Niu, Wenfeng; Fan, Miaomiao

Article

Control and research of computer virus by multimedia technology

International journal of information systems and supply chain management

International Journal of Information Systems and Supply Chain Management
Volume 17 • Issue 1

Control and Research of Computer Virus by Multimedia Technology

Wenfeng Niu, Shanxi Professional College of Finance, China
Miaomiao Fan, Zibo Vocational Institute, China*

ABSTRACT

The rapid development of multimedia technology has brought great changes to people's lives and production. Computer viruses also spread widely through the network. In order to solve the above problems, this article intends to use multimedia technology to control computer viruses, and proposes a virus control method based on SICES model. According to the controlled SICES model and the set objective function, the influence of users' online behavior patterns on virus propagation can be explored, and an optimal control problem is proposed. Through theoretical analysis, the existence of optimal control is proved, and the optimal system is obtained. Numerical experiments show the effectiveness of the optimal control strategy. In addition, in order to optimize the objective function to make its value smaller, and to control the proportion of infected nodes at a lower level, users should choose the corresponding online behavior mode according to different network structures. For example, on the WS small world network, the network should be frequently disconnected or always kept online.

KEYWORDS

Multimedia technology, SICES virus control model, spread of computer virus

INTRODUCTION

In the 1960s, Von Neumann, who is regarded as the father of computers, put forward a theory in his book *The Computer and The Brain* that computer code would be able to reproduce—in essence, copy itself and damage other machines, just like a biological virus (Liu & Wang, 2021). So, the concept of computer viruses emerged with electronic computers themselves. The creation and spread of computer viruses are the inevitable result of the development of software technology.

Computer viruses are clearly defined in the Regulations of the People's Republic of China on the Security Protection of Computer Information Systems as "a group of computer instructions or program codes that are compiled or inserted into computer programs that damage computer functions or data, affect the use of computing, and can be self-copied." Globally, computer network viruses can be of two types: First, in a narrow sense, computer network viruses can only exist within computer networks, and the viruses only target networks. Secondly, in a broader sense, whether the virus is

DOI: 10.4018/IJISSCM.333896 *Corresponding Author

aimed at the network or the computer, if it can spread on the network and cause some damage at the same time, it can be called a computer network virus (Thimbleby et al., 1998).

With the continuous development of multimedia technology, many computer viruses spread through the network system and seriously threaten its functioning. These viruses are programs that can cause great damage to the computer system by causing harm such as deleting programs, destroying data, clearing system memory, or deleting important information in the operating system. When there are a large number of computer viruses circulating, especially viruses that are seriously destructive, they pose a great threat to individuals and enterprises. This is why it is very important to develop computer virus models to better understand the behavior of computer viruses and also to prevent and stop the spread of viruses (Bi et al., 2017).

A computer virus intrusion is considered to be a serious network security incident. The virus originates from the destructive computer's code. This kind of virus can obtain authority over the infected computer and use this to steal users information; these types of incidents have caused immeasurable losses to society (Liu et al., 2023). In recent years, with the popularity of the Internet and the Internet of Things, the destructive power of viruses is also increasing, and some viruses can even threaten people's lives. In order to effectively curb the spread of viruses and reduce economic and personal losses, people need to master the laws of virus transmission and control. Therefore, research on strategies to control computer virus transmission has great practical significance and commercial value (Zhu et al., 2023).

There are many kinds of computer viruses with different functions, all of which pose a great threat to national security and social property (Balthrop et al., 2004). Some computer viruses will damage computer software and hardware resources, some can tamper with data and mislead administrators, and others can invade the financial system and steal financial information. Some viruses can even be implanted into medical chips and become lethal weapons (Fatima et al., 2018).

According to the article, "China's Internet network security situation in the first half of 2019," released by the National Computer Network Emergency Technology Processing and Coordination Center, just in the first half of 2019, the number of hosts infected with computer viruses in China was about 2.4 million. Further, about 39,000 computer virus manufacturers located abroad controlled about 2.1 million hosts in China. In addition to these staggering numbers, the number of mobile Internet viruses is as high as 1.03 million, and the number of security vulnerabilities is 5,859 (Loch et al., 1992). Compared to the number of security incidents related to cloud platforms in 2018, the number has further intensified (Liu & Wang, 2021). Also, the security situation of networked industrial equipment, especially smart grid, is grim. According to a report by Ren & Xu (2017), up to 2017, medium and high-risk vulnerabilities have been found in six categories of power grid products from 28 manufacturers and in more than 70 models.

Some viruses are deployed for economic benefits, while others are for political and military purposes, such as the Stuxnet virus (Zarin et al., 2023). This virus was detected for the first time in June 2010, aiming at targeted attacks on infrastructure (energy) facilities, such as nuclear power plants, dams, and the national grid. In one case, this virus was used to attack Iran's uranium enrichment equipment, causing Iran's nuclear power plant to delay power generation. Incidents like these signify that viruses may be weapons of war in this new era. Another front in which computer viruses wage war in our time is in the field of information dissemination.

The idea of virus propagation system can be summarized as follows: first, the system lures the target to switch to the counterfeit network; that is, it captures the target with the counterfeit network (service provider), and then it "forces" the target to "involuntarily" make wrong operations to spread computer virus programs in the target (Özdemir et al., 2020).

Computer viruses are not independent executable programs, so they need to be parasitic in an executable program. Under normal circumstances, the life cycle of computer viruses needs to go through four different stages, namely: incubation, infection, trigger, and diffusion. Most computer virus programs are composed of the boot module, the destruction presentation module, and the infection

module. Infectivity is the most basic feature, which belongs to the virus regeneration mechanism. Most viruses spread wantonly through operating system files, application files, network information, and other channels. In general, computer viruses are effective weapons developed by individuals or organizations for economic, political, and military purposes to obtain certain benefits.

When it comes to computer viruses, we must think of network security, even national security. While actively studying virus prevention strategies, countries are also speeding up the development of powerful viruses. In essence, computer virus warfare is a struggle between people and between nations. In order to protect computers from viruses, people have developed countermeasures such as firewalls, intrusion detection systems, and anti-virus software and patches. In recent years, network science has become a popular new subject (She et al., 2009). As a hot research field of network science, computer virus propagation dynamics has also entered a period of rapid development. Its purpose is to explore the propagation law of computer viruses through dynamic system modeling and provide a basis for formulating countermeasures (Baleanu et al., 2023).

This paper posits the use of multimedia technology to control computer viruses, and it also proposes a virus control method based on the SICES model. Based on the controlled SICES model and the set objective function, it will explore the impact of online user behavior patterns on virus propagation and use this information to propose the optimal control problem. Through theoretical analysis, the existence of optimal control is proven and the optimal system is obtained.

MATERIALS AND METHODS

Computer virus propagation dynamics is a new discipline which aims to establish the corresponding dynamic system model, analyze the propagation law of the virus, and propose effective control strategies according to the special properties of particular computer viruses and the key factors affecting virus propagation. Since the birth of this field of research, several scholars have devoted themselves to the study of computer virus propagation models and they have made impressive progress.

Virus Propagation Models

Computer virus propagation models can be roughly divided into two types, depending on their time units. These two types are:

1. Discrete-time virus propagation model: The time unit of this type of model is discrete, and the nodes only change states at discrete time points. Therefore, this kind of model is more suitable for numerical simulation experiments that can roughly understand the propagation law of computer viruses and that have a certain scientific and guiding nature. However, the conclusions obtained from this kind of model are difficult to promote to the theoretical level.
2. Continuous-time virus propagation model: The time unit of this kind of model is continuous, and the node can change its state at any continuous time point (Tang & Wu, 2017). Therefore, this kind of model is more suitable for theoretical analysis. Through the qualitative analysis theory of the differential dynamic system, this kind of model can be theoretically analyzed and mathematically proved, and it can more accurately predict the propagation law of computer viruses. While this model is quite scientific and instructive, the conclusions obtained from this kind of model must pass the test of discrete numerical simulation experiments (Odeh & Abu Tal, 2023).

Since computer viruses pose a great threat to human lives and livelihoods, both academia and the industry have been increasing investments and research to try and curb their spread. Laypeople, too, can do their part to help in the battle against computer viruses. All computer users should improve their security awareness, avoid browsing suspicious websites, and update anti-virus software and

patches in a timely manner. Network security companies should improve their ability to check and kill viruses using anti-virus software, issue virus alerts in a timely manner, and develop new patches. Also, government departments must formulate more detailed laws and regulations governing the control and spread of viruses. While any kind of virus will eventually become less effective and die out, the struggle against new viruses has always existed.

The two main types of computer virus control strategies are node immunity and controllable variable adjustment. Let us look at each of these in some detail.

Node Immunity

Node Immunization is a concept in graph theory used to describe network management strategies for selecting nodes for protection or removal in a network. The goal of this strategy is to maximize the stability, robustness, and anti-interference ability of the network. In networks, node immunity is typically applied in the following scenarios:

1. Disease transmission model: Node immunity can be used to select key nodes to control or slow down the spread of diseases. By protecting or removing nodes with important connections and influence, the speed and scope of disease transmission in the network can be reduced.
2. Network attack defense: In the field of network security, node immunity can be used to select key nodes to improve network security. By protecting or removing vulnerable nodes, the risk of malicious attacks on the network can be reduced.
3. Information dissemination in social networks: Node immunity can also be applied to research on information dissemination in social networks. By selecting key nodes for information dissemination, the efficiency and scope of information dissemination can be effectively improved.

Antivirus software and patches are popular among users and are the most commonly used antivirus measures. Therefore, installing antivirus programs and patches on network devices is one of the most effective measures to curb the spread of computer viruses (Kumar et al., 2021).

Node immunization generally includes three types:

4. Directed random immunization scheme: The core idea of this scheme is to select some nodes randomly from the network to implement immunity. This immunization program is cost-effective and simple to implement, but the effect is not ideal.
5. Directed immunization scheme: This scheme, also known as the target immune scheme, selects some nodes from the network to implement immunity according to certain rules (Sumeyra, 2021). Some scholars have proved that the directed immune scheme is superior to the random immune scheme, and other scholars proposed a directed immune scheme based on a scale-free network.
6. Acquaintance immunization scheme: The core idea of the acquaintance immunization scheme is to immunize some nodes, and then the immunized nodes will immunize their neighbors (Ahmed et al., 2021). Some scholars have found the acquaintance immunization scheme to be better than the random immunization scheme, and its effect is similar to that of the directed/ target immunization. However, the acquaintance immunization scheme does not even need to understand the global information of the network, which makes it stronger than the target immunization strategy when this aspect is considered. The acquaintance immunization scheme draws on the idea of distribution, and it pushes research about immunization schemes to new heights.

Controllable Variable Adjustment

When establishing a computer virus propagation model, some variables can be set as controllable variables. It is also an important way to study computer virus control strategies to curb virus propagation by adjusting the value of controllable variables (Fatima et al., 2021). According to the

different modeling methods, the controllable variable adjustment can be roughly divided into the following two types:

1. Compartment level controllable variable adjustment: Here, the controllable variables of all nodes are controlled as a whole, so flexible changes cannot be made according to the actual state and safety needs of each node.
2. Node level controllable variable adjustment. Flexible changes can be made, according to the actual state and security requirements of different nodes, with good results. However, this adjustment has the problems of large calculation and high cost.

Virus Control Methods

Most computer viruses spread through the Internet. Usually, computer network viruses are in a state of attack, infection, and latency, which is very similar to the mode of transmission of biological viruses (Li et al., 2023). Therefore, in the process of exploring computer network viruses, we can also directly learn from the methods used to control biological viruses. Generally speaking, a computer network is a unity composed of multiple computers connected according to corresponding ways, and the characteristics and structures of these computer connections are similar (Ju et al., 2022). When a computer virus spreads in the network, it usually relies on a corresponding carrier, such as e-mail. In addition, the spread of computer viruses in the network must also rely on various means and conditions. Therefore, on an abstract level, the environmental conditions of propagation mainly include random structure and isomorphic mixing. In the computer network, because all nodes are close to other nodes, each node is very likely to be infected by other nodes, and the probability of infection is almost the same for all the nodes.

The continuous time virus propagation model mainly includes two parts: state variables and system parameters. Among them, some system parameters are controllable, and the spread of computer viruses can be restrained by adjusting these controllable parameters.

The state variable is used to describe the infection status or other related information of each node in the network in the continuous time virus propagation model. Specifically, in the virus propagation model, there are four common state variables. The infected state is used to indicate whether the node has been infected with a virus. It can usually be represented by binary variables, such as 1 for infection and 0 for non infection. Recovered state is used to indicate whether the node has recovered from the infection state. You can also use binary variable representation. Infection level is a variable used to indicate the infection degree of nodes. A real value can be used to indicate the degree or probability of infection. Other relevant information, according to the specific virus transmission model, may also have other state variables, such as the behavior characteristics of nodes, immune status, etc. These state variables describe the different states of nodes in the process of virus propagation and the corresponding attributes. By modeling and analyzing the state variables, we can better understand the virus propagation mechanism in the network, and design the corresponding control strategy.

System parameter adjustment strategies can be roughly divided into the following two types: static parameter adjustment and dynamic parameter adjustment (White, 1998). Static parameter adjustment is using optimization technology or algorithms to obtain parameter adjustment schemes under the condition of limited cost, so as to achieve more effective suppression of virus transmission. The biggest advantage of this strategy is that it requires less computation. The disadvantage is that once the parameter adjustment scheme is determined, it will not change, and it cannot adapt to the situation where the network state is constantly changing.

On the other hand, dynamic parameter adjustment is to regard controllable parameters as a function of time and use the relevant theory and methods of optimal control to obtain a parameter adjustment scheme. This will have the desirable effect of curbing virus transmission at a lower cost.

The advantage of this strategy is that it is suitable for situations where the network state is constantly changing, but its disadvantage is that the calculation amount is large (Shahid et al., 2021).

Research on the dynamic parameter adjustment of computer viruses has attracted the attention of scholars for the past six years. They have investigated a control strategy based on fully interconnected networks, a control strategy based on scale-free networks, and the control strategy based on arbitrary networks. Based on previous studies, this paper applies the SICES model to simulate and control and viruses, and it intends to find a suitable virus propagation control method to contribute to computer network security (Sung et al., 2014).

Some mainstream virus propagation models include the following:

- Considering that the nodes in the *R* compartment are only temporarily safe and may not have immunity to new viruses, Piqueira et al. proposed the SIRS (Susceptible Affected Recovered Susceptible) model on the basis of the SIR model (Yang & Wang, 2023).
- In order to focus on the impact of external nodes on virus transmission, Gan et al. regarded external nodes as a single class, introduced the *E* (external) warehouse, and proposed the SIES (Sustainable Affected External Usable) model.
- Considering the latency of viruses, Richard and Mark introduced the *E* (exposed) compartment where all nodes in the incubation period are considered as a class. This was based on the SIS model and proposed the SEIS (Susceptible Exposed Affected Susceptible) model.

RESULTS AND DISCUSSION

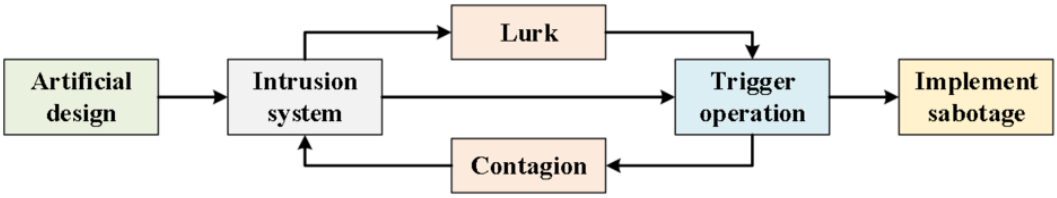
In this era of mobile Internet, various online social networks are popular, such as QQ, WeChat, microblog, Facebook, and X (formerly Twitter). While online social networks are deeply rooted in people's work and lives, they also provide a variety of shortcuts for the spread of new viruses. Due to the huge scale, privacy requirements, and time variability of online social networks, it is extremely difficult to clarify their structural laws. Therefore, it is very valuable to study the propagation of viruses on any network.

Network viruses may replicate themselves and cause problems like changing the executable components of application software or systems, deleting files, changing data, or refusing to provide services. In recent decades, the large-scale outbreak of computer viruses has caused huge economic losses to society. However, the development of patches to combat these viruses often lags behind the evolution of viruses. To solution to this problem requires a comprehensive understanding of the way viruses spread from a macro perspective and the formulation of effective preventive measures.

Figure 1 shows a computer virus propagation mechanism. When the system is running, the artificially designed virus enters the internal storage of the system through the virus carrier (that is, the external storage of the system), hides in the internal storage, and monitors the operation of the system from within the internal storage of the system. To save the virus infection module in the computer's memory, the virus boot module often modifies the entry address of the system interrupt vector. This makes the interrupt vector point to the virus program infection module. In this way, once the system performs disk read/write operations or system function calls, the virus infection module will be activated. After judging that the infection conditions are met, the infection module uses the system read/write disk interrupt to infect the virus itself to the read/write disk or loaded program—that is, to implement virus infection. Then, it transfers to the original interrupted service program to perform the original operation.

In the network, nodes are divided into online nodes and offline nodes. We usually pay attention to whether online nodes are infected by viruses. Even if we study the impact of offline nodes on online nodes, we only reflect the rate at which offline nodes access the network, and do not consider them as a single category. At the same time, we are not aware if the user's online behavior patterns—such as always online, always offline, or sometimes online and sometimes offline—will affect the spread

Figure 1. Computer virus propagation process



of the virus. Therefore, it is necessary to study external nodes (nodes that are not connected to the network for the time being) as a class. In order to focus on the impact of external nodes on virus transmission, some scholars treat external nodes as a single class, introduce a new reserve unit, and propose a SIES model based on fully interconnected networks.

This section fully considers the impact of countermeasures and external nodes on virus propagation on any network and proposes the SICES (Sustainable - Affected - Countermeasured - External – Sustainable) model. Based on this model, this paper regards the reaction rate as a function that changes with time, studies the optimal control strategy of the virus, and proposes the corresponding optimal control problem.

The new model marks the nodes in the network as $1,2,\cdots,N$, if the virus transmission network and the countermeasures distribution network are the same network, connected and fixed, and their adjacency matrix is $\mathbf{A}=[a_{ij}]_{N\times N}$, where $a_{ii}=0$. In the model applied in this paper, which is inspired by the SICS model and SIES model, network nodes can be roughly divided into internal and external nodes. Among them, internal nodes are divided into online vulnerable nodes, online poison nodes, and online security nodes. All nodes disconnected from the network are regarded as one kind, that is, external nodes. Among them, online vulnerable nodes are not infected, but do not have immunity to new viruses. After taking the latest countermeasures, they become online safe nodes. Online poisoned nodes can infect vulnerable nodes and become online safe nodes after taking the latest countermeasures. The online security node is not infected, and countermeasures are taken. After the countermeasures fail, it becomes an online vulnerable node. Also, the external node is a node temporarily disconnected from the network since external nodes are regarded as a single class, regardless of their state before network disconnection.

In this paper, vulnerable nodes, poisoned nodes, and secure nodes refer to online nodes. The above nodes correspond to fragile state, poisoned state, secure state, and offline state respectively, and their occurrence probability can be expressed as $S_i(t)$, $I_i(t)$, $C_i(t)$, and $E_i(t)$, respectively. The theoretical basis of the new model needs to be based on the following assumptions, and its schematic diagram is shown in Figure. 2:

1. First, every vulnerable node, poisoned node, and secure node on the line are offline at a constant positive rate.
2. Second, affected by the infected nodes, each vulnerable node *i* becomes an infected node at the rate $\beta\sum_j a_{ij}I_j(t)$ at time *t*, where β is a normal number.
3. Third, affected by countermeasures, each vulnerable node or poisoned node *i* becomes a safe node at the rate $\sum_j a_{ij}\gamma_j(t)C_j(t)$ at time *t*. $\gamma_j(t)\in L^2[0,T]$ is a controllable reaction rate, $\underline{\gamma}\le\gamma_j(t)\le\overline{\gamma}$, $0\le t\le T$, where $\underline{\gamma}$ and $\overline{\gamma}$ are constants, $0\le\underline{\gamma}<\overline{\gamma}\le 1$.
4. Fourth, since the system is reloaded, each infected node *i* becomes a vulnerable node at a constant positive rate.

5. Fifth, due to the failure of countermeasures, each secure node *i* becomes a vulnerable node at a constant positive rate.
6. Sixth, the control cost per unit time consumed by each infected node *i* at time *t* is $\frac{1}{2}\varepsilon\gamma_i^2(t)$, and $\varepsilon > 0$ is a trade-off factor based on the control effect and control cost. In order to explore the impact of the user's online behavior pattern on the spread of the virus, a more ideal assumption is made below.
7. Seventh, external nodes go online at a constant positive rate and become fragile nodes.

According to the full probability formula, let $\Delta t \to 0$, for $0 \le t \le T$, $1 \le i \le N$, and the node level SICES model of the non-autonomous differential dynamic system, that is, the controlled system, can be obtained.

$$\frac{dS_i(t)}{dt} = \alpha I_i(t) + \theta C_i(t) + \eta E_i(t) - \delta S_i(t) - S_i(t)\sum_j a_{ij}\left[\beta I_j(t) + \gamma_j(t)C_j(t)\right] \tag{1}$$

$$\frac{dI_i(t)}{dt} = -\alpha I_i(t) - \delta I_i(t) + \beta S_i(t)\sum_j a_{ij} I_j(t) - I_i(t)\sum_j a_{ij}\gamma_j(t)C_j(t) \tag{2}$$

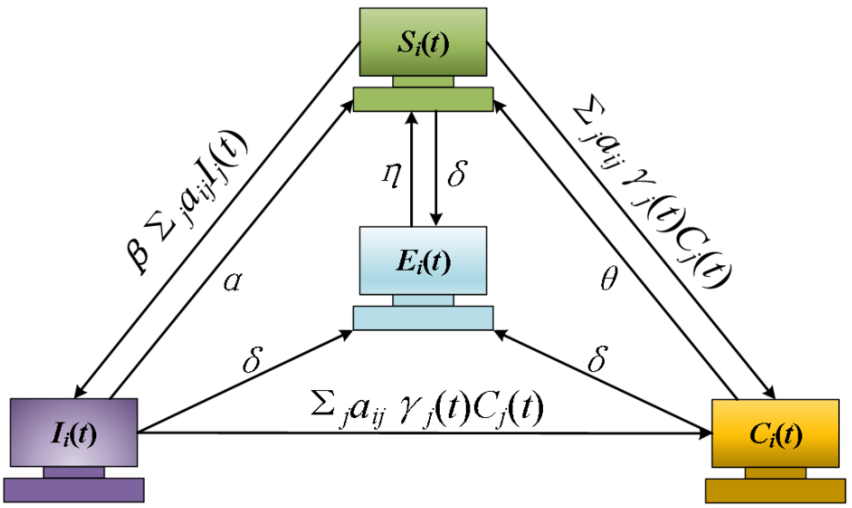
$$\frac{dC_i(t)}{dt} = -\theta C_i(t) - \delta C_i(t) + \left[S_i(t) + I_i(t)\right]\sum_j a_{ij}\gamma_j(t)C_j(t) \tag{3}$$

$$\frac{dE_i(t)}{dt} = \delta\left[S_i(t) + I_i(t) + C_i(t)\right] - \eta E_i(t) \tag{4}$$

Since $S_i(t) + I_i(t) + C_i(t) + E_i(t) \equiv 1$, for $0 \le t \le T$, $1 \le i \le N$, the above system can be reduced to the following non-autonomous differential dynamic system:

$$\frac{dI_i(t)}{dt} = -(\alpha + \delta)I_i(t) + \beta\left[1 - I_i(t) - C_i(t) - E_i(t)\right]\sum_j a_{ij} I_j(t) - I_i(t)\sum_j a_{ij}\gamma_j(t)C_j(t) \tag{5}$$

Figure 2. Schematic diagram of controlled SICES model assumptions



$$\frac{dC_i(t)}{dt} = -(\theta+\delta)C_i(t) + \left[1 - C_i(t) - E_i(t)\right]\sum_j a_{ij}\gamma_j(t)C_j(t) \tag{6}$$

$$\frac{dE_i(t)}{dt} = \delta - (\delta+\eta)E_i(t) \tag{7}$$

Wherein, the initial value of each variable belongs to the following positive invariant set:

$$\copyright = \left\{\left(I_1,\ldots,I_N,C_1,\ldots,C_N,E_1,\ldots,E_N\right) \in \mathbb{R}_+^{3N} : I_i + C_i + E_i \le 1, 1 \le i \le N\right\} \tag{8}$$

The control function $\mathbf{u} = \mathbf{u}(t) = (\gamma_1(t),\cdots,\gamma_N(t))$ can be regarded as the development and installation of the latest patches, anti-virus software, and other countermeasures. Its allowable control set is $U = \left\{\mathbf{u} \in (L^2[0,T])^N : \underline{\gamma} \le \gamma_j(t) \le \overline{\gamma}, 1 \le i \le N\right\}$, and then the optimal control problem is studied.

Let $\mathbf{x} = \mathbf{x}(t) = (\mathbf{I}(t),\mathbf{C}(t),\mathbf{E}(t)) = \left(I_1(t),\ldots,I_N(t),C_1(t),\ldots,C_N(t),E_1(t),\ldots,E_N(t)\right)$, then the above system can be expressed as:

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

As for the initial value $\mathbf{x}(0) \in \Omega$, the goal of establishing the model is to find an optimal control (function) ***u***, so that the proportion of poisoned nodes can be controlled at a low level at the lowest possible cost (the cost brought by countermeasures) within the time period $[0,T]$. In other words, the following optimal control problems need to be solved:

$$(\mathrm{P})\ \mathrm{Minimize}_{\mathbf{u}_{\mathbf{u}\in U}} J(\mathbf{u}) = \int_0^T L(\mathbf{x}(t),\mathbf{u}(t))dt \tag{10}$$

The problem is limited to the initial system or the target system. $J(\mathbf{u})$ is the objective function, also known as the performance index, $L(\mathbf{x},\mathbf{u}) = \sum_i \left(I_i + \frac{1}{2}\varepsilon\gamma_i^2\right)$ is the Lagrange function, and the Hamilton function corresponding to problem (P) is:

$$H(\mathbf{I},\mathbf{C},\mathbf{E},\mathbf{u},\lambda) = L(\mathbf{x},\mathbf{u}) + \sum_i \left(\lambda_{1i}\frac{dI_i}{dt} + \lambda_{2i}\frac{dC_i}{dt} + \lambda_{3i}\frac{dE_i}{dt}\right) \tag{11}$$

λ_{1i}, λ_{2i} and λ_{3i} $(1 \le i \le N)$ are undetermined adjoint functions. The core problem of this model is to solve the optimal system. This paper will give a necessary condition for optimal control, and then deduce the optimal system. Let $\mathbf{u}^*$ be an optimal solution of the optimal control problem (P) and $\mathbf{x}^*$ be the solution of the target system under condition $\mathbf{u} = \mathbf{u}^*$. There is an adjoint function such that:

$$\frac{d\lambda_{1i}^*(t)}{dt} = -1 - \beta\sum_j a_{ij}\lambda_{1j}^*(t)[1 - I_j^*(t) - C_j^*(t) - E_j^*(t)] + \lambda_{1j}^*(t)[\alpha + \delta + \sum_j a_{ij}(\beta I_j^*(t) + \gamma_j^*(t)C_j^*(t))] \tag{12}$$

$$\frac{d\lambda_{2i}^*(t)}{dt} = \beta\lambda_{1i}^*(t)\sum_j a_{ij}I_j^*(t) + \lambda_{2i}^*(t)\left[\delta + \theta + \sum_j a_{ij}\gamma_j^*(t)C_j^*(t)\right] + \gamma_i^*(t)\sum_j a_{ij}\left[\lambda_{1j}^*(t)I_j^*(t) - \lambda_{2j}^*(t)\left(1 - C_j^*(t) - E_j^*(t)\right)\right] \tag{13}$$

$$\frac{d\lambda_{3i}^*(t)}{dt} = \beta\lambda_{1i}^*(t)\sum_j a_{ij}I_j^*(t) + \lambda_{2i}^*(t)\sum_j a_{ij}\gamma_j^*(t)C_j^*(t) + (\delta + \eta)\lambda_{3i}^*(t) \tag{14}$$

Wherein the cross-sectional condition is $\lambda_{1i}^*(T) = \lambda_{2i}^*(T) = \lambda_{3i}^*(T) = 0$. In addition, for $0 \le t \le T$, $1 \le i \le N$, the optimal control function is:

$$\gamma_i^*(t) = \max\left\{\min\left\{\frac{C_i^*(t)}{\varepsilon}\sum_j a_{ij}\left[\lambda_{1j}^*(t)I_j^*(t) - \lambda_{2j}^*(t)\left(1 - C_j^*(t) - E_j^*(t)\right)\right], \bar{\gamma}\right\}, \underline{\gamma}\right\} \tag{15}$$

According to Pontryagin's principle, the following equation can be obtained by using λ_{1i}, λ_{2i} and λ_{3i}, $0 \le t \le T$, $1 \le i \le N$ and other conditions:

$$\frac{d\lambda_{1i}^*(t)}{dt} = -\frac{\partial H\left(\mathbf{I}^*(t), \mathbf{C}^*(t), \mathbf{E}^*(t), \mathbf{u}^*(t), \lambda^*(t)\right)}{\partial I_i} \tag{16}$$

$$\frac{d\lambda_{2i}^*(t)}{dt} = -\frac{\partial H\left(\mathbf{I}^*(t), \mathbf{C}^*(t), \mathbf{E}^*(t), \mathbf{u}^*(t), \lambda^*(t)\right)}{\partial C_i} \tag{17}$$

$$\frac{d\lambda_{3i}^*(t)}{dt} = -\frac{\partial H\left(\mathbf{I}^*(t), \mathbf{C}^*(t), \mathbf{E}^*(t), \mathbf{u}^*(t), \lambda^*(t)\right)}{\partial E_i} \tag{18}$$

The above target system can be obtained through calculation, and the following optimization conditions can be used to obtain the following verification conditions:

$$H\left(\mathbf{I}^*, \mathbf{C}^*, \mathbf{E}^*, \mathbf{u}^*, \lambda^*\right) = \min_{\mathbf{u}\in U} H\left(\mathbf{I}^*, \mathbf{C}^*, \mathbf{E}^*, \mathbf{u}, \lambda^*\right) \tag{19}$$

$$\frac{\partial H\left(\mathbf{I}^*(t), \mathbf{C}^*(t), \mathbf{E}^*(t), \mathbf{u}^*(t), \lambda^*(t)\right)}{\partial \gamma_i} = \varepsilon\gamma_i^*(t) - C_i^*(t)\sum_j a_{ij}\left[\lambda_{1j}^*(t)I_j^*(t) - \lambda_{2j}^*(t)\left(1 - C_j^*(t) - E_j^*(t)\right)\right] = 0 \tag{20}$$

To sum up, the optimality system of the problem (P) can be deduced, and the optimality system is the theoretical basis for finding the numerical solution of the optimal control.

ANALYSIS OF SIMULATION RESULTS

In this paper, the application effect of the above methods is tested through experiments, and the optimal solution can be obtained by using the forward and reverse Euler methods. The classic small world network, namely WS network, is selected as the virus propagation network, and the total number of nodes in this network is N=100.

Let the optimal system parameters set above be:

$\alpha = 0.005, \beta = 0.007, \delta = 0.01, \eta = 0.02, \theta = 0.01, \varepsilon = 1, \underline{\gamma} = 0, \overline{\gamma} = 0.15$, T=50.

First, the variables in the above method are defined:

$I_i(0) = 0.05, C_i(0) = 0.01, E_i(0) = 0.01, 1 \le i \le N$.

Let $\mathbf{u}^*(t)$ be the optimal solution of the target system and $\mathbf{x}^*(t)$ be the solution of the initial system. $\gamma^*(t)$ represents the average optimal control at time *t*, and $I^*(t)$ represents the proportion of infected nodes at time *t*. Figure 3 shows the $I^*(t)$ and $J(\mathbf{u})$ under different control strategies (static control strategy and optimal control strategy). It is easy to see from this figure that the optimal control strategy $\mathbf{u}^*$ can indeed minimize $J(\mathbf{u})$ and control $I^*(t)$ at a low level.

In this paper, the average optimal control and the proportion of infected nodes in the network at different times are gradually counted, and then an average optimal control $\gamma^*(t)$ of the target system and the proportion $I^*(t)$ of infected nodes under different control strategies are shown. The results are shown in Figure 4.

Subsequently, statistical analysis was carried out on the data, such as the network disconnection rate δ versus the average optimal control $\gamma^*(t)$, and the proportion of infected nodes $I^*(t)$. The results are shown in Figure 5.

It can be seen in Figure 5 that increasing δ will consume lower control costs and can obtain smaller performance indicators, which is also helpful to curb virus transmission. In addition, an interesting phenomenon was seen: When $\delta = 0$ is used, smaller performance indicators can also be

Figure 3. $I^*(t)$ and $J(\mathbf{u})$ under different control strategies

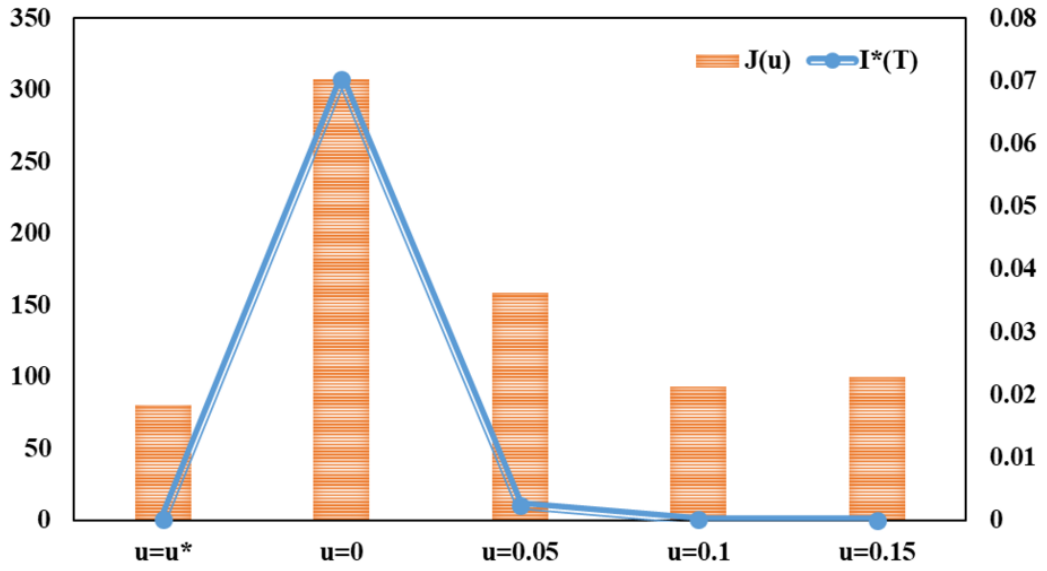


Figure 4. Change curve of $\gamma^*(t)$ at different times

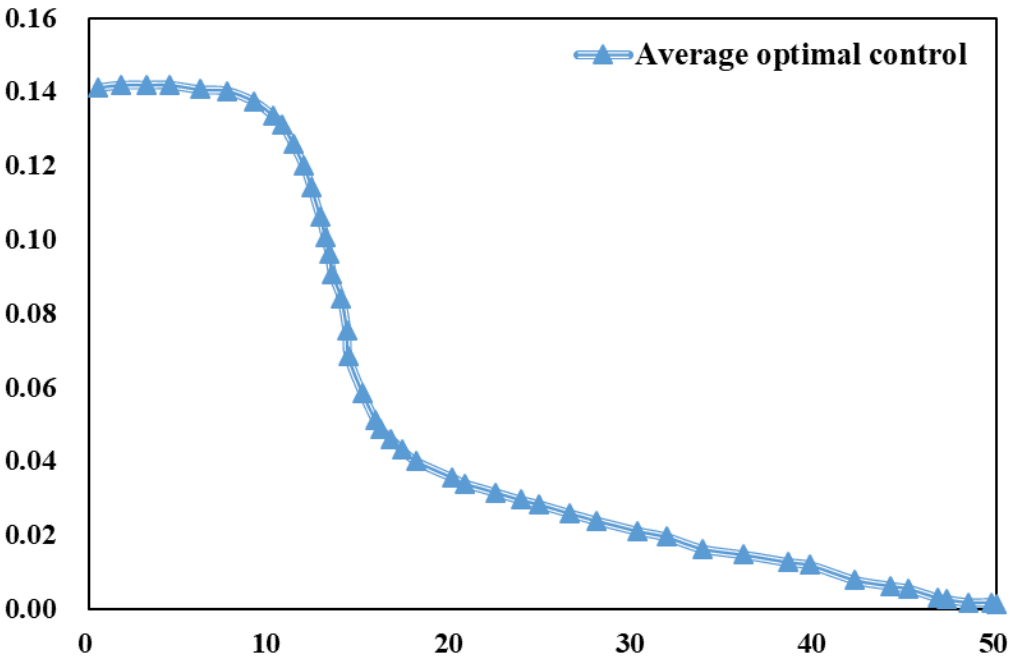
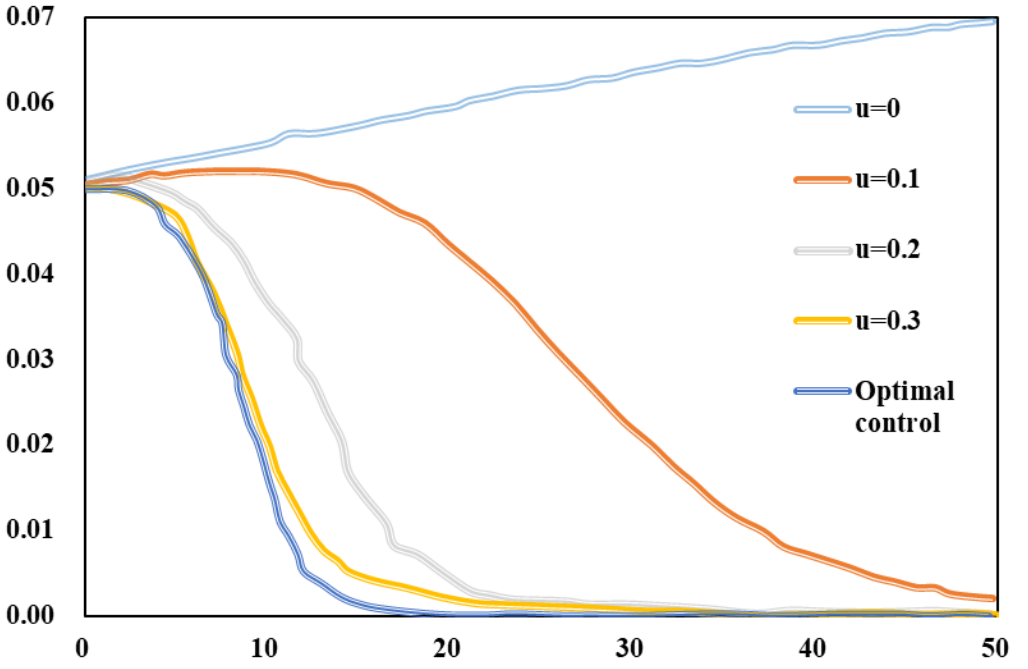


Figure 5. Variation curve of $I^*(t)$ under different times and conditions



obtained, and while the proportion of infected nodes can be controlled at a lower level, more control costs will be consumed.

It can be seen that in order to make the performance index as small as possible and control the proportion of infected nodes at a low level, when we use the network, we can adopt two behavior modes: either disconnect the network frequently or stay online all the time. From the final effect of control, both are effective. Since it is very possible to avoid computer virus attacks by disconnecting the network frequently, this mode does not make good use of countermeasures to combat virus attacks. So, this is a passive defense strategy that relies on luck. On the other hand, users who stay online all the time can receive security alerts, update patches, and install the latest anti-virus software in time, thus staying alert and responsive to computer virus attacks,; however, this will consume more control costs. Figure 6 and Figure 7 show the impact of disconnection rates on virus control.

As can be seen in Figure 6 and Figure 7, although the two modes have their own advantages in terms of the final effect and performance indicators of controlling virus transmission, the latter mode needs to consume more control costs. In real world situations, although we are increasingly dependent on the network, except for a small number of special important nodes that need to be online all the time, most ordinary nodes cannot be online all the time. Therefore, for general-purpose nodes, the former mode is more acceptable than the latter. Finally, the impact of the access rate of external nodes η on the final proportion $I^*(t)$ of infected nodes and the objective function (performance index) $J(\mathbf{u})$ is statistically analyzed. The results are shown in Figure 8.

It can be seen from Figure 8 that both $I^*(t)$ and $J(\mathbf{u})$ are decreasing with respect to η, which means that in order to obtain a smaller objective function and control the proportion of infected nodes at a lower level, external nodes should often connect to the Internet in order to update the latest patches and install the latest anti-virus software in time.

The series of results above leads us to make the following suggestions:

Figure 6 Change curve of $I^*(t)$ under different network disconnection rates

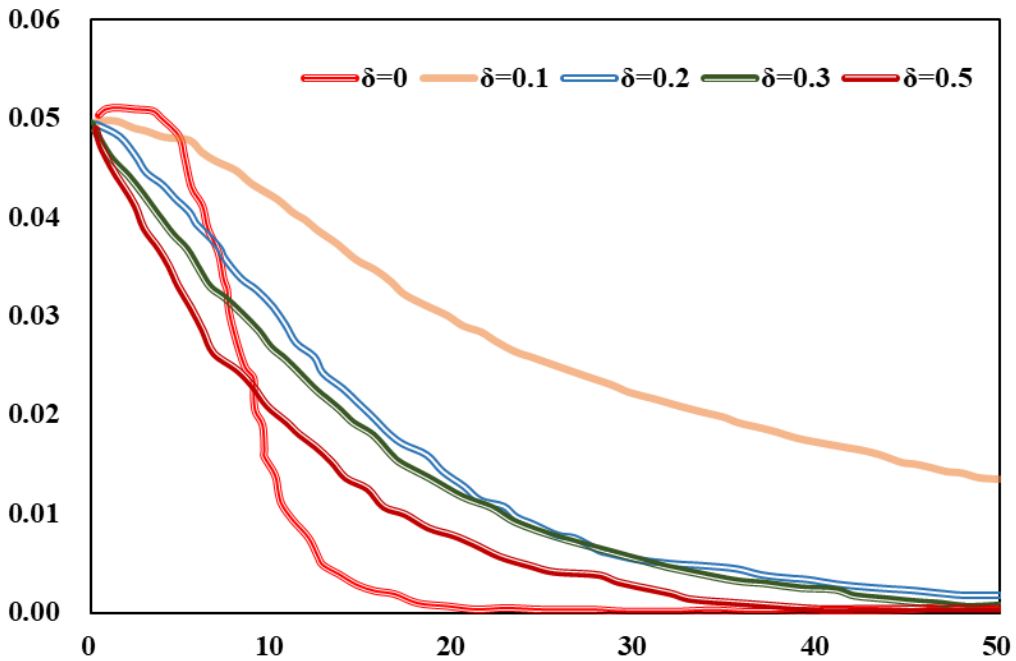


Figure 7 Change curve of $\gamma^*(t)$ under different network disconnection rates

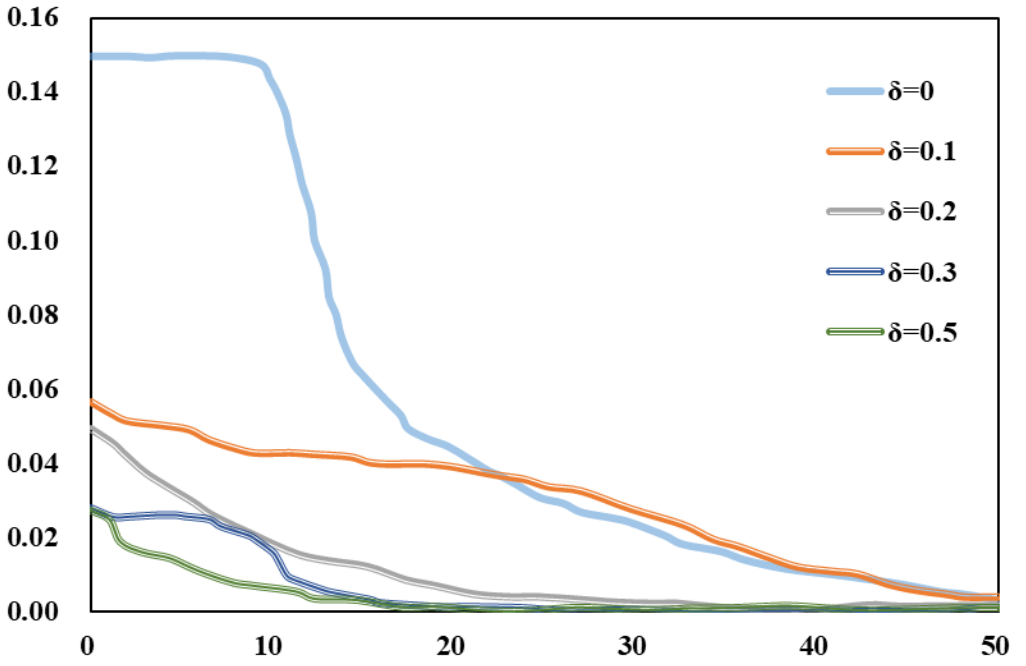
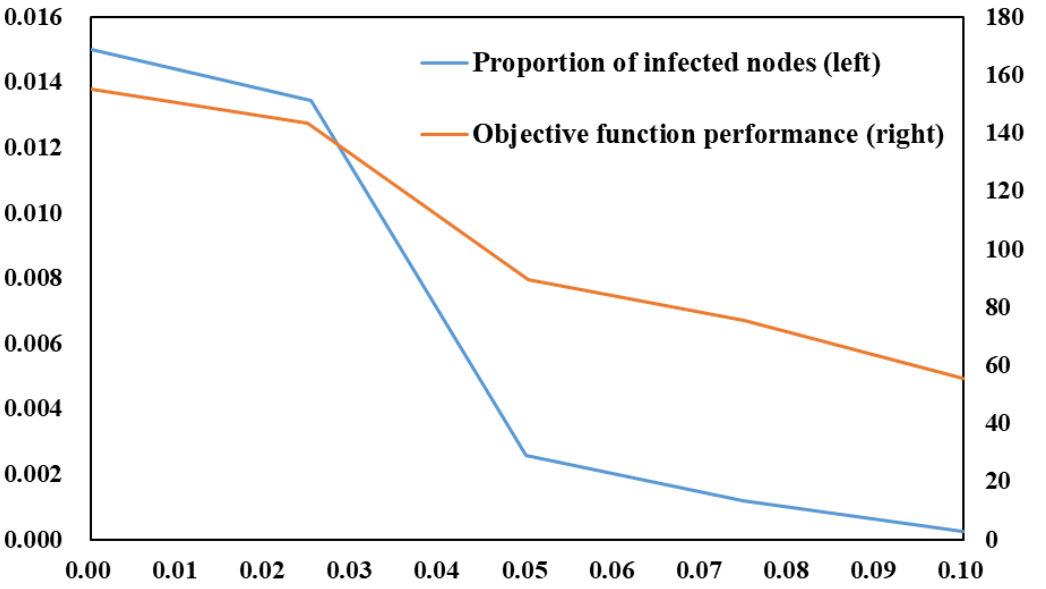


Figure 8 Comparison of $I^*(t)$ and $J(\mathbf{u})$ changes under different access network rates



- When we use computers, tablets, smartphones, and other electronic devices, it is better to temporarily disconnect them from the network when the network is not needed.
- When necessary, we can reconnect to the network, but we should not always remain online.

To sum up, the main experimental results of this section are as follows:

1. The optimal control strategy u* can indeed minimize the objective function $J(\mathbf{u})$ and control the final proportion $I^*(t)$ of the poisoned nodes at a lower level.
2. In order to optimize the objective function to make its value smaller and control the proportion of infected nodes at a lower level, users should choose the corresponding online behavior mode according to different network structures. For example, on the WS small world network, the network should be frequently disconnected or always online.

CONCLUSION

This paper proposes an optimal control problem according to the controlled SICES model and the set objective function in order to achieve the following objectives: to make the countermeasures flexibly applicable to any network; to suppress virus propagation as effectively as possible at a lower cost; and to explore the impact of users' online behavior patterns on virus propagation.

Through theoretical analysis, the existence of optimal control is proved, and the optimal system is obtained. Numerical experiments show the effectiveness of the optimal control strategy. In addition, we come to the conclusion that in order to optimize the objective function to make its value smaller and control the proportion of infected nodes at a lower level, users should choose corresponding online behavior modes according to different network structures. On the WS small world network, users should frequently disconnect from the network or always stay online.

Based on previous research, this paper studies the propagation law and optimal control strategy of computer viruses and has made some achievements in these areas. However, this paper only studies the optimal control strategy of the virus on any network and does not make a theoretical study of the dynamic behavior of virus propagation. This will be tackled in follow-up work.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest to disclose.

FUNDING STATEMENT

This work was not supported by funds from any organization.

ACKNOWLEDGEMENTS

The authors would like to thank those researchers whose techniques have contributed to this research.

REFERENCES

Ahmed, N., Fatima, U., Iqbal, S., Raza, A., Rafiq, M., Aziz-ur-Rehman, M., Saeed, S., Khan, H., & Nisar, K. S. (2021). Spatio-temporal dynamics and structure preserving algorithm for computer virus model. *CMC-Computers. Computers, Materials & Continua*, *68*(1), 201–211. doi:10.32604/cmc.2021.014171

Baleanu, D., Raja, M. A. Z., Alshomrani, A. S., & Hincal, E. (2023). Meyer wavelet neural networks procedures to investigate the numerical performances of the computer virus spread with kill signals. *Fractals*, *31*(02), 2340025. doi:10.1142/S0218348X2340025X

Balthrop, J., Forrest, S., Newman, M. E., & Williamson, M. M. (2004). Technological networks and the spread of computer viruses. *Science*, *304*(5670), 527–529. doi:10.1126/science.1095845 PMID:15105484

Bi, J., Yang, X., Wu, Y., Xiong, Q., Wen, J., & Tang, Y. Y. (2017). On the optimal dynamic control strategy of disruptive computer virus. *Discrete Dynamics in Nature and Society*, *2017*, 1–14. doi:10.1155/2017/8390784

Fatima, U., Ali, M., Ahmed, N., & Rafiq, M. (2018). Numerical modeling of susceptible latent breaking-out quarantine computer virus epidemic dynamics. *Heliyon*, *4*(5), e00631. doi:10.1016/j.heliyon.2018.e00631 PMID:29872764

Fatima, U., Baleanu, D., Ahmed, N., Azam, S., Raza, A., Rafiq, M., & Rehman, M. A. U. (2021). Numerical study of computer virus reaction diffusion epidemic model. *Computers, Materials & Continua*, *66*(3), 3184–3192. doi:10.32604/cmc.2021.012666

Ju, H., Wang, J., Zhu, E., Zhang, X., & Zheng, F. (2022). Design scheme of a docker container file isolation against computer virus spreading. *Mathematical Problems in Engineering*, *2022*, 1–6. Advance online publication. doi:10.1155/2022/5348370

Kumar, P., Erturk, V. S., & Kumar, A. (2021). A new technique to solve generalized Caputo type fractional differential equations with the example of computer virus model. *Journal of Mathematical Extension*, *15*. Advance online publication. doi:10.30495/JME.SI.2021.2052

Li, Y., Ji, W., Weng, J., Wu, X., Shen, X., & Sun, Y. (2023). Virus propagation model and stability analysis of heterogeneous backup network. *Jisuanji Yingyong*, *43*(4), 1176. doi:10.11772/j.issn.1001-9081.2022030409

Liu, H., & Wang, D. (2021). Research on the application of data mining technology in computer network virus defense. *Journal of Physics: Conference Series*, *1992*(2), 022095. doi:10.1088/1742-6596/1992/2/022095

Liu, Y., Zhang, P., Shi, L., & Gong, J. (2023). A Survey of Information Dissemination Model, Datasets, and Insight. *Mathematics*, *11*(17), 3707. doi:10.3390/math11173707

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *Management Information Systems Quarterly*, *16*(2), 173–186. doi:10.2307/249574

Odeh, A., & Abu Taleb, A. (2023). Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection. *Applied Sciences (Basel, Switzerland)*, *13*(21), 11985. doi:10.3390/app132111985

Özdemir, N., Uçar, S., & Billur İskender Eroğlu, B. (2020). Dynamical analysis of fractional order model for computer virus propagation with kill signals. *International Journal of Nonlinear Sciences and Numerical Simulation*, *21*(3-4), 239–247. doi:10.1515/ijnsns-2019-0063

Ren, J., & Xu, Y. (2017). A compartmental model for computer virus propagation with kill signals. *Physica A*, *486*, 446–454. doi:10.1016/j.physa.2017.05.038

Shahid, N., Rehman, M. A. U., Khalid, A., Fatima, U., Shaikh, T. S., Ahmed, N., Alotaibi, H., Ragig, M., Khan, I., & Nisar, K. S. (2021). Mathematical analysis and numerical investigation of advection-reaction-diffusion computer virus model. *Results in Physics*, *26*, 104294. doi:10.1016/j.rinp.2021.104294

She, J. H., Wang, H., Chen, L., & Chen, S. (2009). Improvement of redundancy principle for multimedia technical foreign-language learning. *International Journal of Computer Applications in Technology*, *34*(4), 264–269. doi:10.1504/IJCAT.2009.024078

Sumeyra, U. C. A. R. (2021). Existence results for a computer virus spreading model with Atangana-Baleanu Derivative. *Celal Bayar University Journal of Science*, *17*(1), 67–72. doi:10.18466/cbayarfbe.716573

Sung, P. C., Ku, C. Y., & Su, C. Y. (2014). Understanding the propagation dynamics of multipartite computer virus. *Industrial Management & Data Systems*, *114*(1), 86–106. doi:10.1108/IMDS-04-2013-0197

Tang, C., & Wu, Y. (2017). Global exponential stability of nonresident computer virus models. *Nonlinear Analysis Real World Applications*, *34*, 149–158. doi:10.1016/j.nonrwa.2016.08.003

Thimbleby, H., Anderson, S., & Cairns, P. (1998). A framework for modelling trojans and computer virus infection. *The Computer Journal*, *41*(7), 444–458. doi:10.1093/comjnl/41.7.444

Wang, Z., Nie, X., & Liao, M. (2021). Stability analysis of a fractional-order SEIR-KS computer virus-spreading model with two delays. *Journal of Mathematics*, *2021*, 1–15. doi:10.1155/2021/6144953

Zarin, R., Khaliq, H., Khan, A., Ahmed, I., & Humphries, U. W. (2023). A numerical study based on haar wavelet collocation methods of fractional-order antidotal computer virus model. *Symmetry*, *15*(3), 621. doi:10.3390/sym15030621

Zhu, Q., Loke, S. W., & Zhang, Y. (2018). State-based switching for optimal control of computer virus propagation with external device blocking. *Security and Communication Networks, 2018,* 1-10. Yang, S., & Wang, X. (2023). Analysis of Computer Network Security and Prevention Technology. *Journal of Electronics and Information Science*, *8*(2), 20–24. doi:10.23977/jeis.2023.080204

Zhu, Q., Zhang, G., Luo, X., & Gan, C. (2023). An industrial virus propagation model based on SCADA system. *Information Sciences*, *630*, 546–566. doi:10.1016/j.ins.2022.12.119

Miaomiao Fan is a professor of Zibo Vocational Institute.