Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

The effect of terminal boundary protection on the spread of computer viruses: modeling and simulation*

Kai GAO[1], Lixin ZHANG[2,3], Yabing YAO[4], Yang YANG[4], Fuzhong NIAN[†‡4]

[1]*Network and Information Center, Lanzhou University of Technology, Lanzhou 730000, China*

[2]*Gansu Provincial Key Laboratory of Wearable Computing, Lanzhou 730000, China*

[3]*School of Information Science and Engineering, Lanzhou University, Lanzhou 730000, China*

[4]*School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730000, China*

[†]E-mail: gdnfz@lut.edu.cn

Received Mar. 29, 2024; Revision accepted Sept. 18, 2024; Crosschecked

Abstract: The population of campus network users is diverse and complex, which increases the risk of computer virus infection when the terminal side of the campus network interacts with information. Therefore, it is crucial to explore how computer viruses propagate between terminals in the campus network. In this study, a novel computer virus-spreading model based on the characteristics of the basic network structure and a classical epidemic-spreading dynamics model, combined with actual university situations, is established. The proposed model contains six groups: susceptible group, unisolated latent group, isolated latent group, infection group, recovery group, and crash group. The proposed modelâĂŹs basic reproduction number and disease-free equilibrium point are analyzed. According to real university terminal computer virus propagation data, a basic computer virus infection rate, basic computer virus killing rate, and security protection strategy deployment rate are proposed to define the conversion probability of each group and perceive each groupâĂŹs variation tendency. Furthermore, we analyzed the spreading trend of computer viruses in the campus network in terms of the proposed computer virus spreading model. Specific measures are proposed to suppress the spread of computer viruses in terminals, to ensure the safe and stable operation of the campus network terminals to the greatest extent.

Key words: Campus network terminal security; Spread of computer virus; Model; Analogue simulation; Terminal protection measures

https://doi.org/10.1631/FITEE.2400236 **CLC number:**

1 Introduction

The campus network provides high speed and efficient network connection for the school, supports a variety of network protocols and management strategies, and can meet the needs of different users in the school. The campus network also provides various network services to facilitate the management of the school and the use of teachers and students. The campus network has high bandwidth, wide coverage, information interaction, many users, and other characteristics, and the campus network has become an indispensable part of the study and life of teachers and students. However, because of these characteristics, Trojan horses, viruses, worms, and other computer viruses in the campus network spread quickly, over a wide range, and with strong hidden and destructive characteristics (Husain and Abubakar, 2015; Husain and Suleiman, 2015; Odule and Kaka, 2018; Almiani et al., 2020; Yang LX et al., 2021a; Chen et al., 2023). When universities face

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (Nos. 62266030 and 61863025)

the lateral spread of computer viruses in the campus network, they can usually suppress and block the spread by strengthening the security policy of network security equipment, updating terminal system patches, and installing terminal anti-virus software (Yang LX et al., 2016, 2021b; Zhang XL and Gan, 2017; Lanz et al., 2019; Bahashwan and Al-Tuwairqi, 2021; Epiphaniou et al., 2023). At present, most universities only rely on the above technical means to carry out network security protection, and do not have a deeper level to explore the cross-spread characteristic of computer viruses in the campus network.

Epidemic models, spreading dynamics, and computer virus spreading are hot topics in academic circles (Tanaka et al., 2014; Zhang HF et al., 2014; Wu and Chen, 2017; Cao et al., 2020). Yang XF and Yang (2012) proposed the SLBS model based on the typical computer virus spreading process. Gan et al. (2014) proposed a dynamic model with two kinds of generic nonlinear probabilities (incidence rate and vaccination probability), and pointed out that the generic nonlinear vaccination is helpful in strengthening computer security. Based on the delay-varying SIRC model, Ren et al. (2013) introduced an isolation mechanism to maintain a relatively high number of recovered nodes and a low number of infected nodes to suppress the spread of computer viruses. Zhang CM (2018) proposed a new linear computer virus spread model on multilayer networks based on the SLBS model. Fatima et al. (2018) proposed susceptible latent breaking out quarantine susceptible (SLBQRS) computer virus dynamics. Jackson et al. constructed the SIR Time-delay diffusion model (Jackson and Chen-Charpentier, 2017). Zhang XL and Li (2020) address a dynamic model that incorporates nonlinear countermeasure probability and infected removable storage media to suppress the spread of computer viruses. Nian et al. (2022) studied the propagation relationship of Weibo users and the classical infectious disease model, and proposed the mechanism, effects (impulse effect, clock effect, and herding effect), and scale of virus propagation in online information dissemination. Liu et al. proposed an SIQR epidemic model with a nonlinear incidence rate and two delays. Local stability and existence of Hopf bifurcation were analyzed by combining the time delay due to the latent disease period and the time delay due to the period during which the infected and quarantined individuals are cured as the bifurcation parameter (Liu and Wang, 2016). Alhebshi et al. (2023) proposed a computer virus spread model with fuzzy parameters. Moreover, with fuzziness, two numerical methods, the forward Euler technique and a nonstandard finite difference (NSFD) scheme, respectively, were developed and analyzed. Hoang et al. (2023) applied the Mickens methodology to formulate NSFD schemes for some epidemiological models describing the spread of computer viruses and malware, and demonstrated the advantages of NSFD. Yang LX and Yang (2017) investigated the effect of network topology on the spread of computer viruses in the presence of removable storage media. With the help of the epidemic model and spreading dynamics, this study explored the inherent law of lateral spreading of computer viruses in a campus network based on the characteristics of basic network structure and the spreading dynamics model.

2 Spread dynamics modeling

In the SIR Model (Dietz, 1998), there are three group state categories: susceptible, infected, and recovered. The susceptible group includes people who have not been infected with the disease and are healthy so far. The infected group includes people who have been diagnosed with the disease. The recovery group includes people who have fully recovered from the infection. The state transitions of the three groups are shown in Fig. 1.

Fig. 1 SIR model state transitions

In Fig. 1, the susceptible will become infected with a certain infection probability β, and the infected will recover with a certain recovery probability γ. From this, the mean field equation of the SIR Model can be obtained as shown in Eq. (1). In this model, the transition between group states is simple and direct, but compared with the characteristics of computer virus spread in the campus network environment, it is obviously not reasonable. Therefore, this study improves the SIR Model and combines the characteristics of computer virus propagation to establish a more suitable spreading dynamics model for the campus network environment.

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)I(t)/N, \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = -\beta S(t)I(t)/N - \gamma I(t), \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t). \end{cases} \tag{1}$$

2.1 Definition of the spread model

In the university campus network environment, the spread of computer viruses has the following four basic characteristics:

1. High speed: Because of the large number of users in the campus network, once a user is infected with computer viruses, if no effective protective measures are taken, it will quickly spread to other users.

2. Wide range: The users in the campus network are usually students, they come from different colleges and majors, and the devices they use are also different, so once the computer virus is released, it will affect many users.

3. Strong concealment: Some computer viruses take various measures to hide themselves from being detected by users or security software.

4. High destructive: Because campus network users are usually students, their network security awareness is relatively weak, and some computer viruses may take advantage of studentsâĂŹ curiosity or lack of security awareness to cheat or attack users.

Combined with the above characteristics of computer virus spread, we divided the status of campus network user groups into the following six categories:

1. Susceptible group (S): Personal terminal has not been infected with computer viruses in the campus network user groups.

2. Unisolated latent group (P_c): The personal terminal has actually been infected with computer viruses, but the user is yet aware, and the east-west direction of the terminal has not deployed security protection strategies in advance of the campus network user groups (such as terminal installation of anti-virus software, open firewall).

3. Isolated latent group (P_q): The personal terminal has actually been infected with computer viruses, but the user is yet aware, and the east-west direction of the terminal has been deployed in advance of the security protection strategy of the campus network user group.

4. Infection group (I): Personal terminals have been infected with computer viruses, and users are aware of the presence of campus network user groups.

5. Recovery group (R): Personal terminals have been infected with computer viruses after successful application of antivirus of campus network user groups.

6. Crash group (D): Personal terminal is down (such as completely losing control of the host) due to computer virus infection of campus network user groups.

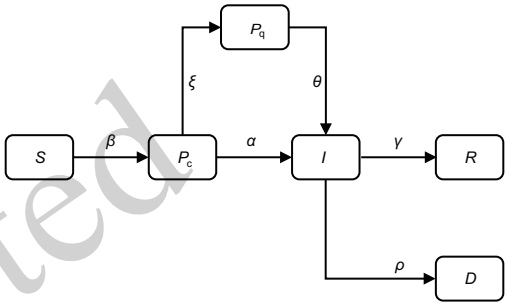

Fig. 2 State transition of computer virus spread dynamics model in campus network

Among the six groups, some susceptible groups will first be transformed into unisolated latent groups due to failure to deploy security protection strategies in advance. Subsequently, some of the unisolated latent groups will be directly transformed into infection groups due to the lack of network security awareness and other reasons, and some of the unisolated latent groups will be transformed into isolated latent groups due to the timely deployment of security protection strategies. The isolated latent group is not absolutely safe. For example, the isolated latent groups infected with 0 day or high-risk computer viruses will also turn into infection groups. Finally, the infection groups will be transformed into recovery groups if the anti-virus is successful, otherwise the infection groups will be transformed into crash groups. The state transitions of these six population classes are shown in Fig. 2, and the mean field equation is given in Eq. (2).

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)P_{\mathrm{c}}(t), \\ \frac{\mathrm{d}P_{\mathrm{c}}(t)}{\mathrm{d}t} = \beta S(t)P_{\mathrm{c}}(t) - \alpha P_{\mathrm{c}}(t) - \xi P_{\mathrm{c}}(t), \\ \frac{\mathrm{d}P_{\mathrm{q}}(t)}{\mathrm{d}t} = \xi P_{\mathrm{c}}(t) - \theta P_{\mathrm{q}}(t), \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \alpha P_{\mathrm{c}}(t) + \theta P_{\mathrm{q}}(t) - \gamma I(t) - \rho I(t), \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t), \\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} = \rho I(t). \end{cases} \tag{2}$$

The relevant parameters in Eq. (2) are defined as follows:

$$N = S(t) + P_{\mathrm{c}}(t) + P_{\mathrm{q}}(t) + I(t) + R(t) + D(t). \tag{3}$$

In Eq. (3), N denotes the total number of nodes in the network, and the number transition between groups in the network follows Eq. (3).

Probability of S transitioning to P_{c}: the probability that susceptible group S transform into unisolated latent group P_{c} is β, which is expressed as follows:

$$\begin{aligned} \beta &= \sum_{j \in \Pi(i)} \frac{G(i|j)}{C([x_j = S] \cup [x_i = I])/\mathrm{Len}(\Pi(i))} \\ &= \sum_{j \in \Pi(i)} \frac{\mathrm{Len}(\Pi(i)) * G(i|j)}{C([x_j = S] \cup [x_i = I])}. \end{aligned} \tag{4}$$

In Eq. (4), $\Pi(i)$ represents the set of neighbor nodes of node i in the network, $G(i|j)$ represents the basic computer virus infection rate between nodes i and j, and $C([x_j = S] \cup [x_i = I])/\mathrm{Len}(\Pi(i))$ represents the proportion of the number of nodes i that belong to the infected group to the total number of neighbor nodes of node i when node j belongs to the susceptible group. For node i, the basic infection rate of a computer virus between nodes i and j should be calculated by considering all its neighbor nodes j, and the ratio of the number of nodes i that belong to the infected group to the total number of neighbor nodes of node i when node j belongs to the susceptible group to the proportion of the total number of neighbor nodes of node i should be calculated. Then the ratios are summed to obtain the probability β that the susceptible group transforms to the unisolated latent group.

Probability of P_{c} transitioning to P_{q}: the probability that unisolated latent group P_{c} transforms into isolated latent group P_{q} is ξ, which is expressed as follows:

$$\begin{aligned} \xi &= \sum_{j \in \Pi(i)} \frac{U(i|j)}{C([x_j = P_{\mathrm{c}}] \cup [x_i = S])/\mathrm{Len}(\Pi(i))} \\ &= \sum_{j \in \Pi(i)} \frac{\mathrm{Len}(\Pi(i)) * U(i|j)}{C([x_j = P_{\mathrm{c}}] \cup [x_i = S])}. \end{aligned} \tag{5}$$

In Eq. (5), $U(i|j)$ represents the probability that the security protection strategy between nodes i and j has been deployed, and $C([x_j = P_{\mathrm{c}}] \cup [x_i = S])/\mathrm{Len}(\Pi(i))$ represents the proportion of the number of nodes i that belong to the susceptible group to the total number of neighbor nodes of node i when node j belongs to the unisolated latent group. For node i, considering all its neighbor nodes j, it is necessary to calculate the ratio of the probability that the security protection strategy between node i and j has been deployed and the ratio of the number of nodes i that belong to the susceptible group to the total number of neighbor nodes of node i when node j belongs to the unisolated latent group; then the ratios are summed to obtain the probability ξ that the unisolated latent group transforms to the isolated latent group.

Probability of P_{q} transitioning to I: the probability that isolated latent group P_{q} transforms into infection group I is θ, which is expressed as follows:

$$\begin{aligned} \theta &= \sum_{j \in \Pi(i)} \frac{G(i|j) * (1/K(i|j))}{C([x_j = P_{\mathrm{q}}] \cup [x_i = S - P_{\mathrm{c}}])/\mathrm{Len}(\Pi(i))} \\ &= \sum_{j \in \Pi(i)} \frac{\mathrm{Len}(\Pi(i)) * G(i|j)}{C([x_j = P_{\mathrm{q}}] \cup [x_i = S - P_{\mathrm{c}}]) * K(i|j)}. \end{aligned} \tag{6}$$

In Eq. (6), $K(i|j)$ represents the basic killing rate of a computer virus between nodes i and j, and $C([x_j = P_{\mathrm{q}}] \cup [x_i = S - P_{\mathrm{c}}])/\mathrm{Len}(\Pi(i))$ represents the proportion of the number of nodes i that belong to the susceptible group and not to the unisolated latent group to the total number of neighbor nodes of node i when node j belongs to the isolated latent group. For node i, considering all its neighbor nodes j, it is necessary to calculate the ratio of the infection rate of a computer virus killed between nodes i and j and the proportion of the number of nodes i that belong to the susceptible group and not to the unisolated latent group when node j belongs to the isolated latent group to the total number of neighbor nodes of node i; then the ratios are summed to ob-

tain the probability θ that the isolated latent group transforms to the infection group.

Probability of P_c transitioning to I: the probability that unisolated latent group P_c transforms into infection group I is α, which is expressed as follows:

$$\begin{aligned}\alpha &= \sum_{j\in\Pi(i)} \frac{G(i|j)}{C([x_j=P_c]\cup[x_i=S-P_q])/\mathrm{Len}(\Pi(i))}\\ &= \sum_{j\in\Pi(i)} \frac{\mathrm{Len}(\Pi(i))*G(i|j)}{C([x_j=P_c]\cup[x_i=S-P_q])}.\end{aligned} \tag{7}$$

In Eq. (7), $C([x_j = P_c] \cup [x_i = S - P_q])/\mathrm{Len}(\Pi(i))$ represents the proportion of the number of nodes i that belong to the susceptible group and do not belong to the isolated latent group to the total number of neighbor nodes of node i when node j belongs to the unisolated latent group. For node i, the basic infection rate of a computer virus between nodes i and j should be calculated considering all its neighbor nodes j, and the ratio of the number of nodes i that belong to the susceptible group and not to the isolated latent group to the total number of neighbor nodes of node i when node j belongs to the unisolated latent group; then the ratios are summed to obtain the probability α that the unisolated latent group transforms to the infection group.

Probability of I transitioning to R: the probability that infection group I transforms into recovery group R is γ, which is expressed as follows:

$$\begin{aligned}\gamma &= \sum_{j\in\Pi(i)} \frac{K(i|j)}{C([x_j=I]\cup[x_i=S-P_c-P_q])/\mathrm{Len}(\Pi(i))}\\ &= \sum_{j\in\Pi(i)} \frac{\mathrm{Len}(\Pi(i))*K(i|j)}{C([x_j=I]\cup[x_i=S-P_c-P_q])}.\end{aligned} \tag{8}$$

In Eq. (8), $C([x_j = I]\cup[x_i = S-P_c-P_q])/\mathrm{Len}(\Pi(i))$ represents the ratio of the number of nodes i that belong to the susceptible group and not to the isolated or unisolated latent groups to the total number of neighbor nodes of node i when node j belongs to the infected group. For node i, the basic killing rate of a computer virus between nodes i and j should be calculated considering all its neighbor nodes j, and the ratio of the number of nodes i that belong to the susceptible group and not to the isolated or unisolated latent groups to the total number of neighbor nodes of node i when node j belongs to the infected group should be calculated; then the ratios are summed to obtain the probability γ that the infection group transforms to the recovery group.

Probability of I transitioning to D: the probability that infection group I transforms into crash group D is ρ, which is expressed as follows:

$$\begin{aligned}\rho &= \sum_{j\in\Pi(i)} \frac{1-K(i|j)}{C([x_j=I]\cup[x_i=S-P_c-P_q])/\mathrm{Len}(\Pi(i))}\\ &= \sum_{j\in\Pi(i)} \frac{\mathrm{Len}(\Pi(i))*(1-K(i|j))}{C([x_j=I]\cup[x_i=S-P_c-P_q])}.\end{aligned} \tag{9}$$

In Eq. (9), for node i, the basic survival rate of a computer virus should be calculated by considering all its neighbor nodes j, and the ratio of the number of nodes i that belong to the susceptible group and not to the isolated or unisolated latent groups to the total number of neighbor nodes of node i when node j belongs to the infected group should be calculated; then the ratios are summed to obtain the probability ρ that the infection group transforms to the crash group.

2.2 Stability analysis of the spread model

The stability of the disease-free equilibrium point of the spread model can be judged by calculating the basic reproduction number. The basic reproduction number R_0 is a basic parameter that describes the ability of computer viruses to spread. It reflects the average number of new terminals infected by a terminal that has been infected with computer viruses without any external interference. If $R_0 > 1$, the computer virus may spread continuously because each infected terminal will infect more than one new terminal. Conversely, if $R_0 < 1$, the computer virus spread will gradually decrease and may eventually disappear. In other words, the disease-free equilibrium point has local asymptotic stability.

To determine R_0, for the dynamic model of the infected population, we can rewrite Eq. (2) as follows:

$$\frac{dI(t)}{dt} = (\alpha P_c(t) + \theta P_q(t)) * \Psi - (\gamma+\rho) * I(t). \tag{10}$$

In Eq. (10), $\Psi = \sum \frac{kp(k)I}{\langle k\rangle}$ is the probability that the other end of each edge connecting a susceptible

$$J_0 = \begin{bmatrix} -(\gamma+\rho)+\frac{\alpha+\theta}{\langle k\rangle}p(1) & \frac{\alpha+\theta}{\langle k\rangle}2p(2) & \dots & \frac{\alpha+\theta}{\langle k\rangle}np(n) \\ 2\frac{\alpha+\theta}{\langle k\rangle}p(1) & -(\gamma+\rho)+2\frac{\alpha+\theta}{\langle k\rangle}2p(2) & \dots & 2\frac{\alpha+\theta}{\langle k\rangle}np(n) \\ \vdots & \vdots & & \vdots \\ n\frac{\alpha+\theta}{\langle k\rangle}p(1) & n\frac{\alpha+\theta}{\langle k\rangle}2p(2) & \dots & -(\gamma+\rho)+n\frac{\alpha+\theta}{\langle k\rangle}np(n) \end{bmatrix}. \tag{11}$$

group node points to an infection group node, and $p(k)$ is the degree distribution. We assume that the maximum degree of the network is n, so the Jacobian matrix of Eq. (10) at the disease-free equilibrium point $I = 0$ is presented in Eq. (11).

The characteristic polynomial of the matrix J_0 is as follows:

$$\begin{aligned} |J_0 - \mu E| = (&-(\gamma+\rho)-\mu+(\alpha+\theta)\frac{\sum_{k=1}^{n} k^2 p(k)}{\langle k\rangle}) \\ &* (-(\gamma+\rho)-\mu)^{n-1}. \end{aligned} \tag{12}$$

If the Eq. (12) zero solution has local asymptotic stability, then all eigenvalues Âţ of the matrix J_0 are less than zero. In this case, $\mu = -(\gamma+\rho)+(\alpha+\theta)\frac{\sum_{k=1}^{n} k^2 p(k)}{\langle k\rangle} < 0$, so the basic reproduction number is as follows:

$$R_0 = \frac{(\alpha+\theta)\langle k^2\rangle}{(\gamma+\rho)\langle k\rangle}. \tag{13}$$

This also proves that the disease-free equilibrium point has local asymptotic stability. The determination of the basic reproduction number of the spread model and the proof that the disease-free equilibrium point has local asymptotic stability strengthen the credibility of the model.

3 Experiments

To make the simulation results of Eq. (2) more realistic concerning the characteristics of the spread of computer viruses, it is necessary to focus on the analysis of the basic infection rate of the computer virus $G(i|j)$, the basic killing rate of the computer virus $K(i|j)$, and the security protection strategy deployment rate $U(i|j)$, three parameters between the nodes of the virus on the spread of computer viruses in the campus network. Therefore, with the permission of the university, we logged in to its terminal security management system and downloaded the computer virus protection report for 140 days from March 8 to October 19, 2023. The descriptive statistical analysis method is used to describe the statistical data characteristics in the report, and the final values of the three parameters are obtained as follows:

1. The basic infection rate of the computer virus: During the 140 days from March 8 to October 19, 2023, the terminal security management system showed that a total of 2703 terminals had been infected with a computer virus, with an average of 19 terminals infected every day. As of October 19, 2023, the total number of terminals in the terminal security management system showed that there were 3,915 office terminals. Therefore, $G(i|j) = 19/3915 \approx 0.005$.

2. The basic killing rate of the computer virus: From March 8, 2023 to October 19, 2023, the virus processing statistics of the terminal security management system showed that a total of 41,600 viruses were found, among which 38,473 viruses were repaired, deleted, and trusted. Therefore, $K(i|j) = 38473/41600 \approx 0.925$.

3. The security protection strategy deployment rate: As of October 19, 2023, there were 2507 faculty members, each of whom was equipped with a desktop computer and a laptop computer. Therefore, it is estimated that there were 5014 office terminals in the entire university. The security protection strategy deployment rate at the end of each month from March 8 to October 19, 2023 is shown in Table 1. In Table 1, the number of office terminals is from the universityâĂŹs terminal safety management system. The security protection strategy deployment rate is the ratio of the number of office terminals that have installed terminal security management software to the total number of office terminals in the entire school. Therefore, $U(i|j) = (0.626+0.713+0.728+0.759+0.766+0.769+0.77+0.78+0.781)/9 \approx 0.744$.

After determining $G(i|j)$, $K(i|j)$, and $U(i|j)$, we set the experimental unit time as 1 day, the total number of network nodes $N = 5000$, and the average degree of network nodes $\langle k \rangle = 20$. The number of nodes in the initial susceptible population was $S(0) = 4950$ and the number of nodes in the initial unisolated latent population was $P_c(0) = 50$ before the simulated virus spread started. The hardware configuration of our experimental environment was 11th Gen Intel(R) Core(TM) i5-11400 @ 2.60GHz, 32GB memory, and all simulation models were implemented using Python 3.9.

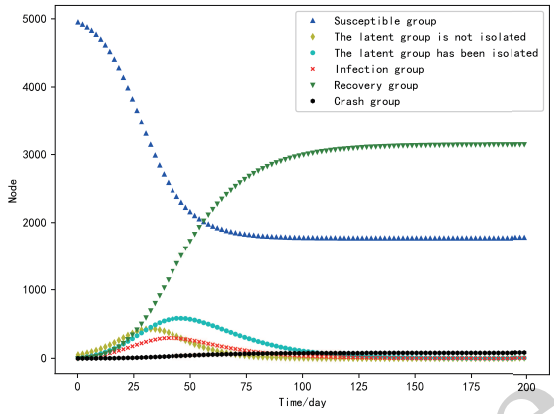

Fig. 3 Number of nodes varies with time when $G(i|j) \approx 0.005$, $K(i|j) \approx 0.925$, and $U(i|j) \approx 0.744$

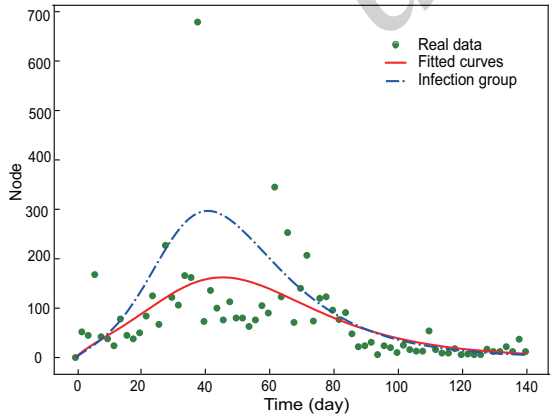

Fig. 4 Comparison of the fitted curves to real data and the trend of the infection group when $G(i|j) \approx 0.005$, $K(i|j) \approx 0.925$, and $U(i|j) \approx 0.744$

When $G(i|j) \approx 0.005$, $K(i|j) \approx 0.925$, and $U(i|j) \approx 0.744$, $\beta \approx 0.296$, $\xi \approx 0.095$, $\alpha \approx 0.091$, $\theta \approx 0.049$, $\rho \approx 0.005$, and $\gamma \approx 0.200$ are deduced, and the simulation results of Eq. (2) are shown in Fig. 3. To verify the prediction ability and rationality of the newly proposed spread model based on empirical testing, we intercepted the statistical data of the computer virus infection trend in the universityâĂŹs terminal security management system during 140 days from March 8 to October 19, 2023, and compared it with the change trend of the infection group in Fig. 3 after fitting, as shown in Fig. 4. In Fig. 4, the green dots are the real computer virus infection trend statistics, the red solid line is the fitting curve of the real statistics, and the blue dashed line is the change curve of the infection groups when $G(i|j) \approx 0.005$, $K(i|j) \approx 0.925$, and $U(i|j) \approx 0.744$. It can be clearly seen that the trend of the fitting curve of the real statistical data is basically consistent with the change trend of the infection groups in Fig. 3, which proves the predictive ability and rationality of the spread model, and the credibility of the model is further strengthened.

Table 1 Statistical table of the security protection strategy deployment rate

Data	Number of office terminals	$U(i\|j)$
2023.03.08	3141	0.626
2023.03.31	3575	0.713
2023.04.30	3648	0.728
2023.05.31	3804	0.759
2023.06.30	3839	0.766
2023.07.31	3854	0.769
2023.08.31	3859	0.770
2023.09.30	3911	0.780
2023.10.10	3915	0.781

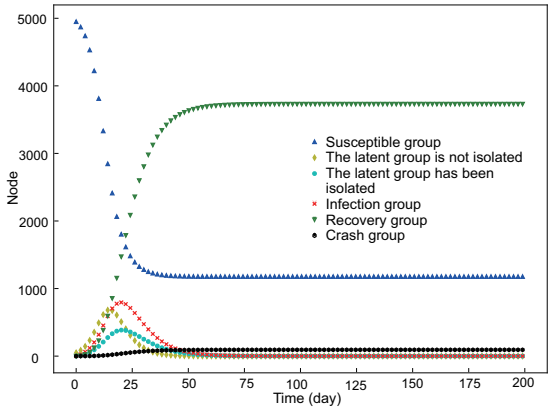

Fig. 5 Number of nodes varies with time when $G(i|j) = 0.01$

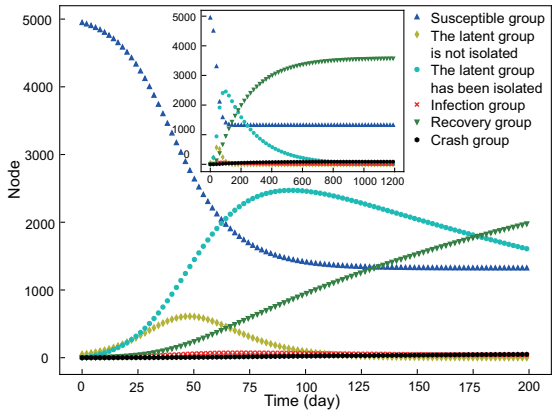

Fig. 6 Number of nodes varies with time when $G(i|j) = 0.001$

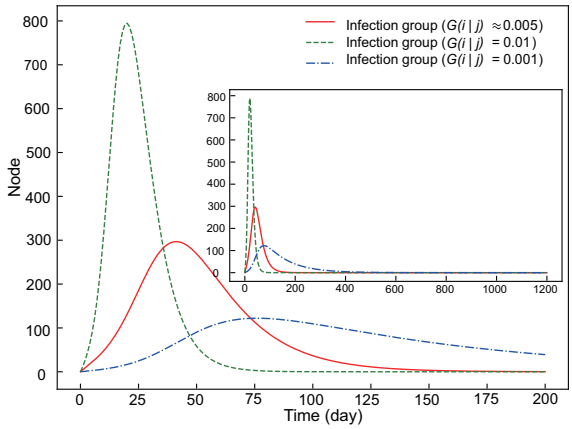

Fig. 7 Comparison of the number of simultaneously infection group over time with different $G(i|j)$

3.1 Effect of $G(i|j)$ on the spread of the computer virus

Let $K(i|j)$ and $U(i|j)$ remain unchanged, and assume that $G(i|j)$ increases to 0.01, that is, the basic infection rate of the computer virus increases. In this case, $\beta \approx 0.601$, $\xi \approx 0.095$, $\alpha \approx 0.225$, $\theta \approx 0.120$, $\rho \approx 0.005$, and $\gamma \approx 0.200$. The simulation results of Eq. (2) are shown in Fig. 5. When the basic infection rate of the computer virus decreases, that is, when $G(i|j)$ is 0.001, $\beta \approx 0.190$, $\xi \approx 0.095$, $\alpha \approx 0.011$, $\theta \approx 0.005$, $\rho \approx 0.005$, and $\gamma \approx 0.200$, the simulation results of Eq. (2) are shown in Fig. 6.

By comparing the change trend of the number of nodes in Figs. 3, 5, and 6, it can be found that the risk of computer virus infection increases with the increase of $G(i|j)$. From day 0 to 20, the trend in the susceptible group declines faster and faster, indicating that the susceptible group changes into the unisolated latent group faster; then, the unisolated latent group also begins to partially change into the isolated latent group, but this occurs slowly. This indicates that the isolation of high-risk computer viruses is more difficult, and as a result, the number of nodes in the infection group is also maximized.

When $G(i|j)$ decreases, the risk of virus infection decreases, and the decline in the number of nodes in the susceptible group continues until day 125. During this period, the number of infection and crash group nodes hardly increases. During days 0âĂŞ80, the number of isolated latent group nodes continues to increase, which indicates that low-risk computer viruses are easier to isolate. This is one of the reasons why the number of infection and crash group nodes have not significantly increased. The comparison of the change in the number of infection group nodes under different 7 is shown in Fig. 7, which shows more intuitively that with decreasing 7, the peak value of the number of infection group nodes is smaller and the trend of change is slower.

3.2 Effect of $K(i|j)$ on the spread of the computer virus

The simulation results of Eq. (2) are shown in Fig. 8, assuming that $K(i|j)$ increases to 0.975 with $\beta \approx 0.296$, $\xi \approx 0.095$, $\alpha \approx 0.091$, $\theta \approx 0.027$, $\rho \approx 0.003$, and $\gamma \approx 0.394$, leaving $G(i|j)$ and $U(i|j)$ unchanged. When $K(i|j)$ is reduced to 0.875, where $\beta \approx 0.296$, $\xi \approx 0.095$, $\alpha \approx 0.091$, $\theta \approx 0.068$, $\rho \approx 0.008$, and $\gamma \approx 0.027$, the simulation results of Eq. (2) are shown in Fig. 9. By comparing the trend in the number of nodes in Figs. 3, 8, and 9, it can be found that with increasing $K(i|j)$, the efficiency of killing computer viruses is higher, the trend of the infection group is gentler, and the number of isolated latent group nodes transformed into infection group nodes decreases simultaneously, which indicates that the efficient virus killing method can quickly suppress the spread of the computer virus.

When $K(i|j)$ decrease, the computer virus killing efficiency decrease. From the 25th to the 50th day, the number of infection group nodes continued to increase, because many isolated latent group nodes changed into infection group nodes. Simultaneously, the number of crash group nodes started to increase, indicating that as the computer virus killing rate decreases, the probability of infection group nodes turning into crash group nodes increases

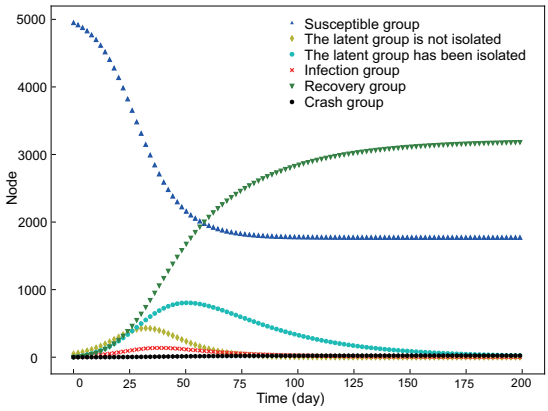

Fig. 8 Number of nodes varies with time when $K(i|j) = 0.975$

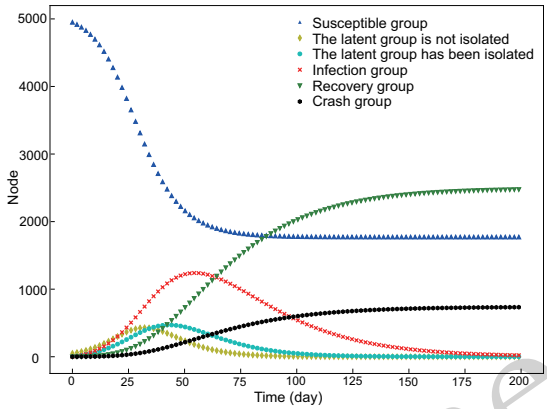

Fig. 9 Number of nodes varies with time when $K(i|j) = 0.875$

rapidly. The comparison of the changes in the number of infection group nodes under different $K(i|j)$ is shown in Fig. 10. It can be seen that as $K(i|j)$ decreases, the number of infection group nodes has a larger peak value, a more rapid upward trend, and a longer time to fall back. The comparison of the change in the number of crash group nodes under different values is shown in Fig. 11, which shows that the smaller $K(i|j)$ is, the larger the number of crash group nodes eventually becomes.

3.3 Effect of $U(i|j)$ on the spread of the computer virus

The simulation results of Eq. (2) are shown in Fig. 12, assuming that $(i|j)$ increases to 0.844 with $\beta \approx 0.296$, $\xi \approx 0.186$, $\alpha \approx 0.091$, $\theta \approx 0.049$, $\rho \approx 0.005$, and $\gamma \approx 0.200$, leaving $G(i|j)$ and $K(i|j)$ unchanged. $U(i|j)$ to 0.644, where $\beta \approx 0.296$, $\xi \approx 0.026$, $\alpha \approx 0.091$, $\theta \approx 0.049$, $\rho \approx 0.005$, and $\gamma \approx 0.200$, the simulation results of Eq. (2) are shown in Fig. 13. By comparing the trend in the number of nodes in Figs. 3, 12, and 13, it can be found that with increasing $U(i|j)$, the security protection strategy deployment improves. From day 0 to day 25, the declining trend of the susceptible group is greatly slowed down, indicating that the speed and number of the susceptible group nodes turning into unisolated latent group nodes are decreasing, and the number of infection and crash group nodes are also decreasing.

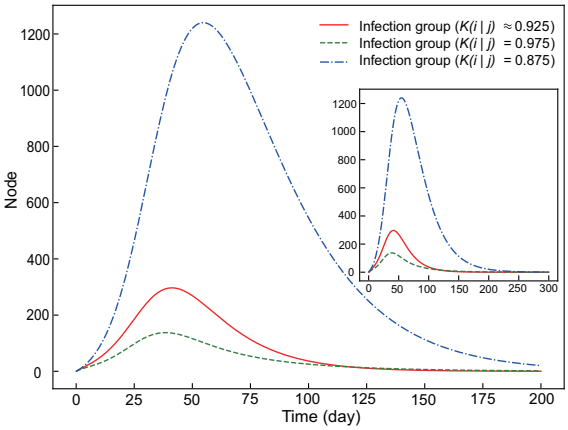

Fig. 10 Comparison of the number of simultaneously infection group over time with different $K(i|j)$

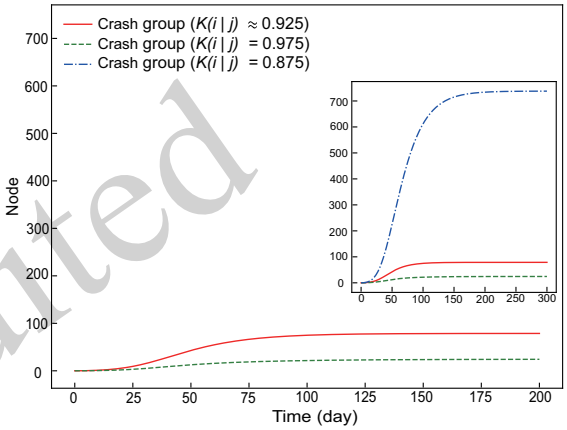

Fig. 11 Comparison of the number of simultaneously crash group over time with different $K(i|j)$

When $U(i|j)$ decreases, the security protection strategy deployment decreases, both the decline rate of susceptible group nodes and the growth rate of unisolated latent group nodes increase rapidly from the beginning, which indicates that the computer virus spread will accelerate from the beginning when the terminal lacks a protective security strategy. From the 30th to the 100th day, the number of infection group nodes increased to the highest point and then began to decline, but the decline was slow, which also showed that with the reduction of the

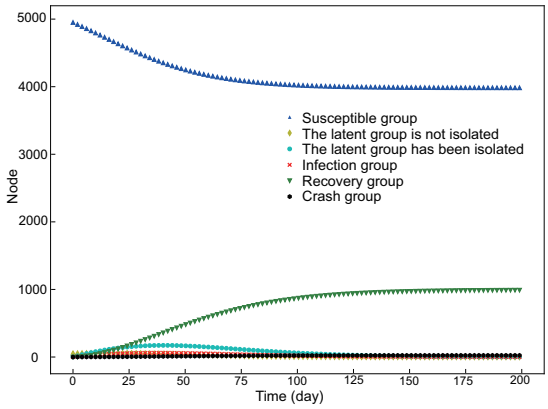

Fig. 12 Number of nodes varies with time when $U(i|j) = 0.844$

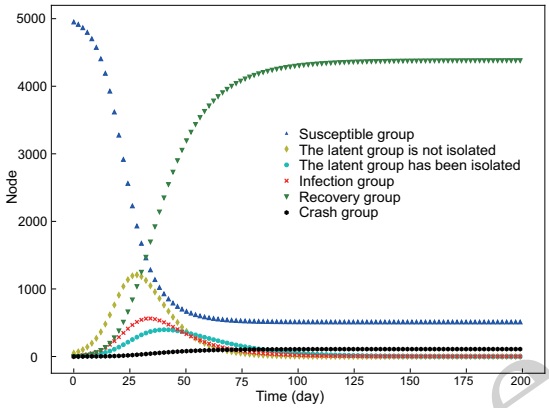

Fig. 13 Number of nodes varies with time when $U(i|j) = 0.644$

security protection strategy deployment rate, it became increasingly more difficult to kill the computer virus, as shown in Fig. 14.

3.4 Experimental results

The experimental results show that in the process of computer virus propagation, by adjusting $G(i|j)$, $K(i|j)$, and $U(i|j)$, the computer virus can effectively control the spread in the campus network. Specifically, $G(i|j)$ is reduced, and then the probability β that the susceptible group is transformed into the unisolated latent group, the probability θ that the isolated latent group is transformed into the infection group, and the probability α that the unisolated latent group is transformed into the infection group. For example, let the network border security equipment as much as possible to intercept computer viruses, or strengthen the network east-west traffic security protection and so on. By increasing $K(i|j)$, the probability θ of the isolated latent group transforming into the infection group and the probability

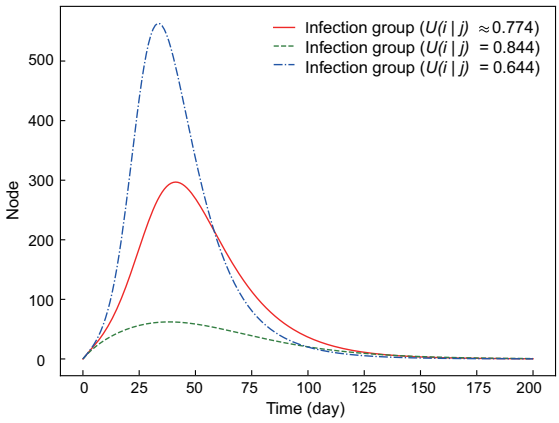

Fig. 14 Comparison of the number of simultaneously infection group over time with different $U(i|j)$

ρ of the infection group transforming into the crash group were reduced, and the probability γ of the infection group transforming into the recovery group was increased. Such as expanding the terminal security management system of the virus library, enhance the ability to kill viruses and so on. Increasing $U(i|j)$, and then increasing the probability ξ that the unisolated latent group changes into the isolated latent group. For example, as soon as possible to fully popularize the installation of terminal security management software, enhance terminal anti-virus capabilities and so on. These methods can effectively control the spread of computer viruses, achieve the purpose of controlling the spread of the virus in the campus network. The experimental results show that in the process of computer virus propagation, adjusting $G(i|j)$, $K(i|j)$, and $U(i|j)$, can effectively control computer virus spread in the campus network. Specifically, when $G(i|j)$ is reduced, the probability β that the susceptible group is transformed into the unisolated latent group, the probability θ that the isolated latent group is transformed into the infection group, and the probability α that the unisolated latent group is transformed into the infection group all increased; for example, let the network border security equipment intercept computer viruses as much as possible to, or strengthen the network east-west traffic security protection, and so on. By increasing $K(i|j)$, the probability θ of the isolated latent group transforming into the infection group and the probability ρ of the infection group transforming into the crash group were reduced, and the probability γ of the infection group transforming into the recovery group was increased; for example, expanding the

terminal security management system of the virus library, enhancing the ability to kill viruses, and so on. Increasing $U(i|j)$ increases the probability ξ that the unisolated latent group changes into the isolated latent group; for example, popularize the installation of terminal security management software as soon as possible, enhance terminal anti-virus capabilities, and so on. These methods can effectively control the spread of computer viruses and achieve the goal of controlling the spread of the virus in the campus network.

4 Discussion

4.1 Limitations

First, the spread model proposed in this paper is based on the propagation mechanism of computer viruses in a real university campus network environment, so the applicability of the model in the campus network and the same type of Local Area Network (LAN) structure has been verified. However, the robustness of the empirical test can be further enhanced because confirming the reliability of the model with only one validation limits its applicability to specific influencing factors in arbitrarily larger and more complex scenarios. Second, describing potential additional factors and how they can be integrated into the model is also one of the most important current limitations.

4.2 Future works

First, to consolidate the reliability of the model, multiple verifications should be done in future work. For example, the focus of real data collection in future work could involve larger and more complex Metropolitan Area Network (MAN) and Wide Area Network (WAN) environments. Because there are many different local area networks and individuals in MAN and WAN environments, we can use fractal thinking to treat each LAN as a whole, and then analyze specific problems based on this model. If the simulation results are similar to the fit to the real data, that is enough to further reinforce the reliability of the model.

Second, this study simply quantifies the basic infection rate of the computer virus, the basic killing rate of the computer virus, and the security protection strategy deployment rate based on computer virus protection report data in a university terminal security management system. However, in a complex real network environment, the advancement of computer virus detection technology, the deployment of security software, and user behavior will affect the basic killing rate of the computer virus. Policies and regulations issued by officials at all levels, the organizational management level, and user education and training will affect the security protection strategy deployment rate. The basic computer virus infection rate is affected by its own spreading ability, security vulnerabilities, and user security awareness. Therefore, it is necessary to identify the interaction among the above factors, further improve the mathematical equations and models, and improve the applicability value of the model.

5 Conclusions

According to the characteristics of lateral transmission of computer viruses in the campus network, this study constructed a transmission dynamics model including six groups: the susceptible group, unisolated latent group, isolated latent group, infection group, recovery group, and crash group. We systematically analyzed the mechanism of computer virus lateral transmission in a campus network using real computer virus protection data. The basic computer virus infection rate, the basic killing rate of the computer virus, and the security protection strategy deployment rate are proposed to quantitatively evaluate the risk of computer virus diffusion. Based on the experiment, in campus network security protection, the defender can increase the basic computer virus killing rate, increase the security protection strategy deployment rate, and reduce the basic computer virus infection rate, to limit the spread of the computer virus.

Specifically, the basic computer virus infection rate can be reduced by regularly scanning and repairing the security vulnerabilities of campus network user terminals, or training campus network users in network security awareness and skills to more safely use the network. In addition, a campus network east-west traffic firewall should be established along with effective isolation office areas, teaching areas, business areas, and other areas, and the terminal security management system virus library can be expanded and the systemâĂŹs real-time killing ability

can be enhanced to increase the basic computer virus killing rate. The establishment of a perfect network security management system, timely publicity of the latest network security information, and installation of unified anti-virus software on all campus terminals can increase the security protection strategy deployment rate. These measures will minimize the spread of computer viruses and reduce the risk of transmission.

Contributors

Kai GAO designed the research. Lixin ZHANG processed the data. Kai GAO drafted the paper. Yabing YAO and Yang YANG helped organize the paper. Fuzhong NIAN and Lixin ZHANG revised and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

References

Alhebshi RM, Ahmed N, Baleanu D, et al., 2023. Modeling of computer virus propagation with fuzzy parameters. *Comput Mater Con*, 74(3):5663-5678. https://doi.org/10.32604/cmc.2023.033319

Almiani M, AbuGhazleh A, Al-Rahayfeh A, et al., 2020. Deep recurrent neural network for IoT intrusion detection system. *Simul Model Pract Theory*, 101:102031. https://doi.org/10.1016/j.simpat.2019.102031

Bahashwan WS, Al-Tuwairqi SM, 2021. Modeling the effect of external computers and removable devices on a computer network with heterogeneous immunity. *Int J Differ Equ*, 2021:6694098. https://doi.org/10.1155/2021/6694098

Cao JD, Liu Y, Lu JQ, et al., 2020. Complex systems and networks with their applications. *Front Inform Technol Electron Eng*, 21(2):195-198. https://doi.org/10.1631/FITEE.2020000

Chen J, Wu DD, Xie RY, 2023. Artificial intelligence algorithms for cyberspace security applications: a technological and status review. *Front Inform Technol Electron Eng*, 24(8):1117-1142. https://doi.org/10.1631/FITEE.2200314

Dietz K, 1988. The first epidemic model: a historical note on P.D. ENâĂŹKO. *Aust J Stat*, 30A(1):56-65. https://doi.org/10.1111/j.1467-842X.1988.tb00464.x

Epiphaniou G, Hammoudeh M, Yuan H, et al., 2023. Digital twins in cyber effects modelling of IoT/CPS points of low resilience. *Simul Model Pract Theory*, 125:102744. https://doi.org/10.1016/j.simpat.2023.102744

Fatima U, Ali M, Ahmed N, et al., 2018. Numerical modeling of susceptible latent breaking-out quarantine computer virus epidemic dynamics. *Heliyon*, 4(5):e00631. https://doi.org/10.1016/j.heliyon.2018.e00631

Gan CQ, Yang XF, Zhu QY, 2014. Global stability of a computer virus propagation model with two kinds of generic nonlinear probabilities. *Abstr Appl Anal*, 2014:735327. https://doi.org/10.1155/2014/735327

Hoang MT, Ngo TKQ, Tran DH, 2023. Dynamically consistent nonstandard numerical schemes for solving some computer virus and malware propagation models. *Math Found Comput*, 6(4):704-727. https://doi.org/10.3934/mfc.2022042

Husain R, Abubakar M, 2015. A study on friends model of a computer worm defense system. *Int J Eng Appl Sci*, 2(3):56-59.

Husain R, Suleiman B, 2015. Modeling and simulation of worm propagation and attacks against campus network. *Int J Eng Appl Sci*, 2(8):57-60.

Jackson M, Chen-Charpentier BM, 2017. Modeling plant virus propagation with delays. *J Comput Appl Math*, 309:611-621. https://doi.org/10.1016/j.cam.2016.04.024

Lanz A, Rogers D, Alford TL, 2019. An epidemic model of malware virus with quarantine. *J Adv Math Comput Sci*, 33(4):1-10. https://doi.org/10.9734/jamcs/2019/v33i430182

Liu J, Wang K, 2016. Hopf bifurcation of a delayed SIQR epidemic model with constant input and nonlinear incidence rate. *Adv Differ Equ*, 2016(1):168. https://doi.org/10.1186/s13662-016-0899-y

Nian FZ, Li JZ, Diao HY, et al., 2022. Weibo core user mining and propagation scale predicting. *Chaos Solitons Fractals*, 156:111869. https://doi.org/10.1016/j.chaos.2022.111869

Odule TJ, Kaka OA, 2018. Understanding and managing the dynamics of computer viruses. *Adv Multidiscip Sci Res J*, 4(1):113-120.

Ren JG, Xu YH, Zhang CM, 2013. Optimal control of a delay-varying computer virus propagation model. *Discrete Dyn Nat Soc*, 2013:210291. https://doi.org/10.1155/2013/210291

Tanaka G, Urabe C, Aihara K, 2014. Random and targeted interventions for epidemic control in metapopulation models. *Sci Rep*, 4:5522. https://doi.org/10.1038/srep05522

Wu QC, Chen SF, 2017. Susceptible-infected-recovered epidemics in random networks with population awareness. *Chaos*, 27(10):103107. https://doi.org/10.1063/1.4994893

Yang LX, Yang XF, 2017. The effect of network topology on the spread of computer viruses: a modelling study. *Int J Comput Math*, 94(8):1591-1608. https://doi.org/10.1080/00207160.2016.1226499

Yang LX, Draief M, Yang XF, 2016. The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model. *Phys A: Stat Mech Appl*, 450:403-415. https://doi.org/10.1016/j.physa.2016.01.026

Yang LX, Huang KF, Yang XF, et al., 2021. Defense against advanced persistent threat through data backup and recovery. *IEEE Trans Netw Sci Eng*, 8(3):2001-2013. https://doi.org/10.1109/TNSE.2020.3040247

Yang LX, Li PD, Yang XF, et al., 2021. Effective quarantine and recovery scheme against advanced persistent threat. *IEEE Trans Syst Man Cybern Syst*, 51(10):5977-5991. https://doi.org/10.1109/TSMC.2019.2956860

Yang XF, Yang LX, 2012. Towards the epidemiological modeling of computer viruses. *Discrete Dyn Nat Soc*, 2012:259671. https://doi.org/10.1155/2012/259671

Zhang CM, 2018. Global behavior of a computer virus propagation model on multilayer networks. *Secur Commun Netw*, 2018:2153195. https://doi.org/10.1155/2018/2153195

Zhang HF, Xie JR, Tang M, et al., 2014. Suppression of epidemic spreading in complex networks by local information based behavioral responses. *Chaos*, 24(4):043106. https://doi.org/10.1063/1.4896333

Zhang XL, Gan CQ, 2017. Optimal and nonlinear dynamic countermeasure under a node-level model with nonlinear infection rate. *Discrete Dyn Nat Soc*, 2017:2836865. https://doi.org/10.1155/2017/2836865

Zhang XL, Li Y, 2020. Modelling and analysis of propagation behavior of computer viruses with nonlinear countermeasure probability and infected removable storage media. *Discrete Dyn Nat Soc*, 2020:8814319. https://doi.org/10.1155/2020/8814319