2N\times 1}$ *is globally asymptotically stable in* Ω *if* $\lambda_{max} < R_0$.

Proof. Let $C = \Omega$, $A = W$, and $Q = Y$. As matrix W^T is irreducible and all of its nondiagonal entries are nonnegative, from [31] A^T has a positive eigenvector $z = (z_1, z_2, \ldots, z_{2N})$ corresponding to its eigenvalue ω.

Let $r = \min\{z_i : 1 \le i \le 2N\} > 0$. Then,

$$\begin{aligned}\langle x, z\rangle &\ge r\sum_{i=1}^{2N}x_i = r\|x\|,\\ \langle Q(x), z\rangle &= -\sum_{i=1}^{N}z_i\left(x_i+x_{i+N}\right)\sum_j h_{ij}\left(x_j+x_{N+j}\right)\\ &\le 0.\end{aligned} \tag{24}$$

$\langle Q(x), z\rangle = 0$ implies that $x = 0$. Hence, the claimed result follows from Lemma 4. □

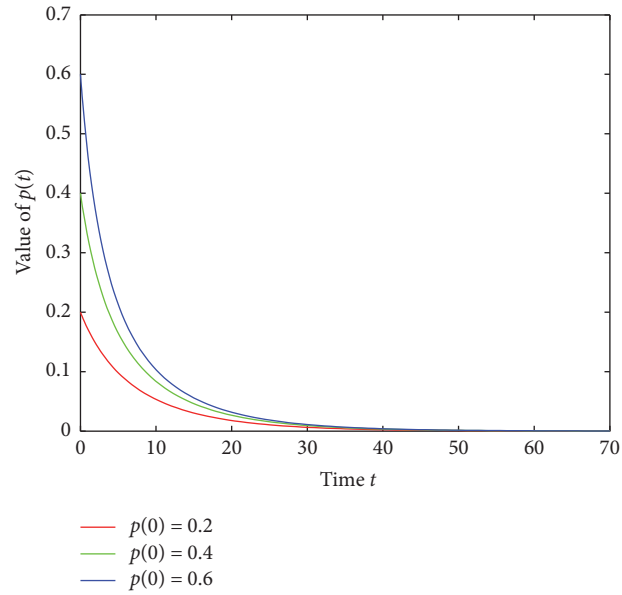


FIGURE 3: The time plot of $p(t)$ for Example 1 with different initial values.

Second, we investigate the properties of system (7) when $\lambda_{\max} > R_0$. From Lemma 4 and Theorem 1, we can easily get the following results.

Theorem 6. *Consider linear system (7). If* $\lambda_{max} > R_0$, *we have*

$$\begin{aligned}&\sum_i\left(l_i(t)+b_i(t)\right) > 0 \Longrightarrow\\ &\liminf_{t\to\infty}\sum_i\left(l_i(t)+b_i(t)\right) > 0.\end{aligned} \tag{25}$$

Remark 7. Theorem 5 shows that the global stability of the virus-free equilibrium implies that the viruses will decline to extinction.

Remark 8. Theorem 6 shows that if $\lambda_{\max} > R_0$, then, computer viruses in the network will persist.

4. Numerical Simulations

In this section, the main theorems of this paper are verified by some numerical simulations. Let $p(t)$ represent the percentage of infected nodes in all nodes at time t, $p(t) = (1/N)\sum_{i=1}^{N}(l_i(t) + b_i(t))$.

(1) We consider a two-layer complete graph, which has 250 nodes, and the infection rate of the 1st and the 2nd layer subnetwork is $\beta_1 = 0.0005$ and $\beta_2 = 0.0007$, respectively. Then, $\lambda_{\max} = 0.2988$.

Example 1. Based on (1), Figure 3 shows the dynamic behavior of system (7) with $\alpha = 0.4$, $\gamma = 0.5$, and $\eta = 0.4$ for different initial conditions. By calculation, $R_0 = 0.4$. Because of $\lambda_{\max} < R_0$, computer virus would die out.

Example 2. Based on (1), Figure 4 reveals the dynamic behavior of system (7) with $\alpha = 0.4$, $\gamma = 0.5$, and $\eta = 0.12$

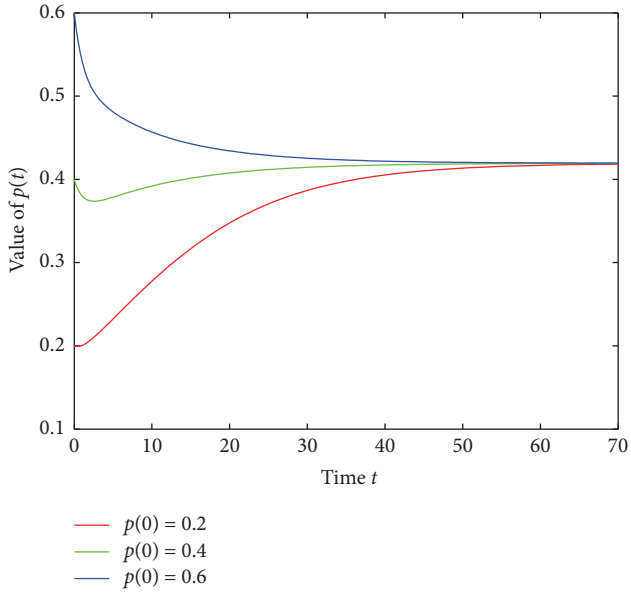


FIGURE 4: The time plot of $p(t)$ for Example 2 with different initial values.

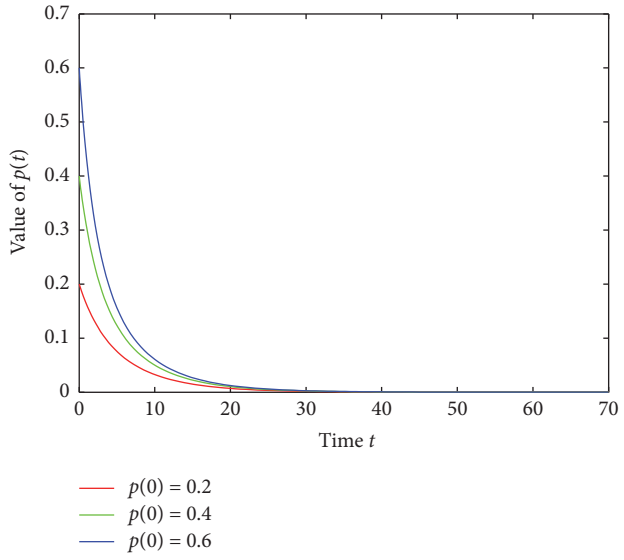


FIGURE 5: The time plot of $p(t)$ for Example 3 with different initial values.

in different initial conditions. Then $R_0 = 0.1742$. Because of $\lambda_{\max} > R_0$, computer virus would persist.

(2) We take a three-layer Erdos–Renyi random graph, which has 250 nodes, with random connection probability 0.8. The infection rate of the 1st, 2nd, and 3rd layer subnetwork is $\beta_1 = 0.0005$, $\beta_2 = 0.0006$, and $\beta_3 = 0.0007$, respectively. Then, $\lambda_{\max} = 0.3583$.

Example 3. Based on (2), Figure 5 illustrates the dynamic behavior of system (7) with $\alpha = 0.4$, $\gamma = 0.5$, and $\eta = 0.6$ for different initial conditions. By calculation, $R_0 = 0.4909$. Because of $\lambda_{\max} < R_0$, computer virus would die out.

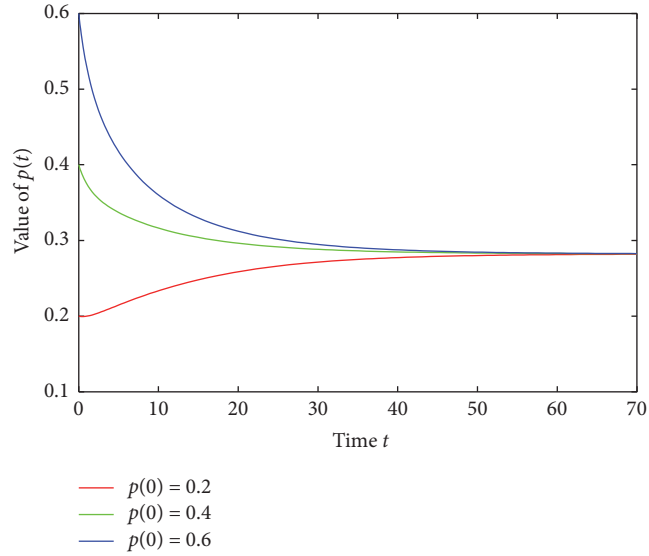


FIGURE 6: The time plot of $p(t)$ for Example 4 with different initial values.

Example 4. Based on (2), Figure 6 shows the dynamic behavior of system (7) with $\alpha = 0.4$, $\gamma = 0.5$, and $\eta = 0.2$ in different initial conditions. Then $R_0 = 0.2571$. Because of $\lambda_{\max} > R_0$, computer virus would persist.

(3) We take a two-layer Barabási–Albert (BA) scale-free graph, which has 250 nodes. The infection rate of the 1st and 2nd layer subnetwork is $\beta_1 = 0.02$ and $\beta_2 = 0.03$, respectively. Then, $\lambda_{\max} = 0.2946$.

Example 5. Based on (3), Figure 7 illustrates the dynamic behavior of system (7) with $\alpha = 0.4$, $\gamma = 0.5$, and $\eta = 0.6$ for different initial conditions. By calculation, $R_0 = 0.4909$. Because of $\lambda_{\max} < R_0$, computer virus would die out.

Example 6. Based on (3), Figure 8 shows the dynamic behavior of system (7) with $\alpha = 0.4$, $\gamma = 0.5$, and $\eta = 0.1$ in different initial conditions. Then $R_0 = 0.15$. Because of $\lambda_{\max} > R_0$, computer virus would persist.

(4) Consider a multilayer network consisting of three subnetworks; each subnetwork has 250 nodes. The subnetwork of the 1st, 2nd, and 3rd is complete connected network, random network, and scale-free network, respectively. And the connection probability of the random subnetworks is 0.7. Besides, the infection rate of the 1st, 2nd, and 3rd subnetwork is $\beta_1 = 0.0002$, $\beta_2 = 0.0003$, and $\beta_3 = 0.001$, respectively. Then, $\lambda_{\max} = 0.2760$.

Example 7. Based on (4), Figure 9 illustrates the dynamic behavior of system (7) with $\alpha = 0.4$, $\gamma = 0.5$, and $\eta = 0.6$ for different initial conditions. By calculation, $R_0 = 0.4909$. Because of $\lambda_{\max} < R_0$, computer virus would die out.

Example 8. Based on (4), Figure 10 shows the dynamic behavior of system (7) with $\alpha = 0.1$, $\gamma = 0.5$, and $\eta = 0.1$ in

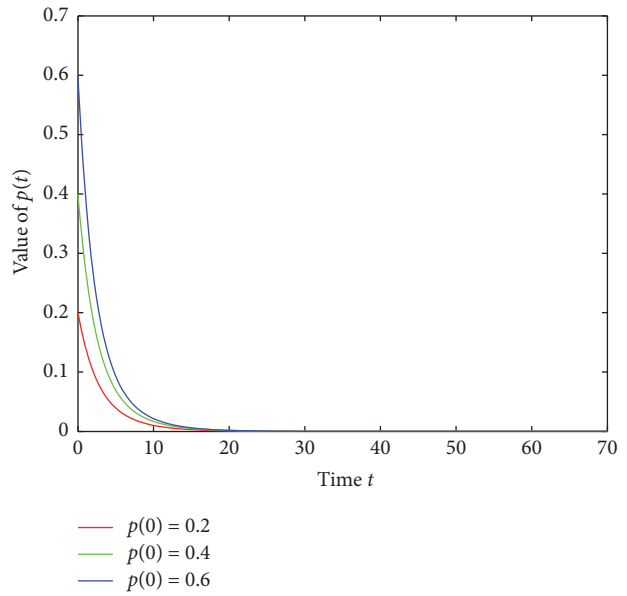


FIGURE 7: The time plot of $p(t)$ for Example 5 with different initial values.

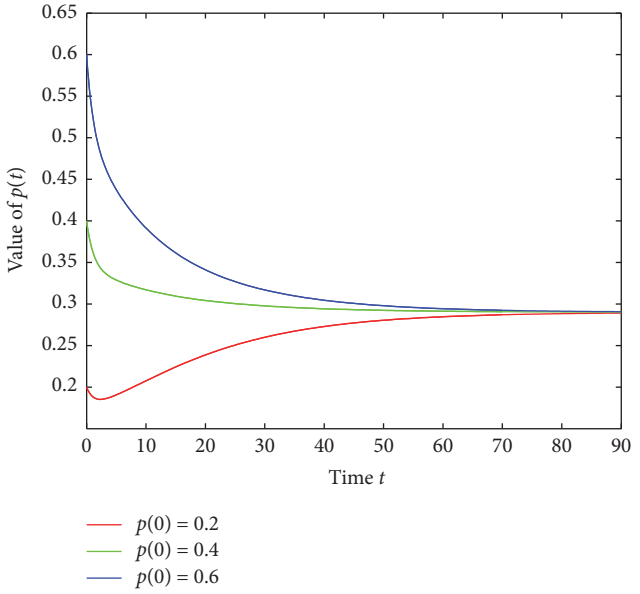


FIGURE 8: The time plot of $p(t)$ for Example 6 with different initial values.

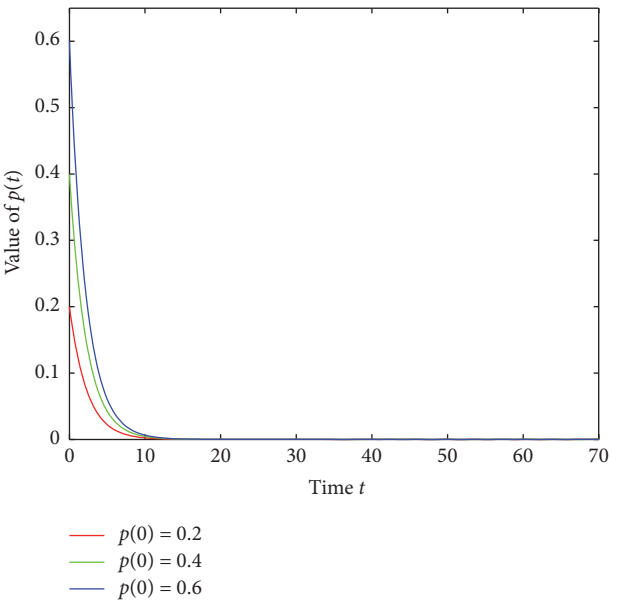


FIGURE 9: The time plot of $p(t)$ for Example 7 with different initial values.

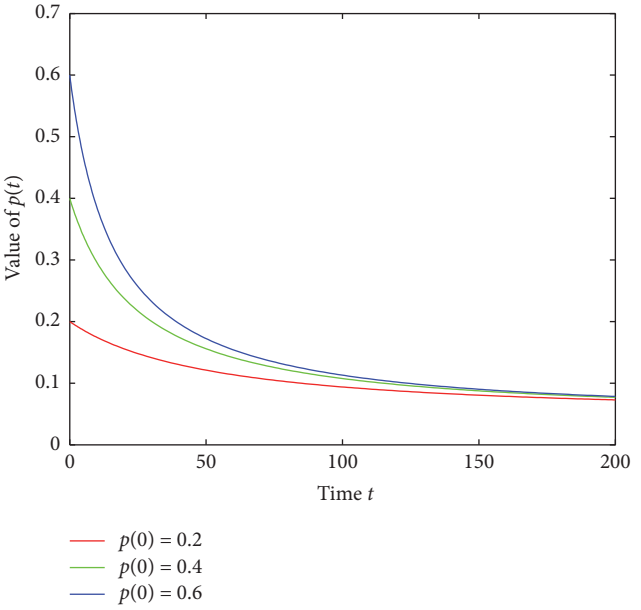


FIGURE 10: The time plot of $p(t)$ for Example 8 with different initial values.

different initial conditions. Then $R_0 = 0.1$. Because of $\lambda_{\max} > R_0$, computer virus would persist.

(5) The propagation threshold R_0 plays a vital role in determining the dynamics of system (7). As $\partial R_0/\partial\alpha > 0$, $\partial R_0/\partial\eta > 0$, R_0 is strictly increasing with respect to the parameters α, η (see Figure 11). As $\partial R_0/\partial\gamma = \eta(\eta-\alpha)/(\eta+\gamma)^2$, when $\eta > \alpha$, R_0 increases as γ increases; when $\eta < \alpha$, R_0 decreases as γ increases (see Figure 12).

5. Conclusions

To explore the propagation mechanism of computer viruses on multilayer network, a novel computer virus propagation model has been proposed. The theoretical analysis of model exhibited that computer viral prevalence is deeply determined by the maximum eigenvalue of the multilayer networks. Then, the global stability of virus-free equilibrium and the persistence of computer virus propagation have been proved. Some numerical simulations have also been given.

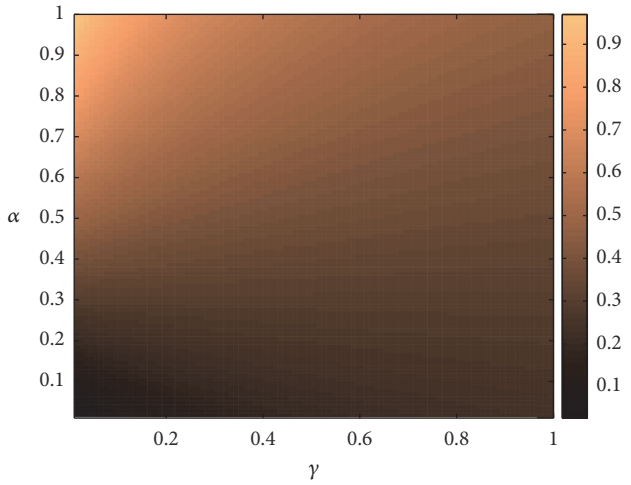


Figure 11: Values of R_0 as a function of varying α and γ with fixing the parameter $\eta = 0.3$.

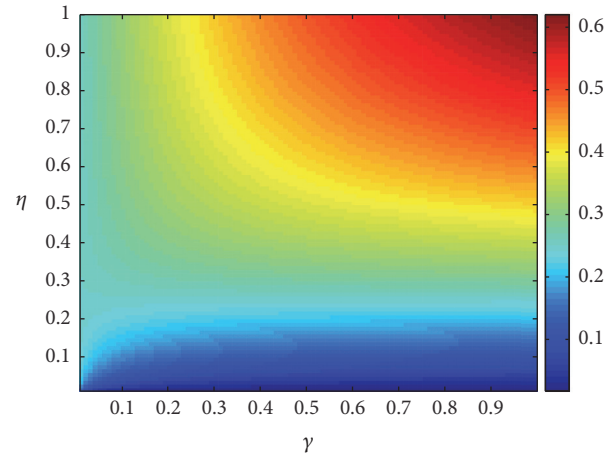


Figure 12: Values of R_0 as a function of varying η and γ with fixing the parameter $\alpha = 0.25$.

As it is well known, the topology of the Internet is varying constantly rather than being static. A dynamic switching network is a network whose links will change (dissipate and emerge) and then the structure of the networks will be different in the distinct time. Therefore, it is of practical importance to understand the effect of dynamic switching networks on virus spreading. Our next work is to study the spreading behavior of computer viruses on dynamic switching networks.

Conflicts of Interest

The author declares that they have no conflicts of interest.

Acknowledgments

This work is supported by Natural Science Foundation of Guangdong Province, China (no. 2014A030310239).

References

[1] F. Cohen, "Computer viruses: theory and experiments," *Computers & Security*, vol. 6, no. 1, pp. 22–35, 1987.

[2] J. Kephart and S. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 343–359, Oakland, CA, USA, 1991.

[3] J. Ren, X. Yang, Q. Zhu, L.-X. Yang, and C. Zhang, "A novel computer virus model and its dynamics," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 1, pp. 376–384, 2012.

[4] Q. Zhu, X. Yang, and J. Ren, "Modeling and analysis of the spread of computer virus," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 5117–5124, 2012.

[5] C. Gan and X. Yang, "Theoretical and experimental analysis of the impacts of removable storage media and antivirus software on viral spread," *Communications in Nonlinear Science and Numerical Simulation*, vol. 22, no. 1-3, pp. 167–174, 2015.

[6] B. K. Mishra and S. K. Pandey, "Dynamic model of worms with vertical transmission in computer network," *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8438–8446, 2011.

[7] 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.

[8] C. Gan, X. Yang, Q. Zhu, J. Jin, and L. He, "The spread of computer virus under the effect of external computers," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1615–1620, 2013.

[9] L.-X. Yang, X. Yang, L. Wen, and J. Liu, "A novel computer virus propagation model and its dynamics," *International Journal of Computer Mathematics*, vol. 89, no. 17, pp. 2307–2314, 2012.

[10] 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.

[11] M. Karsai, M. Kivelä, R. K. Pan et al., "Small but slow world: How network topology and burstiness slow down spreading," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 83, no. 2, Article ID 025102, 2011.

[12] J. C. Wierman and D. J. Marchette, "Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction," *Computational Statistics & Data Analysis*, vol. 45, no. 1, pp. 3–23, 2004.

[13] C. Griffin and R. Brooks, "A note on the spread of worms in scale-free networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 36, no. 1, pp. 198–202, 2006.

[14] 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.

[15] T. Zhou, J.-G. Liu, W.-J. Bai, G. Chen, and B.-H. Wang, "Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 74, no. 5, Article ID 056109, 2006.

[16] https://en.wikipedia.org/wiki/Positive_invariant_set.

[17] H. J. Shi, Z. S. Duan, and G. R. Chen, "An SIS model with infective medium on complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 8-9, pp. 2133–2144, 2008.

[18] L. Wen and J. Zhong, "Global asymptotic stability and a property of the SIS model on bipartite networks," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 2, pp. 967–976, 2012.

[19] A. d'Onofrio, "A note on the global behaviour of the network-based SIS epidemic model," *Nonlinear Analysis: Real World Applications*, vol. 9, no. 4, pp. 1567–1572, 2008.

[20] C. Castellano and R. Pastor-Satorras, "Thresholds for epidemic spreading in networks," *Physical Review Letters*, vol. 105, no. 21, Article ID 218701, 2010.

[21] 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.

[22] M. Draief, A. Ganesh, and L. Massouilié, "Thresholds for virus spread on networks," *The Annals of Applied Probability*, vol. 18, no. 2, pp. 359–378, 2008.

[23] Y. Moreno, R. Pastor-Satorras, and A. Vespignani, "Epidemic outbreaks in complex heterogeneous networks," *The European Physical Journal B*, vol. 26, no. 4, pp. 521–529, 2002.

[24] C. Gan, "Modeling and analysis of the effect of network eigenvalue on viral spread," *Nonlinear Dynamics*, vol. 84, no. 3, pp. 1727–1733, 2016.

[25] P. Van Mieghem and E. Cator, "Epidemics in networks with nodal self-infection and the epidemic threshold," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 86, no. 1, Article ID 016116, 2012.

[26] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos, "Epidemic spreading in real networks: an eigenvalue viewpoint," in *Proceedings of the 22nd International Symposium on Reliable Distributed Systems (SRDS '03)*, pp. 25–34, Florence, Italy, October 2003.

[27] M. Youssef and C. Scoglio, "An individual-based approach to SIR epidemics in contact networks," *Journal of Theoretical Biology*, vol. 283, pp. 136–144, 2011.

[28] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, 2001.

[29] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 63, no. 6, Article ID 066117, 2001.

[30] M. Barthélemy, A. Barrat, R. Pastor-Satorras, and A. Vespignani, "Velocity and hierarchical spread of epidemic outbreaks in scale-free networks," *Physical Review Letters*, vol. 92, no. 17, Article ID 178701, 2004.

[31] A. Lajmanovich and J. A. Yorke, "A deterministic model for gonorrhea in a nonhomogeneous population," *Mathematical Biosciences*, vol. 28, no. 3/4, pp. 221–236, 1976.

Hindawi
Security and Communication Networks
Volume 2018, Article ID 9756982, 11 pages
https://doi.org/10.1155/2018/9756982

Research Article

An Epidemic Model of Computer Worms with Time Delay and Variable Infection Rate

Yu Yao,[1,2] **Qiang Fu**,[1,2] **Wei Yang**,[1,3] **Ying Wang**,[1,2] **and Chuan Sheng**[1,2]

[1]*Key Laboratory of Medical Image Computing, Ministry of Education, Northeastern University, Shenyang 110004, China*
[2]*College of Computer Science and Engineering, Northeastern University, Shenyang 110819, China*
[3]*Software College, Northeastern University, Shenyang 110819, China*

Correspondence should be addressed to Qiang Fu; qiang.fu@outlook.com

Received 13 November 2017; Revised 15 January 2018; Accepted 28 January 2018; Published 6 March 2018

Academic Editor: Angel M. Del Rey

With rapid development of Internet, network security issues become increasingly serious. Temporary patches have been put on the infectious hosts, which may lose efficacy on occasions. This leads to a time delay when vaccinated hosts change to susceptible hosts. On the other hand, the worm infection is usually a nonlinear process. Considering the actual situation, a variable infection rate is introduced to describe the spread process of worms. According to above aspects, we propose a time-delayed worm propagation model with variable infection rate. Then the existence condition and the stability of the positive equilibrium are derived. Due to the existence of time delay, the worm propagation system may be unstable and out of control. Moreover, the threshold τ_0 of Hopf bifurcation is obtained. The worm propagation system is stable if time delay is less than τ_0. When time delay is over τ_0, the system will be unstable. In addition, numerical experiments have been performed, which can match the conclusions we deduce. The numerical experiments also show that there exists a threshold in the parameter a, which implies that we should choose appropriate infection rate $\beta(t)$ to constrain worm prevalence. Finally, simulation experiments are carried out to prove the validity of our conclusions.

1. Introduction

With the deep application of the Internet, network security plays a more and more important role in recent years. Among the security events, the consequences of large-scale network attacks (such as worm attacks and DOS attacks) are especially serious. Meanwhile, the characteristics of worm attacks are wide infection scale, fast spread speed, and serious harm. Consequently, many experts focus on the spread of Internet worms. Some traditional epidemic models of infectious diseases were used to describe the propagation of Internet worms [1] when the Red Code worms broke out. In order to study the spread of malware among mobile phones, the SIS model [2] is proposed by some researchers. Qing and Wen introduced the Kermack-McKendrick model, which is also called SIR model [3]. Then many mathematical models [4–9] inspired by the SIR model have been employed to constrain the propagation of Internet worms. Some research achievements [10–12] showed that the spread dynamic system of malware would be unstable and bifurcation and chaos would appear. Considering the fact that the intrusion detection system (IDS) may lead to time delay, Yao et al. [13–15] obtained the threshold of time delay when Hopf bifurcation occurred. Pulse quarantine strategy [16] also has been taken to constrain the propagation of worms in network. Due to the effect of different topologies, some experts presented different models [9, 17] to analyse the results.

Although most of previous works can offer useful insight into the Internet worm propagations, some of them fail to grasp the detail that has important impact on the worm propagation. Namely, some of the previous models ignore the variation of the infection rate. They usually regard it as a constant that cannot describe the characteristics and dynamics of worm propagation accurately, such as SIS model [18], SIR models [12, 19], SIRS model [20], and SIES model [21]. Moreover, some unconventional models such as delayed models [6, 22] and impulsive models [23, 24] have been proposed. Analogously, these models regard infection rate as a constant as well. In the early stages of worm invasion, the number of infected nodes is small and the linear assumption

is still more reasonable. However, as the number of infected nodes increases, the true infection rate will tend to be saturated, and it can be significantly nonlinear. In this case, the linear assumption will overestimate the harmfulness of the worms and lead to great waste of resources.

In this paper, a variable infection rate is introduced into the worm propagation. Some experts have suggested that worm infection is a nonlinear process. The majority of previous models mentioned above are based on the bilinear incidence rate assumption, which is a good approximation of the general incidence rate in the case where the proportion of infected computers is small. However, in reality, the density of infected computers may be large [25]. To understand the spreading behaviour of worm propagation better, it is necessary to study epidemic models with general incidence rate. The nonlinear infection rate is used to capture the dynamics of overcrowded infectious networks and high viral loads [26]. Gan et al. [25] show that some nonlinear incidence rates may be conducive to the containment of computer viruses. Feng et al. [27] have proposed the SIRS model with a variable infection rate which plays an important role in the spread of the Internet worm. We consider that the vaccinated hosts (the immunizing hosts) may turn to susceptible hosts (the hosts liable to infection by worms) if the worm variants appear or the patches lose efficacy, and this process may take a period of time. Due to the existence of time delay, vaccinated hosts go through a temporary state (delayed state) after the failure of vaccination before becoming susceptible. In this paper, we try to establish a realistic worm propagation model, motivated by the works [7, 27]. This model can give deep insight into predicting worm spread in networks.

The subsequent materials of this work are organized as follows. In Section 2, we present the SIQVD model. Section 3 analyses the stability of equilibrium and the threshold of Hopf bifurcation. In Section 4, we carry out the numerical analysis and simulation of our model. Section 5 gives the conclusion and proposes useful strategies.

2. Model Formulation

We propose a model of worm propagation to describe the spreading behaviour of Internet worms more realistically in this paper. Susceptible hosts can turn to the infectious state by many factors. Many classical models employ bilinear infection rate described by βSI, where β is determined by the probability of transmission contact between S (susceptible hosts) and I (infectious hosts). Previous models usually regard β as a constant. In fact, the worm infection is a nonlinear process so that β should be adjusted to $\beta(t)$. Infectious hosts can change to vaccinated hosts if there are countermeasures applying to them. The countermeasures include antivirus software, firewall, and patching. Meanwhile, we consider zero-day attacks in this paper. Zero-day attacks spread Internet worms through vulnerabilities of the system or software. Usually, the time of the whole process is not over 24 hours. There are no effective and safe patches when the zero-day attacks appear. So quarantine strategy is proposed to control the worm propagation for the hosts without useful patches. The application of the quarantine strategy relies on the hybrid intrusion detection system (IDS). The hybrid IDS not only can detect unknown worms making up for the lack of misuse detection system but also can avoid the high rate of false positives generated by the anomaly detection system. Thus, some hosts are in quarantined state. And the quarantined hosts can turn to vaccinated hosts by installing patches. Usually some patches are temporary and the temporary patches may lose efficacy if we install operating systems. When the worm variants and unknown worms appear, vaccinated hosts may change to susceptible states. This process can generate a time delay which we called delay states.

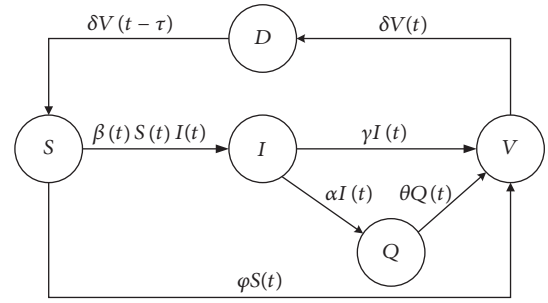


Figure 1: State transition diagram of the SIQVD model.

We assume that all the hosts change over time among five states: susceptible (S), infectious (I), quarantined (Q), vaccinated (V), and delay (D). Let $S(t)$, $I(t)$, $Q(t)$, $V(t)$, and $D(t)$ denote the number of susceptible, infectious, quarantined, vaccinated, and delay hosts, respectively, at time t. We assume that the total number of all the hosts throughout Internet is N. The transition diagram is given in Figure 1.

In order to show the parameters clearly, we list some frequent notations of the model in Notations.

After above description, we can express the model with the following equations:

$$\begin{aligned}
\frac{dS}{dt} &= -\beta(t) I(t) S(t) - \varphi S(t) + \delta V(t-\tau), \\
\frac{dI}{dt} &= \beta(t) I(t) S(t) - (\gamma + \alpha) I(t), \\
\frac{dQ}{dt} &= \alpha I(t) - \theta Q(t), \\
\frac{dV}{dt} &= \varphi S(t) + \gamma I(t) + \theta Q(t) - \delta V(t), \\
\frac{dD}{dt} &= \delta V(t) - \delta V(t-\tau),
\end{aligned} \tag{1}$$

where $\beta(t)$ changes with time t. We regard the infection rate as $\beta(t) = \beta_0 f_1(I(t))$, where f_1 is a nonlinear function of I [27]. For being nonlinear, the function f_1 is assumed to satisfy the following assumptions [28]:

(1) $f_1(0) = 0$.

(2) $f_1'(I) > 0$.

(3) $f_1''(I) < 0$.

(4) $\lim_{t\to\infty} f_1(I) f_1(I) = C < +\infty$.

In other words, f_1 is an increasing function that is bounded (by the constant C).

From the above discussion, we can express the model by the following differential equations:

$$\begin{aligned}
\frac{dS}{dt} &= -\beta_0 f(I(t)) S(t) - \varphi S(t) + \delta V(t-\tau), \\
\frac{dI}{dt} &= \beta_0 f(I(t)) S(t) - (\gamma+\alpha) I(t), \\
\frac{dQ}{dt} &= \alpha I(t) - \theta Q(t), \\
\frac{dV}{dt} &= \varphi S(t) + \gamma I(t) + \theta Q(t) - \delta V(t), \\
\frac{dD}{dt} &= \delta V(t) - \delta V(t-\tau),
\end{aligned} \tag{2}$$

where $f(I(t)) = f_1(I(t))I(t)$.

3. Stability of Equilibrium and Bifurcation Analysis

Let

$$R_0 = \frac{N\delta\beta_0 f'(0)}{(\varphi+\delta)(\alpha+\gamma)}. \tag{3}$$

Theorem 1. *System (2) has a unique positive equilibrium point* $E^* = (S^*, I^*, Q^*, V^*, D^*)$ *when* $R_0 \geq 1$, *where*

$$\begin{aligned}
S^* &= \frac{(\alpha+\gamma) I^*}{\beta_0 f(I^*)}, \\
I^* &= I^*, \\
Q^* &= \frac{\alpha I^*}{\theta}, \\
V^* &= \frac{(\varphi+\beta_0 f(I^*))(\alpha+\gamma)}{\delta\beta_0 f(I^*)} I^*, \\
D^* &= \delta\tau V^*.
\end{aligned} \tag{4}$$

Proof. When system (2) is stable, it satisfies the following equations:

$$\begin{aligned}
-\beta_0 f(I(t)) S(t) - \varphi S(t) + \delta V(t-\tau) &= 0, \\
\beta_0 f(I(t)) S(t) - (\gamma+\alpha) I(t) &= 0, \\
\alpha I(t) - \theta Q(t) &= 0, \\
\varphi S(t) + \gamma I(t) + \theta Q(t) - \delta V(t) &= 0, \\
\delta V(t) - \delta V(t-\tau) &= 0.
\end{aligned} \tag{5}$$

We make $I(t) > 0$; then we have

$$\begin{aligned}
S^* &= \frac{(\alpha+\gamma) I^*}{\beta_0 f(I^*)}, \\
Q^* &= \frac{\alpha I^*}{\theta}, \\
V^* &= \frac{(\varphi+\beta_0 f(I^*))(\alpha+\gamma)}{\delta\beta_0 f(I^*)} I^*, \\
D^* &= \delta\tau V^*.
\end{aligned} \tag{6}$$

Since the total number of hosts in system (5) is N, we can get the following equation of I:

$$\begin{aligned}
H(I) = \frac{(\alpha+\gamma) I}{\beta_0 f(I)} + I + \frac{\alpha I}{\theta} + \frac{(\varphi+\beta_0 f(I))(\alpha+\gamma)}{\delta\beta_0 f(I)} I \\
- N = 0.
\end{aligned} \tag{7}$$

Then we calculate the sign of its derivative as follows:

$$\begin{aligned}
&H'(I) \\
&= \frac{\delta^2\beta_0(\gamma+\alpha)\left[f(I) - If'(I)\right] + \delta^2\beta_0^2 f^2(I)(1+\alpha/\theta)}{\left[\delta\beta_0 f(I)\right]^2} \\
&\quad + \frac{\delta\beta_0^2(\gamma+\alpha) f^2(I) + \delta\beta_0\varphi(\gamma+\alpha)\left[f(I) - If'(I)\right]}{\left[\delta\beta_0 f(I)\right]^2}.
\end{aligned} \tag{8}$$

Since $f_1'(I) < 0$, we can get $f(I) - If'(I) > 0$. As a result, $H'(I) > 0$. If there exists a positive root of $H(I) = 0$, $H(I)$ must satisfy $H(0) < 0$. So we can get

$$\begin{aligned}
H(0) &= \lim_{I\to 0} H(I) = \frac{\delta(\alpha+\gamma) I + \delta\beta_0 f(I) I + (\alpha/\theta)\delta\beta_0 f(I) I + (\varphi+\beta_0 f(I))(\alpha+\gamma) I - N\delta\beta_0 f(I)}{\delta\beta_0 f(I)} \\
&= \frac{(\delta+\varphi)(\alpha+\gamma)}{\delta\beta_0 f'(0)}\left[1 - \frac{N\delta\beta_0 f'(0)}{(\delta+\varphi)(\alpha+\gamma)}\right].
\end{aligned} \tag{9}$$

From (9), we can conclude that $H(0) < 0$ when $R_0 > 1$. Hence, there exists a positive equilibrium point if $R_0 > 1$. The proof is completed. □

Since $Q(t) = N - S(t) - I(t) - V(t) - D(t)$, we can simplify system (2) as follows:

$$\frac{dS(t)}{dt} = -\beta_0 f(I(t)) S(t) - \varphi S(t) + \delta V(t-\tau),$$

$$\begin{aligned}
\frac{dI(t)}{dt} &= \beta_0 f(I(t)) S(t) - (\gamma + \alpha) I(t), \\
\frac{dV(t)}{dt} &= \varphi S(t) + \gamma I(t) \\
&\quad + \theta (N - S(t) - I(t) - V(t) - D(t)) \\
&\quad - \delta V(t), \\
\frac{dD(t)}{dt} &= \delta V(t) - \delta V(t - \tau).
\end{aligned} \tag{10}$$

The Jacobi matrix of system (10) about $E^* = (S^*, I^*, Q^*, V^*, D^*)$ is given by

$$J(E^*) = \begin{pmatrix} \beta_0 f(I) + \varphi & \beta_0 f'(I) S & 0 & -\delta e^{-\lambda\tau} \\ -\beta_0 f(I) & \beta_0 f'(I) S - (\alpha + \gamma) & 0 & 0 \\ 0 & 0 & 0 & \delta e^{-\lambda\tau} - \delta \\ \theta - \varphi & \theta - \gamma & \theta & -\theta - \delta \end{pmatrix}. \tag{11}$$

The characteristic equation of the matrix (11) can be obtained by

$$P(\lambda) + Q(\lambda) e^{-\lambda\tau} = 0. \tag{12}$$

The expressions of $P(\lambda)$ and $Q(\lambda)$ are

$$\begin{aligned}
P(\lambda) &= \lambda^4 + p_3\lambda^3 + p_2\lambda^2 + p_1\lambda + p_0, \\
Q(\lambda) &= q_2\lambda^2 + q_1\lambda + q_0,
\end{aligned} \tag{13}$$

where

$$\begin{aligned}
p_3 &= -\beta_0 f'(I) S + (\alpha + \gamma) + \beta_0 f(I) + \varphi + \theta + \delta, \\
p_2 &= -\beta_0 f'(I) S (\theta + \delta + \varphi) + \beta_0 f(I) (\theta + \delta + \alpha + \gamma) \\
&\quad + (\alpha + \gamma)(\theta + \delta + \varphi) + (\theta + \delta)\varphi + \theta\delta, \\
p_1 &= -\beta_0 f'(I) S (\theta\delta + \delta\varphi + \varphi\theta) \\
&\quad + \beta_0 f(I) (\theta\gamma + \delta\gamma + \alpha\theta + \delta\alpha + \theta\delta) \\
&\quad + (\alpha + \gamma)(\theta\delta + \delta\varphi + \varphi\theta) + \delta\theta\varphi, \\
p_0 &= \left[-\beta_0 f'(I) S\varphi + \beta_0 f(I)(\alpha + \gamma) + (\alpha + \gamma)\varphi\right] \delta\theta, \\
q_2 &= -\varphi\delta, \\
q_1 &= \beta_0 f'(I) S\varphi\delta - \beta_0 f(I)\delta\gamma - (\alpha + \gamma)\delta\varphi - \varphi\theta\delta, \\
q_0 &= -\left[-\beta_0 f'(I) S\varphi + \beta_0 f(I)(\alpha + \gamma) + (\alpha + \gamma)\varphi\right] \delta\theta.
\end{aligned} \tag{14}$$

Theorem 2. *If the condition is satisfied as* (H_1)*, the positive equilibrium* $E^* = (S^*, I^*, Q^*, V^*, D^*)$ *is locally asymptotically stable without time delay.*

$$\begin{aligned}
(H_1): \quad & p_3 > 0, \\
& p_3(p_2 + q_2) - (p_1 + q_1) > 0, \\
& (p_1 + q_1) > 0.
\end{aligned} \tag{15}$$

Proof. When $\tau = 0$, (12) simplifies to

$$\lambda^4 + p_3\lambda^3 + (p_2 + q_2)\lambda^2 + (p_1 + q_1)\lambda + p_0 + q_0 = 0. \tag{16}$$

According to Routh-Hurwitz criterion, all the roots of (16) have negative real parts. Hence, we can deduce that the positive equilibrium $E^* = (S^*, I^*, Q^*, V^*, D^*)$ is locally asymptotically stable without time delay. The proof is completed. □

Assuming that $\lambda = iw$ is the root of (12), we substitute it into (12). After separating the real and imaginary parts, we can get the following two equations:

$$\begin{aligned}
& w^4 - p_2 w^2 + p_0 + \left(q_0 - q_2 w^2\right) \cos(w\tau) \\
& \quad + q_1 w \sin(w\tau) = 0.
\end{aligned} \tag{17}$$

$$\begin{aligned}
& -p_3 w^3 + p_1 w - \left(q_0 - q_2 w^2\right) \sin(w\tau) \\
& \quad + q_1 w \cos(w\tau) = 0,
\end{aligned} \tag{18}$$

Uniting (17) and (18), we can obtain

$$\begin{aligned}
& \left(q_0 - q_2 w^2\right)^2 + (q_1 w)^2 \\
& \quad = \left(w^4 - p_2 w^2 + p_0\right)^2 + \left(-p_3 w^3 + p_1 w\right)^2.
\end{aligned} \tag{19}$$

It can be written as

$$w^8 + D_3 w^6 + D_2 w^4 + D_1 w^2 + D_0 = 0, \tag{20}$$

where

$$\begin{aligned}
D_3 &= p_3^2 - 2p_2, \\
D_2 &= 2p_0 + p_2^2 - 2p_3 p_1 - q_2^2, \\
D_1 &= p_1^2 - 2p_2 p_0 + 2q_0 q_2 - q_1^2, \\
D_0 &= p_0^2 - q_2^2.
\end{aligned} \tag{21}$$

Let $z = w^2$; then (20) can be turned into

$$h(z) = z^4 + D_3 z^3 + D_2 z^2 + D_1 z + D_0. \tag{22}$$

Theorem 3. *Assume that* (H_1) *is satisfied;* (a) $D_0 \geq 0$, $\Delta \geq 0$, $z_1 > 0$, *or* $h(z_1) > 0$; (b) $D_0 \geq 0$, $\Delta < 0$, *and there is no* $z^* \in (z_1, z_2, z_3)$ *such that* $z^* > 0$ *and* $h(z^*) \leq 0$. *Then the positive equilibrium* $E^* = (S^*, I^*, Q^*, V^*, D^*)$ *of system (1) is absolutely stable. Namely,* $E^* = (S^*, I^*, Q^*, V^*, D^*)$ *is asymptotically stable for any time delay* $\tau \geq 0$.

Assume that the coefficients in $h(z)$ satisfy the following condition:

(H_3): (a) $D_0 \geq 0,\ \Delta \geq 0,\ z_1 > 0$, or $h(z_1) > 0$; (b) $D_0 \geq 0, \Delta < 0$, and there is no $z^* \in (z_1, z_2, z_3)$ such that $z^* > 0$ and $h(z^*) \leq 0$.

According to previous lemmas, it can be known that (22) has at least a positive root w_0, which also means that the characteristic equation (12) has a pair of purely imaginary roots $\pm iw_0$.

Since the pair of purely imaginary roots $\pm w_0$ is the roots of (12), we can get the corresponding $\tau_k > 0$ by uniting (17) and (18).

$$\tau_k = \frac{1}{w_0}\arccos\left[\frac{\left(q_2w^2 - q_0\right)\left(w^4 - p_2w^2 + p_0\right) + \left(p_3w^3 - p_1w\right)q_1w}{\left(q_2w^2 - q_0\right)^2 + \left(q_1w\right)^2}\right] + \frac{2k\pi}{w_0}. \tag{23}$$

Let $\lambda(\tau) = v(\tau) + iw(\tau)$ be the root of (12). It is satisfied that $v(\tau_k) = 0,\ w(\tau_k) = w_0$.

Lemma 4. *Suppose that $h'(z_0) \neq 0$. If $\tau = \tau_0$, then $\pm iw_0$ is a pair of purely imaginary roots of (12). Moreover, if the conditions in Lemma 3.4 (1) in [14] are satisfied, then*

$$\frac{d\,\mathrm{Re}\,\lambda\left(\tau_0\right)}{d\tau} > 0. \tag{24}$$

This means that there exists at least one eigenvalue with positive real part when $\tau > \tau_k$. Differentiating on both sides of (12) with respect to τ, we can obtain

$$\begin{aligned}\left(\frac{d\lambda}{d\tau}\right)^{-1} &= \frac{4\lambda^3 + 3p_3\lambda^2 + 2p_2\lambda + p_1 + \left(2q_2\lambda + q_1\right)e^{-\lambda\tau} - \left(q_2\lambda^2 + q_1\lambda + q_0\right)\tau e^{-\lambda\tau}}{\left(q_2\lambda^2 + q_1\lambda + q_0\right)\lambda e^{-\lambda\tau}} \\ &= \frac{\left(4\lambda^3 + 3p_3\lambda^2 + 2p_2\lambda + p_1\right)e^{\lambda\tau}}{\left(q_2\lambda^2 + q_1\lambda + q_0\right)\lambda} + \frac{2q_2\lambda + q_1}{\left(q_2\lambda^2 + q_1\lambda + q_0\right)\lambda} - \frac{\tau}{\lambda}.\end{aligned} \tag{25}$$

According to (17) and (18), we obtain the following:

$$\begin{aligned}\mathrm{sgn}\left[\frac{d\,\mathrm{Re}\,\lambda}{d\tau}\right]_{\tau=\tau_k} &= \mathrm{sgn}\left[\mathrm{Re}\left(\frac{d\lambda}{d\tau}\right)^{-1}\right]_{\lambda=iw_0} \\ &= \mathrm{sgn}\left[\mathrm{Re}\left(\frac{\left(4\lambda^3 + 3p_3\lambda^2 + 2p_2\lambda + p_1\right)e^{\lambda\tau}}{\left(q_2\lambda^2 + q_1\lambda + q_0\right)\lambda} + \frac{2q_2\lambda + q_1}{\left(q_2\lambda^2 + q_1\lambda + q_0\right)\lambda} - \frac{\tau}{\lambda}\right)\right]_{\lambda=iw_0} \\ &= \mathrm{sgn}\left[\mathrm{Re}\left(\frac{\left(-4{w_0}^3 i - 3p_3{w_0}^2 + 2p_2iw_0 + p_1\right)\left(\cos\left(w_0\tau_k\right) + i\sin\left(w_0\tau_k\right)\right) + 2q_2iw_0 + q_1}{\left(-q_2{w_0}^2 + q_1w_0i + q_0\right)iw_0}\right)\right] \\ &= \mathrm{sgn}\frac{1}{\Gamma}\left[4w_0^8 + \left(3p_3^2 - 6p_2\right)w_0^6 + \left(4p_0 + 2p_2^2 - 4p_3p_1 - 2q_2^2\right)w_0^4 + \left(p_1^2 - 2p_2p_0 + 2q_0q_2 - q_1^2\right)w_0^2\right] \\ &= \mathrm{sgn}\frac{w_0^2}{\Gamma}\left(4w_0^6 + 3D_3w_0^4 + 2D_2w_0^2 + D_1\right) = \mathrm{sgn}\frac{w_0^2}{\Gamma}\left\{h'\left(w_0^2\right)\right\} = \mathrm{sgn}\left\{h'\left(w_0^2\right)\right\},\end{aligned} \tag{26}$$

where $\Gamma = (q_0w_0 - q_2w_0^3)^2 + (q_1w_0^2)^2$.

Then it follows hypothesis (H_3) and $h'(w_0^2) \neq 0$. Therefore

$$\left.\frac{d\left(\mathrm{Re}\,\lambda\right)}{d\tau}\right|_{\tau=\tau_k} > 0. \tag{27}$$

According to Routh's theorem, the root of characteristic equation (12) crosses from left to right on the imaginary axis as τ continuously varies from a value less than τ_k to one greater than τ_k. Hence, according to Hopf bifurcation theorem for functional differential equations, the transverse

condition holds and the conditions for Hopf bifurcation are satisfied at $\tau = \tau_k$.

Theorem 5. *Supposing that the conditions* (H_1) *and* (H_2) *are satisfied,*

(1) *when* $\tau < \tau_0$, *the positive equilibrium* $E^* = (S^*, I^*, Q^*, V^*, D^*)$ *of system (2) is locally asymptotically stable and it is unstable when* $\tau \geq \tau_0$,

(2) *when system (2) satisfies* (H_3), *the system undergoes a Hopf bifurcation at the positive equilibrium* $E^* = (S^*, I^*, Q^*, V^*, D^*)$ *when* $\tau = \tau_0$.

This implies that when the time delay $\tau < \tau_0$, *the system will stabilize at its equilibrium point, which is beneficial for us to implement a containment strategy; when the delay* $\tau \geq \tau_0$, *the system will be unstable and worms cannot be effectively controlled.*

4. Numerical Simulations and Simulations Experiments

In order to verify the theorems proposed in this paper, we have made the numerical experiments in this section. We select the Slammer worm for experiments. The total number of hosts N is assumed as 400000. Based on the actual situation, the worm's average scan rate is $\eta = 4000$ per second. We can calculate the infection rate $\beta = \eta/2^{32} = 0.00000093$. The susceptible hosts change to vaccinated hosts at rate $\varphi = 0.001$. The recovered rate of infectious hosts is set as $\gamma = 0.002$. The quarantine rate α of infectious hosts is 0.2 and the immunity rate θ of quarantined hosts is 0.05. The vaccinated hosts lose immunity at rate $\delta = 0.08$. We choose the nonlinear function $f_1(I(t)) = 1/(1 + aI(t))$; then we have $f(I(t)) = I(t)/(1 + aI(t))$, where a is the parameter that represents the infection rate sensitivity to the number of infected hosts $I(t)$ [27]. When a is zero, it means that the infection rate is a constant. Then we can get $R_0 = 1.819 > 1$. At first, the number of infectious hosts is five and the others' states are susceptible.

When $\tau = 10 < \tau_0$, we can see the changes of the numbers of four kinds of hosts in Figure 2. From Figure 2, we can find that every kind of hosts will be stable when $t = 400$, which implies that E^* is locally asymptotically stable. Figure 3 shows the numbers of susceptible, infectious, quarantined, vaccinated, and delayed hosts when $\tau = 60 > \tau_0$. In this figure, it can be clearly found that the curves of hosts are fluctuant and it is hard for us to predict the propagation of worms.

In order to see the influence of time delay, Figure 4 shows the number of infectious hosts in the same coordinate with different time delays $\tau = 5$, $\tau = 15$, $\tau = 45$, and $\tau = 65$. Initially, time delay has little effect in the initial stage of worm propagation, which can be obtained by the overlap of the four curves. With the increase of time delay, the curve begins to oscillate. The infecting process gets unstable with time delay passing through the threshold τ_0, which meets our conclusions.

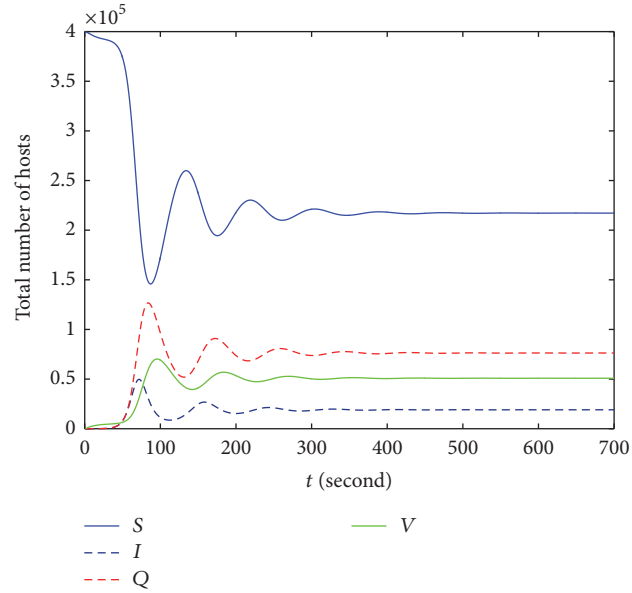


Figure 2: The worm propagation of the four kinds of hosts' results with $\tau < \tau_0$.

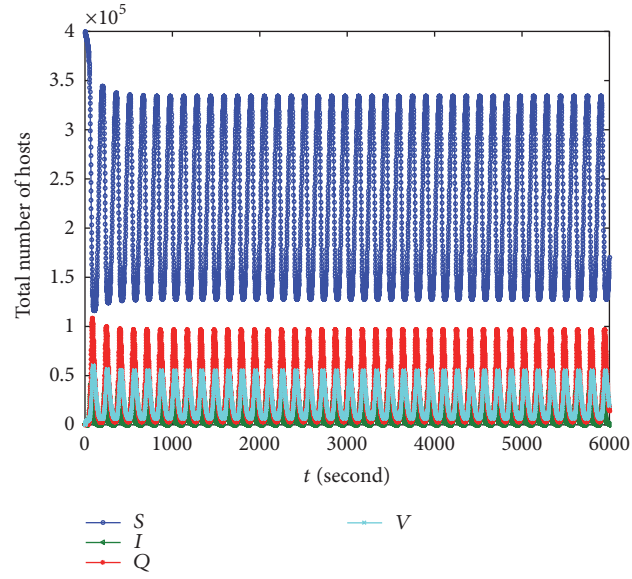


Figure 3: The worm propagation of the four kinds of hosts' results with $\tau > \tau_0$.

Figures 5 and 6 show the number of infected hosts in the same condition with $a = 0.0000001$, $a = 0.000001$, and $a = 0.00001$ when $\tau < \tau_0$ and $\tau > \tau_0$. From these two figures, we can get the conclusion that the larger a is, the lower peak of the number of infectious hosts is. Therefore, we can choose appropriate a to get proper $\beta(t)$ to constrain the spread of Internet worms.

Figure 7 shows the phase portrait of susceptible hosts $S(t)$ and infectious hosts $I(t)$ of system (2) when $\tau = 30 < \tau_0$. Moreover, Figure 8 shows the condition when $\tau = 60 > \tau_0$. From the figures, we can find that the curve converges to

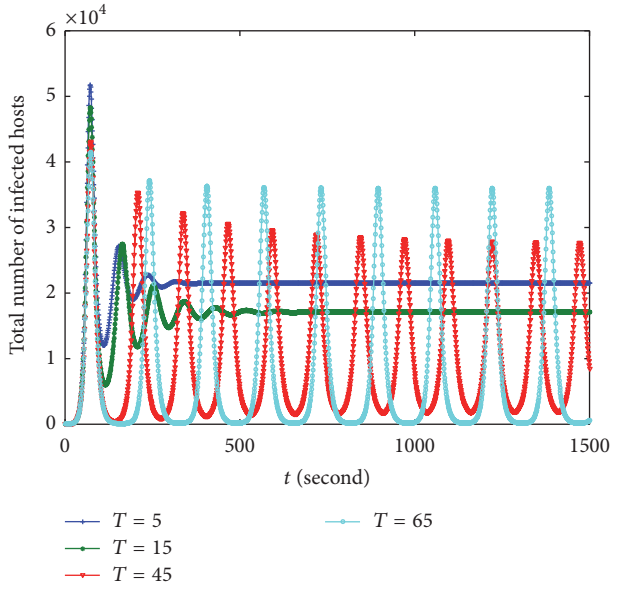


Figure 4: The number of infected hosts $I(t)$ with the change of τ.

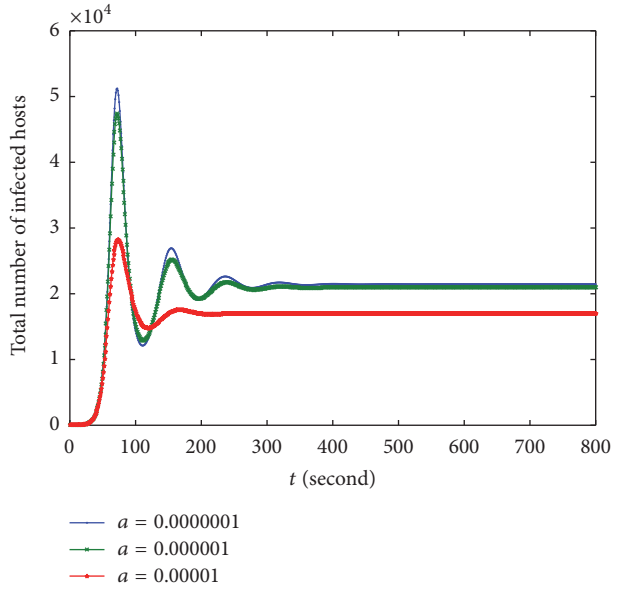


Figure 5: Relationship between a and the number of $I(t)$ when $\tau = 5$.

a fixed point, which implies that the system is stable when $\tau = 30 < \tau_0$ and the curve radiates to a limit cycle, which implies that the system is unstable when $\tau = 60 > \tau_0$. Figures 9 and 10 are the projection of the phase portrait of system (2) in (S, I, V)-space at $\tau = 30$ and $\tau = 60$. The same conclusion can be obtained by the figures.

Figure 11 gives the bifurcation diagram of system (2) with the parameter $a = 0.0000001$. It can be easily obtained that the Hopf bifurcation occurs at $\tau = \tau_0 = 37$, which is similar to results of theoretical derivation. Figure 12 gives the bifurcation diagram of system (2) with the parameter $a = 0.00001$. The Hopf bifurcation occurs at $\tau = \tau_0 = 76$.

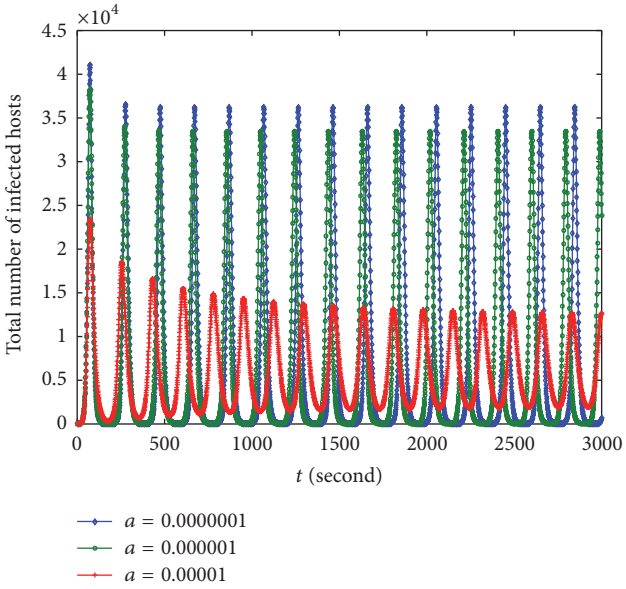


Figure 6: Relationship between a and the number of $I(t)$ when $\tau = 85$.

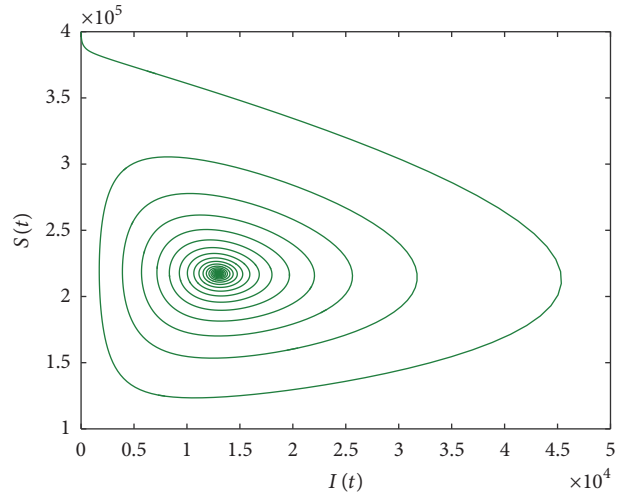


Figure 7: The phase portrait of $S(t)$ and $I(t)$ when $\tau = 30$.

Comparing the two figures, it is shown that the parameter a has effect on the time of Hopf bifurcation occurrence. As the parameter a increases, the Hopf bifurcation occurs at a later time.

In order to simulate the actual behaviour of worm propagation and verify the correctness of the theoretical analysis and numerical simulation, we carry out the discrete-time simulation, which is an expanded version of Zou et al.'s [7] program. The simulation experiment is used to simulate the worm propagation in the real network. There are 400000 hosts in our simulation experiments. At first, we randomly choose five hosts in the network to be infectious hosts and the others' states are set to be susceptible. In the simulation experiments, the implementation of transition rates of the worm propagation model depends on probability.

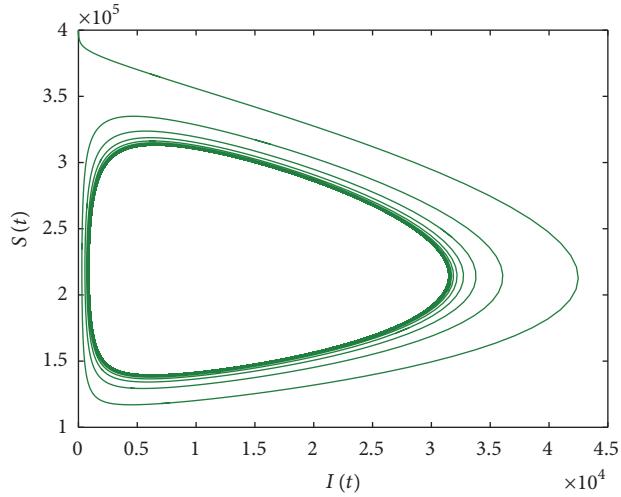


Figure 8: The phase portrait of $S(t)$ and $I(t)$ when $\tau = 50$.

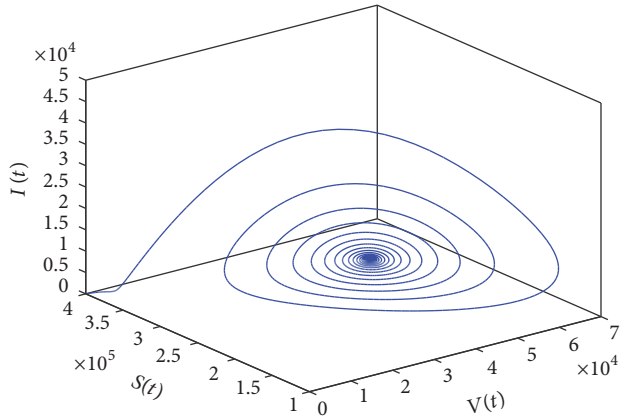


Figure 9: The projection of the phase portrait of system (2) in (S, I, V)-space when $\tau = 30$.

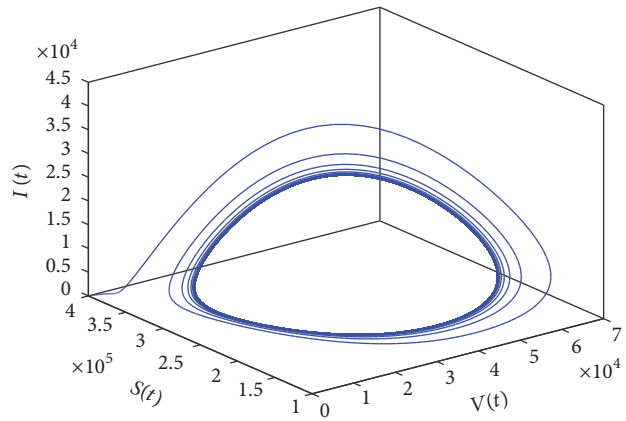


Figure 10: The projection of the phase portrait of system (2) in (S, I, V)-space when $\tau = 50$.

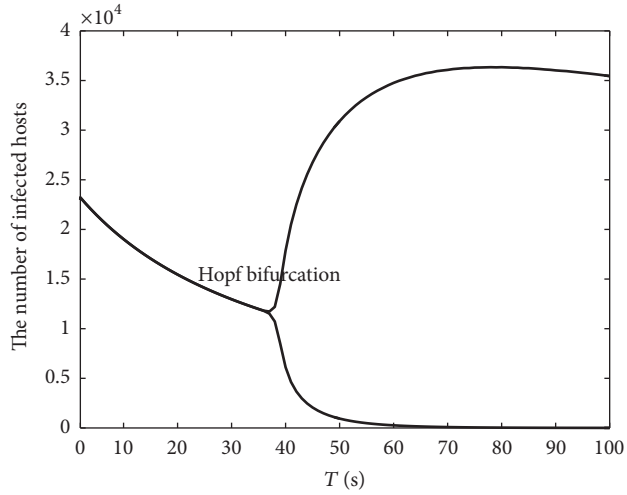


Figure 11: Bifurcation diagram of system (2) with $a = 0.0000001$.

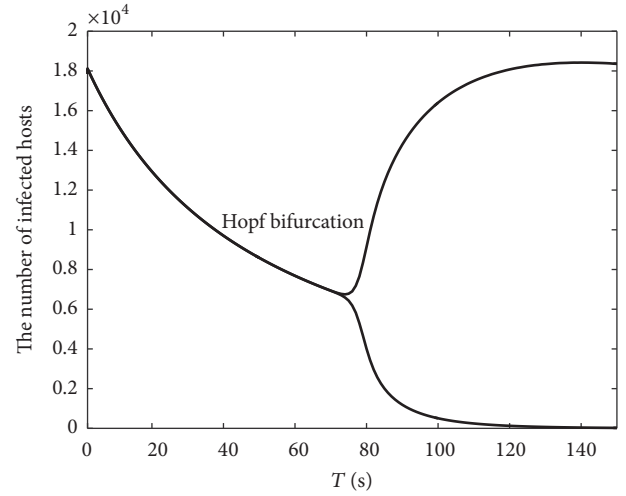


Figure 12: Bifurcation diagram of system (2) with $a = 0.00001$.

Figure 13 shows the comparisons between numerical and simulation curves of susceptible, infectious, quarantined, and vaccinated hosts when $\tau = 10 < \tau_0$, which implies that the simulation curves match the numerical curves very well.

When the value of τ increases and passes over the threshold value of τ_0, namely, $\tau = 60 > \tau_0$, numerical and simulation curves of susceptible, infectious, quarantined, and vaccinated hosts can also match very well as Figure 14 shows. We can find that there exists a difference between numerical and simulation curves because of the high precision of numerical and simulation curves because of the high precision of numerical experiment. However, the small difference does not affect the validity of our conclusions.

5. Conclusions

In this paper, we propose a SIQVD model with the variable infection rate based on the consideration of a quarantine strategy. Then we analyse the stability of the positive equilibrium and Hopf bifurcation. The critical time delay τ_0 in which Hopf bifurcation appears is obtained. Through the theoretical analysis, the useful conclusions are obtained, which can be verified by the numerical experiments and simulations. The following conclusions can be derived by the currentresearch:

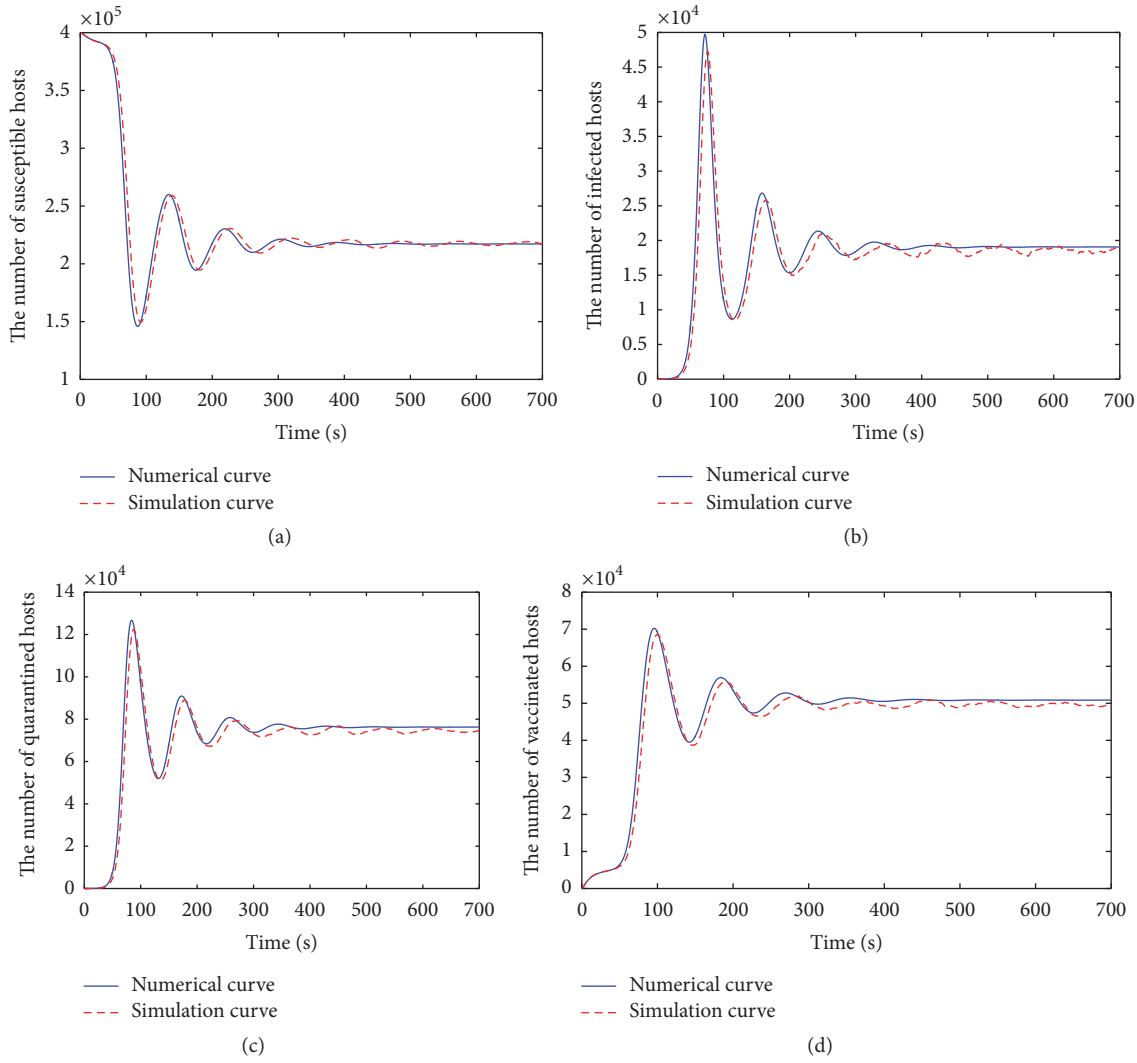


FIGURE 13: Comparisons between numerical and simulation curves of system (2) when $\tau = 10 < \tau_0$.

(1) The worm propagation system is stable when time delay $\tau < \tau_0$. In this condition, we can predict the spread of worms correctly, and the worms can be reduced to a low extent at last.

(2) The worm propagation system is unstable when time delay $\tau \geq \tau_0$, and the system is out of control. Therefore, time delay should be controlled in a proper range: $\tau < \tau_0$.

(3) When parameter a increases an order of magnitude, the infection rate reduces and the peak of the number of infected hosts will decrease very obviously. Meanwhile, R_0 will be reduced by the decrease of $f'(0)$. Hence, there exists a threshold for a, and we can choose proper infection rate by adjusting the value of a to control the prevalence of worms.

The worm propagation model can be used for Internet worms, such as Code Red worms, Slammer worms, and Witty worms. It can predict the spreading behaviour of Internet worms more realistically. In our future work, we will focus more on the network structure and study it further.

Notations

$S(t)$: The number of susceptible hosts at time t
$I(t)$: The number of infectious hosts at time t
$Q(t)$: The number of quarantined hosts at time t
$V(t)$: The number of vaccinated hosts at time t
$D(t)$: The number of delay hosts at time t
N: The total number of hosts throughout Internet
$\beta(t)$: The infection rate at time t
β_0: The initial infection rate
φ: The immune rate of susceptible hosts
γ: The recovered rate of infectious hosts
α: The quarantine rate of infectious hosts
θ: The immunity rate of quarantined hosts
δ: The rate at which the vaccinated hosts lose immunity.

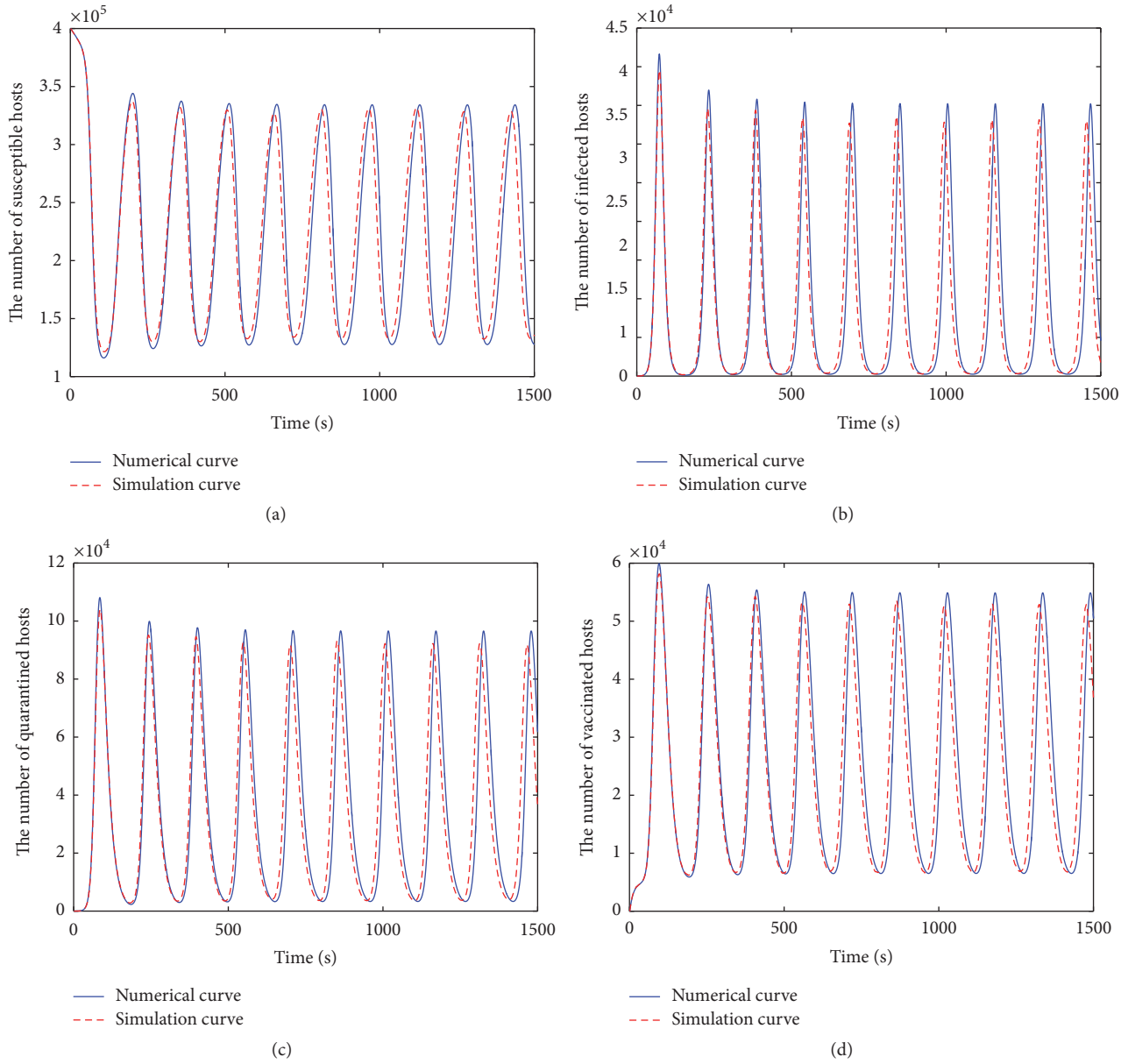


FIGURE 14: Comparisons between numerical and simulation curves of system (2) when $\tau = 60 > \tau_0$.

Conflicts of Interest

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

Acknowledgments

This paper is supported by Program for Fundamental Research Funds of the Central Universities (Grants nos. N150402006 and N161704005) and the Doctoral Scientific Research Foundation of Liaoning Province (20170520122).

References

[1] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time," pp. 149–169, 2002.

[2] J. C. Martin, L. L. Burge, J. I. Gill, A. N. Washington, and M. Alfred, "Modelling the spread of mobile malware," *International Journal of Computer Aided Engineering and Technology (IJCAET)*, vol. 2, no. 1, pp. 3–14, 2010.

[3] S. H. Qing and W. P. Wen, "A survey and trends on internet worms," *Computers & Security*, vol. 24, no. 4, pp. 334–346, 2005.

[4] K. M. Bimal and K. S. Dinesh, "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.

[5] R. Xu, Z. Ma, and Z. Wang, "Global stability of a delayed SIRS epidemic model with saturation incidence and temporary immunity," *Computers & Mathematics with Applications. An International Journal*, vol. 59, no. 9, pp. 3211–3221, 2010.

[6] 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.

[7] C. C. Zou, W. B. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense," in *Proceedings of the ACM Workshop on Rapid Malcode (WORM '03)*, pp. 51–60, Washington, DC, USA, October 2003.

[8] B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Applied Mathematical Modelling*, vol. 37, no. 6, pp. 4103–4111, 2013.

[9] R. Albert and A. L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.

[10] J. Ren, Y. Xiaofan, and L. X. Yang, "A delayed computer virus propagation model and its dynamics Chaos," *Chaos, Solitons & Fractals*, vol. 45, no. 1, pp. 74–79, 2012.

[11] 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.

[12] Q. Zhu, X. Yang, and J. Ren, "Modeling and analysis of the spread of computer virus," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 5117–5124, 2012.

[13] Y. Yao, X. W. Xie, H. Guo, G. Yu, F. X. Gao, and X. J. Tong, "Hopf bifurcation in an Internet worm propagation model with time delay in quarantine," *Mathematical and Computer Modelling*, vol. 57, no. 11-12, pp. 2635–2646, 2013.

[14] Y. Yao, W. Xiang, A. Qu, G. Yu, and F. Gao, "Hopf bifurcation in an SEIDQV worm propagation model with quarantine strategy," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 304868, 18 pages, 2012.

[15] Y. Yao, X. Feng, W. Yang, W. Xiang, and F. Gao, "Analysis of a delayed internet worm propagation model with impulsive quarantine strategy," *Mathematical Problems in Engineering*, vol. 5, p. 2014, 2014.

[16] Y. Yao, L. Guo, and H. Guo, "Pulse quarantine strategy of internet worm propagation: Modelling and analysis," *Computers Electrical Engineering*, vol. 38, no. 5, pp. 1047–1061, 2012.

[17] L. X. Yang, X. Yang, J. Liu, Q. Zhu, and C. Gan, "Epidemics of computer viruses: s complex-network approach," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8705–8717, 2013.

[18] O. J. Kephart, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, Calif, USA, 1991.

[19] J. Ren, X. Yang, Q. Zhu, L. Yang, and C. Zhang, "A novel computer virus model and its dynamics," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 1, pp. 376–384, 2012.

[20] C. Gan, X. Yang, W. Liu, Q. Zhu, and X. Zhang, "Zhang Propagation of Computer Virus under Human Intervention: A Dynamical Model," in *Discrete Dynamics in Nature and Society*, pp. 203–222, 203-222, 2012.

[21] C. Gan, X. Yang, Q. Zhu, J. Jin, and L. He, "The spread of computer virus under the effect of external computers," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1615–1620, 2013.

[22] X. Han and Q. Tan, "Dynamical behavior of computer virus on Internet," *Applied Mathematics and Computation*, vol. 217, no. 6, pp. 2520–2526, 2010.

[23] X. Yang and L. X. Yang, "Towards the epidemiological modeling of computer viruses," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 259671, 2012.

[24] C. Zhang, Y. Zhao, and Y. Wu, "An impulse model for computer viruses," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 260962, 13 pages, 2012.

[25] C. Gan, X. Yang, W. Liu, Q. Zhu, and X. Zhang, "An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate," *Applied Mathematics and Computation*, vol. 222, pp. 265–274, 2013.

[26] C. M. A. Pinto, "Effects of dynamic quarantine and nonlinear infection rate in a model for computer worms propagation," in *Proceedings of the International Conference on Numerical Analysis and Applied Mathematics 2014, ICNAAM 2014*, Greece, September 2014.

[27] L. Feng, X. Liao, Q. Han, and H. Li, "Dynamical analysis and control strategies on malware propagation model," *Applied Mathematical Modelling*, vol. 37, no. 16-17, pp. 8225–8236, 2013.

[28] S. M. Moghadas and A. B. Gumel, "Global stability of a two-stage epidemic model with generalized non-linear incidence," *Mathematics and Computers in Simulation*, vol. 60, no. 1-2, pp. 107–118, 2002.

Hindawi
Security and Communication Networks
Volume 2018, Article ID 2975376, 14 pages
https://doi.org/10.1155/2018/2975376

Research Article

Defending against the Advanced Persistent Threat: An Optimal Control Approach

Pengdeng Li,[1,2] Xiaofan Yang,[1,2] Qingyu Xiong,[1,2] Junhao Wen,[1,2] and Yuan Yan Tang[3]

[1]*Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing University, Chongqing 400044, China*
[2]*School of Software Engineering, Chongqing University, Chongqing 400044, China*
[3]*Department of Computer and Information Science, The University of Macau, Macau*

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

Received 30 September 2017; Accepted 28 January 2018; Published 27 February 2018

Academic Editor: Angel M. Del Rey

The new cyberattack pattern of advanced persistent threat (APT) has posed a serious threat to modern society. This paper addresses the APT defense problem, that is, the problem of how to effectively defend against an APT campaign. Based on a novel APT attack-defense model, the effectiveness of an APT defense strategy is quantified. Thereby, the APT defense problem is modeled as an optimal control problem, in which an optimal control stands for a most effective APT defense strategy. The existence of an optimal control is proved, and an optimality system is derived. Consequently, an optimal control can be figured out by solving the optimality system. Some examples of the optimal control are given. Finally, the influence of some factors on the effectiveness of an optimal control is examined through computer experiments. These findings help organizations to work out policies of defending against APTs.

1. Introduction

Nowadays, the daily operation of most organizations, ranging from large enterprises and financial institutions to government sectors and military branches, depends largely on computers and networks. However, this dependency renders the organizations vulnerable to a wide range of cyberattacks. Traditional cyberattacks include computer viruses, worms, and spyware. Conventional cyber defense measures including firewall and intrusion detection turn out to be effective in withstanding these cyberattacks [1, 2].

The cybersecurity landscape has changed drastically over the past few years. A new type of cyberattack—advanced persistent threat (APT)—has posed an unprecedentedly serious threat to modern society. According to report, many high-profile organizations have experienced APTs [3], and the number of APTs has been increasing rapidly [4]. Compared with traditional cyberattacks, APTs exhibit two distinctive characteristics: (a) The attacker of an APT is a well-resourced and well-organized group, with the goal of stealing as many sensitive data as possible from a specific organization. (b) Based on meticulous reconnaissance, the attacker is going to launch a preliminary advanced social engineering attack on a few target users to gain footholds in the organization and then to gain access to critical information stealthily and slowly [5–7]. Due to these characteristics, APTs can evade traditional detection, causing tremendous damage to organizations. To date, the detection of APTs is far from mature [8, 9]. Consequently, the APT defense problem, that is, the problem of how to effectively defend against APTs, has become a major concern in the field of cybersecurity.

As a branch of applied mathematics, optimal control theory aims to solve a class of optimization problems in which, subject to a set of dynamic constraints, we seek to find a function (control) so that an objective functional is optimized [10, 11]. In real world applications, the set of dynamic constraints represents a dynamic environment, a control represents a time-varying strategy, and the objective functional represents an index to be maximized or minimized. Optimal control theory has been successfully applied

to some aspects of cybersecurity [12–19]. To our knowledge, the APT defense problem has yet to be addressed in the framework of optimal control theory. To model the problem as an optimal control problem, we have to formulate an APT defense strategy as a control, characterize the state evolution of an organization as a set of dynamic constraints, and quantify the effectiveness of an APT defense strategy as an objective functional. The key to the modeling process is to accurately characterize the state evolution of an organization by employing the epidemic modeling technique [20].

Individual-level epidemic models refer to epidemic models in which the state evolution of each individual in a population is characterized by one or a few separate differential equations. As compared with the coarse-fined state-level epidemic models [21–26] and the intermediate degree-level epidemic models [27–33], the finest individual-level epidemic models can characterize spreading processes more accurately, because they can perfectly accommodate the network topology. The individual-level epidemic modeling technique has been successfully applied to areas such as the epidemic spreading [34–37], the malware spreading [38–43], and the rumor spreading [44]. In particular, a number of APT attack-defense models have recently been proposed by employing this technique [45–48].

This paper focuses on the APT defense problem. Based on a novel individual-level APT attack-defense model, the effectiveness of an APT defense strategy is quantified. On this basis, the APT defense problem is modeled as an optimal control problem, in which an optimal control represents a most effective APT defense strategy. The existence of an optimal control to the optimal control problem is proved, and an optimality system for the optimal control problem is derived. Therefore, an optimal control can be figured out by solving the optimality system. Some examples of the optimal control are presented. Finally, the influence of some factors on the effectiveness of an optimal control is examined through computer simulations. To our knowledge, this is the first time the APT defense problem is dealt with in this way. These findings help organizations to work out policies of defending against APTs.

The remaining materials are organized in this fashion. Section 2 models the APT defense problem as an optimal control problem. Section 3 studies the optimal control problem. Some most effective APT defense strategies are given in Section 4. Section 5 discusses the influence of different factors on the optimal effectiveness. This work is closed by Section 6.

2. The Modeling of the APT Defense Problem

The goal of this paper is to solve the following problem.

The APT Defense Problem. Defend an organization against APTs in an effective way.

To achieve the goal, we have to model the problem. The modeling process consists of the following four steps.

Step 1. Introduce preliminary terminologies and notations.

Step 2. Establish an APT attack-defense model.

Step 3. Quantify the effectiveness of an APT defense strategy.

Step 4. Model the APT defense problem as an optimal control problem.

Now, let us proceed by following this four-step procedure.

2.1. Preliminary Terminologies and Notations. Consider an organization with a set of N computer systems labeled $1, 2, \ldots, N$. Let $G = (V, E)$ denote the access network of the organization, where (a) each node stands for a system, that is, $V = \{1, 2, \ldots, N\}$, and (b) $(i, j) \in E$ if and only if system i has access to system j. Let $\mathbf{A} = [a_{ij}]_{N\times N}$ denote the adjacency matrix for the network, that is, $a_{ij} = 1$ or 0 according to $(i, j) \in E$ or not.

Suppose an APT campaign to the organization starts at time $t = 0$ and terminates at time $t = T$. Suppose at any time $t \in [0, T]$ every node in the organization is either *secure*, that is, under the defender's control, or *compromised*, that is, under the attacker's control. Let $X_i(t) = 0$ and 1 denote the event that node i is secure and compromised at time t, respectively. The vector

$$\mathbf{X}(t) = \left[X_1(t), X_2(t), \ldots, X_N(t)\right] \tag{1}$$

stands for the *state* of the organization at time t. Let $S_i(t)$ and $C_i(t)$ denote the probability of the event that node i is secure and compromised at time t, respectively. That is,

$$\begin{aligned} S_i(t) &= \Pr\left\{X_i(t) = 0\right\}, \\ C_i(t) &= \Pr\left\{X_i(t) = 1\right\}. \end{aligned} \tag{2}$$

As $S_i(t) + C_i(t) \equiv 1$, the vector

$$\mathbf{C}(t) = \left[C_1(t), \ldots, C_N(t)\right]^T \tag{3}$$

stands for the *expected state* of the organization at time t.

From the attacker's perspective, each secure node in the organization is subject to the external attack. Let a_i denote the cost per unit time for attacking a secure node i. The vector

$$\mathbf{a} = \left[a_1, \ldots, a_N\right] \tag{4}$$

stands for an *attack strategy*. Additionally, each secure node is vulnerable to all the neighboring compromised nodes.

From the defender's perspective, each secure node in the organization is protected from being compromised. Let $x_i(t)$ denote the cost per unit time for protecting the secure node i at time t. The vector-valued function

$$\mathbf{x}(t) = \left[x_1(t), \ldots, x_N(t)\right], \quad 0 \le t \le T, \tag{5}$$

stands for a *prevention strategy*. Additionally, each compromised node in the organization is recovered. Let $y_i(t)$ denote the cost per unit time for recovering the compromised node i at time t. The vector-valued function

$$\mathbf{y}(t) = \left[y_1(t), \ldots, y_N(t)\right], \quad 0 \le t \le T, \tag{6}$$

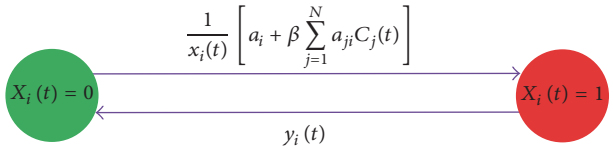


Figure 1: The diagram of state transitions of a node under the hypotheses (H_1)–(H_3).

stands for a *recovery strategy*. We refer to the vector-valued function

$$\begin{aligned}\mathbf{u}(t) &= [\mathbf{x}(t), \mathbf{y}(t)] \\ &= [x_1(t), \ldots, x_N(t), y_1(t), \ldots, y_N(t)], \quad 0 \le t \le T\end{aligned} \tag{7}$$

as an *APT defense strategy*.

2.2. An APT Attack-Defense Model. For fundamental knowledge on differential dynamical systems, see [49]. For our purpose, let us impose a set of hypotheses as follows.

- (H_1) Due to the external attack and prevention, a secure node i gets compromised at time t at the average rate $a_i/x_i(t)$. The rationality of this hypothesis lies in that the average rate is proportional to the attack cost per unit time and is inversely proportional to the prevention cost per unit time.
- (H_2) Due to the internal infection and prevention, a secure node i gets compromised at time t at the average rate $\beta\sum_{j=1}^{N}a_{ji}C_j(t)/x_i(t)$, where $\beta > 0$ is a constant, which we refer to as the *infection force*. The rationality of this assumption lies in that the average rate is proportional to the probability of each neighboring node being compromised and is inversely proportional to the prevention cost per unit time.
- (H_3) Due to the recovery, a compromised node i becomes secure at time t at the average rate $y_i(t)$. The rationality of this assumption lies in that the average rate is proportional to the recovery cost per unit time.

According to these hypotheses, the state transitions of a node are shown in Figure 1. Hence, the time evolution of the expected state of the organization obeys the following dynamical system:

$$\begin{aligned}\frac{dC_i(t)}{dt} &= \frac{1}{x_i(t)}\left[a_i+\beta\sum_{j=1}^{N}a_{ji}C_j(t)\right][1-C_i(t)] \\ &\quad - y_i(t)C_i(t), \quad 0 \le t \le T,\ i = 1, \ldots, N.\end{aligned} \tag{8}$$

We refer to the model as the *APT attack-defense model*.

The APT attack-defense model can be written in matrix-vector notation as

$$\frac{d\mathbf{C}(t)}{dt} = \mathbf{F}(\mathbf{C}(t), \mathbf{u}(t)), \quad 0 \le t \le T. \tag{9}$$

2.3. The Effectiveness of an APT Defense Strategy. The defender's goal is to find the most effective APT defense strategy. To achieve the goal, we have to quantify the effectiveness of an APT defense strategy. For this purpose, let us introduce an additional set of hypotheses as follows.

- (H_4) The prevention cost per unit time is bounded from above by $\overline{x}$ and from below by $\underline{x} > 0$, and the recovery cost per unit time is bounded from above by $\overline{y}$ and from below by $\underline{y} > 0$. That is, the admissible set of APT defense strategies is given by

$$\begin{aligned}\mathcal{U} = \Big\{\mathbf{u} \in \left(L^2[0,T]\right)^{2N} \mid 0 < \underline{x} \le x_i(t) \le \overline{x},\ 0 < \underline{y} \\ \le y_i(t) \le \overline{y},\ 0 \le t \le T,\ 1 \le i \le N\Big\},\end{aligned} \tag{10}$$

  where $L^2[0,T]$ denote the set of all the Lebesgue square integrable functions defined on the interval $[0,T]$ [50].
- (H_5) The amount of losses caused by a compromised node i in the infinitesimal time interval $[t, t+dt]$ is $w_i dt$, where $w_i = \sum_{j=1}^{N}a_{ij}$ stands for the out-degree of node i in the network. The rationality of this hypothesis lies in that the more nodes a node has access to, the more serious the consequence when it is compromised [51, 52].

According to the hypotheses, the expected loss of the organization in the time horizon $[0,T]$ when implementing an APT defense strategy $\mathbf{u} = [\mathbf{x}, \mathbf{y}]$ is

$$\text{Loss}(\mathbf{u}) = \sum_{i=1}^{N}\int_0^T w_i C_i(t)\,dt, \tag{11}$$

and the overall cost for implementing the APT defense strategy is

$$\text{Cost}(\mathbf{u}) = \sum_{i=1}^{N}\int_0^T [x_i(t) + y_i(t)]\,dt. \tag{12}$$

Hence, the effectiveness of the APT defense strategy $\mathbf{u}$ can be measured by the quantity

$$\begin{aligned}J(\mathbf{u}) &= \text{Loss}(\mathbf{u}) + \text{Cost}(\mathbf{u}) \\ &= \sum_{i=1}^{N}\int_0^T w_i C_i(t)\,dt + \sum_{i=1}^{N}\int_0^T [x_i(t) + y_i(t)]\,dt.\end{aligned} \tag{13}$$

Obviously, the smaller this quantity, the more effective the APT defense strategy. Let

$$L(\mathbf{C}(t), \mathbf{u}(t)) = \sum_{i=1}^{N}[w_i C_i(t) + x_i(t) + y_i(t)]. \tag{14}$$

Then

$$J(\mathbf{u}) = \int_0^T L(\mathbf{C}(t), \mathbf{u}(t))\,dt. \tag{15}$$

2.4. The Modeling of the APT Defense Strategy. Based on the previous discussions, the APT defense problem boils down to the following optimal control problem:

$$\begin{aligned} \min_{\mathbf{u}\in\mathcal{U}} \quad & J(\mathbf{u}) = \int_0^T L(\mathbf{C}(t), \mathbf{u}(t))\, dt, \\ \text{subject to} \quad & \frac{d\mathbf{C}(t)}{dt} = \mathbf{F}(\mathbf{C}(t), \mathbf{u}(t)), \quad 0 \le t \le T, \\ & \mathbf{C}(0) = \mathbf{C}_0. \end{aligned} \tag{16}$$

Here, each control stands for an APT defense strategy, the objective functional stands for the effectiveness of an APT defense strategy, the set of constraints stands for the time evolution of the expected state of the organization, an optimal control stands for a most effective APT defense strategy, and the optimal value stands for the effectiveness of a most effective APT defense strategy.

3. A Theoretical Analysis of the Optimal Control Problem

For fundamental knowledge on optimal control theory, see [10, 11]. This section is devoted to studying the optimal control problem (16).

3.1. The Existence of an Optimal Control. As an optimal control to problem (16) represents a most effective APT defense strategy, it is critical to show that the problem does have an optimal control. For this purpose, we need the following lemma [11].

Lemma 1. *Problem (16) has an optimal control if the following five conditions hold simultaneously.*

- (C_1) $\mathcal{U}$ *is closed and convex.*
- (C_2) *There is* $\mathbf{u} \in \mathcal{U}$ *such that the adjunctive dynamical system is solvable.*
- (C_3) $\mathbf{F}(\mathbf{C}, \mathbf{u})$ *is bounded by a linear function in* $\mathbf{C}$.
- (C_4) $L(\mathbf{C}, \mathbf{u})$ *is convex on* $\mathcal{U}$.
- (C_5) $L(\mathbf{C}, \mathbf{u}) \ge c_1\|\mathbf{u}\|^\rho + c_2$ *for some vector norm* $\|\cdot\|$, $\rho > 1$, $c_1 > 0$ *and* c_2.

Next, let us show that the five conditions in Lemma 1 indeed hold.

Lemma 2. *The admissible set* $\mathcal{U}$ *is closed.*

Proof. Let $\mathbf{u} = (x_1, \ldots, x_N, y_1, \ldots, y_N)$ be a limit point of $\mathcal{U}$, and let $\mathbf{u}^{(n)} = (x_1^{(n)}, \ldots, x_N^{(n)}, y_1^{(n)}, \ldots, y_N^{(n)})$, $n = 1, 2, \ldots$, be a sequence of points in $\mathcal{U}$ that approaches $\mathbf{u}$. As $(L^2[0,T])^{2N}$ is complete, we have $\mathbf{u} \in (L^2(0,T))^{2N}$. Hence, the claim follows from the observation that

$$\begin{aligned} &\underline{x} \le x_i(t) = \lim_{n\to\infty} x_i^{(n)}(t) \le \overline{x}, \\ &\underline{y} \le y_i(t) = \lim_{n\to\infty} y_i^{(n)}(t) \le \overline{y}, \\ &\qquad 0 \le t \le T,\ 1 \le i \le N. \end{aligned} \tag{17}$$

□

Lemma 3. *The admissible set* $\mathcal{U}$ *is convex.*

Proof. Let $\mathbf{u}^{(1)} = (x_1^{(1)}, \ldots, x_N^{(1)}, y_1^{(1)}, \ldots, y_N^{(1)})$, $\mathbf{u}^{(2)} = (x_1^{(2)}, \ldots, x_N^{(2)}, y_1^{(2)}, \ldots, y_N^{(2)}) \in \mathcal{U}$, $0 < \eta < 1$. As $(L^2[0,T])^{2N}$ is a real vector space, we get $(1-\eta)\mathbf{u}^{(1)}(t) + \eta\mathbf{u}^{(2)}(t) \in (L^2[0,T])^{2N}$. So, the claim follows from the observation that

$$\begin{aligned} &\underline{x} \le (1-\eta)\, x_i^{(1)}(t) + \eta x_i^{(2)}(t) \le \overline{x}, \\ &\underline{y} \le (1-\eta)\, y_i^{(1)}(t) + \eta y_i^{(2)}(t) \le \overline{y}, \\ &\qquad 0 \le t \le T,\ 1 \le i \le N. \end{aligned} \tag{18}$$

□

Lemma 4. *There is* $\mathbf{u} \in \mathcal{U}$ *such that the associated adjunctive dynamical system is solvable.*

Proof. Consider the adjunctive dynamical system

$$\frac{d\mathbf{C}(t)}{dt} = \mathbf{F}(\mathbf{C}(t), \overline{\mathbf{u}}), \quad 0 \le t \le T, \tag{19}$$

where $\mathbf{u}(t) \equiv \overline{\mathbf{u}} = (\overline{x}, \ldots, \overline{x}, \overline{y}, \ldots, \overline{y})$. As $\mathbf{F}(\mathbf{C}, \overline{\mathbf{u}})$ is continuously differentiable, the claim follows from the Continuation Theorem for Differential Dynamical Systems [49]. □

Lemma 5. $\mathbf{F}(\mathbf{C}, \mathbf{u})$ *is bounded by a linear function in* $\mathbf{C}$.

Proof. The claim follows from the observation that, for $0 \le t \le T$, $i = 1, 2, \ldots, N$,

$$\begin{aligned} &\frac{1}{x_i(t)}\left[a_i + \beta\sum_{j=1}^N a_{ji}C_j(t)\right]\left[1 - C_i(t)\right] - y_i(t)\, C_i(t) \\ &\le \frac{1}{\underline{x}}\left[a_i + \beta\sum_{j=1}^N a_{ji}C_j(t)\right] - \underline{y}C_i(t). \end{aligned} \tag{20}$$

□

Lemma 6. $L(\mathbf{C}, \mathbf{u})$ *is convex on* $\mathcal{U}$.

Proof. Let $\mathbf{u}^{(1)}, \mathbf{u}^{(2)} \in \mathcal{U}$, $0 < \eta < 1$. Then

$$\begin{aligned} &L\left(\mathbf{C}, (1-\eta)\,\mathbf{u}^{(1)} + \eta\mathbf{u}^{(2)}\right) \\ &\quad = (1-\eta)\, L\left(\mathbf{C}, \mathbf{u}^{(1)}\right) + \eta L\left(\mathbf{C}, \mathbf{u}^{(2)}\right). \end{aligned} \tag{21}$$

□

Lemma 7. *One has* $L(\mathbf{C}, \mathbf{u}) \ge (1/\max\{\overline{x}, \overline{y}\})\|\mathbf{u}\|_2^2$.

Proof. We have

$$\begin{aligned} L(\mathbf{C}, \mathbf{u}) &= \sum_{i=1}^N (w_i C_i + x_i + y_i) \ge \sum_{i=1}^N (x_i + y_i) \\ &\ge \sum_{i=1}^N \left(\frac{x_i^2}{\overline{x}} + \frac{y_i^2}{\overline{y}}\right) \ge \frac{1}{\max\{\overline{x}, \overline{y}\}}\|\mathbf{u}\|_2^2. \end{aligned} \tag{22}$$

□

Based on Lemmas 1–7, we get the following result.

Theorem 8. *Problem (16) has an optimal control.*

This theorem guarantees that there is a most effective APT defense strategy.

3.2. The Optimality System. It is known that the optimality system for an optimal control problem offers a method for numerically solving the problem. This subsection is intended to present the optimality system for problem (16). For this purpose, consider the corresponding Hamiltonian

$$H\left(\mathbf{C}\left(t\right),\mathbf{u}\left(t\right),\lambda\left(t\right)\right)=\sum_{i=1}^{N}\left[w_iC_i\left(t\right)+x_i\left(t\right)+y_i\left(t\right)\right]+\sum_{i=1}^{N}\lambda_i\left(t\right)\left\{\frac{1}{x_i\left(t\right)}\left[a_i+\beta\sum_{j=1}^{N}a_{ji}C_j\left(t\right)\right]\left[1-C_i\left(t\right)\right]-y_i\left(t\right)C_i\left(t\right)\right\},\tag{23}$$

where $\lambda=(\lambda_1,\ldots,\lambda_N)^T$ is the adjoint.

Theorem 9. *Suppose* $\mathbf{u}^*$ *is an optimal control to problem (16) and* $\mathbf{C}^*$ *is the solution to the adjunctive dynamical system with* $\mathbf{u}=\mathbf{u}^*$. *Then, there exists* λ^* *with* $\lambda^*(T)=\mathbf{0}$ *such that, for* $0\le t\le T$, $1\le i\le N$,

$$\frac{d\lambda_i^*\left(t\right)}{dt}=-w_i+y_i^*\left(t\right)\lambda_i^*\left(t\right)+\frac{\lambda_i^*\left(t\right)}{x_i^*\left(t\right)}\left[a_i+\beta\sum_{j=1}^{N}a_{ji}C_j^*\left(t\right)\right]-\beta\sum_{j=1}^{N}\frac{a_{ij}\left[1-C_j^*\left(t\right)\right]\lambda_j^*\left(t\right)}{x_j^*\left(t\right)},$$

$$x_i^*\left(t\right)=\max\left\{\min\left\{\left[\lambda_i^*\left(t\right)\left[a_i+\beta\sum_{j=1}^{N}a_{ji}C_j^*\left(t\right)\right]\left[1-C_i^*\left(t\right)\right]\right]^{1/2},\overline{x}\right\},\underline{x}\right\},\tag{24}$$

$$y_i^*\left(t\right)=\begin{cases}\underline{y}, & \lambda_i^*\left(t\right)C_i^*\left(t\right)<1,\\ \overline{y}, & \lambda_i^*\left(t\right)C_i^*\left(t\right)>1.\end{cases}$$

Proof. According to the Pontryagin Minimum Principle [10], there exists λ^* such that

$$\frac{d\lambda_i^*\left(t\right)}{dt}=-\frac{\partial H\left(\mathbf{C}^*\left(t\right),\mathbf{u}^*\left(t\right),\lambda^*\left(t\right)\right)}{\partial C_i},\quad 0\le t\le T,\ 1\le i\le N.\tag{25}$$

Thus, the first N equations in the claim follow by direct calculations. As the terminal cost is unspecified and the final state is free, the transversality condition $\lambda^*(T)=\mathbf{0}$ holds. By using the optimality condition

$$\mathbf{u}^*\left(t\right)=\arg\min_{\mathbf{u}\in\mathscr{U}}\ H\left(\mathbf{C}^*\left(t\right),\mathbf{u}\left(t\right),\lambda^*\left(t\right)\right),\quad 0\le t\le T.\tag{26}$$

we get (a) either

$$\frac{\partial H\left(\mathbf{C}^*\left(t\right),\mathbf{u}^*\left(t\right),\lambda^*\left(t\right)\right)}{\partial x_i}=1-\frac{\lambda_i^*\left(t\right)}{\left(x_i^*\left(t\right)\right)^2}\left[a_i+\beta\sum_{i=1}^{N}a_{ji}C_j^*\left(t\right)\right]\left[1-C_i^*\left(t\right)\right]=0\tag{27}$$

or $x_i^*(t)=\underline{x}$ or $x_i^*(t)=\overline{x}$ and (b)

$$y_i^*\left(t\right)=\arg\min_{\underline{y}\le y_i(t)\le\overline{y}}\left(1-\lambda_i^*\left(t\right)C_i^*\left(t\right)\right)y_i\left(t\right)=\begin{cases}\underline{y}, & \lambda_i^*\left(t\right)C_i^*\left(t\right)<1,\\ \overline{y}, & \lambda_i^*\left(t\right)C_i^*\left(t\right)>1.\end{cases}\tag{28}$$

Combining the above discussions, we get the optimality system for problem (16) as follows.

$$\frac{dC_i\left(t\right)}{dt}=\frac{1}{x_i\left(t\right)}\left[a_i+\beta\sum_{j=1}^{N}a_{ji}C_j\left(t\right)\right]\left[1-C_i\left(t\right)\right]-y_i\left(t\right)C_i\left(t\right),$$

$$\frac{d\lambda_i\left(t\right)}{dt}=-w_i+y_i\left(t\right)\lambda_i\left(t\right)+\frac{\lambda_i\left(t\right)}{x_i\left(t\right)}\left[a_i+\beta\sum_{j=1}^{N}a_{ji}C_j\left(t\right)\right]-\beta\sum_{j=1}^{N}\frac{a_{ij}\left[1-C_j\left(t\right)\right]\lambda_j\left(t\right)}{x_j\left(t\right)},$$

$$x_i(t) = \max\left\{\min\left\{\left[\lambda_i(t)\left[a_i + \beta\sum_{j=1}^{N} a_{ji}C_j(t)\right]\left[1 - C_i(t)\right]\right]^{1/2}, \overline{x}\right\}, \underline{x}\right\},$$

$$y_i(t) = \begin{cases} \underline{y}, & \lambda_i(t)\,C_i(t) < 1, \\ \overline{y}, & \lambda_i(t)\,C_i(t) > 1, \end{cases} \tag{29}$$

where $\mathbf{C}(0) = \mathbf{C}_0$, $\lambda(T) = \mathbf{0}$, $0 \le t \le T$, $1 \le i \le N$. □

Applying the forward-backward Euler scheme to the optimality system, we can obtain an optimal control to problem (16), that is, a most effective APT defense strategy.

4. Some Most Effective APT Defense Strategies

In this section, we give some most effective APT defense strategies by solving the optimality system (29). For ease in observation, let us introduce two functions as follows. For an admissible control $\mathbf{u}$ to problem (16), define the *cumulative effectiveness (CE)* as

$$\begin{aligned} \mathrm{CE}(t;\mathbf{u}) &= \sum_{i=1}^{N}\int_0^t w_i C_i(s)\,ds \\ &\quad + \sum_{i=1}^{N}\int_0^t \left[x_i(s) + y_i(s)\right]ds, \quad 0 \le t \le T, \end{aligned} \tag{30}$$

and define the *superposed control (SC)* as

$$\mathrm{SC}(t;\mathbf{u}) = \sum_{i=1}^{N}\left[x_i(t) + y_i(t)\right], \quad 0 \le t \le T. \tag{31}$$

Obviously, we have $\mathrm{CE}(T;\mathbf{u}) = J(\mathbf{u})$.

For some optimal control problems, let us give the cumulative effectiveness and superposed control for an optimal control.

Example 10. Consider problem (16) in which G is a scale-free network with $N = 100$ nodes which is generated by executing the algorithm given in [53], $T = 20$, $\beta = 0.001$, $\underline{x} = \underline{y} = 0.1$, $\overline{x} = \overline{y} = 0.7$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$. An optimal control to the problem is obtained by solving the optimality system (29). Figure 2 plots the cumulative effectiveness and superposed control for the optimal control. For comparison purpose, the cumulative effectiveness and superposed control for three admissible static controls are also shown in Figure 2.

Example 11. Consider problem (16) in which G is a small-world network with $N = 100$ nodes which is generated by executing the algorithm given in [54], $T = 20$, $\beta = 0.001$, $\underline{x} = \underline{y} = 0.1$, $\overline{x} = \overline{y} = 0.7$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$. An optimal control to the problem is obtained by solving the optimality system (29). Figure 3 depicts the cumulative effectiveness and superposed control for the optimal control. For comparison purpose, the cumulative effectiveness and superposed control for three admissible static controls are also shown in Figure 3.

Example 12. Consider problem (16) in which G is a realistic network given in [55], $T = 20$, $\beta = 0.001$, $\underline{x} = \underline{y} = 0.1$, $\overline{x} = \overline{y} = 0.7$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$. An optimal control to the problem is obtained by solving the optimality system (29). Figure 4 exhibits the cumulative effectiveness and superposed control for the optimal control. For comparison purpose, the cumulative effectiveness and superposed control for three admissible static controls are also shown in Figure 4.

It is seen from the above three examples that a most effective APT defense strategy is significantly superior to any static APT defense strategy in terms of the effectiveness. This observation justifies our method. Additionally, the superposed control drops rapidly to a lower value.

5. Further Discussions

This section is devoted to examining the influence of different factors on the optimal effectiveness of an admissible APT defense strategy. For ease in understanding these influences, let us introduce three quantities as follows. For an optimal control $\mathbf{u}^*$ to problem (16), let OL^*, OC^*, and OJ^* denote the corresponding expected loss, overall cost, and effectiveness, respectively. That is,

$$\begin{aligned} \mathrm{OL}^* &= \mathrm{Loss}\left(\mathbf{u}^*\right), \\ \mathrm{OC}^* &= \mathrm{Cost}\left(\mathbf{u}^*\right), \\ \mathrm{OJ}^* &= \mathrm{OL}^* + \mathrm{OC}^* = J\left(\mathbf{u}^*\right). \end{aligned} \tag{32}$$

5.1. The Bounds on the Admissible Controls. Definitely, the four bounds on the admissible controls affect the optimal effectiveness of an admissible APT defense strategy. Now, let us examine these influences.

Example 13. Consider a set of problems (16) in which G is the scale-free network generated in Example 10, $T = 20$, $\beta = 0.001$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$.

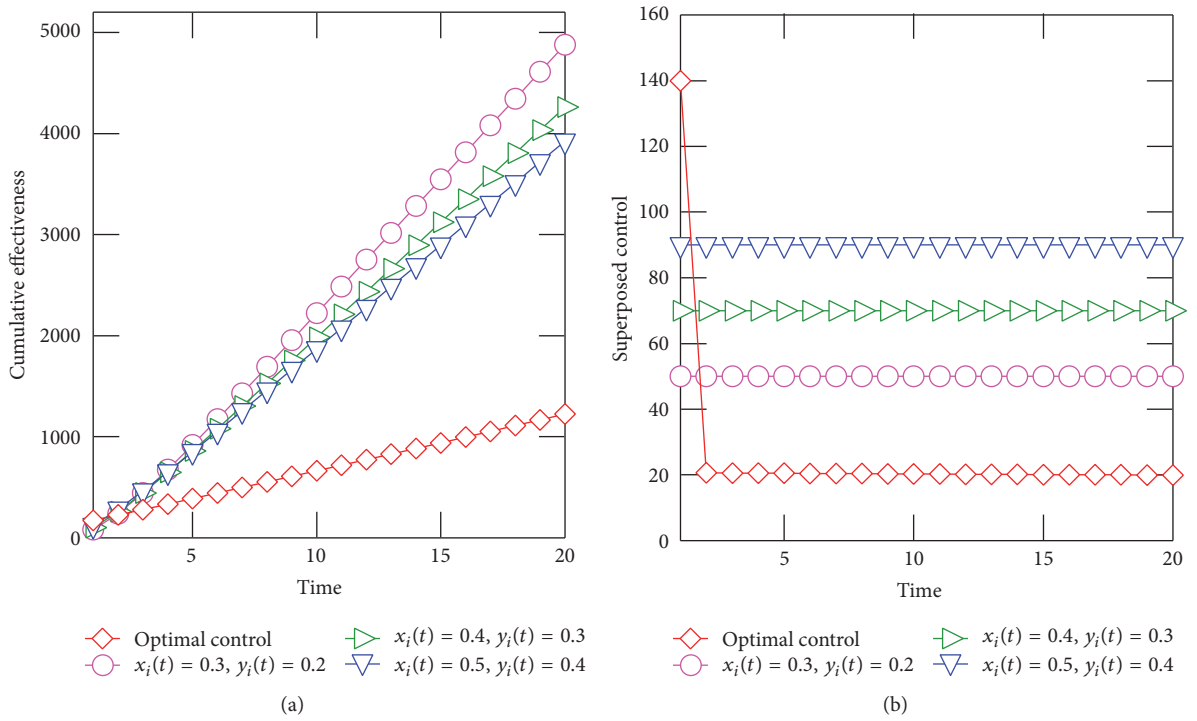


FIGURE 2: The cumulative effectiveness and superposed control for the optimal control and a few static controls in Example 10.

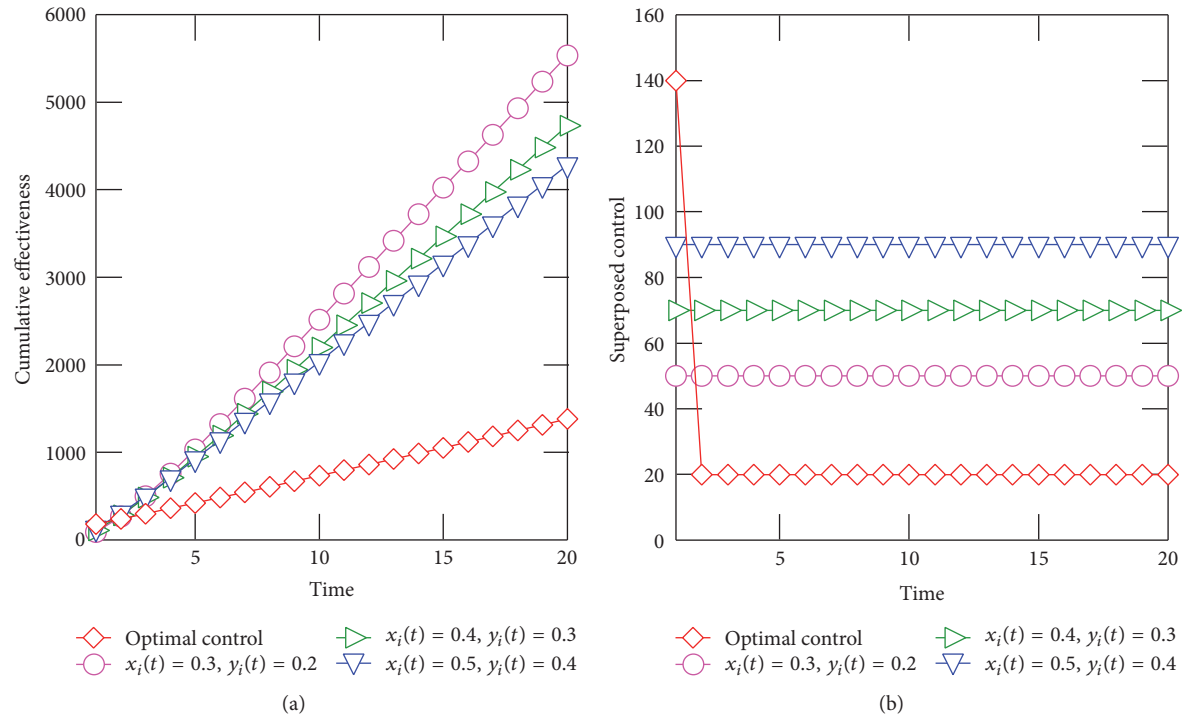


FIGURE 3: The cumulative effectiveness and superposed control for the optimal control and a few static controls in Example 11.

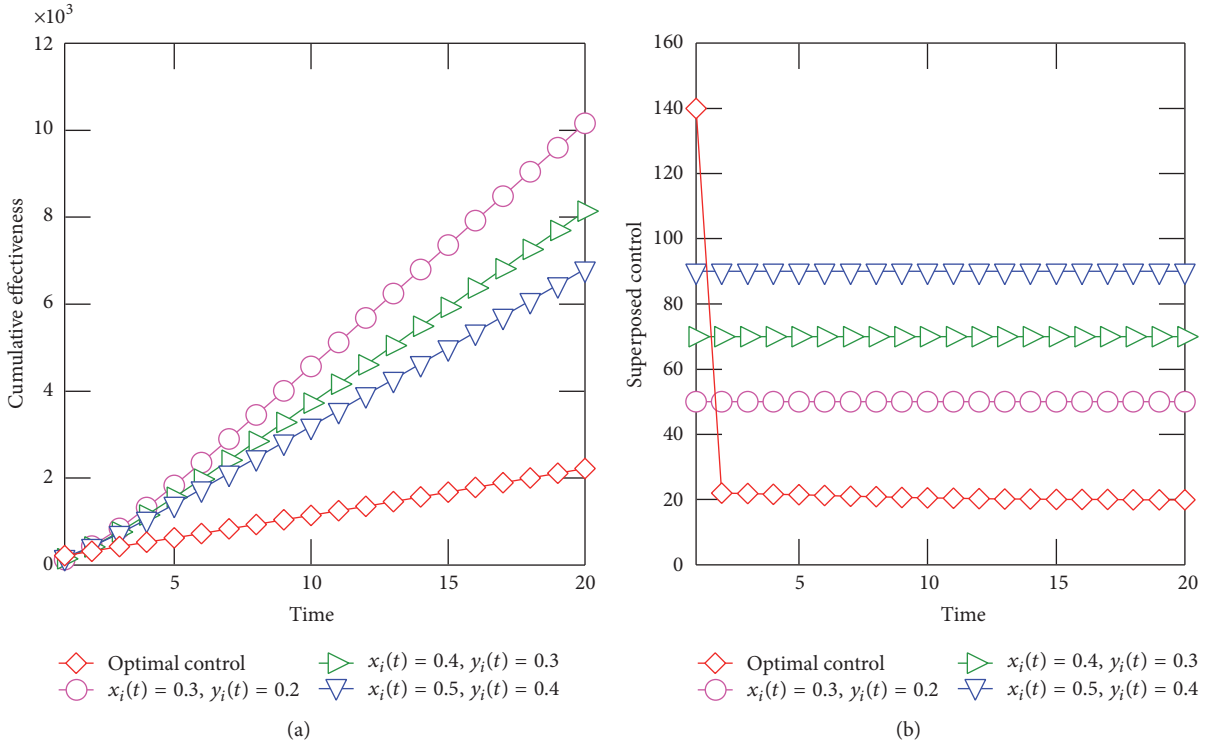


Figure 4: The cumulative effectiveness and superposed control for the optimal control and a few static controls in Example 12.

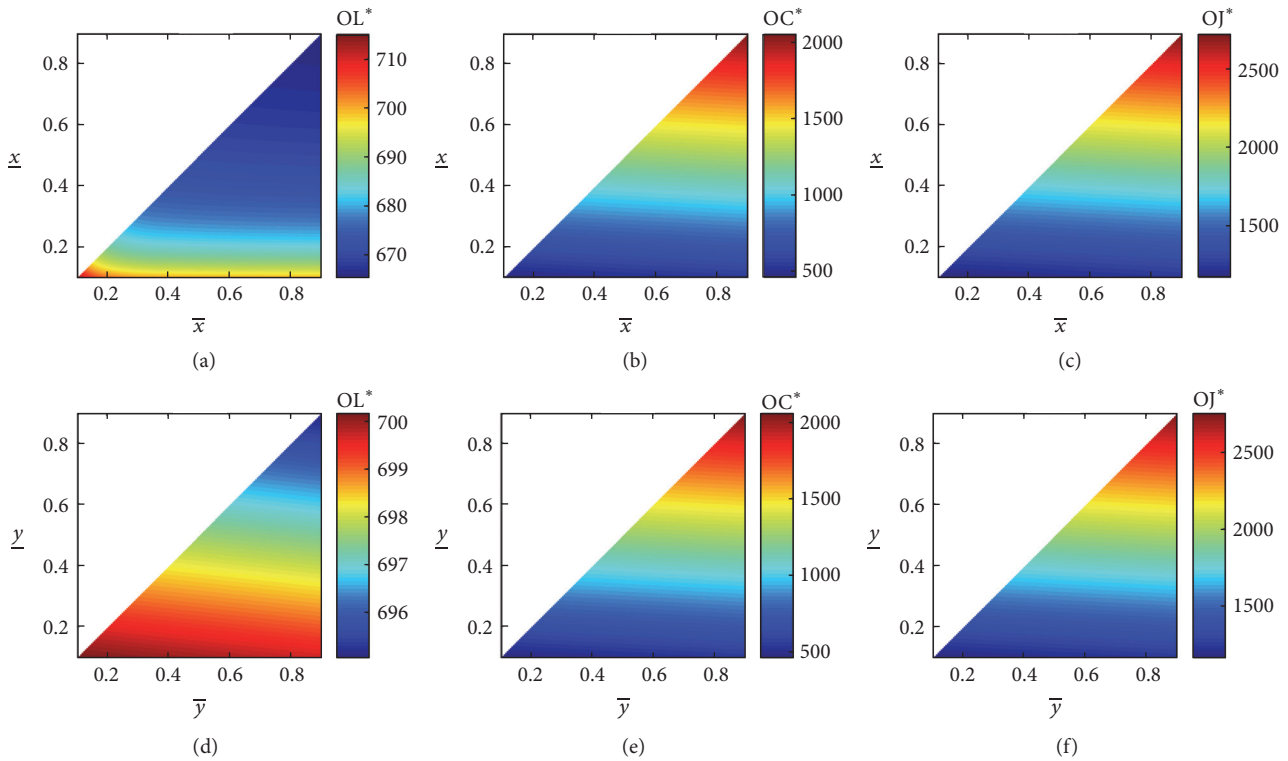


Figure 5: The influence of the four bounds on OL*, OC*, and OJ* in Example 13.

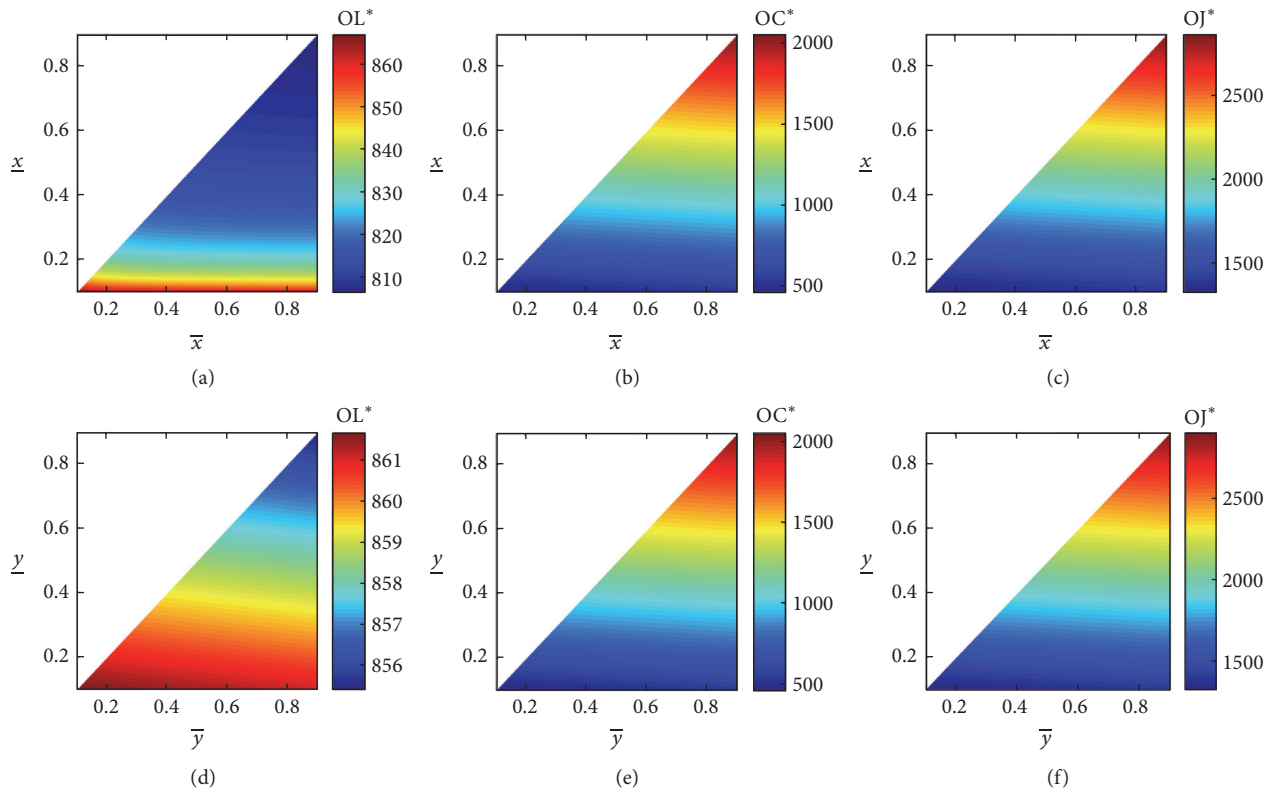


Figure 6: The influence of the four bounds on OL^*, OC^*, and OJ^* in Example 14.

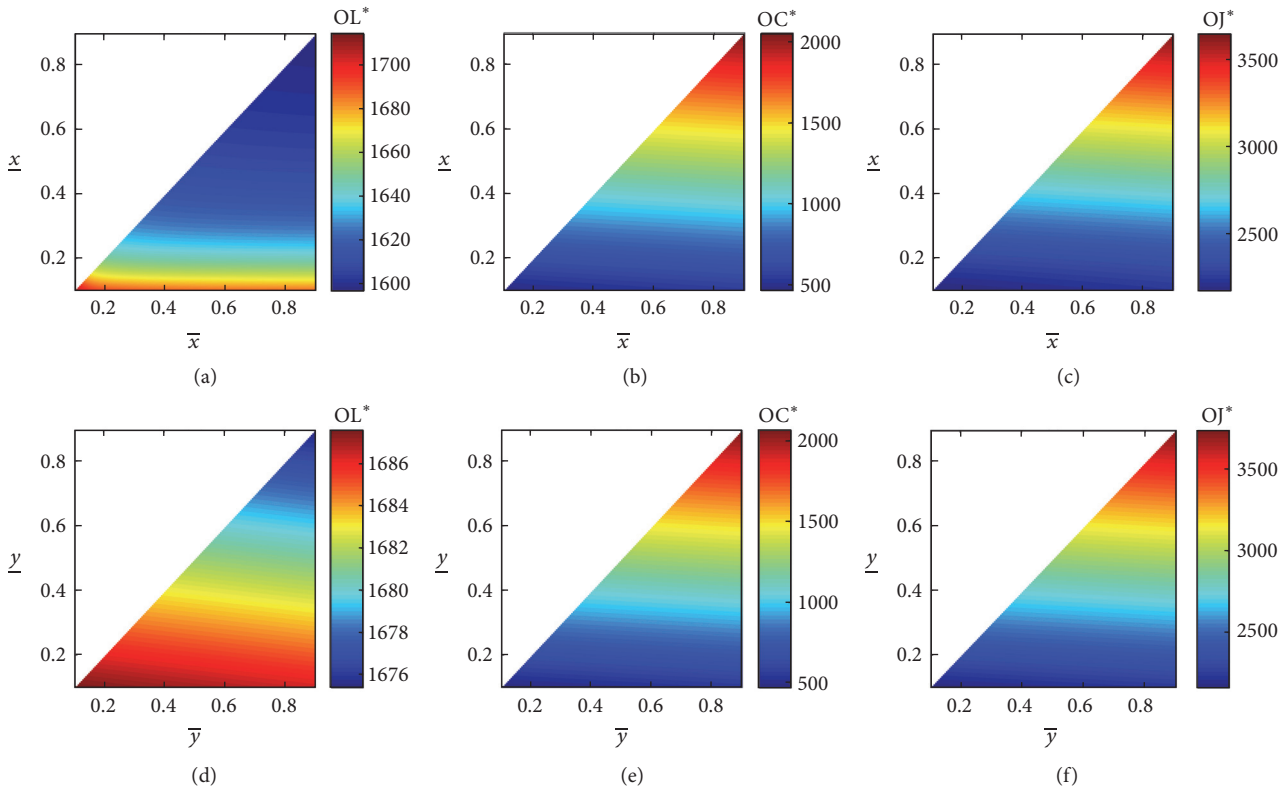


Figure 7: The influence of the four bounds on OL^*, OC^*, and OJ^* in Example 15.

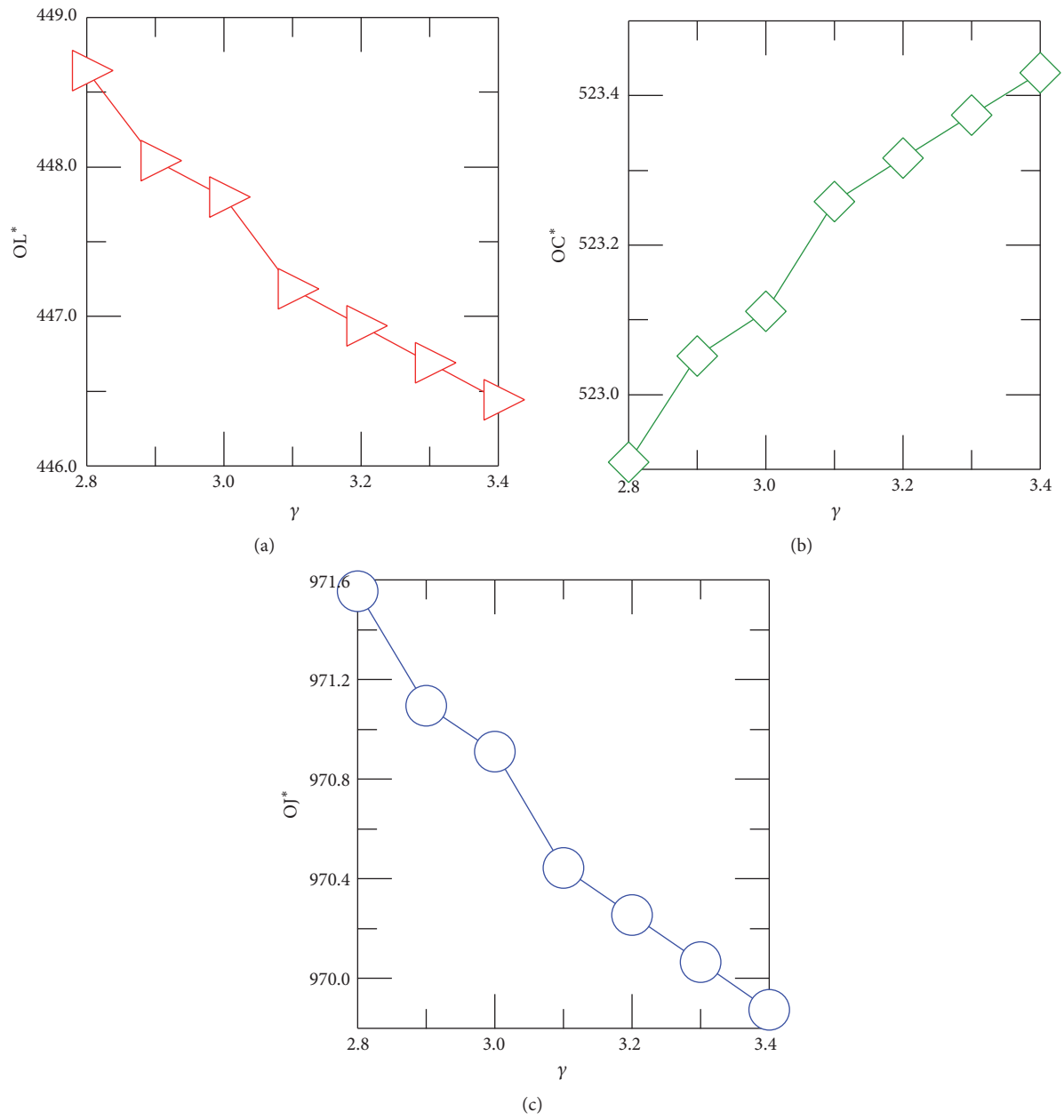


Figure 8: The influence of the power-law exponent of a scale-free network on OL^*, OC^*, and OJ^* in Example 16.

(a) Let $\underline{y} = 0.1$, $\overline{y} = 0.7$. Figures 5(a)–5(c) exhibit the influence of $\underline{x}$ and $\overline{x}$ on OL^*, OC^*, and OJ^*, respectively.

(b) Let $\underline{x} = 0.1$, $\overline{x} = 0.7$. Figures 5(d)–5(f) display the influence of $\underline{y}$ and $\overline{y}$ on OL^*, OC^*, and OJ^*, respectively.

Example 14. Consider a set of problems (16) in which G is the small-world network generated in Example 11, $T = 20$, $\beta = 0.001$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$.

(a) Let $\underline{y} = 0.1$, $\overline{y} = 0.7$. Figures 6(a)–6(c) exhibit the influence of $\underline{x}$ and $\overline{x}$ on OL^*, OC^*, and OJ^*, respectively.

(b) Let $\underline{x} = 0.1$, $\overline{x} = 0.7$. Figures 6(d)–6(f) display the influence of $\underline{y}$ and $\overline{y}$ on OL^*, OC^*, and OJ^*, respectively.

Example 15. Consider a set of problems (16) in which G is the realistic network given in Example 12, $T = 20$, $\beta = 0.001$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$.

(a) Let $\underline{y} = 0.1$, $\overline{y} = 0.7$. Figures 7(a)–7(c) exhibit the influence of $\underline{x}$ and $\overline{x}$ on OL^*, OC^*, and OJ^*, respectively.

(b) Let $\underline{x} = 0.1$, $\overline{x} = 0.7$. Figures 7(d)–7(f) display the influence of $\underline{y}$ and $\overline{y}$ on OL^*, OC^*, and OJ^*, respectively.

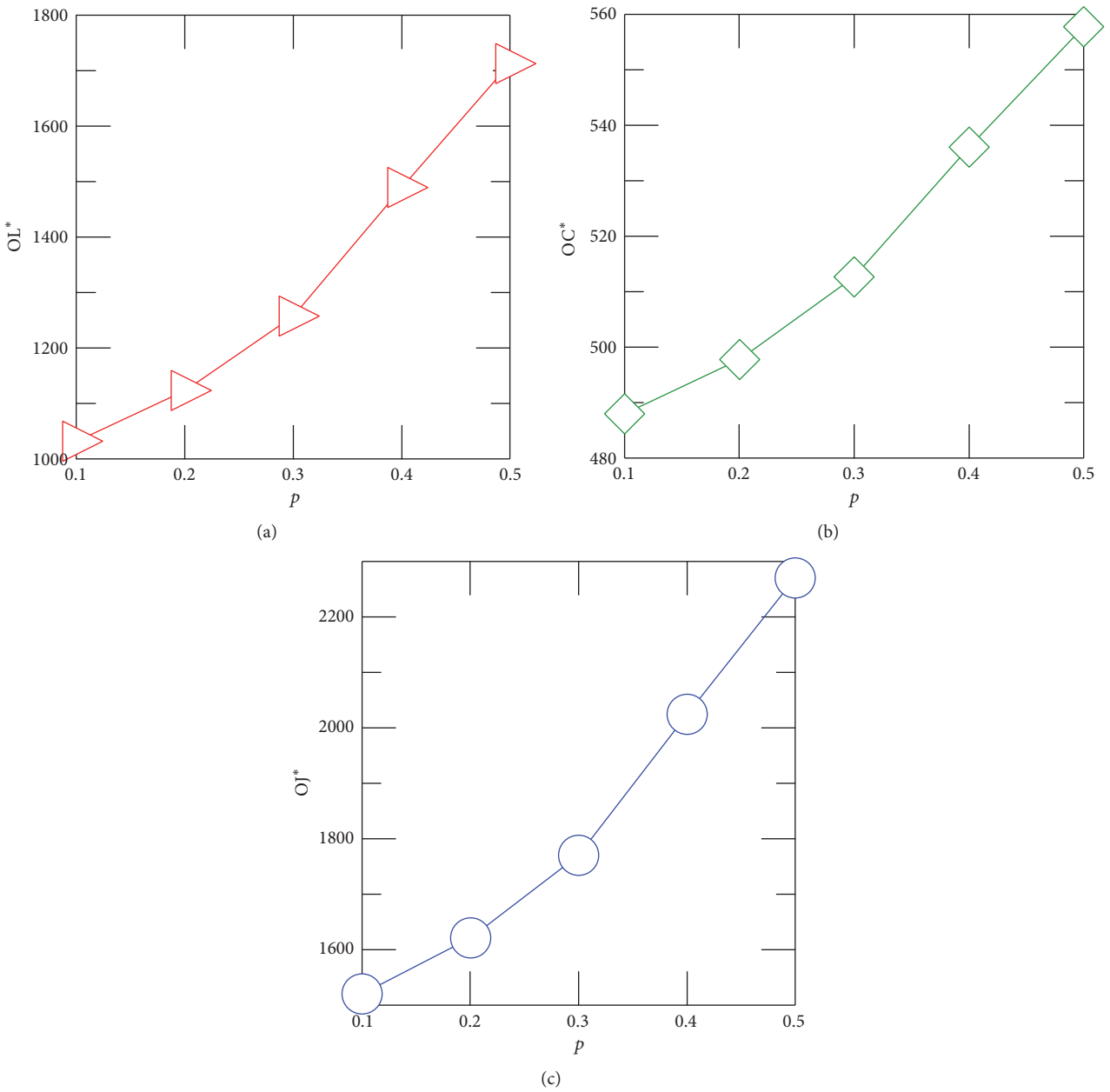


FIGURE 9: The influence of the edge-rewiring probability of a small-world network on OL*, OC*, and OJ* in Example 17.

The following conclusions are drawn from the above three examples.

(a) With the increase of the two lower bounds, OL* goes down, but OC* and OJ* go up. In practice, the two lower bounds should be chosen carefully so that a balance between the expected loss and the overall cost is achieved.

(b) The influence of the two upper bounds on OL*, OC*, and OJ* is almost negligible.

5.2. The Network Topology. Obviously, the topology of the network in an organization affects the optimal effectiveness of an admissible APT defense strategy. Now, let us inspect this influence.

Example 16. Consider a set of problems (16) in which $G \in \{G_i: 1 \le i \le 7\}$, where G_i is a scale-free network with $N = 100$ nodes and a power-law exponent of $\gamma_i = 2.7 + 0.1 \times i$, $T = 20$, $\beta = 0.001$, $\underline{x} = \underline{y} = 0.1$, $\overline{x} = \overline{y} = 0.7$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$. Figure 8 displays the influence of the power-law exponent on OL*, OC*, and OJ*, respectively.

It is seen from this example that, with the increase of the power-law exponent of a scale-free network, OL* and OJ* decline, but OC* inclines. It is well known that the heterogeneity of a scale-free network increases with

its power-law exponent. Therefore, a homogeneously mixed access network is better in terms of the optimal defense effectiveness.

Example 17. Consider a set of problems (P) in which $G \in \{G_i: 1 \le i \le 5\}$, where G_i is a small-world network with $N = 100$ nodes and an edge-rewiring probability of $p_i = 0.1 \times i$, $T = 20$, $\beta = 0.001$, $\underline{x} = \underline{y} = 0.1$, $\overline{x} = \overline{y} = 0.7$, $a_i = 0.1$, $0 \le i \le N$, and $C_i(0) = 0.1$, $0 \le i \le N$. Figure 9 exhibits the influence of the edge-rewiring probability on OL^*, OC^*, and OJ^*, respectively.

It is seen from this example that, with the increase of the randomness of a small-world network, OL^*, OC^*, and OJ^* rise rapidly. Hence, a randomly connected access network is better from the perspective of the optimal defense effectiveness.

6. Concluding Remarks

This paper has addressed the APT defense problem, that is, the problem of how to effectively defend against APTs. By introducing an APT attack-defense model and quantifying the effectiveness of an APT defense strategy, we have modeled the APT defense problem as an optimal control problem in which an optimal control represents a most effective APT defense strategy. Through theoretical study, we have presented the optimality system for the optimal control problem. This implies that an optimal control can be derived by solving the optimality system. The influence of some factors on the optimal effectiveness of an APT defense strategy has been examined.

There are many relevant problems to be resolved. The expected loss and overall cost of an APT defense strategy should be appropriately balanced to adapt to specific application scenarios. In practice, the implementation of a recommended defense strategy needs a great effort; the security level of all the systems in an organization must be labeled accurately [6], the defense budget must be made, and the robustness of the defense strategy must be evaluated. As the topology of the access network in an organization may well vary with time, the approach proposed in this work should be adapted to time-varying networks [56–59]. It is of practical importance to deal with the APT defense problem in the game-theoretical framework, where the attacker is strategic [60–63].

Conflicts of Interest

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

Acknowledgments

This work is supported by National Natural Science Foundation of China (Grant no. 61572006), National Sci-Tech Support Program of China (Grant no. 2015BAF05B03), and Fundamental Research Funds for the Central Universities (Grant no. 106112014CDJZR008823).

References

[1] G. K. Kostopoulos, *Cyberspace and Cybersecurity*, Taylor & Francis, 2012.

[2] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.

[3] N. Virvilis, D. Gritzalis, and T. Apostolopoulos, "Trusted computing vs. Advanced persistent threats: Can a defender win this game?" in *Proceedings of the 10th IEEE International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and 10th IEEE International Conference on Autonomic and Trusted Computing, ATC 2013*, pp. 396–403, December 2013.

[4] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," *PLoS ONE*, vol. 12, no. 1, Article ID e0168675, 2017.

[5] C. Tankard, "Advanced Persistent threats and how to monitor and deter them," *Network Security*, vol. 2011, no. 8, pp. 16–19, 2011.

[6] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*, Elsevier, 2013.

[7] T. Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization*, McGraw-Hill Education, 2015.

[8] I. Friedberg, F. Skopik, G. Settanni, and R. Fiedler, "Combating advanced persistent threats: from network event correlation to incident detection," *Computers & Security*, vol. 48, pp. 35–57, 2015.

[9] M. Marchetti, F. Pierazzi, M. Colajanni, and A. Guido, "Analysis of high volumes of network traffic for Advanced Persistent Threat detection," *Computer Networks*, vol. 109, pp. 127–141, 2016.

[10] D. E. Kirk, *Optimal Control Theory: An Introduction*, Dover Publications, 2004.

[11] D. Liberzon, *Calculus of Variations and Optimal Control Theory: A Concise Introduction*, Princeton University Press, 2012.

[12] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," in *Proceedings of the IEEE INFOCOM 2010*, pp. 1–9, March 2010.

[13] M. H. Khouzani and S. Sarkar, "Maximum damage battery depletion attack in mobile sensor networks," *Institute of Electrical and Electronics Engineers Transactions on Automatic Control*, vol. 56, no. 10, pp. 2358–2368, 2011.

[14] J. Ren, Y. Xu, and C. Zhang, "Optimal control of a delay-varying computer virus propagation model," *Discrete Dynamics in Nature and Society*, vol. 2013, Article ID 210291, 7 pages, 2013.

[15] L. Chen, K. Hattaf, and J. Sun, "Optimal control of a delayed SLBS computer virus model," *Physica A: Statistical Mechanics and its Applications*, vol. 427, pp. 244–250, 2015.

[16] 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.

[17] C. Nowzari, V. M. Preciado, and G. . Pappas, "Analysis and control of epidemics: a survey of spreading processes on complex networks," *IEEE Control Systems Magazine*, vol. 36, no. 1, pp. 26–46, 2016.

[18] 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.

[19] W. Liu and S. Zhong, "Web malware spread modelling and optimal control strategies," *Scientific Reports*, vol. 7, Article ID 42308, 2017.

[20] N. F. Britton, *Essential Mathematical Biology*, Springer Undergraduate Mathematics Series, Springer, 2003.

[21] J. R. Piqueira and V. O. Araujo, "A modified epidemiological model for computer viruses," *Applied Mathematics and Computation*, vol. 213, no. 2, pp. 355–360, 2009.

[22] L. Feng, X. Liao, H. Li, and Q. Han, "Hopf bifurcation analysis of a delayed viral infection model in computer networks," *Mathematical and Computer Modelling*, vol. 56, no. 7-8, pp. 167–179, 2012.

[23] B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Applied Mathematical Modelling*, vol. 37, no. 6, pp. 4103–4111, 2013.

[24] Y. Yao, N. Zhang, W. Xiang, G. Yu, and F. Gao, "Modeling and analysis of bifurcation in a delayed worm propagation model," *Journal of Applied Mathematics*, vol. 2013, Article ID 927369, 11 pages, 2013.

[25] 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.

[26] J. Ren and Y. Xu, "A compartmental model for computer virus propagation with kill signals," *Physica A: Statistical Mechanics and its Applications*, vol. 486, pp. 446–454, 2017.

[27] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, 2001.

[28] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics in finite size scale-free networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 65, no. 3, Article ID 035108, 2002.

[29] C. Castellano and R. Pastor-Satorras, "Thresholds for epidemic spreading in networks," *Physical Review Letters*, vol. 105, no. 21, Article ID 218701, 2010.

[30] L.-X. Yang, X. Yang, J. Liu, Q. Zhu, and C. Gan, "Epidemics of computer viruses: s complex-network approach," *Applied Mathematics and Computation*, vol. 219, no. 16, pp. 8705–8717, 2013.

[31] J. Ren, J. Liu, and Y. Xu, "Modeling the dynamics of a network-based model of virus attacks on targeted resources," *Communications in Nonlinear Science and Numerical Simulation*, vol. 31, no. 1-3, pp. 1–10, 2016.

[32] W. Liu, C. Liu, Z. Yang, X. Liu, Y. Zhang, and Z. Wei, "Modeling the propagation of mobile malware on complex networks," *Communications in Nonlinear Science and Numerical Simulation*, vol. 37, pp. 249–264, 2016.

[33] L.-X. Yang and X. Yang, "The effect of network topology on the spread of computer viruses: a modelling study," *International Journal of Computer Mathematics*, vol. 94, no. 8, pp. 1591–1608, 2017.

[34] 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.

[35] P. Van Mieghem, "The N-intertwined SIS epidemic network model," *Computing*, vol. 93, no. 2-4, pp. 147–169, 2011.

[36] F. D. Sahneh, F. N. Chowdhury, and C. M. Scoglio, "On the existence of a threshold for preventive behavioral responses to suppress epidemic spreading," *Scientific Reports*, vol. 2, article 632, 2012.

[37] F. D. Sahneh, C. Scoglio, and P. Van Mieghem, "Generalized epidemic mean-field model for spreading processes over multilayer complex networks," *IEEE/ACM Transactions on Networking*, vol. 21, no. 5, pp. 1609–1620, 2013.

[38] 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.

[39] 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. 3, Article ID 2348835, 2012.

[40] 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.

[41] L. Yang, M. Draief, and X. Yang, "Heterogeneous virus propagation in networks: a theoretical study," *Mathematical Methods in the Applied Sciences*, vol. 40, no. 5, pp. 1396–1413, 2017.

[42] 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.

[43] 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*, no. 99, 2017.

[44] L. Yang, P. Li, X. Yang, Y. Wu, and Y. Y. Tang, "On the competition of two conflicting messages," *Nonlinear Dynamics*, vol. 91, no. 3, pp. 1853–1869, 2018.

[45] S. Xu, W. Lu, and H. Li, "A stochastic model of active cyber defense dynamics," *Internet Mathematics*, vol. 11, no. 1, pp. 23–61, 2015.

[46] R. Zheng, W. Lu, and S. Xu, "Active cyber defense dynamics exhibiting rich phenomena," in *Proceedings of the Symposium and Bootcamp on the Science of Security, HotSoS 2015*, April 2015.

[47] L.-X. Yang, P. Li, X. Yang, and Y. Y. Tang, "Security evaluation of the cyber networks under advanced persistent threats," *IEEE Access*, vol. 5, pp. 20111–20123, 2017.

[48] R. Zheng, W. Lu, and S. Xu, "Preventive and Reactive Cyber Defense Dynamics Is Globally Stable," *IEEE Transactions on Network Science and Engineering*, 2017.

[49] R. C. Robinson, *An Introduction to Dynamical Systems: Continuous and Discrete*, Pearson Education, Inc., 2004.

[50] E. M. Stein and R. Shakarchi, *Real analysis*, vol. 3 of *Princeton Lectures in Analysis*, Princeton University Press, Princeton, NJ, 2005.

[51] D. Kempe, J. Kleinberg, and E. Tardos, "Influential nodes in a diffusion model for social networks," in *Proceedings of ICALP*, pp. 1127–1138, 2005.

[52] W. Chen, Y. Wang, and S. Yang, "Efficient influence maximization in social networks," in *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '09)*, pp. 199–208, ACM, July 2009.

[53] A.-L. Barabasi and R. Albert, "Emergence of scaling in random networks," *American Association for the Advancement of Science: Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[54] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[55] http://konect.uni-koblenz.de/networks/arenas-email.

[56] Y. Schwarzkopf, A. Rákos, and D. Mukamel, "Epidemic spreading in evolving networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 82, no. 3, Article ID 036112, 2010.

[57] P. Holme and J. Saramäki, "Temporal networks," *Physics Reports*, vol. 519, no. 3, pp. 97–125, 2012.

[58] M. Karsai, N. Perra, and A. Vespignani, "Time varying networks and the weakness of strong ties," *Scientific Reports*, vol. 4, article no. 4001, 2014.

[59] E. Valdano, L. Ferreri, C. Poletto, and V. Colizza, "Analytical computation of the epidemic threshold on temporal networks," *Physical Review X*, vol. 5, no. 2, Article ID 021005, 2015.

[60] T. Alpcan and T. Basar, *Network Security: A Decision and Game-Theoretic Approach*, Cambridge University Press, 2010.

[61] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, article 25, 2013.

[62] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 472–486, 2013.

[63] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *Proceedings of the 34th IEEE Annual Conference on Computer Communications and Networks, IEEE INFOCOM 2015*, pp. 747–755, May 2015.