Hindawi
Complexity
Volume 2021, Article ID 6639632, 9 pages
https://doi.org/10.1155/2021/6639632

Research Article

Modeling and Analysis of the Spread of Malware with the Influence of User Awareness

Qingyi Zhu, Xuhang Luo, and Yuhang Liu

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

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

Received 17 December 2020; Revised 19 May 2021; Accepted 13 October 2021; Published 1 November 2021

Academic Editor: Marcus Aguiar

By incorporating the security awareness of computer users into the susceptible-infected-susceptible (SIS) model, this study proposes a new malware propagation model, named the SID model, where D compartment denotes the group of nodes with user awareness. Through qualitative analysis, the basic reproductive number R_0 is given. Furthermore, it is proved that the virus-free equilibrium is globally asymptotically stable if R_0 is less than one, whereas the viral equilibrium is globally asymptotically stable if R_0 is greater than one. Then, some numerical examples are given to demonstrate the analytical results. Finally, we put forward some efficient control measures according to the theoretical and experimental analysis.

1. Introduction

Malware is the generic term used to designate any informatics program created deliberately to carry out an unauthorized activity that, in many cases, is harmful to the system in which it has been lodged [1]. There is an increasing trend in both the number and types of malware. According to the report in [2], there is an exponential growth in the number of viruses, and in 2017, there are 15,107,232 different malware files that we had never seen before, mainly because of the improvement of technology and the increasing Internet population. Hence, there are lots of researchers trying to develop effective methods and tools to detect malware from a microperspective [3–5].

Although the scientific approach to combating malware is mainly focused on the design of efficient methods to detect and remove malware [6], it is also worth modeling the propagation behaviors of malware and developing effective control strategies, furthermore, to prevent its outbreak. Most of these models are dynamical systems of ordinary differential equations [7]. They are compartmental, that is, the nodes are divided into different types, such as susceptible, exposed, infectious, recovered, and quarantined. Thus, a great number of models (SIS models [8, 9], SIR models [10, 11], SEIR models [12], and SIRQ models [13]) have been proposed.

In recent years, most malware propagation models are proposed by incorporating some new compartments into the existing models. In [14], by considering the protected nodes in cloud, Gan et al. proposed an SIP model for computer virus propagation. More specifically, the protected nodes in cloud can be not infected but might be converted into an S compartment in a certain probability. Similarly, considering the devices that can be infected by the malware but cannot be damaged, an SIRC model is built in [15], where C denotes the carrier device.

On the other hand, user's awareness also has gained a lot of attention from researchers. In [16], the authors pointed out that the missing of user awareness might cause some security issues. In [17], Furnell also claimed that phishing is a significant security threat, and the problem cannot be completely solved by technology alone; in this context, user awareness is highly required. It is no doubt that user awareness is essential for cybersecurity. Considering that user awareness also plays an important role in slowing down the propagation of malware, an improved model based on the SLIR model with user awareness has been put forward in [18]. In [18], the user whose computer is not infected or

exposed is probable to install antivirus programs, and the probability here is called user awareness.

In [1], the author raised the issue that the infection rate of computers may vary from computer to computer. For example, if users are worried about security issues, the infection rate should be reduced. In contrast, if users have dangerous behaviors, the infection rate should be higher. Inspired by this, this study aims to address the issue of different infection rates of computers with/without user awareness. Different from the work in [18], a new compartment (D compartment) is incorporated into the classical SIS model. Here, D compartment denotes the group of nodes with security awareness, whereas S represents the node with dangerous behaviors. Obviously, the infection rate of D nodes is less than S nodes. Besides, in [19, 20], the author proposed S and W compartments similar to S and D compartments in this article, where the conversion rate of the two is a constant. However, we noticed that the change in user awareness is related to the number of infections. The higher the number of infections, the higher the awareness of users. So, we consider that the rate of consciousness conversion is related to the number of infections.

The main contributions of this work are as follows:

(1) A new model describing computer virus propagation is built from the perspective of user awareness

(2) Two equilibrium of the model is obtained: the virus-free equilibrium point and the viral equilibrium, and furthermore, their local and global stabilities are proved, respectively.

(3) Through qualitative analysis and simulation experiments, effective control measures are proposed to prevent the outbreak and spread of malware

The remaining materials of this study are organized as follows: Section 2 formulates the proposed propagation model of malware. In Section 3, local stabilities of both the infection-free and viral equilibria are analyzed, respectively, while Section 4 deals with the global stabilities of the two equilibria. In Section 5, some numerical simulations are performed to illustrate the obtained theoretical results and efficient control measures. Finally, Section 6 summarizes this work and gives some shortcomings.

2. Mathematical Framework

The model proposed in this work is a compartmental model where the computers are divided into 3 classes: susceptible nodes (S) which can be infected by malware easily, nodes with user awareness (D) which can be infected by malware more difficult than S nodes, and infected nodes (I) which can infect other nodes. The transfer diagram is shown in Figure 1. The following notations and assumptions will be adopted in the sequel.

2.1. Notations

$S(t)$: the number of S nodes at time t

$D(t)$: the number of D nodes at time t

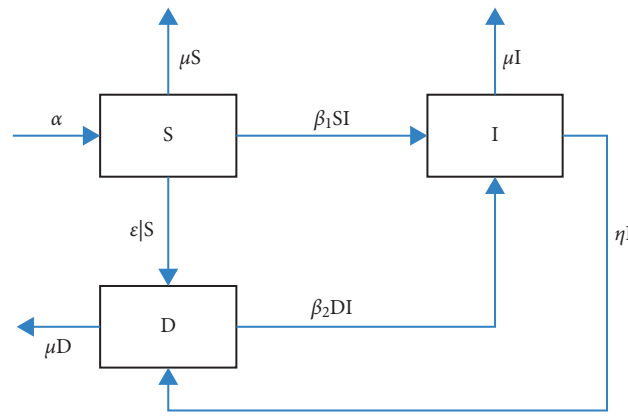

Figure 1: The transfer diagram of the model.

$I(t)$: the number of I nodes at time t

$N(t)$: the total number of nodes at time t

α: the rate at which the node connects to the network

μ: the rate at which the node disconnects to the network

β_1: the infection rate of S nodes caused by an I node

β_2: the infection rate of D nodes caused by an I node. Obviously, $\beta_2 < \beta_1$.

ϵ: the conversion rate from S nodes to D nodes caused by an I node

η: the recovery rates of I nodes due to the effect of antivirus software

2.2. Model Assumptions

(i) All newly accessed nodes are S nodes

(ii) At time t, the infection force from S to I is given by $\beta_1 S(t)I(t)$, and the infection force from D to I is given by $\beta_2 D(t)I(t)$.

(iii) Due to the spread of malware, users gradually become conscious. At time t, the conversion force from S to D is given by $\varepsilon S(t)I(t)$.

(iv) At time t, the users of the recovered nodes all have improved, and the recovered force of I nodes is $\eta I(t)$.

2.3. Model Formulation. Considering the above assumptions, the dynamics of the model is governed by the following system of ordinary differential equations:

$$\begin{cases} \dfrac{dS}{dt} = \alpha - \mu S - \beta_1 SI - \epsilon IS, \\ \dfrac{dD}{dt} = \epsilon IS + \eta I - \beta_2 DI - \mu D, \\ \dfrac{dI}{dt} = \beta_1 SI + \beta_2 DI - \eta I - \mu I. \end{cases} \tag{1}$$

According to $N(t) = S(t) + D(t) + I(t)$, we have $dN/dt = \alpha - \mu N$. Obviously, when $t \longrightarrow \infty$, $N \longrightarrow \alpha/\mu$.

Thus, system (1) can be reduced to the following limit system:

$$\begin{cases} \dfrac{\mathrm{d}S}{\mathrm{d}t} = \alpha - \mu S - \beta_1 SI - \epsilon IS, \\ \dfrac{\mathrm{d}I}{\mathrm{d}t} = \beta_1 SI + \beta_2 \left(\dfrac{\alpha}{\mu} - S - I\right) I - \eta I - \mu I. \end{cases} \tag{2}$$

It is easy to verify that all feasible solutions of equation (2) are bounded and finally fall inside the region Ψ defined as

$$\Psi = \left\{(S, I):\ S \geq 0, I \geq 0, D + I \leq \frac{\alpha}{\mu}\right\}. \tag{3}$$

Obviously, system (2) has infection-free equilibrium $E_0 = (\alpha/\mu, 0)$.

The basic reproduction number R_0 is defined as the average number of computers infected by an infected device during the period from infection. R_0 often serves as a threshold parameter that predicts whether an infection will spread. For system (2), we have

$$R_0 = \frac{\beta_1 \alpha}{\mu(\mu + \eta)}. \tag{4}$$

If $R_0 > 1$, system (2) has a viral equilibrium $E^* = (S^*, I^*)$:

$$\begin{aligned} I^* &= \frac{\sqrt{b^2 - 4ac} - b}{2a}, \\ S^* &= \frac{\alpha}{\mu + \beta_1 I^* + \varepsilon I^*}, \end{aligned} \tag{5}$$

where

$$\begin{aligned} a &= \mu\beta_2(\beta_1 + \varepsilon), \\ b &= \mu^2(\beta_1 + \beta_2 + \varepsilon) + (\beta_1 + \varepsilon)(\mu\eta - \beta_2\alpha), \\ c &= \mu\left(\mu^2 + \mu\eta - \beta_1\alpha\right). \end{aligned} \tag{6}$$

3. Local Stability

In this section, we will analyze the two local stabilities of the equilibria of the system.

Theorem 1. *E_0 is locally asymptotically stable if $R_0 < 1$. Whereas, E_0 is unstable if $R_0 > 1$.*

Proof. By linearizing system (2) at E_0, we get the characteristic equation:

$$\begin{vmatrix} \lambda + \mu & \beta_1 \dfrac{\alpha}{\mu} + \varepsilon \\ 0 & \lambda + \eta + \mu - \beta_1 N \dfrac{\alpha}{\mu} \end{vmatrix} = 0. \tag{7}$$

Thus,

$$(\lambda + \alpha)\left(\lambda + \eta + \mu - \beta_1 N \frac{\alpha}{\mu}\right) = 0, \tag{8}$$

$$\begin{aligned} \lambda_1 &= -\mu < 0, \\ \lambda_2 &= -\eta - \mu + \beta_1 N \frac{\alpha}{\mu}. \end{aligned} \tag{9}$$

On the one hand, all roots of equation (8) have negative real parts, and hence, E_0 is locally asymptotically stable if $R_0 < 1$. On the other hand, equation (8) has at least one root with positive real, and hence, E_0 is unstable if $R_0 > 1$. □

Theorem 2. *E^* is locally asymptotically stable if $R_0 > 1$.*

Proof. By linearizing system (2) at E^*, we get the characteristic equation:

$$\begin{vmatrix} \lambda + \mu + \beta_1 I^* + \varepsilon I^* & \beta_1 S^* + \varepsilon S^* \\ \beta_2 I^* - \beta_1 I^* & \lambda + \beta_2 S^* + 2\beta_1 I^* + \eta + \mu - \beta_1 S^* - \beta_2 \dfrac{\alpha}{\mu} \end{vmatrix} = 0. \tag{10}$$

Thus,

$$\lambda^2 + k_1\lambda + k_2 = 0, \tag{11}$$

where

$$\begin{cases} k_1 = \beta_2 S^* + 3\beta_1 I^* + \eta + 2\mu + \varepsilon I^* - \beta_1 S^* - \beta_2 \dfrac{\alpha}{\mu}, \\ k_2 = (\mu + \beta_1 I^* + \varepsilon I^*)\left(\beta_2 S^* + 2\beta_1 I^* + \eta + \mu - \beta_1 S^* - \beta_2 \dfrac{\alpha}{\mu}\right) + I^* S^* (\beta_1 + \varepsilon)(\beta_1 - \beta_2). \end{cases} \tag{12}$$

The following inequality can be obtained from Section 2: $\beta_1 > \beta_2$. We can also obtain an equation from the second equation of system (2): $\beta_1 S^* + \beta_2(\alpha/\mu) = \beta_2 S^* + \beta_2 I^* + \eta + \mu$.

We have $k_1 = 2\beta_1 I^* + \mu + \varepsilon I^* + (\beta_1 - \beta_2) I^* > 0$ and $\beta_2 S^* + 2\beta_1 I^* + \eta + \mu - \beta_1 S^* - \beta_2(\alpha/\mu) = \beta_1 I^* > 0$, so $k_2 > 0$.

It follows from the Hurwitz [21] criterion that the two roots of (11) have negative real parts. Thus, the claimed result follows. □

4. Global Stability

Theorem 2 has revealed that the equilibrium E^* and E_0 in the system (2) are locally asymptotically stable, respectively. Then, we intend to analyze the global stability of the SID epidemic model in this section. A famous method is for determining a system whether having periodic orbits is the Bendixson–Dulac [22] criterion. The following lemma will be useful in the sequel before proving the global stability of equilibrium points.

Lemma 1. *The system has no periodic orbits in* Ψ *for system (2).*

Proof. Define

$$\begin{aligned} h_1(S, I) &= \alpha - \mu S - \beta_1 SI - \varepsilon IS, \\ h_2(S, I) &= \beta_1 SI + \beta_2 \frac{\alpha}{\mu} I - \beta_2 SI - \beta_2 I^2 - \eta I - \mu I. \end{aligned} \tag{13}$$

Constructing Dulac function [22],

$$F(D, I) = \frac{1}{SI}. \tag{14}$$

In the interior of Ψ, one can get

$$\frac{\partial(Fh_1)}{\partial S} + \frac{\partial(Fh_2)}{\partial I} = -\frac{\alpha}{S^2 I} - \frac{\beta_2}{S} < 0. \tag{15}$$

Therefore, it follows from the Bendixson–Dulac criterion [22] that the interior of Ψ for system (2) does not contain periodic orbit.

We should take into account the boundary of Ψ after considering the interior area. Assume that an arbitrary point $(\widetilde{S}, \widetilde{I})$ is on the edge of the Ψ. After that, the following three possibilities will be discussed, respectively:

(1) Case 1: when $0 < \widetilde{S} \le \alpha/\mu$ and $\widetilde{I} = 0$, then

$$\frac{\mathrm{d}}{I}\mathrm{d}t\Big|_{(\widetilde{S},\widetilde{I})} = 0. \tag{16}$$

(2) Case 2: when $0 < \widetilde{I} \le \alpha/\mu$ and $\widetilde{S} = 0$, then

$$\frac{\mathrm{d}S}{\mathrm{d}t}\Big|_{(\widetilde{S},\widetilde{I})} = \alpha > 0. \tag{17}$$

(3) Case 3: when $\widetilde{S} + \widetilde{I} = \alpha/\mu$, $\widetilde{S} \neq 0$, and $\widetilde{I} \neq 0$, then

$$\begin{aligned} \frac{\mathrm{d}(S+I)}{\mathrm{d}t}\Big|_{(\widetilde{S},\widetilde{I})} &= \alpha + \beta_2 I\left(\frac{\alpha}{\mu} - I - S\right) - \mu(S+I) \\ &\quad - \epsilon IS - \eta I = -\epsilon IS - \eta I < 0. \end{aligned} \tag{18}$$

Thus, it complies with the above three cases that there is no periodic orbit getting past $(\widetilde{S}, \widetilde{I})$ for system (2). In brief, there is no periodic orbit within $\widetilde{\Omega}$ for system (2). Now, the proof has been completed.

Then, we can set out to prove the equilibria E^* and E_0 of system (2) are global asymptotically stable in corresponding conditions, respectively. □

Theorem 3. *E_0 is globally asymptotically stable with respect to Ψ if $R_0 < 1$, whereas E^* is globally asymptotically stable with respect to Ψ if $R_0 > 1$.*

Proof. With the basis of Theorems 1 and 2 and Lemma 1, according to the Poincare–Bendixson theorem [22], one can get that the equilibrium E^* is globally asymptotically stable for system (2) with respect to Ψ if $R_0 > 1$, and E_0 is globally asymptotically stable with respect to Ψ if $R_0 < 1$. Now, we accomplish the proof. □

Remark 1. Theorems 1–3 have presented a phenomenon that the malware cannot be completely suppressed if $R_0 > 1$. But according to Theorem 1, some factors can also suppress the spread of malware. In another aspect, with these related parameters, the proportion of infected can be reduced. This also provides an effective direction to curb the spread of malware in computers.

5. Numerical Simulations

This section is to give some numerical simulations to verify our theoretical results.

Example 1. Consider system (1) with parameters $\alpha = 1, \mu = 0.1, \epsilon = 0.02$, $\beta_1 = 0.05$, $\beta_2 = 0.02$, and $\eta = 0.45$; then, $R_0 = 0.91 < 1$, and some initial values are given in Table 1.

In Figure 2, E_0 is globally stable if $R_0 < 1$. What is more, we can get a conclusion that the initial value has nothing to do with the global stability if $R_0 < 1$.

Example 2. Consider system (1) with parameters $\alpha = 1, \mu = 0.1, \epsilon = 0.02$, $\beta_1 = 0.1$, $\beta_2 = 0.05$, and $\eta = 0.45$;

Table 1: Simulation initial values.

Initial value	$S(0)$	$D(0)$	$I(0)$
Case 1	2	0	8
Case 2	4	0	6
Case 3	6	0	4
Case 4	2	3	5
Case 5	4	4	2

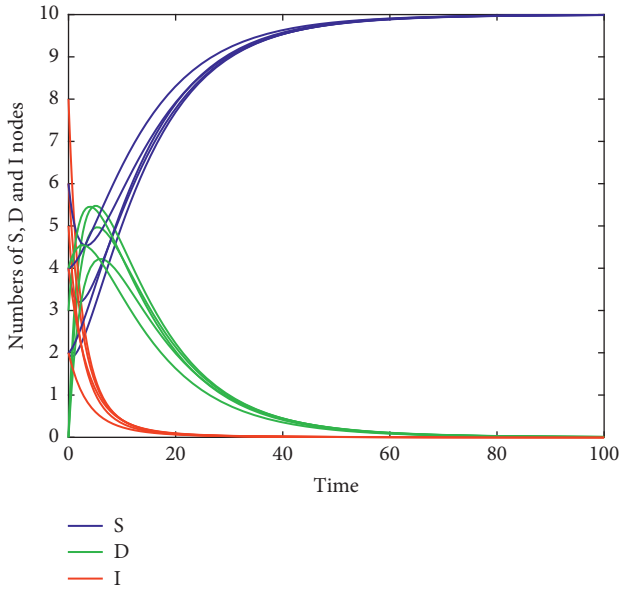

Figure 2: The time plot for the system given in Example 1.

then, $R_0 = 1.82 > 1$, and the initial values of the system are kept the same as given in Table 1.

In Figure 3, E^* is globally stable if $R_0 > 1$. We can also find that the initial value has no effect on the spread of malware if $R_0 > 1$. By comparing Figure 2 with Figure 3, keeping the basic reproduction number $R_0 < 1$ is an effective way to prevent the breakout of malware.

Example 3. We will illustrate the influence of different the awareness conversion rate $\epsilon = \{0.02, 0.08, 0.14, 0.20, 0.26\}$ on system (1). Consider system (1) with parameters $\alpha = 1, \mu = 0.1, \beta_1 = 0.1$, $\beta_2 = 0.02$, and $\eta = 0.1$ and with initial conditions $S(0) = 9$, $D(0) = 0$, and $I(0) = 1$.

Since user awareness plays an important role in malware propagation, Figure 4 shows time plots of the number of infected users with varied awareness conversion rates. We can find that the higher the awareness conversion rate, the smaller the number of infected users. So, raising user awareness can effectively control the number of infected users.

Example 4. Due to the importance of R_0, we will discuss how parameters affect the evolution of malware propagation over time. The parameters are given in Table 2.

We can find that R_0 and β_1 have a positive linear relationship as shown in Figure 5. Therefore, we can keep the contact rate β_1 at a low level to prevent the spread of malware

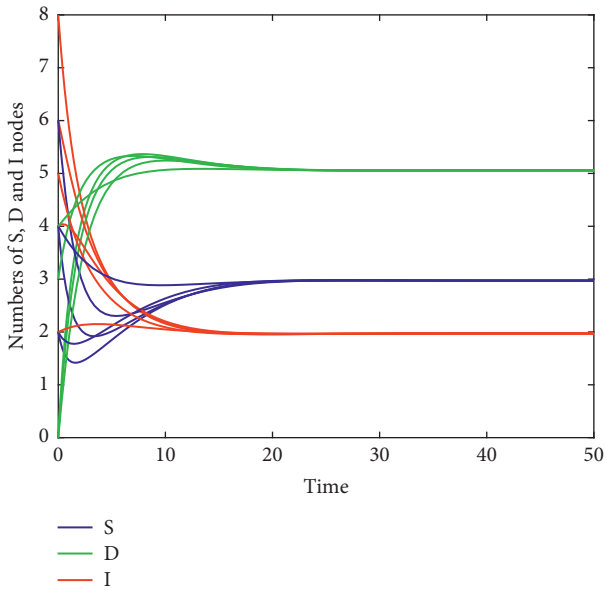

Figure 3: The time plots for the system given in Example 2.

in computers effectively. R_0 and α have a positive linear relationship in Figure 6. Figure 7 shows that R_0 decreases as μ increases. Thus, it is reasonable to reduce the online rate of the computer and increase the disconnect rate of computer

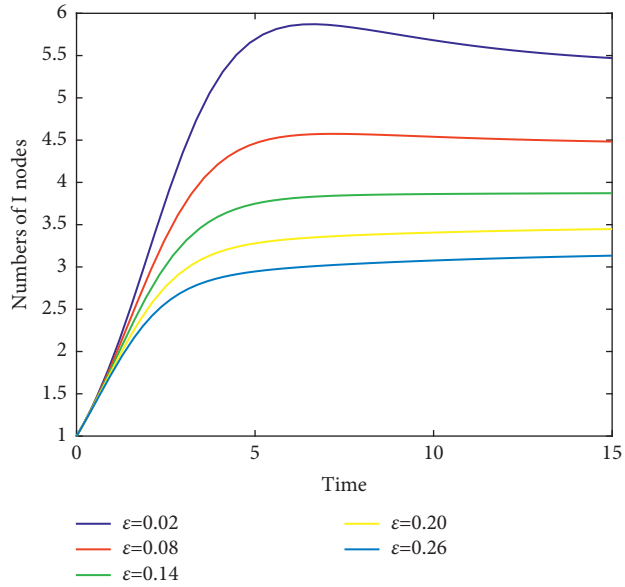

Figure 4: The time plots of number of infected nodes of the system with conditions given in Example 3.

Table 2: Simulation parameters.

Figures	β_1	α	μ	η
Figure 5	*	1	0.1	0.6
Figure 6	0.05	*	0.1	0.6
Figure 7	0.05	1	*	0.6
Figure 8	0.05	1	0.1	*

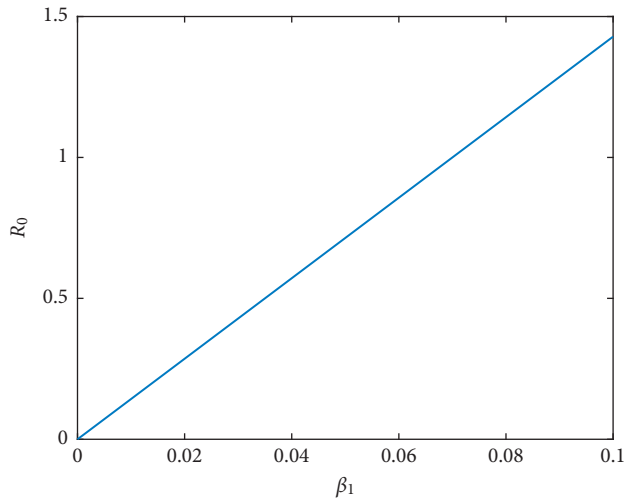

Figure 5: The effect of β_1 on R_0.

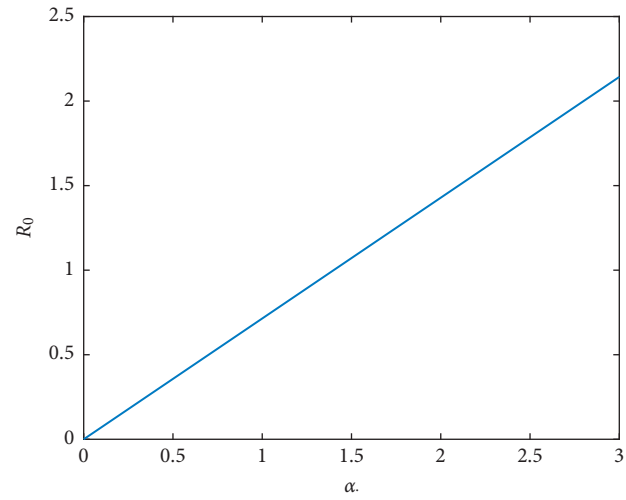

Figure 6: The effect of α on R_0.

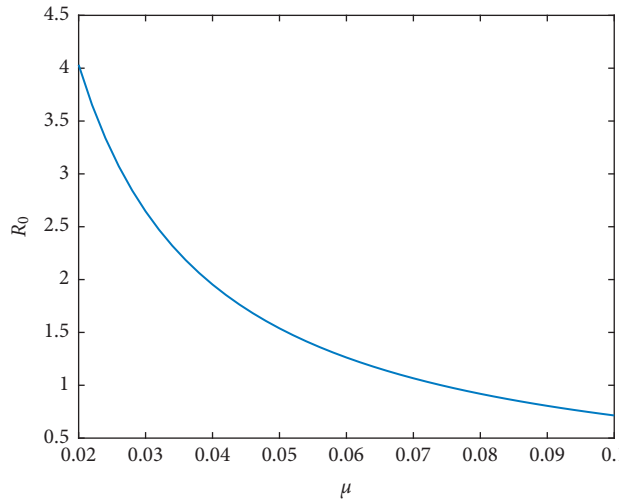

Figure 7: The effect of μ on R_0.

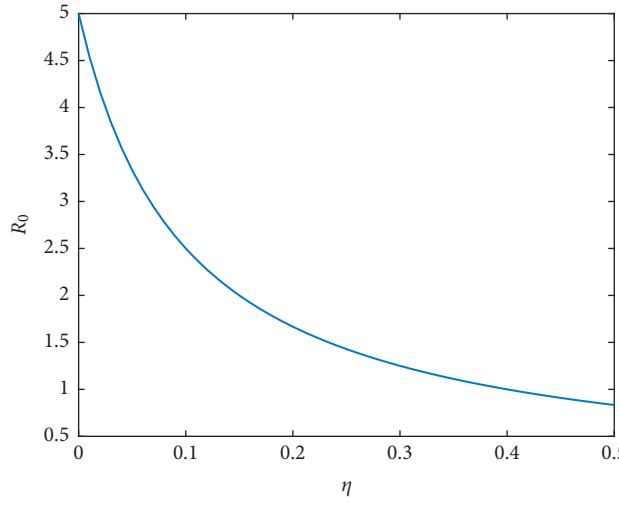

Figure 8: The effect of η on R_0.

Table 3: Simulation parameters.

Parameters	α	μ	β_1	β_2	η	ϵ	β	η_1
Case 1	1	0.1	0.1	0.05	0.2	0.04	0.1	0.2
Case 2	1	0.1	0.3	0.1	0.2	0.02	0.3	0.2
Case 3	1	0.1	0.5	0.2	0.2	0.04	0.5	0.2

when the malware spreads and breaks out. Figure 8 shows that R_0 will drop sharply if the recovery rate increased. So, installing the latest antimalware software on computers is another effective countermeasure to control the propagation of malware.

Example 5. Finally, we compare the SIS model with our proposed model through several sets of simulation experiments. The SIS model with the infection rate β and the recovery rate η_1 have been proposed in [23]. Here, $\beta = \beta_1$ and $\eta_1 = \eta$. The initial conditions are $S(0) = 6$, $D(0) = 0$, and $I(0) = 4$. The parameters are given in Table 3.

In Figure 9, we can clearly see that the final number of infected nodes in the SID model is always smaller than the corresponding number in the SIS model. So, it makes sense to improve the security awareness of users.

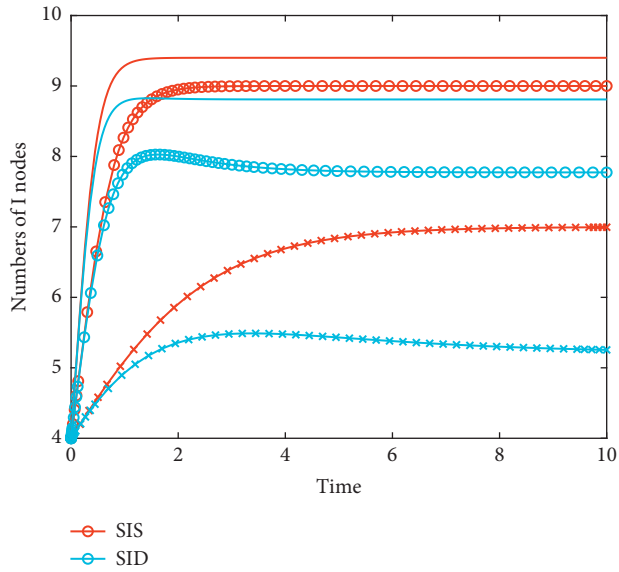

Figure 9: The time plots for the system given in Example 5.

6. Conclusion

Inspired that user awareness plays an important role in the spread of malware, a new model based on the SIS model is proposed. Through mathematical analysis and simulation experiments, the rationality of the model is verified, and it is proposed that if we improve user awareness before malware propagation, then preventing the spread of malware will be achieved. Moreover, biological and malware models have many similar behaviors. Hence, it makes sense to compare biological and malware models. The novel coronavirus infectious disease is commonly known as COVID-19 and has become the greatest challenge in this world [24]. To study the spread of the coronavirus, there are plenty of mathematical models about COVID-19 [25–27]. The model proposed in this article can also be used to describe the propagation of COVID-19. In this context, S node represents people who have not taken any measures against COVID-19, D node represents people who have taken measures against COVID-19, such as wearing a mask or staying at home, and I node represents people who have been infected and can infect others.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61903056 and 61702066) and the Chongqing Research Program of Basic Research and Frontier Technology (cstc2019jcyj-msxmX0681 and cstc2018jcyjAX0154).

References

[1] A. M. del Rey and M. Angel, "Mathematical modeling of the propagation of malware: a review," *Security and Communication Networks*, vol. 8, no. 15, pp. 2561–2579, 2015.

[2] Panda Security, *PandaLabs Annual Report*, Panda Security, Bilbao, Spain, 2017.

[3] Y. Dai, H. Li, Y. Qian, Y. Guo, R. Yang, and M. Zheng, "Using IRP and local alignment method to detect distributed malware," *Computers Security*, vol. 100, Article ID 102109, 2020.

[4] P. Vinod, A. Zemmari, and M. Conti, "A machine learning based approach to detect malicious android apps using discriminant system calls," *Future Generation Computer Systems*, vol. 94, pp. 333–350, 2019.

[5] F. Abri, S. Siami-Namini, M. A. Khanghah, F. M. Soltani, and A. S. Namin, "Can machine/deep learning classifiers detect zero-day malware with high accuracy?" in *Proceedings of the IEEE International Conference on Big Data (Big Data)*, pp. 3252–3259, IEEE, Los Angeles, CA, USA, December 2019.

[6] A. Damodaran, F. D. Troia, C. A. Visaggio, T. H. Austin, and M. Stamp, "A comparison of static, dynamic, and hybrid analysis for malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 13, no. 1, pp. 1–12, 2017.

[7] J. D. Hernández Guillén and A. Martín del Rey, "A mathematical model for malware spread on WSNs with population dynamics," *Physica A: Statistical Mechanics and Its Applications*, vol. 545, Article ID 123609, 2020.

[8] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 343–359, IEEE, Oakland, CA, USA, 1999.

[9] I. Tomovski, I. Trpevski, and L. Kocarev, "Topology independent SIS process: an engineering viewpoint," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 3, pp. 627–637, 2014.

[10] 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.

[11] 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.

[12] 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.

[13] C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 138–147, Washington, DC, USA, November 2002.

[14] C. Gan, Q. Feng, X. Zhang, Z. Zhang, and Q. Zhu, "Dynamical propagation model of malware for cloud computing security," *IEEE Access*, vol. 8, pp. 20325–20333, 2020.

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

[16] M. O'Neill, S. Ruoti, K. Seamons, and D. Zappala, "TLS proxies: friend or foe?" in *Proceedings of the 2016 Internet Measurement Conference*, pp. 551–557, Santa Monica, CA, USA, November 2016.

[17] S. Furnell, "Still on the hook: the persistent problem of phishing," *Computer Fraud & Security*, vol. 2013, no. 10, pp. 7–12, 2013.

[18] X. Zhang, S. Chen, H. Lu, and F. Zhang, "An improved computer multi-virus propagation model with user awareness," *Journal of Information and Computational Science*, vol. 8, no. 16, pp. 4301–4308, 2011.

[19] W. S. Bahashwan and S. M. Al-Tuwairqi, "Modeling the effect of external computers and removable devices on a computer network with heterogeneous immunity," *International Journal of Differential Equations*, vol. 2021, Article ID 6694098, 13 pages, 2021.

[20] S. M. Al-Tuwairqi and W. S. Bahashwan, "A dynamic model of viruses with the effect of removable media on a computer network with heterogeneous immunity," *Advances in Difference Equations*, vol. 2020, no. 1, pp. 1–20, 2020.

[21] E. A. Barbashin, *Introduction to the Theory of Stability*, Walters-Noordhoff, Groningen, Netherlands, 1970.

[22] R. C. Robinson, *An Introduction to Dynamical Systems: Continuous and Discrete*, Prentice-Hall, Upper Saddle River, NJ, USA, 2004.

[23] W. O. Kermack and A. G. Mckendrick, "Contributions to the mathematical theory of epidemics. II. the problem of endemicity," *Proceedings of the Royal Society of London. Series A*, vol. 138, no. 834, pp. 55–83, 1932.

[24] S. Ullah and M. A. Khan, "Modeling the impact of non-pharmaceutical interventions on the dynamics of novel coronavirus with optimal control analysis with a case study," *Chaos, Solitons, and Fractals*, vol. 139, Article ID 110075, 2020.

[25] M. A. Khan, A. Atangana, E. Alzahrani, and A. Fatmawati, "The dynamics of COVID-19 with quarantined and isolation," *Advances in Difference Equations*, vol. 2020, no. 1, p. 425, 2020.

[26] M. A. Khan and A. Atangana, "Modeling the dynamics of novel coronavirus (2019-nCov) with fractional derivative," *Alexandria Engineering Journal*, vol. 59, no. 4, pp. 2379–2389, 2020.

[27] M. S. Alqarni, M. Alghamdi, T. Muhammad, A. S. Alshomrani, and M. Altaf Khan, "Mathematical modeling for novel coronavirus (COVID-19) and control," *Numerical Methods for Partial Differential Equations*, 2020.