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

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 Science and Artificial Intelligence, Lanzhou University of Technology, Lanzhou 730000, China*

[†]E-mail: gdnfz@lut.edu.cn

Received Mar. 29, 2024; Revision accepted Sept. 18, 2024; Crosschecked Aug. 5, 2025; Published online Sept. 5, 2025

Abstract: The diversity and complexity of the user population on the campus network increase the risk of computer virus infection during terminal information interactions. Therefore, it is crucial to explore how computer viruses propagate between terminals in such a network. In this study, we establish a novel computer virus spreading model based on the characteristics of the basic network structure and a classical epidemic-spreading dynamics model, adapted to real-world university scenarios. The proposed model contains six groups: susceptible, unisolated latent, isolated latent, infection, recovery, and crash. We analyze the proposed model's basic reproduction number and disease-free equilibrium point. Using real-world university terminal computer virus propagation data, a basic computer virus infection rate, a basic computer virus removal rate, and a security protection strategy deployment rate are proposed to define the conversion probability of each group and perceive each group's variation tendency. Furthermore, we analyze the spreading trend of computer viruses in the campus network in terms of the proposed computer virus spreading model. We propose specific measures to suppress the spread of computer viruses in terminals, ensuring 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:** TP309.5

1 Introduction

The campus network provides high-speed and efficient network connections for the school, supports a variety of network protocols and management strategies, and meets the different needs of its users. It also provides various network services to facilitate the administrative management and the use of faculty and students. Characterized by high bandwidth, wide coverage, intensive information interaction, and many users, the campus network has become an indispensable part of academic and campus life. However, due to these characteristics, computer viruses such as Trojan horses, malware, and worms spread quickly in the campus network, 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 facing the lateral spread of computer viruses, universities 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

‡ Corresponding author

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

ORCID: Fuzhong NIAN, https://orcid.org/0000-0002-2179-0895

© Zhejiang University Press 2025

(Yang LX et al., 2016, 2021b; Zhang XL and Gan, 2017; Lanz et al., 2019; Bahashwan and Al-Tuwairqi, 2021; Epiphaniou et al., 2023). Currently, most universities rely on only 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) developed a dynamic model with two kinds of generic nonlinear probabilities (incidence rate and vaccination probability), pointing out that the generic nonlinear vaccination helps strengthen 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 an SLBQS computer virus dynamics. Jackson and Chen-Charpentier (2017) constructed the SIR time-delay diffusion model. To further combat virus spread, Zhang XL and Li (2020) addressed a dynamic model that incorporates nonlinear countermeasure probability and infected removable storage media. 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 and Wang (2016) proposed an SIQR epidemic model with a nonlinear incidence rate and two time delays. They employed this model to analyze the local stability and the existence of Hopf bifurcation by combining the latent period delay and the recovery period delay as bifurcation parameters. 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, were developed and analyzed. Hoang et al. (2023) applied Mickens' methodology to formulate NSFD schemes for some epidemiological models describing the spread of computer viruses and malware, and demonstrated the advantages of NSFD. Additionally, Yang LX and Yang (2016) investigated the effect of network topology on virus spread 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 the basic network structure and the spreading dynamics model.

2 Spread dynamics modeling

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

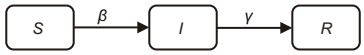

Fig. 1 SIR model group transitions. *S*: susceptible group; *I*: infection group; *R*: recovery group

Susceptible individuals become infected with an infection rate β, while infected individuals recover with a recovery rate γ. From these transition rules, the mean field equations of the SIR model are shown as follows:

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

where $S(t)$ represents the number of individuals in the susceptible group at time t, $I(t)$ represents the number of individuals in the infection group at time t, $R(t)$ represents the number of individuals in the recovery group at time t, and N_{T} represents the total number of individuals across the susceptible, infection, and recovery groups.

In this model, transitions between groups are simple and direct, but compared with the characteristics of computer virus spread in the campus network environment, it is not reasonable. To address the limitation, 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.

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: Due to the large number of users in the campus network, once a user is infected with a computer virus, it can spread quickly to others if no effective protective measures are taken.

2. Wide range: Users in the campus network are usually students from different colleges and majors, using a variety of devices. Once a computer virus is released, it can affect a large number of users.

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

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

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

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

2. Unisolated latent group (P_{c}): Personal terminals have been infected with computer viruses, but the user is yet unaware, 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 and open firewall).

3. Isolated latent group (P_{q}): Personal terminals have been infected with computer viruses, but the user is unaware, and the east-west direction of the terminal has been deployed in advance of the security protection strategy of the campus network user groups.

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

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

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

Among the six groups, some susceptible individuals will first transition into the unisolated latent group due to the failure to deploy security protection strategies in advance. Subsequently, a portion of the unisolated latent group will progress to the infection group due to the lack of network security awareness and other factors, and a portion of the unisolated latent group will transition into the isolated latent group due to the timely deployment of security protection strategies. However, the isolated latent group is not safe; for instance, the isolated latent group infected with zero-day or high-risk computer viruses may turn into the infection group. Finally, the infection group will progress to the recovery group if the anti-virus measures are successful; otherwise, the infection group will move to the crash group. The transitions of these six population classes are shown in Fig. 2, and α, β, γ, ξ, θ, and ρ are the transition probabilities between them, respectively. The mean field equation is obtained by

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

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

where N denotes the total number of nodes in the network, and the transition between groups in the network follows Eqs. (2) and (3).

Probability of S transitioning to P_{c}: The rate that susceptible group S transforms into unisolated latent group P_{c} is β, which is expressed as follows:

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

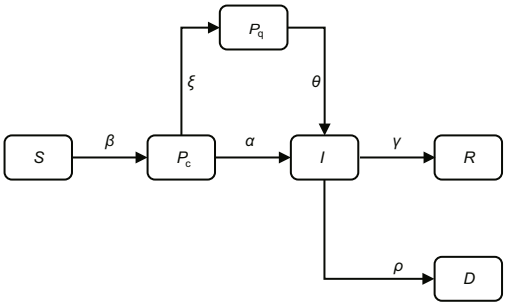

Fig. 2 Group transition of the computer virus spreading dynamics model in a campus network

where $\Pi(i)$ denotes the set of neighbor nodes of node i in the network, $G(i|j)$ represents the basic infection rate of the computer virus 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 infected node i to the total number of the neighbor nodes of node i, when node j belongs to the susceptible group.

Probability of P_c transitioning to P_q: The rate that the unisolated latent group P_c transforms into the isolated latent group P_q is denoted by ξ, expressed as follows:

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

where $U(i|j)$ denotes the rate that a security protection strategy has been implemented between nodes i and j. $C([x_j = P_c] \cup [x_i = S])/\mathrm{Len}(\Pi(i))$ represents the ratio of the number of susceptible node i to the total number of the neighbor nodes of node i, when node j belongs to the unisolated latent group.

Probability of P_q transitioning to I: The rate that the isolated latent group P_q transforms into the infection group I is θ, which is expressed as follows:

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

where $K(i|j)$ denotes the basic removal rate of the computer virus between nodes i and j. $C([x_j = P_q] \cup [x_i = S - P_c])/\mathrm{Len}(\Pi(i))$ represents the ratio of the number of susceptible node i (but not in the unisolated latent group) to the total number of the neighbor nodes of node i, when node j is in the isolated latent group.

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

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

where $C([x_j = P_c] \cup [x_i = S - P_q])/\mathrm{Len}(\Pi(i))$ denotes the ratio of the number of susceptible node i (but not in the isolated latent group) to the total number of neighbor nodes of node i, when node j belongs to the unisolated latent group.

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

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

where $C([x_j = I] \cup [x_i = S - P_c - P_q])/\mathrm{Len}(\Pi(i))$ denotes the ratio of the number of susceptible node i (but not in the isolated or unisolated latent group) to the total number of neighbor nodes of node i, when node j belongs to the infection group.

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

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

2.2 Stability analysis of the spread model

The stability of the disease-free equilibrium point in the spread model can be determined by calculating the basic reproduction number R_0. R_0 is a fundamental parameter that describes the spreading capability of computer viruses. It reflects the average number of new terminals infected by a single infected terminal without any external interference. If $R_0 > 1$, computer viruses may spread continuously because each infected terminal will infect more

than one new terminal. Conversely, if $R_0 < 1$, the spread of computer viruses will gradually decrease and may eventually disappear. In other words, the disease-free equilibrium point is locally asymptotically stable.

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

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} = (\alpha P_{\mathrm{c}}(t) + \theta P_{\mathrm{q}}(t)) * \Psi - (\gamma + \rho) * I(t), \tag{10}$$

where $\Psi = \sum \frac{kp(k)I}{\langle k \rangle}$ is the rate that the other end of an edge connected to a susceptible node points to an infection node, $\langle k \rangle$ denotes the average degree of network nodes, 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) evaluated at the disease-free equilibrium point $I = 0$ is presented in Eq. (11) at the bottom of this page.

The characteristic polynomial of matrix $\boldsymbol{J_0}$ is obtained by

$$||\boldsymbol{J_0} - \mu \boldsymbol{E}|| = \left(-(\gamma + \rho) - \mu + (\alpha + \theta) \frac{\sum_{k=1}^{n} k^2 p(k)}{\langle k \rangle} \right) \cdot (-(\gamma + \rho) - \mu)^{n-1}, \tag{12}$$

where $\boldsymbol{E}$ denotes the identity matrix. If the zero solution of Eq. (12) is locally asymptotically stable, then all eigenvalues μ of matrix $\boldsymbol{J_0}$ 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 expressed as

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

This also confirms the local asymptotic stability of the disease-free equilibrium point. Determining the basic reproduction number and proving the local asymptotic stability of the disease-free equilibrium point enhance the model's credibility.

3 Simulations

3.1 Simulation setting

To enhance the realism of the simulation results obtained from Eq. (2) when modeling the characteristics of the spread of computer viruses, it is necessary to focus on analyzing three key parameters governing virus transmission dynamics between nodes within the campus network. These parameters are the basic infection rate of the computer virus $G(i|j)$, the basic removal rate of the computer virus $K(i|j)$, and the security protection strategy deployment rate $U(i|j)$. Therefore, with the authorization of the university, we accessed its terminal security management system and downloaded a computer virus protection report from March 8 to October 19, 2023. The terminal security system did not produce a daily virus protection report every day over this period (particularly during the summer vacation), with a total of 140 report-generation days. The descriptive statistical analysis method was used to describe the statistical data characteristics in the report, and the final values of the three parameters were obtained as follows:

1. The basic infection rate of the computer virus $G(i|j)$: During the 140 d from March 8 to October 19, 2023, the terminal security management system recorded a total of 2703 terminal infections, with an average of 19 terminal infections per day. As of October 19, 2023, the total number of office terminals was 3915. Therefore, $G(i|j) = 19/3915 \approx 0.005$.

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

3. The security protection strategy deployment rate $U(i|j)$: As of October 19, 2023, there were 2507 faculty members in the university, each equipped

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

with one desktop and one laptop, resulting in a total of 5014 office terminals. Table 1 shows the security protection strategy deployment rate at the end of each month from March 8 to October 19, 2023. The office terminal count was obtained from the university's terminal safety management system. The security protection strategy deployment rate is defined as the ratio of the number of office terminals with installed terminal security management software to the total number of office terminals across the entire university. Therefore, $U(i|j) = (0.626 + 0.713 + 0.728 + 0.759 + 0.766 + 0.769 + 0.77 + 0.78 + 0.781)/9 \approx 0.744$.

Table 1 Statistical table of the security protection strategy deployment rate

Date	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

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

3.2 Simulation results

For $G(i|j) \approx 0.005$, $K(i|j) \approx 0.925$, and $U(i|j) \approx 0.744$, we derived $\beta \approx 0.296$, $\xi \approx 0.095$, $\alpha \approx 0.091$, $\theta \approx 0.049$, $\rho \approx 0.005$, and $\gamma \approx 0.200$. The simulation results of Eq. (2) are shown in Fig. 3. To verify the predictive capability and rationality of the proposed spread model through empirical testing, we intercepted the statistical data of the computer virus infection trend in the university's terminal security management system during 140 d (from March 8 to October 19, 2023), and compared the statistical data with the fitted trend of the infection group, as shown in Fig. 4.

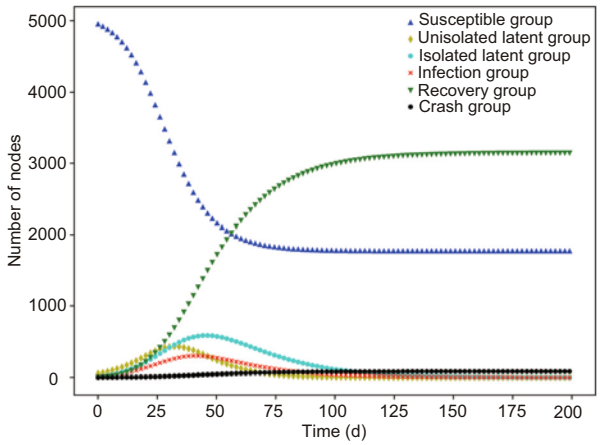

Fig. 3 Number of nodes varies with time when $G(i|j) \approx 0.005$, $K(i|j) \approx 0.925$, and $U(i|j) \approx 0.744$

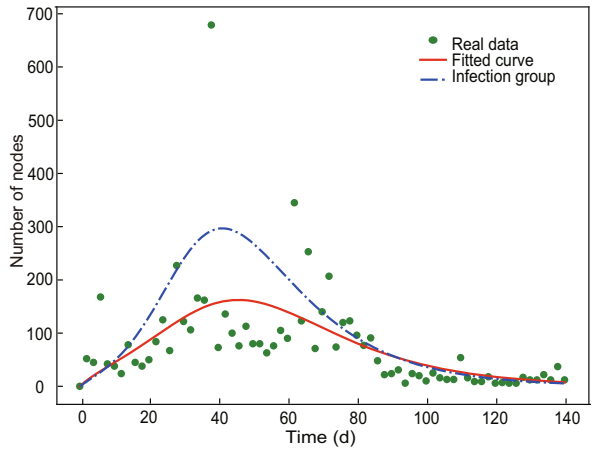

Fig. 4 Comparison of the fitted curve to real-world data and the trend of the infection group when $G(i|j) \approx 0.005$, $K(i|j) \approx 0.925$, and $U(i|j) \approx 0.744$. References to color refer to the online version of this figure

In Fig. 4, the green dots are the actual statistical data for the computer virus infection trend, the red solid line is the fitted curve of these real-world data, and the blue dashed line indicates the change curve of the infection group 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 fitted curve of the real-world statistical data is basically consistent with the change trend of the infection group shown in Fig. 3. This agreement demonstrates the predictive capability and rationality of the spread model, further

strengthening the credibility of the model.

3.2.1 Effect of $G(i|j)$ on the spread of computer viruses

Let $K(i|j)$ and $U(i|j)$ remain unchanged, and let $G(i|j)$ increase to 0.01, representing an increase in the basic infection rate of the computer virus. 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. Conversely, when the basic infection rate of the computer virus decreases, specifically when $G(i|j) = 0.001$, with $\beta \approx 0.190$, $\xi \approx 0.095$, $\alpha \approx 0.011$, $\theta \approx 0.005$, $\rho \approx 0.005$, and $\gamma \approx 0.200$, the corresponding simulation results of Eq. (2) are shown in Fig. 6.

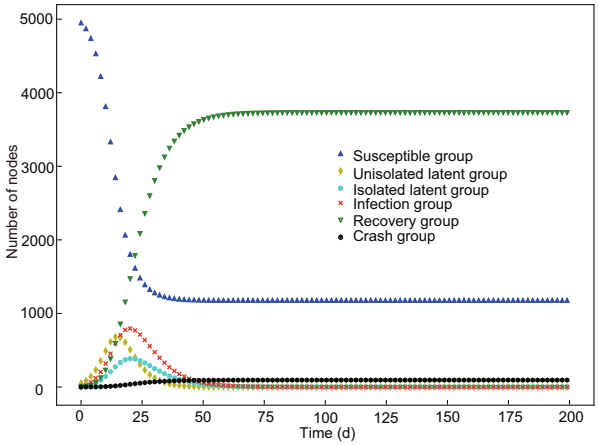

Fig. 5 Number of nodes varies with time when $G(i|j) = 0.01$

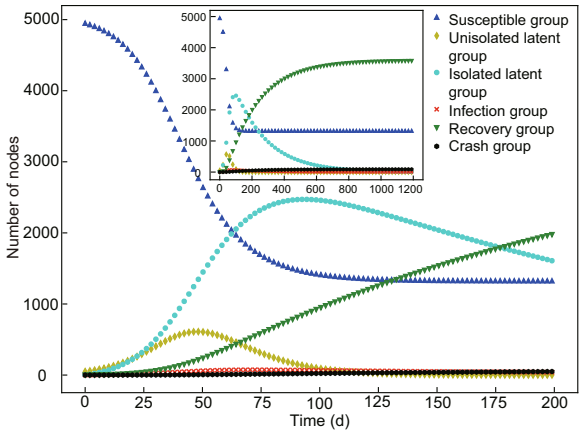

Fig. 6 Number of nodes varies with time when $G(i|j) = 0.001$

By comparing the change trends of the number of nodes in Figs. 3, 5, and 6, it can be observed that the risk of computer virus infection increases with $G(i|j)$. From day 0 to 20, the susceptible group declines at an accelerating rate, indicating a faster conversion from the susceptible group to the unisolated latent group. Subsequently, the unisolated latent group begins to partially transition into the isolated latent group, although this process occurs slowly. This suggests that isolating high-risk computer viruses is more difficult, thereby resulting in the number of nodes in the infection group reaching a peak.

Conversely, when $G(i|j)$ decreases, the infection risk diminishes, and the number of nodes in the susceptible group continues to decline until day 125. During this period, the sizes of the infection and crash groups increase hardly. From day 0 to 80, the isolated latent group steadily increases, indicating that low-risk computer viruses are easier to isolate. This is one of the reasons why the numbers of nodes in the infection and crash groups have not significantly increased. Fig. 7 illustrates the comparison of the change in the number of nodes in the infection group under different $G(i|j)$'s, showing more intuitively that with decreasing $G(i|j)$, the peak value of the infection group is lower and the trend of change is slower.

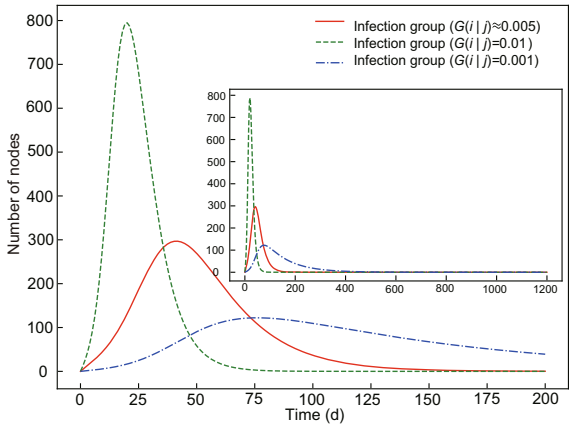

Fig. 7 Comparison of the number of nodes in the infection groups over time with different $G(i|j)$'s

3.2.2 Effect of $K(i|j)$ on the spread of computer viruses

Keeping $G(i|j)$ and $U(i|j)$ unchanged, when $K(i|j)$ 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 $\gamma \approx 0.394$, the simulation results of Eq. (2) are shown in Fig. 8.

When $K(i|j)$ is reduced to 0.875 with $\beta \approx 0.296$, $\xi \approx 0.095$, $\alpha \approx 0.091$, $\theta \approx 0.068$, $\rho \approx 0.008$, and $\gamma \approx 0.027$, the simulation results of Eq. (2) are shown in Fig. 9. By comparing the trends in the number of nodes in Figs. 3, 8, and 9, it can be observed that as $K(i|j)$ increases, the efficiency of removing computer viruses is higher, the trend of the infection group is gentler, and the number of nodes transitioning from the isolated latent group into the infection group decreases simultaneously. This indicates that an efficient virus removal method can quickly suppress the spread of computer viruses.

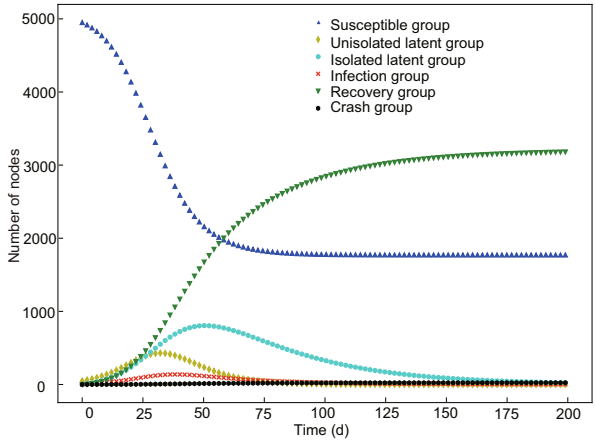

Fig. 8 Number of nodes varies with time when $K(i|j) = 0.975$

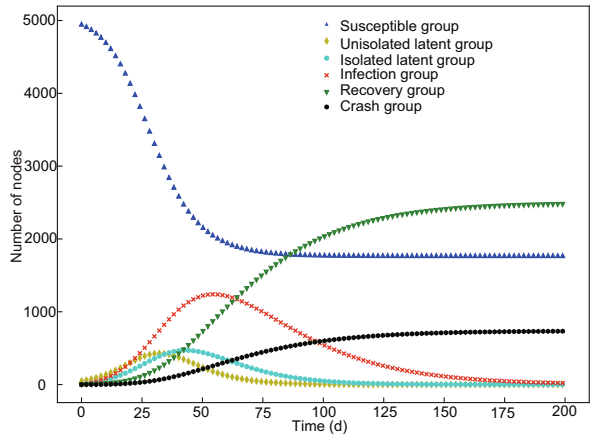

Fig. 9 Number of nodes varies with time when $K(i|j) = 0.875$

As $K(i|j)$ decreases, the efficiency of removing computer viruses is reduced. From day 25 to 50, the number of nodes in the infection group continues to increase due to an enhanced transition from the isolated latent group. Simultaneously, the number of nodes in the crash group begins to rise, indicating that as the computer virus removal rate decreases, the rate of infection nodes transitioning into crash nodes increases rapidly. Fig. 10 shows the comparison of the changes in the number of nodes in the infection group under different $K(i|j)$ values. When $K(i|j)$ decreases, the infection group reaches a higher peak value, exhibits a steeper upward trend, and takes longer to decline. The comparison of the change in the number of nodes in the crash group with different $K(i|j)$'s is shown in Fig. 11, indicating that the smaller the $K(i|j)$, the larger the number of nodes in the crash group.

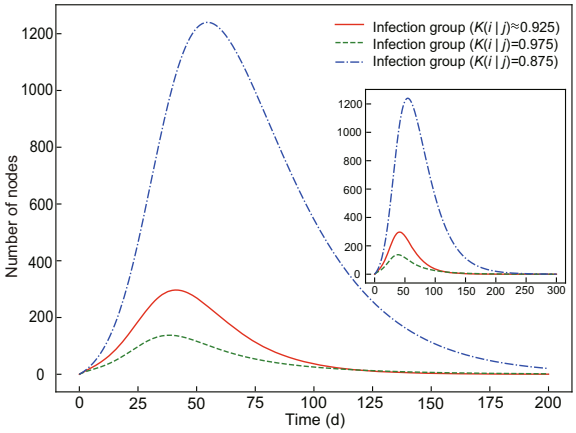

Fig. 10 Comparison of the number of nodes in the infection groups over time with different $K(i|j)$'s

3.2.3 Effect of $U(i|j)$ on the spread of computer viruses

Keeping $G(i|j)$ and $K(i|j)$ unchanged, when $U(i|j)$ 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 $\gamma \approx 0.200$, simulation results of Eq. (2) are illustrated in Fig. 12. When $U(i|j)$is reduced to 0.644 with $\beta \approx 0.296$, $\xi \approx 0.026$, $\alpha \approx 0.091$, $\theta \approx 0.049$, $\rho \approx 0.005$, and $\gamma \approx 0.200$, the simulation results of Eq. (2) are shown in Fig. 13. By comparing the trends in the number of nodes in Figs. 3, 12, and 13, it can be found that as $U(i|j)$ increases, the efficiency of deploying the security protection strategy increases. From day 0 to 25, the declining trend of the susceptible group is greatly slowed down, indicating that the speed and the number of susceptible nodes transitioning into unisolated latent nodes decrease, and the numbers of nodes in the infection and crash groups also decrease.

When $U(i|j)$ decreases, the deployment of the

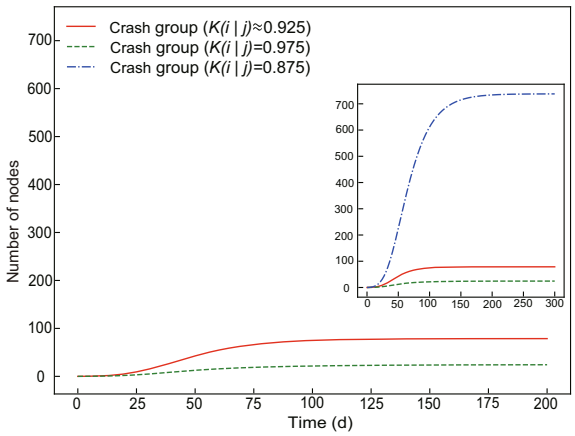

Fig. 11 Comparison of the number of nodes in the crash groups over time with different $K(i|j)$'s

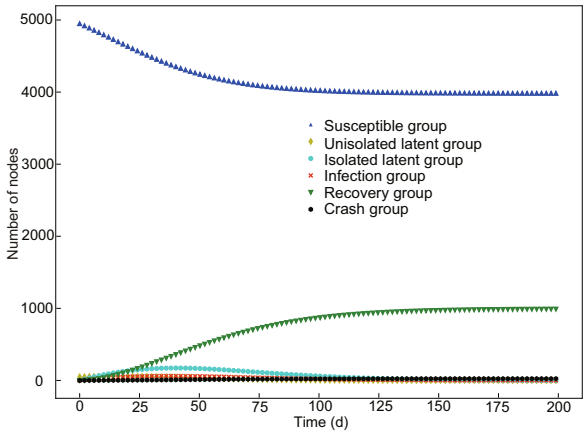

Fig. 12 Number of nodes varies with time when $U(i|j) = 0.844$

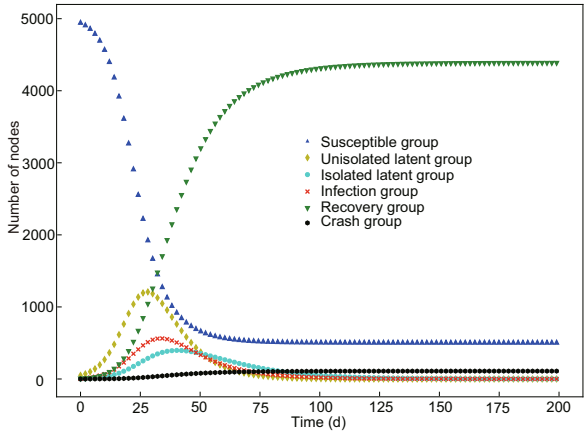

Fig. 13 Number of nodes varies with time when $U(i|j) = 0.644$

security protection strategy is reduced. The decline rate of the susceptible group and the growth rate of the unisolated latent group increase rapidly from the outset, indicating that the computer virus spreading accelerates from the beginning when terminals lack a security protection strategy. From day 30 to 100, the number of nodes in the infection group rises to its peak value and then begins to decline slowly, suggesting that as the security protection strategy deployment rate decreases, removing the computer virus becomes more difficult, as illustrated in Fig. 14.

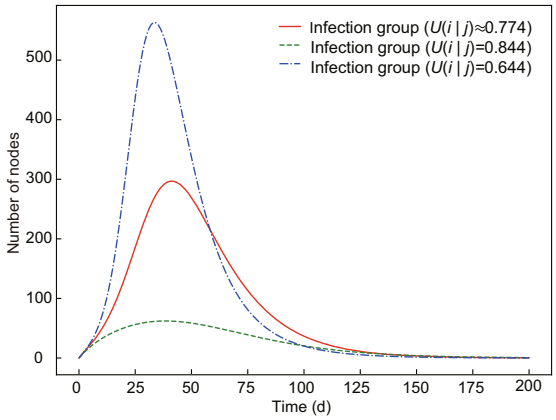

Fig. 14 Comparison of the number of nodes in the infection groups over time with different $U(i|j)$'s

3.3 Summary

The simulation results indicate that during the process of computer virus propagation, adjusting $G(i|j)$, $K(i|j)$, and $U(i|j)$ can effectively control the spread of computer viruses in the campus network. Specifically, when $G(i|j)$ is reduced, the rate β of the susceptible group transitioning into the unisolated latent group, the rate θ of the isolated latent group transitioning into the infection group, and the rate α of the unisolated latent group transitioning into the infection group all increase. For example, this can be achieved by maximizing the intercept of computer viruses by the network border security equipment and strengthening security protection for the east-west network traffic. By increasing $K(i|j)$, the rate θ of the isolated latent group transforming into the infection group and the rate ρ of the infection group transforming into the crash group are reduced, while the rate γ of the infection group transforming into the recovery group is increased. Measures for this include expanding the virus database of the terminal security management system and enhancing the virus removal capabilities. Increasing $U(i|j)$ raises the rate ξ of the unisolated latent group transitioning into the isolated latent group. For example, this

can be accomplished by popularizing the installation of terminal security management software as soon as possible and enhancing terminal anti-virus capabilities. These measures can effectively control the spread of computer viruses, achieving the goal of controlling the spread of computer viruses in the campus network.

4 Discussion

4.1 Limitations

The spread model proposed in this study is based on the propagation mechanism of computer viruses in a real university campus network environment, so its applicability is validated in the campus network and with the same type of local area network (LAN) structure. However, the robustness of the empirical test can be further enhanced because confirming the model's reliability with only one validation limits its applicability to specific influencing factors in larger and more complex scenarios. Furthermore, describing potential additional factors and how they can be integrated into the model remains one of the most important limitations of the current study.

4.2 Future work

To consolidate the reliability of the model, multiple validations should be conducted in future work. For example, real-world data collection could be extended to larger and more complex network environments, such as the metropolitan area network (MAN) and wide area network (WAN). Given the presence of numerous distinct LANs and diverse users in MAN and WAN, the fractal method could be employed to treat each LAN as a whole, analyzing specific problems based on this model. If simulation results closely match the real-world data, the reliability of the model would be further reinforced.

Furthermore, this study quantifies the basic infection rate, the basic removal rate, and the security protection strategy deployment rate using computer virus protection report data from a university's terminal security management system. However, these parameters could be influenced by several factors in a complex real network environment. The advancement of computer virus detection technology, the deployment of security software, and user behaviors can affect the basic removal rate of the computer virus. Policies and regulations from different administrative levels, organizational management, and user education and training can impact the security protection strategy deployment rate. Meanwhile, the virus's spreading capability, security vulnerabilities, and user security awareness can influence the basic computer virus infection rate. Therefore, it is essential to analyze the interactions among these factors, refine 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 constructs a transmission dynamics model including six groups: susceptible group, unisolated latent group, isolated latent group, infection group, recovery group, and crash group. We systematically analyze the mechanism of computer virus lateral transmission in a campus network using real computer virus protection data. The basic infection rate, the basic removal rate, and the security protection strategy deployment rate are proposed to quantitatively evaluate the risk of virus diffusion. Simulation results indicate that in campus network security protection, defenders can limit the spread of computer viruses by increasing the basic computer virus removal rate and security protection strategy deployment rate while reducing the basic computer virus infection rate.

Specifically, the basic infection rate can be reduced by regularly scanning and patching security vulnerabilities in campus network user terminals, or by training campus network users in network security awareness and skills to promote safer network usage. Additionally, establishing an east-west traffic firewall across the campus network along with effectively isolating office areas, teaching areas, and business areas, expanding the terminal security management system's virus library, and enhancing the system's real-time removal capability can increase the basic removal rate. The establishment of a comprehensive 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 minimize

the spread of computer viruses and reduce the risk of transmission.

Contributors

Kai GAO designed the research and drafted the paper. Lixin ZHANG processed the data. 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.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Alhebshi RM, Ahmed N, Baleanu D, et al., 2023. Modeling of computer virus propagation with fuzzy parameters. *Comput Mater Contin*, 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. EN'KO. *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*, 2016:168. 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 Solit Fract*, 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. *Discr Dynam 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, 2016. 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., 2021a. 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., 2021b. 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. *Discr Dynam 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. *Discr Dynam 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. *Discr Dynam Nat Soc*, 2020:8814319. https://doi.org/10.1155/2020/8814319