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