Hindawi
International Journal of Intelligent Systems
Volume 2024, Article ID 3943882, 16 pages
https://doi.org/10.1155/2024/3943882

Research Article

Dynamics and Control Strategies for SLBRS Model of Computer Viruses Based on Complex Networks

Wei Tang, [1,2,3] **Hui Yang**, [2,3] **and Jinxiu Pi**[2,3]

[1]*School of Information Engineering, Guizhou Open University, Guiyang, Guizhou 550023, China*
[2]*School of Mathematics and Statistics, Guizhou University, Guiyang, Guizhou 550025, China*
[3]*Guizhou Provincial Key Laboratory for Games Decision-Making and Control Systems, Guiyang, Guizhou 550025, China*

Correspondence should be addressed to Hui Yang; huiyang@gzu.edu.cn

Received 27 March 2023; Revised 3 March 2024; Accepted 17 April 2024; Published 14 May 2024

Academic Editor: Alexander Hošovský

The proliferation of computer viruses has escalated in recent years, posing threats not only to individuals' safety and property but also to societal well-being. Consequently, effectively curtailing virus spread has become an urgent imperative. To address this issue, our paper introduces a new virus propagation model and associated control strategy. First, diverging from conventional approaches in network virus literature, we propose a susceptible-latent-breaking-out-recovered-susceptible (SLBRS) virus propagation model tailored to the topological characteristics of scale-free networks, thus comprehensively incorporating network structure's impact on virus propagation. Second, we analyze the model's foundational properties, derive the basic reproduction number, and demonstrate the existence and global asymptotic stability of disease-free equilibrium. Finally, leveraging global stability of the model at the disease-free equilibrium, we integrate the target immunization strategy (TIS) and the acquaintance immunization strategy (AIS) to devise an optimal control strategy. The paper's findings offer fresh insights into disease-free equilibrium existence and stability, furnishing a more dependable approach to curbing network virus dissemination. The simulation results demonstrate the persistent presence of network viruses in the absence of control measures and the instability of the disease-free equilibrium. However, effective control is achieved after implementing immunization measures.

1. Introduction

Human and many biological populations have been facing the threat of viral epidemics. The spread of epidemics usually causes large numbers of deaths and significant economic losses. In particular, the novel coronavirus pneumonia (COVID-19) has rapidly disseminated across numerous countries and regions worldwide due to its high contagiousness [1]. The new "COVID-19" outbreak in 2019, in the current, its global impact is still very severe [2, 3]. Similar to the spread of biological virus, the spread of computer virus plays a vital role in the development and stability of human society [4]. Well-known computer viruses, including the Stuxnet virus (2010) [5], Wannacry (2017) [6], and Phishing e-mail (2020) [7], have caused billions of dollars in economic losses to many countries and regions around the world. Nowadays, hackers use computer viruses to illegally collect a large amount of private data and hijack the use rights of computers, making the virus spread quickly in cyberspace and difficult to control [8]. For example, ransomware wannacry (2017) [6] is a software virus that hijacks user data, spreads via the web or e-mail, replicates itself and spreads quickly. Ransomware wannacry locks down systems in a way that cannot be reversed by knowledgeable people, and its victims are mostly industry organizations and large corporations. Once infected, users have to pay a ransom to decrypt it, which causes instability of computer data. Although much has been done to prevent the spread of computer viruses, the human fight against viruses is still in its infancy [9, 10]. Due to the intricate nature of computer networks, the investigation of computer virus models and their corresponding control strategies has emerged as a focal point in contemporary research, concurrently bearing significance in the realm of biological virus prevention and control.

1.1. Related Works. Over the past few decades, numerous scholars have endeavored to explore the impact of complex network structures on virus propagation models, aiming to formulate a virus transmission model that aligns with real-world conditions [11, 12]. In terms of network structure, models s like regular networks, small-world networks [13], and scale-free networks [14] provide some new directions for the study of infectious diseases. For virus transmission models on different network structures, Kleczkowski and Grenfell [15] and Moore and Newman [16] established different infectious disease models on the small-world networks and provided the critical threshold of infectious disease. Subsequently, Pastor-Satorras, and Vespignani introduced the earliest infectious disease models like the susceptible-infected-recovered (SIR), susceptible-infected-recovered-susceptible (SIRS), and susceptible-exposed-infected-recovered (SEIR) models on scale-free networks [17, 18]. Inspired by these researches, Liu and Zhang [19] investigated the transmission threshold and stability of the SEIRS model based on the research nodes of Olinky and Stone [20] and Joo and Lebowitz [21], and they have obtained many valuable conclusions. To quantitatively assess the security of virus systems, Tang et al. [26] employs safety entropy to analyze the security situation of the susceptible-latent-break-out-recovered-susceptible (SLBRS) model based on the work of Yang et al. [22] and Zhang and Yang [23]. Take some novel modeling methods for example, Naik [24] and Ahmad et al. [25] delved into a fractional-order SIR epidemic model incorporating memory, conducting modeling and numerical research on bovine babesiosis disease. Very recently, Sun, Ghori, and del Rey built different virus models to analyze the key problems such as periodic infection rate [27], global dynamics and bifurcation analysis [28], and mutation transmission [29]. However, these models overlook the influence of virus spread within complex network structures, particularly the dynamics of computer virus propagation in scale-free networks, which brings an opportunity to our work.

In addition to exploring the various modes of virus propagation on complex networks, it is imperative to consider effective control strategies for mitigating the spread of network viruses. Regarding the control strategy for virus models, Pastor-Satorras and Vespignani [30] provided an idea and theoretical framework for virus control on complex networks. Bai et al. [31] compared the differences in control effect between random immunity and target immunity. As research progressed, people began to discuss the role of network structure and infectivity in virus control, Masuda [32], Zhang and Fu [33], Wu et al. [34], and Buono and Braunstein [35] discussed the relationship between network immunity and network structure, and these studies provide more perspectives and ideas for network virus immunization. To improve the effectiveness of immune control, Yang et al. [36] proposed optimal dynamic immunization of controllable heterogeneous nodes under the SIRS model, Cao et al. [37] compared the control effects of the Susceptible-Infectious-Carriers-Recovered (SICR) model across various immunization strategies by examining the stability of the viral system dynamics, and Xia et al. [41] proposed an improved target immunization strategy based on two rounds of selection. Additionally, to combat malicious attacks in the Internet of Things and sensor networks, numerous effective control methods integrate machine learning theory [38], knowledge-driven [39], and data-driven methods [40], resulting in significant control efficacy. Compared with the control effect of the biological virus COVID-19, Li and Guo [42] analyzed the optimal control and effectiveness of the novel COVID-19 model of the Omicron strain. Guo and Li [43] conducted fractional-order modeling and optimal control of a new online game addiction model based on real data. The above work has a good enlightening significance for us to carry out the control of network viruses.

Although computer viruses and biological viruses have great differences in the way of transmission and influence, the control of the two kinds of viruses has many similar rules [44, 45]. For example, the control of the new corona virus mainly adopts the idea of isolation control and acquaintance immunization. This method focuses on the key populations in the infected population to effectively control the spread of the virus. For scale-free computer networks, the network structure not only affects virus propagation but also plays a key role in virus control. Therefore, how to design an effective control strategy based on the virus propagation dynamics is an important research topic. This paper designs an improved target immune control strategy based on the transmission law of computer viruses, which also provides a meaningful reference for solving the transmission of biological viruses.

1.2. Motivations and Contributions. Inspired by the above literature, we studied the SLBRS model and its control strategy on scale-free networks. The contributions are as follows:

(1) We present a novel SLBRS model embedded within a scale-free network framework and proceed to analyze its fundamental dynamic characteristics. Initially, we delineate the structural attributes and parameters of the scale-free network environment serving as the habitat for viruses. Subsequently, we devised a model for computer virus propagation on scale-free networks, with the aim of deepening our understanding of virus dissemination dynamics. Furthermore, we innovate the node state transition mode and system parameters. Our study extends classical models (SI, SIR, and SIS) on complex networks to address the deficiency in parameter design observed in prior research.

(2) We calculate the basic reproduction number and conduct an analysis of the stability of this model at the disease-free equilibrium. Furthermore, we establish the stability of the disease-free equilibrium and demonstrate the persistence of the disease for a finite size of the scale-free network.

(3) We propose an improved target immune control scheme based on the stability of the model SLBRS. Different from previous literature, this paper fully considers the influence of network structure on virus transmission and control effect. We combine the advantages of target immunity and acquaintance immunity to improve virus control.

(4) This novel control strategy combines the strengths of target immunization and acquaintance immunization in mitigating network virus propagation. It not only demonstrates a superior efficacy in control but also furnishes valuable insights for combating biological viruses. We perceive this as an innovative endeavor in both theoretical inquiry and practical application.

1.3. Organization. The subsequent sections are structured as follows: Section 2 presents the model formulation. In Section 3, we derive the basic reproduction number and demonstrate the stability analysis of the disease-free equilibrium, accompanied by the corresponding simulation results. Section 4 introduces the target immune control scheme for the SLBRS model and validates the control effectiveness under the enhanced immunization strategy. Finally, Section 5 provides the conclusions of the study.

2. Proposed the SLBRS Model

In this section, we introduce the parameters of the model and scale-free network, and propose a new SLBRS computer virus model on scale-free networks.

2.1. Scale-Free Networks and Model Assumptions. A complex network is a topological structure composed of many nodes and intricate relationships among nodes. One of the most important types of complex networks, scale-free networks, has attracted a great deal of research. Because the dynamic behavior of the network is affected by the network topology, statistical characteristics and formation mechanism, we divide the network into different types, including regular networks, random networks, small-world networks, and scale-free networks, etc. In order to investigate the propagation patterns of computer network viruses in real-world scenarios, it is imperative to conduct a comprehensive analysis of the topological characteristics of four fundamental network models. An intriguing observation is the prevalence of power-law degree distributions in many real networks, indicating that the probability distribution function of degree approximately follows the form $P(k) \sim k^{-\gamma}$.

As indicated in Table 1, it is evident that the scale-free network conforms to a power-law distribution. Scale-free networks exhibit a notable presence of highly connected nodes alongside numerous nodes with relatively few connections. The probability of connecting new nodes to existing nodes in a scale-free network is proportional to the degree of existing nodes, and repeated links are not allowed in the process of network generation. In computer networks, the scale-free network is used to describe the growing and preferentially open real world. The topological characteristic parameters of the scale-free network are set as shown in Table 2.

In a scale-free network, virus nodes are classified into four distinct types: susceptible (S), latent (L), breaking-out (B), and recovered (R). Susceptible and recovered nodes are denoted as healthy, while latent and breaking-out nodes are referred to as diseased. In practical computer networks, each host is regarded as a network node, with the ability to transition between these four states. The detailed descriptions of these parameters are listed in Table 3.

In reality, computer networks are regarded as scale-free network, because a few computer nodes have a large number of linked nodes, while a large number of computer nodes only connect to a few neighbor nodes. The schematic diagrams of the scale-free network are shown in Figure 1.

In the SLBRS model, computers connected to the Internet are categorized into four compartments: uninfected computers lacking immunity (S computers), latent infected computers (L computers), breaking-out infected computers (B computers), and computers with temporary immunity (R computers). Figure 2 shows the transition between these four states.

2.2. Model Description. In the SLBRS model of a computer network, where each host is represented by a network node and hosts communicate with each other through connecting edges, viruses spread along these connections. Let $S_k(t)$, $L_k(t)$, $B_k(t)$ and $R_k(t)$ be the densities of S, L, B and R node of degree k at time t, respectively. The SLBRS model on a scale-free network can be described as follows:

$$\begin{cases} \dfrac{dS_k}{dt} = -kS_k \displaystyle\sum_{m=1}^{M} \dfrac{p(m\,|\,k)}{m} \left(\alpha_1 \phi(m) L_m + \alpha_2 \varphi(m) B_m\right) + \mu R_k, \\[2ex] \dfrac{dL_k}{dt} = \alpha_1 k S_k \displaystyle\sum_{m=1}^{M} \dfrac{p(m\,|\,k)}{m} \phi(m) L_m - (\beta + \gamma_1) L_k, \\[2ex] \dfrac{dB_k}{dt} = \alpha_2 k S_k \displaystyle\sum_{m=1}^{M} \dfrac{p(m\,|\,k)}{m} \varphi(m) B_m + \beta L_k - \gamma_2 B_k, \\[2ex] \dfrac{dR_k}{dt} = \gamma_1 L_k + \gamma_2 B_k - \mu R_k. \end{cases} \tag{1}$$

The transmission diagram of SLBRS model is shown in Figure 2(a). Let $S(L, B, R)$ denote a node state as a susceptible (latent, breaking-out, recovered) node, then $S_k(L_k, B_k, R_k)$ is a susceptible (latent, breaking-out, recovered) node with a node degree of k. Obviously, α_1 and α_2 are associated with infection rates, and γ_1 and γ_2 are related to the recovery rate. $p(m\,|\,k)$ denotes the degree correlation between a node of degree k and a node of degree m. Considering uncorrelated networks, $p(m\,|\,k) = mp(m)/\langle k\rangle$. $\phi(m)$ and $\varphi(m)$ are the total effective contact time between the L node and the B node with degree m and its neighbor node in unit time. To

Table 1: The main topological features of the network models.

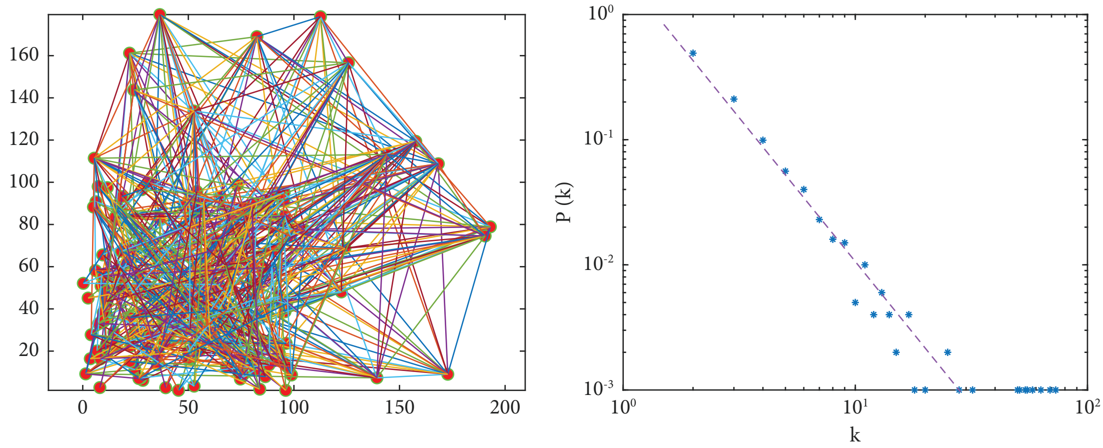
Models	Average distance	Cluster coefficient	Degree distribution
Regular network	Big	Big	δ distribution
Random network	Small	Small	Poisson distribution
Small-world network	Small	Big	Index distribution
Scale-free network	Small	Small	Power law distribution
Computer network	Small	Big	Approximate power-law distribution

Table 2: Parameters description of scale-free network.

Symbol	Parameter description	Value
k	The node degree of the network	(1, 100)
$p(k)$	The degree of distribution	$2m^2k^{-3}$
$\langle k\rangle$	Average degree of network	$\sum_{k=1}^{N} kp(k)$
L	Average distance of network	$lnN/\ln(lnN)$

Table 3: Description of parameters.

Parameters	Meaning description
α_1	Conversion rate of susceptible node S_k to latent node L_k
α_2	Conversion rate of susceptible node S_k to breaking-out node B_k
μ	Conversion rate of susceptible node S_k to recovered node R_k
β	Conversion rate of latent node L_k to breaking node B_k
γ_1	Conversion rate of latent node L_k to recovered node R_k
γ_2	Conversion rate of breaking-out node B_k to recovered node R_k
$\phi(m)$	Total effective contact time between latent node L_k and each edge
$\varphi(m)$	Total effective contact time between breaking-out node B_k and each edge



(a)

(b)

Figure 1: (a) The network is referred to as a BA scale-free network. Using the preferential attachment algorithm, we generate a BA scale-free network with 100 vertices; (b) degree distribution diagram of the scale-free networks.

simplify the calculation of the model, assuming that each contact time is equal, then $\phi(m)/m$ and $\varphi(m)/m$ are the contact times of the L node and the B node with each edge. At this point, $\alpha_1\phi(m)/m$ and $\alpha_2\varphi(m)/m$ are the probability of S nodes contacting L nodes or B nodes and being infected within unit time.

In the model SLBRS, each individual has the same probability of being in contact with its neighbors and the ability of each node to be infected by the virus is proportional to its degree, i.e., $\phi(m)$ or $\varphi(m)$ is equal to αm, where α is a positive constant and $0 \le \alpha \le 1$. Further, to simplify the complexity of the model, we assume that the

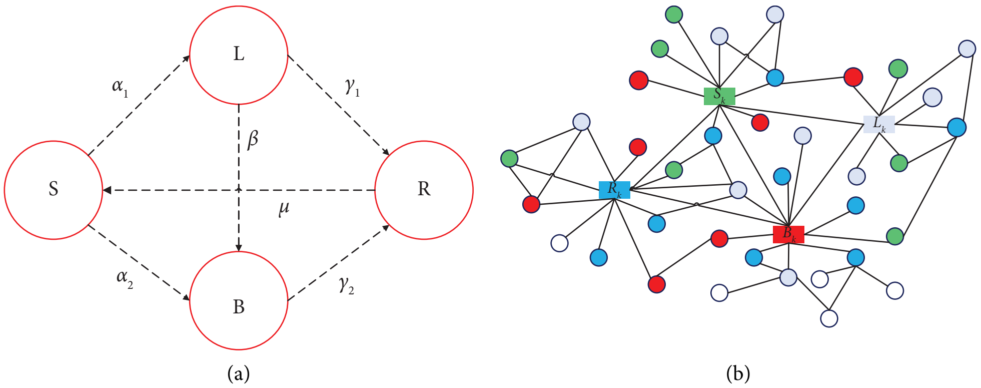


Figure 2: (a) State transition diagrams for the four computer states in the SLBRS model; (b) schematic illustration of the propagation of a cyber virus on a scale-free network.

effective contact time between the L node (B node) and its neighbor nodes is a fixed constant, denoted as A_1 (A_2), i.e., $\phi(m) = A_1$, $\varphi(m) = A_2$. Based on the above model assumptions, the dynamic system (1) can be simplified as

$$\begin{cases} \dfrac{dS_k}{dt} = -\dfrac{kS_k}{\langle k\rangle}\displaystyle\sum_{m=1}^{M}(\alpha_1 A_1 L_m + \alpha_2 A_2 B_m)p(m) + \mu R_k, \\ \dfrac{dL_k}{dt} = \alpha_1\dfrac{kS_k}{\langle k\rangle}\displaystyle\sum_{m=1}^{M} A_1 p(m)L_m - (\beta+\gamma_1)L_k, \\ \dfrac{dB_k}{dt} = \alpha_2\dfrac{kS_k}{\langle k\rangle}\displaystyle\sum_{m=1}^{M} A_2 p(m)B_m + \beta L_k - \gamma_2 B_k, \\ \dfrac{dR_k}{dt} = \gamma_1 L_k + \gamma_2 B_k - \mu R_k. \end{cases} \tag{2}$$

It is evident that these variables adhere to the normalization condition, namely,

$$S_k(t) + L_k(t) + B_k(t) + R_k(t) = 1. \tag{3}$$

In the system (2), the global densities of all nodes are

$$\begin{aligned} S(t) &= \sum_{m=1}^{M} p(m)S_m(t), L(t) = \sum_{m=1}^{M} p(m)L_m(t), \\ B(t) &= \sum_{m=1}^{M} p(m)B_m(t), R(t) = \sum_{m=1}^{M} p(m)R_m(t). \end{aligned} \tag{4}$$

The initial conditions of system (2) is $S_k^0 = 1 - L_k^0 - B_k^0 - R_k^0 \geq 0, L_k^0 \geq 0, B_k^0 \geq 0, R_k^0 \geq 0$.

3. Dynamical Behavior of the SLBRS Model

3.1. The Basic Reproduction Number R_0. The number R_0 represents the average number of nodes infected by a single virus node before it recovers. A higher value indicates a faster spread of the virus within the system and a larger number of infected nodes. The basic reproduction number of system (2) is calculated by the existence of positive equilibrium. Let the right-hand side of system (2) to be zero to obtain the positive equilibrium (S_k, L_k, B_k, R_k), which satisfies the following equations:

$$\begin{cases} -\dfrac{k}{\langle k\rangle}(\alpha_1 A_1 L(t) + \alpha_2 A_2 B(t))S_k + \mu R_k = 0, \\ \alpha_1\dfrac{k}{\langle k\rangle}A_1 L(t)S_k - (\beta+\gamma_1)L_k = 0, \\ \alpha_2\dfrac{k}{\langle k\rangle}A_2 B(t)S_k + \beta L_k - \gamma_2 B_k = 0, \\ \gamma_1 L_k + \gamma_2 B_k - \mu R_k = 0. \end{cases} \tag{5}$$

According the normalization condition, the system (5) simplifies as

$$\begin{cases} R_k = \dfrac{1}{\mu}\dfrac{k}{\langle k\rangle}(\alpha_1 A_1 L(t) + \alpha_2 A_2 B(t))S_k, \\ L_k = \dfrac{1}{\beta+\gamma_1}\alpha_1\dfrac{k}{\langle k\rangle}A_1 L(t)S_k, \\ B_k = \dfrac{1}{\gamma_2}\left(\alpha_2\dfrac{k}{\langle k\rangle}A_2 B(t)S_k + \beta L_k\right), \\ \gamma_1 L_k + \gamma_2 B_k - \mu R_k = 0. \end{cases} \tag{6}$$

We calculate the basic reproduction number R_0 by system (6).

Theorem 1. *The number R_0 of system (6) is $R_0 = (\mu\beta(\alpha_1 A_1 + (\beta+\gamma_1)\alpha_2 A_2))/(\gamma_2(\beta+\gamma_1))$.*

Proof. According to system (6), we have

$$\begin{aligned}
L_k &= \frac{\alpha_1 k/\langle k\rangle A_1 L(t)}{\beta+\gamma_1} S_k = \frac{k\alpha_1 A_1 L(t)}{\langle k\rangle(\beta+\gamma_1)} S_k,\\
B_k &= \frac{1}{\gamma_2}\left(\alpha_2 \frac{k}{\langle k\rangle} A_2 B(t) S_k + \beta L_k\right),\\
B_k &= \frac{k(\beta+\gamma_1)\alpha_2 A_2 B(t) + k\beta\alpha_1 A_1 L(t)}{\langle k\rangle \gamma_2(\beta+\gamma_1)} S_k,\\
R_k &= \frac{k}{\mu\langle k\rangle}(\alpha_1 A_1 L(t) + \alpha_2 A_2 B(t)) S_k.
\end{aligned} \tag{7}$$

Since

$$S_k(t) + L_k(t) + B_k(t) + R_k(t) = 1, \tag{8}$$

then

$$B_k = \frac{k\mu\beta(\alpha_1 A_1 + (\beta+\gamma_1)\alpha_2 A_2)B(t)}{\mu\langle k\rangle\beta\gamma_2(\beta+\gamma_1) + (k\alpha_1(\mu(\beta+\gamma_2)+\gamma_2(\beta+\gamma_1))A_1 + k\alpha_2\beta(\beta+\gamma_1)(\mu+\gamma_2)A_2)B(t)}. \tag{9}$$

Let

$$\begin{aligned}
a_0 &= \mu\langle k\rangle\,\beta\gamma_2(\beta+\gamma_1),\\
a_1 &= k\mu\beta(\alpha_1 A_1 + (\beta+\gamma_1)\alpha_2 A_2),\\
a_2 &= k\alpha_1(\mu(\beta+\gamma_2)+\gamma_2(\beta+\gamma_1))A_1\\
&\quad + k\alpha_2\beta(\beta+\gamma_1)(\mu+\gamma_2)A_2.
\end{aligned} \tag{10}$$

Then

$$\begin{aligned}
B_k &= \frac{a_1 B(t)}{a_0 + a_2 B(t)},\\
B(t) &= \sum_{k=1}^{M} p(k)B(k) = \sum_{k=1}^{M} \frac{a_1 p(k) B(t)}{a_0 + a_2 B(t)}.
\end{aligned} \tag{11}$$

To calculate the basic reproduction number R_0 of this model, let $\theta = \sum_{m=1}^{M} mp(m)\rho(m)/\langle k\rangle$ denote the probability that a susceptible node of degree k is infected by a Breaking-out node each time, where $\rho(m) = B_m/N_m$. We construct the auxiliary function $F(\theta)$, then we have

$$\begin{aligned}
\theta &= \sum_{k=1}^{M} \frac{a_1 p(k)\theta}{a_0 + a_2\theta},\\
F(\theta) &= \theta - \sum_{k=1}^{M} \frac{a_1 p(k)\theta}{a_0 + a_2\theta}.
\end{aligned} \tag{12}$$

And, we calculate the monotonicity of the function

$$\begin{aligned}
\frac{dF(\theta)}{d\theta} &= 1 - \sum_{k=1}^{M} \frac{a_0 a_1 p(k)}{(a_0 + a_2\theta)^2},\\
\frac{d^2F(\theta)}{d\theta^2} &= \sum_{k=1}^{M} \frac{2a_0 a_1 a_2 p(k)}{(a_0 + a_2\theta)^3},
\end{aligned} \tag{13}$$

because

$$\begin{aligned}
&F(0) = 0, \quad F(1) = 1 - \sum_{k=1}^{M} \frac{a_1 p(k)}{a_0 + a_2} > 0,\\
&\left.\frac{dF(\theta)}{d\theta}\right|_{\theta=0} = 1 - \sum_{k=1}^{M} \frac{a_1 p(k)}{a_0},\\
&\left.\frac{dF(\theta)}{d\theta}\right|_{\theta=0} = 1 - \sum_{k=1}^{M} \frac{k\mu\beta(\alpha_1 A_1 + (\beta+\gamma_1)\alpha_2 A_2)p(k)}{\mu\langle k\rangle\beta\gamma_2(\beta+\gamma_1)}.
\end{aligned} \tag{14}$$

So, the only necessary and sufficient condition that $F(\theta)$ has a unique positive solution in $0 \leq \theta \leq 1$ is

$$\left.\frac{dF(\theta)}{d\theta}\right|_{\theta=0} = 1 - \frac{\mu\beta(\alpha_1 A_1 + (\beta+\gamma_1)\alpha_2 A_2)}{\gamma_2(\beta+\gamma_1)}. \tag{15}$$

Thus, we get the basic reproduction number R_0 from (15), i.e.,

$$R_0 = \frac{\mu\beta(\alpha_1 A_1 + (\beta+\gamma_1)\alpha_2 A_2)}{\gamma_2(\beta+\gamma_1)}. \tag{16}$$

□

Consequently, when $R_0 > 0$, system (1) has a unique endemic equilibrium E_1. The endemic equilibrium indicates that virus nodes in a network system will persist over time, creating a stable state. The endemic equilibrium is a relatively stable state, once this state is broken, it may lead to the outbreak of endemic diseases.

3.2. *The Existence and Stability of Disease-Free Equilibrium.*

In order to analyze the existence of disease-free equilibrium point in the given computer virus network and to determine the global stability of the system, we reduce the system (2) as follows:

$$\begin{cases} \dfrac{dL_k}{dt} = \alpha_1 \dfrac{k}{\langle k \rangle} \sum\limits_{m=1}^{M} A_1 p(m) L_m (1 - L_k - B_k - R_k) - (\beta + \gamma_1) L_k, \\ \dfrac{dB_k}{dt} = \alpha_2 \dfrac{k}{\langle k \rangle} \sum\limits_{m=1}^{M} A_2 p(m) B_m (1 - L_k - B_k - R_k) + \beta L_k - \gamma_2 B_k, \\ \dfrac{dR_k}{dt} = \gamma_1 L_k + \gamma_2 B_k - \mu R_k. \end{cases} \tag{17}$$

Theorem 2. *The disease-free equilibrium point $E_0\{(1,0,0,0)\}$ of the system is unstable.*

Proof. The system (2) at the disease-free equilibrium point $E_0\{(1,0,0,0)\}$ be written as

$$\begin{cases} \dfrac{dL_k}{dt} = \alpha_1 \dfrac{A_1}{\langle k \rangle} k \sum\limits_{m=1}^{M} p(m) L_m - (\beta + \gamma_1) L_k, \\ \dfrac{dB_k}{dt} = \alpha_2 \dfrac{A_2}{\langle k \rangle} k \sum\limits_{m=1}^{M} p(m) B_m + \beta L_k - \gamma_2 B_k, \\ \dfrac{dR_k}{dt} = \gamma_1 L_k + \gamma_2 B_k - \mu R_k. \end{cases} \tag{18}$$

The Jacobian is a $3M \times 3M$ matrix,

$$J_{E_0} = \begin{pmatrix} A_1 & B_{12} & \cdots & B_{1M} \\ B_{21} & A_2 & \cdots & B_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ B_{M1} & B_{M2} & \cdots & A_M \end{pmatrix}_{3M\times 3M}, \tag{19}$$

where

$$A_j = \begin{pmatrix} \alpha_1 A_1 j p(j)/\langle k \rangle - (\beta + \gamma_1) & 0 & 0 \\ \beta & \alpha_2 A_2 j p(j)/\langle k \rangle - \gamma_2 & 0 \\ -\mu & \gamma_1 & \gamma_2 \end{pmatrix},$$
$$B_{ij} = \begin{pmatrix} \alpha_1 A_1 i p(j)/\langle k \rangle & 0 & 0 \\ 0 & \alpha_2 A_2 i p(j)/\langle k \rangle & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{20}$$

Its characteristic polynomial is

$$(x - \gamma_2)^M \left(x - \frac{\alpha_2 A_2 j p(j) - \langle k \rangle \gamma_2}{\langle k \rangle} \right)^M \left(x - \frac{\alpha_1 A_1 j p(j) - \langle k \rangle (\beta + \gamma_1)}{\langle k \rangle} \right)^M = 0. \tag{21}$$

Therefore, all characteristic roots are

$$\begin{aligned} x_1 &= \gamma_2, \\ x_2 &= \frac{\alpha_2 A_2 j p(j) - \langle k \rangle \gamma_2}{\langle k \rangle}, \\ x_3 &= \frac{\alpha_1 A_1 j p(j) - \langle k \rangle (\beta + \gamma_1)}{\langle k \rangle}. \end{aligned} \tag{22}$$

According to Hurwitz criterion, no matter whether R_0 is greater than 1, the characteristic equation has roots of positive real part, which indicates that the disease-free equilibrium point $E_0\{(1,0,0,0)\}$ of the system is unstable.

3.3. Simulation Results and Discussion. To verify the correctness of the theory proposed in Section 3, simulation experiments are carried out from three perspectives.

(1) When the model parameters and the initial values of the nodes are the same, we analyze the effect of different network average degree $\langle k \rangle$ on virus propagation. As shown in Figure 3, the greater the average degree of network nodes, the stronger the ability of computer virus to spread on the network at the initial moment. Figure 3 shows that if the computer virus preferentially infects nodes with higher than average degree in the network, the virus will spread rapidly at the initial moment and the network is under severe security threat.

(2) When model parameters and node degrees of the SLBRS model are the same, we analyze the influence of virus propagation at different initial values. In our experiment, we divided 1000 nodes into four different states, including S nodes, L nodes, B nodes, and R nodes. As shown in Figure 4, we analyzed the influence of initial values of four types of nodes in different states on the dynamics of network evolution. Figure 4 shows that the more network nodes are infected at the initial moment, the faster the network virus spreads and the greater the pressure to carry out virus control.

(3) When the initial value and node degree of the model are the same, we tried to study the influence of

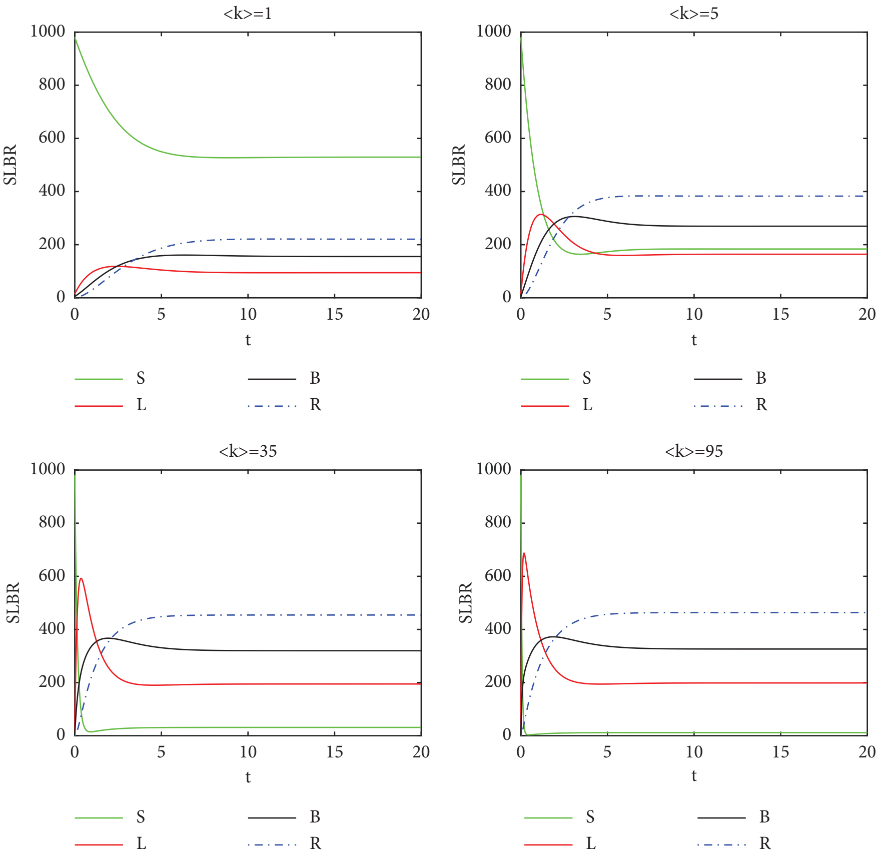


Figure 3: Exploring the influence of different average degree $\langle k \rangle$ on the SLBRS model. The figure shows the dynamical behaviors of nodes with $\langle k \rangle = 1, 5, 35, 95$ and the densities of each population as function of time t. Parameters are chosen as $\alpha_1 = 0.4, \alpha_2 = 0.3, \gamma_1 = 0.36, \gamma_2 = 0.42, \beta = 0.48, \mu = 0.45, A_1 = A_2 = 0.5$.

different parameters on virus transmission. Figure 5 shows the dynamic behaviors under different model parameters. By selecting different model parameters to carry out a large number of data experiments, the following conclusions are drawn. First, the virus always persists in the system regardless of the values taken for the model parameters. Second, the proportion of infected nodes in the system becomes larger as the parameter α_1, α_2 become larger, and becomes smaller as the parameter γ_1, γ_2 become larger.

To further analyze dynamical behavior of viruses on scale-free networks, we simulate the propagation characteristics of viruses using the NetLogo simulation tool. The parameter of the model selected in Figure 6 is $[\alpha_1, \alpha_2, \gamma_1, \gamma_2, \beta, \mu] = [0.55, 0.45, 0.35, 0.25, 0.35, 0.65]$. As can be seen from Figure 6, although the number of recovered nodes in the system increases over time, the virus nodes will always exist in the system. Based on the above discussion, we verify the existence of disease-free equilibrium of SLBRS model and the global stability of the system, and the simulation results agree with the life circumstances.

From Figures 3–6, we get three conclusions. Firstly, as the degree of nodes in the network increases, the faster the virus will infect the network system, and the system will soon be occupied by the virus nodes. This shows that the key nodes in the network system with a high degree play an important role in the spread of the virus. Secondly, the growth trend of network viruses in different initial value states remains relatively stable, and the number of L nodes and B nodes in the network remains between 200 and 400. Finally, the network system is sensitive to different model parameters. The greater the infectivity of the virus is, the faster the outbreak speed of nodes will be, and the lower the network security it gets.

In conclusion, if there is no strengthening of immune control measures, the viruses will persist the entire cyberspace. Meanwhile, the disease-free equilibrium point of the network system is unstable, and the disease tends to be in positive equilibrium.

4. The Immunization Strategy for the SLBRS Model

In complex networks, the main channels for virus propagation include emails, links, mobile hard drives, wearable devices, etc. The targets of virus attacks are mainly core nodes and groups in critical positions, which pose a huge security risk in cyberspace. To ensure network availability and robustness, infectious disease control requires full consideration of network topology and virus

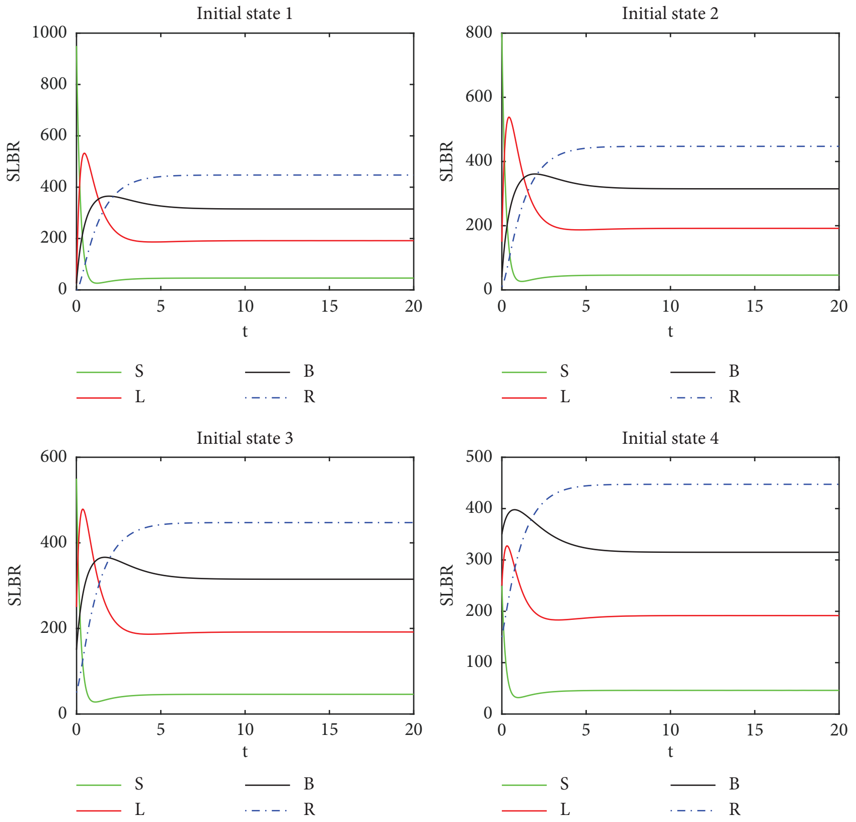


Figure 4: Consider the effect of different node initial values on the SLBRS model. The figure shows the dynamic behaviors of initial states of [950, 25, 25, 0], [800, 150, 40, 10], [550, 250, 150, 50] and [500, 200, 200, 100], and the density of each population as a function of time t. Other parameters are $\alpha_1 = 0.4, \alpha_2 = 0.3, \gamma_1 = 0.36, \gamma_2 = 0.42, \beta = 0.48, \mu = 0.45, A_1 = A_2 = 0.5$.

transmissibility, and the design of targeted immunization strategies to control the spread of viruses.

For the dynamics model of infectious diseases on scale-free networks, since the spread of network viruses is highly dependent on the structure of the network, the network nodes are classified according to the node state and degree distribution characteristics, which helps to carry out immune control. The core nodes within the network are typically prime targets for immune control. Immunization extends to the neighboring nodes of these core nodes, effectively targeting nodes with a degree greater than k within this vicinity.

In this section, we further discuss the immunization effect of the SLBRS model on target immunization and its improved strategy. First, we introduce the specific approach and immunization effect of the target immunization strategy. Second, We propose a new target immunization strategy to improve the efficiency of global immunization, i.e., immunizing key nodes while simultaneously immunizing their neighboring nodes.

4.1. Target Immunization Strategy. Among the existing immunization strategies, the classical immunization strategies containing proportional immunization, targeted immunization, acquaintance immunization, and active immunization are widely known. Since different immunization strategies have different control effects on different virus models, the selection of immunization strategies is very important. For example, the proportional immunization scheme needs to immunize a large number of network nodes, so it is difficult to achieve herd immunity.

In a computer virus network, because scale-free networks are heterogeneous and native, target immunization of nodes in the network with a degree greater than a certain value may be a more effective scheme, but target immunization requires global information of the network and it is difficult in practical applications. For network attacks, choosing acquaintance immunization or active immunization strategy is a more desirable strategy. On the one hand, acquaintance immunization does not need to grasp the global information of the complex network and also has a better immunization effect on the system. On the other hand, the immunization cost of acquaintance immunization is low, and the efficiency of immunization can also meet the needs of practical work.

To improve the effectiveness of immune control, we propose a novel active immunization strategy that combines target immunity and acquaintance immunity.

We initially introduce an upper threshold κ, where all nodes with connectivity $k > \kappa$ are immunized. In other words, we define the immunization rate δ_k as follows:

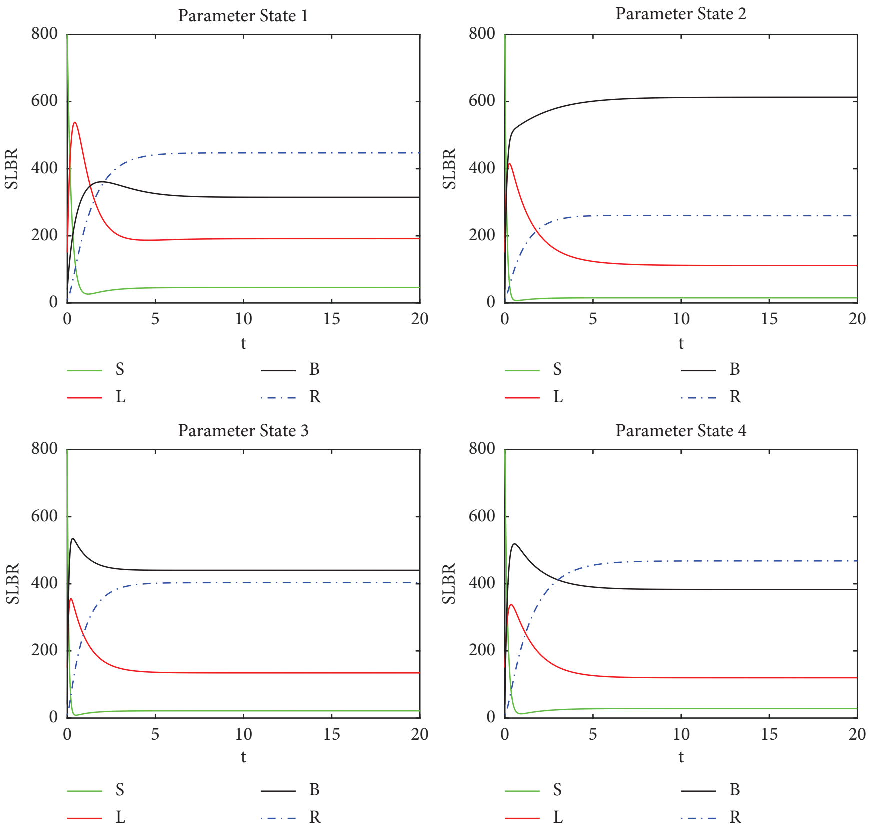


Figure 5: Consider the effects of four different sets of model parameters on the SLBRS model. $[\alpha_1, \alpha_2, \gamma_1, \gamma_2, \beta, \mu] = [0.4, 0.3, 0.36, 0.42, 0.48, 0.45]$, $[0.5, 0.4, 0.3, 0.2, 0.3, 0.6]$, $[0.5, 0.6, 0.3, 0.55, 0.4, 0.7]$, and $[0.25, 0.3, 0.22, 0.42, 0.3, 0.4]$ and the density of each population as a function of time t.

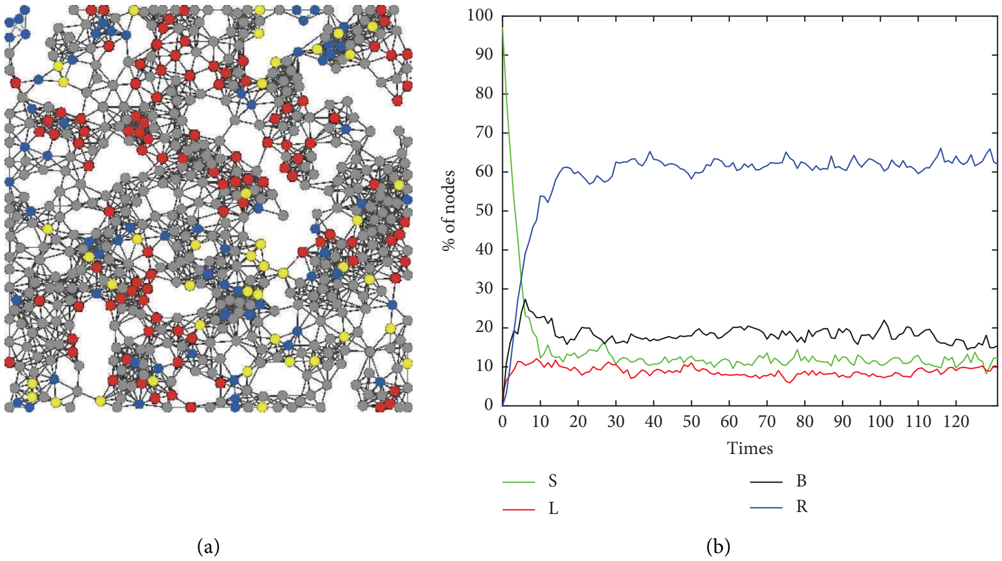


Figure 6: (a) The spread of viruses on scale-free networks; (b) dynamical behavior of four types of nodes on the scale-free network. The number of recovered and infected nodes tends to stabilize over time.

$$\delta_k = \begin{cases} 1, & k > \kappa, \\ c, & k = \kappa, \\ 0, & k < \kappa, \end{cases} \tag{23}$$

where $0 < c \leqslant 1$, and $\sum_k \delta_k P(k) = \overline{\delta}$, and $\overline{\delta}$ is the average immunization rate. $P(k)$ is the degree distribution of the nodes with degree k. The immunized SLBRS model is expressed as

$$\begin{cases} \dfrac{dS_k}{dt} = -\dfrac{k}{\langle k \rangle} \displaystyle\sum_{m=1}^{M} (\alpha_1 A_1 L_m + \alpha_2 A_2 B_m) p(m) (1 - \delta_k) S_k + \mu (1 - \delta_k) R_k, \\ \dfrac{dL_k}{dt} = \alpha_1 \dfrac{k}{\langle k \rangle} \displaystyle\sum_{m=1}^{M} A_1 p(m) L_m (1 - \delta_k) S_k - (\beta + \gamma_1) L_k, \\ \dfrac{dB_k}{dt} = \alpha_2 \dfrac{k}{\langle k \rangle} \displaystyle\sum_{m=1}^{M} A_2 p(m) B_m (1 - \delta_k) S_k + \beta L_k - \gamma_2 B_k, \\ \dfrac{dR_k}{dt} = \gamma_1 L_k + \gamma_2 B_k - \mu (1 - \delta_k) R_k. \end{cases} \tag{24}$$

When the computer virus spreads in the network, we select the nodes whose node degree is greater than the threshold κ for target immunization. The effect of immunization control on system (2) is analyzed by simulation experiments, as shown in Figure 7.

As we all know, when controlling the spread of network viruses using a target immunization strategy, we should not only consider the initial state of the system but also strengthen the control of susceptible and recovered nodes. It can be seen from Figure 7 that the larger the proportion of target immunization of nodes, the more effective the virus control is. If the upper threshold of the node degree value is smaller, the success rate of immunization is higher. However, the cost of target immunization is large, so target immunization is generally used at the beginning of a virus outbreak. To further reduce the impact of the limitations of the target immunization strategy, improve its effectiveness and reduce the cost of the target immunization strategy, we propose the following improvement strategy.

4.2. Improved Target Immunization Strategy. When dealing with virus events in large-scale computer networks, people usually target immunization of diseased nodes, but it is difficult to ensure the efficiency and effectiveness of immunization. For this reason, we can first select some of the key nodes from all the network nodes as the immunization object, and then classify the selected nodes into healthy nodes and diseased nodes, and finally take different immunization measures for these two types of nodes for system control. For example, controlling server nodes can avoid the risk of a large number of associated hosts going down. At the same time, the improved immunization strategy has merit for the control of the new coronavirus pneumonia (COVID-19).

The idea of this immunization strategy mainly consists of the following steps. First, the nodes with proportion f are randomly selected from N nodes, then the number of selected nodes is fN, where the proportion of f is determined according to the security situations of the network system and the correlation characteristics among the nodes. The goal is to make immunization as efficient as possible without knowing the global information of the network. Second, in order to improve the network immunization effect, the network administrator needs to identify the status of the elected nodes and classify these nodes into healthy and diseased nodes. Third, the acquaintance immunization strategy is applied to the neighboring nodes of the healthy nodes, i.e., immunizing the nodes with degree values greater than κ among the neighboring nodes to reduce the risk of virus transmission. Finally, since the diseased nodes with node degree greater than k have extremely strong virus infectivity in the network, it is necessary to utilize the target immunization strategy to target immunization of these nodes to block the spread of viruses from the source of virus outbreaks. That is to say, the target immunization strategy is used to control the nodes with degree greater than k among the diseased nodes, so that the virus cannot be transmitted to the neighboring nodes through these key nodes. In order to achieve the expected immunization effect, it is necessary to adjust the immunization ratio and target according to the actual situation in the computer network.

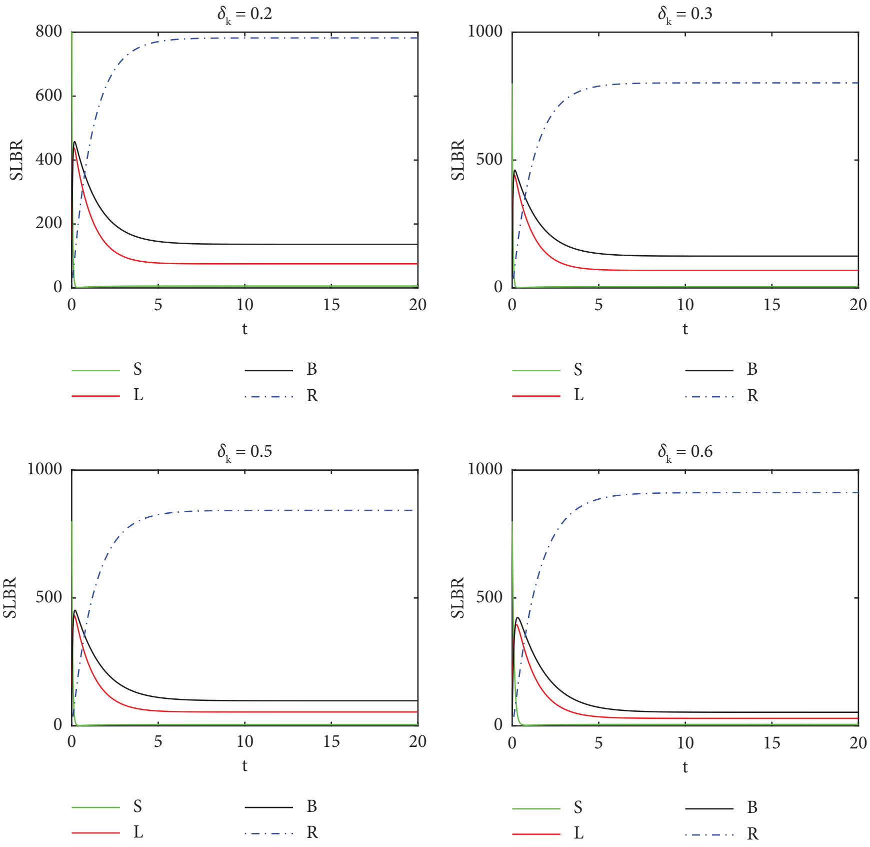


Figure 7: Trend of virus control effect with immunization ratio based on target immunization strategy. The initial states of this model is [800, 150, 40, 10], and model parameters are chosen as $\alpha_1 = 0.35, \alpha_2 = 0.6, \gamma_1 = 0.56, \gamma_2 = 0.62, \beta = 0.3, \mu = 0.4, A_1 = A_2 = 0.5$.

The immunized SLBRS model is expressed as

$$\begin{cases} \dfrac{dS_k}{dt} = -\dfrac{k}{\langle k\rangle}\displaystyle\sum_{m=1}^{M}(\alpha_1 A_1 L_m + \alpha_2 A_2 B_m)p(m)(1-\delta_k)S_k + \mu(1-\delta_k)R_k, \\ \dfrac{dL_k}{dt} = \alpha_1\dfrac{k}{\langle k\rangle}\displaystyle\sum_{m=1}^{M} A_1 p(m)L_m(1-\delta_k)S_k - (\beta+\gamma_1)L_k, \\ \dfrac{dB_k}{dt} = \alpha_2\dfrac{k}{\langle k\rangle}\displaystyle\sum_{m=1}^{M} A_2 p(m)B_m(1-\delta_k)S_k + \beta L_k - \gamma_2 f_k B_k, \\ \dfrac{dR_k}{dt} = \gamma_1 L_k + \gamma_2 f_k B_k - \mu(1-\delta_k)R_k. \end{cases} \tag{25}$$

where δ_k is given by the piecewise function above, f_k refers to the proportion of nodes with degrees greater than k selected for immunization among Breaking-out nodes. In general, it is easy to find the key nodes in the network system where security faults occur, and the harm of these nodes to the whole system is closely related to the number of its neighbor nodes. Consequently, we get a better immune effect by selecting a few Breaking-out nodes with a degree greater than k for target immunity. The simulation results are shown in Figure 8.

To ensure the security of the network system, it is imperative to enhance the efficacy of virus control while effectively containing the spread of network viruses. In the context of the new SLBRS virus propagation model on scale-free networks, we implement a target control strategy and propose an enhanced target immune control strategy. After

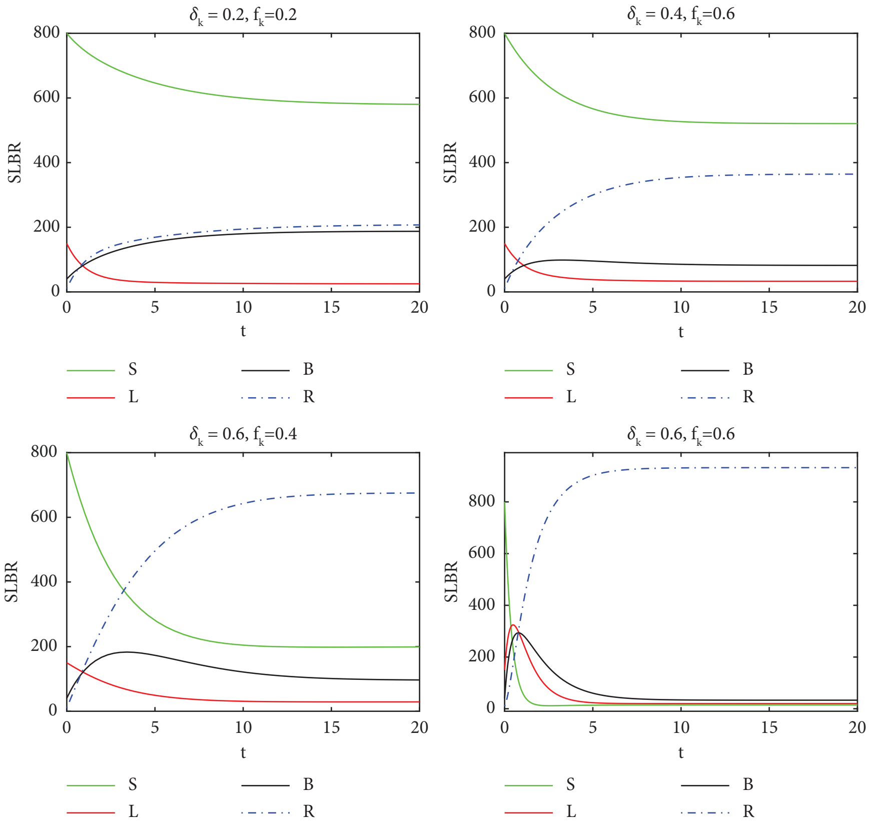


Figure 8: Effectiveness of the improved target immunization strategy for the SLBRS model. The initial state is [800, 150, 40, 10], and model parameters are $\alpha_1 = 0.45, \alpha_2 = 0.6, \gamma_1 = 0.56, \gamma_2 = 0.62, \beta = 0.6, \mu = 0.4, A_1 = A_2 = 0.5$.

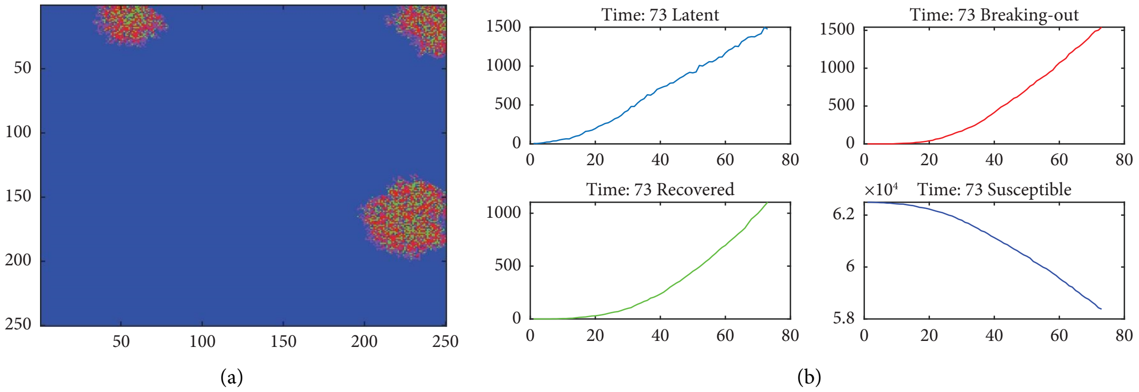
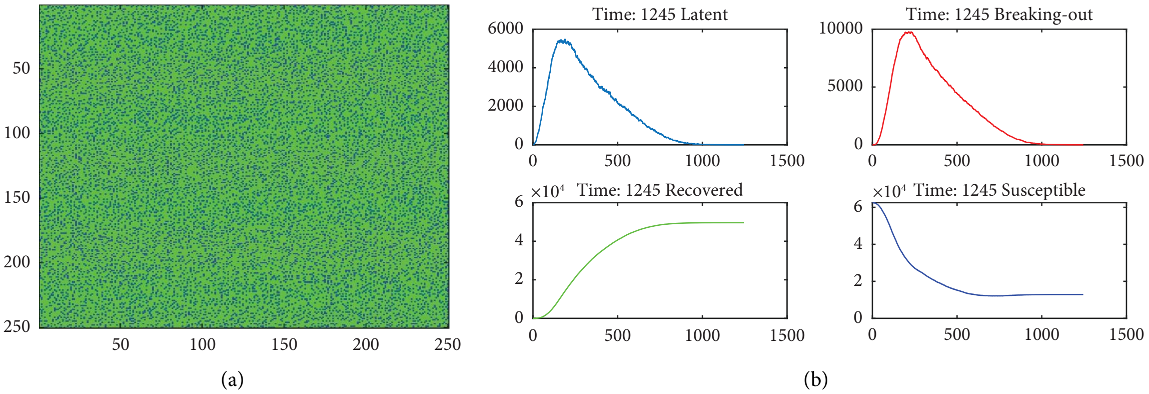


Figure 9: (a) In the initial stage of virus propagation, the network has only a few L and B nodes. At this time, the network virus spreads rapidly and the security of the system decreases rapidly; (b) the figure shows the trend of the four types of nodes in the network at virus propagation time 73. It can be seen that the number of L nodes, B nodes, and R nodes increases rapidly over time and the number of S nodes decreases rapidly.

comparing the control effects of the two strategies, two comments can be given: on the one hand, the two immune control strategies have high control effects on the SLBRS virus model, but they differ in the efficiency of control. On the other hand, the improved target immunization strategy can improve the timeliness of control, and it is suitable for network security managers to adopt this strategy for security control.

To test the control effect of the immunization strategy in this paper, we give the control effect of the system in the initial and stable periods of virus transmission.

As shown in Figures 9 and 10, the control of network viruses not only requires the selection of key nodes as immune objects but also reduces the infection of key nodes to their neighbors, which is determined by the characteristics of scale-free networks. Therefore, the combination of target immunization and



(a)

(b)

Figure 10: (a) Immunity effect analysis: at the virus propagation time 1245, the network virus system is in a stable state by applying the target immune control strategy to the network system. At this point, the virus nodes in the system are rapidly decreasing after reaching the peak, and the system is eventually occupied by the R nodes; (b) shows the stable trend of virus propagation. The L nodes and B nodes within the system are completely controlled, and the S nodes are transformed into R nodes over time.

acquaintance immunization strategies can effectively control the spread of the virus. As an application, the security of a computer network requires the control of core nodes, especially the key nodes in the center of the network. At the same time, it is necessary to strengthen the protection mechanism of these main nodes and their associated nodes, such as enhancing the deployment of intrusion detection.

5. Conclusions

In this paper, we investigate a novel SLBRS computer virus model building upon previous literature models such as [19, 26, 36, 41], focusing predominantly on virus propagation characteristics and control strategies within scale-free networks. It is observed that system (2) displays two equilibria, namely the disease-free equilibrium E_0 and the endemic equilibrium E_1. The global stability analysis was conducted for both equilibria by examining the basic reproduction number R_0. The disease-free equilibrium E_0 has been demonstrated to be unstable, while the endemic equilibrium E_1 exists under certain conditions. Furthermore, a target immunization strategy was implemented to achieve effective control of the proposed SLBRS epidemic model based on the scale-free network. As far as the author knows, this represents an innovative approach to epidemic modeling in the literature, which combines the target immunization strategy and acquaintance immunization strategy. The results show that the improved targeted immunization scheme is an accurate and effective method, which can solve the problem that the virus will persist in the system in the SIR Model, and effectively improve the system security.

In the realm of infectious diseases, uncertainties and unknown variables pose significant challenges in developing accurate models for computer virus transmission based on complex networks. Generally, scale-free network structures are better suited for such scenarios, as they can capture network heterogeneity and preferential linking. Therefore, the application of the findings in this paper within the realm of cyberspace could potentially lead to the development of effective strategies for the prevention, treatment, and control of severe infectious diseases. The insights from this study are relevant to network security experts and biomedical scientists alike, aiding in the formulation of comprehensive evaluation and treatment protocols for diseases such as Wannacry, phishing e-mail attacks, HIV, COVID-19, and beyond. Compared with the existing research work, the scheme in this paper has a wider scope of application in terms of modeling methods and virus control effects, and effectively compensates for the shortcomings of past studies.

Recent computer viruses, including ransomware, phishing emails, and trojans, are a major threat to humanity in cyberspace. Faced with the major threat posed by viruses to cyberspace, the application of the proposed method in network security situation awareness and other network virus outbreaks needs to be further studied. Similar to the transmission and control of biological viruses, the application of this research method to the transmission of biological viruses is a new idea for future research, which will provide a valuable reference for the control of biological viruses.

Data Availability

This study did not use relevant data. Data from previous studies have been cited in the references.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study received support from the Guizhou Provincial Science and Technology Projects (ZK[2022] General 168) and the National Science Foundation of China (grant 11271098).

References

[1] Y. Guo and T. Li, “Modeling the competitive transmission of the Omicron strain and Delta strain of COVID-19,” *Journal of Mathematical Analysis and Applications*, vol. 526, no. 2, Article ID 127283, 2023.

[2] C. Y. Yang and J. Wang, "A mathematical model for the novel coronavirus epidemic in Wuhan, China," *Mathematical Biosciences and Engineering*, vol. 17, no. 3, pp. 2708–2724, 2020.

[3] Y. Guo and T. Li, "Modeling and dynamic analysis of novel coronavirus pneumonia (COVID-19) in China," *Journal of Applied Mathematics and Computing*, vol. 68, no. 4, pp. 2641–2666, 2022.

[4] S. Chen, M. Small, and X. Fu, "Global stability of epidemic models with imperfect vaccination and quarantine on scale-free networks," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 1583–1596, 2020.

[5] J. P. Farwell, R. Rohozinski, and Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[6] S. Mohurle and M. Patil, "A brief study of wannacry threat: ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938–1940, 2017.

[7] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," *Artificial Intelligence Review*, vol. 53, no. 7, pp. 5019–5081, 2020.

[8] M. K. Hasan, T. M. Ghazal, R. A. Saeed et al., "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Communications*, vol. 16, no. 5, pp. 421–432, 2022.

[9] R. Zarin, H. Khaliq, A. Khan, D. Khan, A. Akgül, and U. W. Humphries, "Deterministic and fractional modeling of a computer virus propagation," *Results in Physics*, vol. 33, Article ID 105130, 2022.

[10] P. A. Naik, Z. Eskandari, A. Madzvamuse, Z. Avazzadeh, and J. Zu, "Complex dynamics of a discrete-time seasonally forced SIR epidemic model," *Mathematical Methods in the Applied Sciences*, vol. 46, no. 6, pp. 7045–7059, 2023.

[11] R. M. May and A. L. Lloyd, "Infection dynamics on scale-free networks," *Physical Review A*, vol. 64, no. 6, Article ID 066112, 2001.

[12] Z. Hai-Feng, M. Small, and F. Xin-Chu, "Different epidemic models on complex networks," *Communications in Theoretical Physics*, vol. 52, no. 1, pp. 180–184, 2009.

[13] D. Watts and S. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[14] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[15] A. Kleczkowski and B. T. Grenfell, "Mean-field-type equations for spread of epidemics: the 'small world' model," *Physica A: Statistical Mechanics and Its Applications*, vol. 274, no. 1-2, pp. 355–360, 1999.

[16] C. Moore and M. Newman, "Epidemics and percolation in small-world networks," *Physical Review A*, vol. 61, no. 5, pp. 5678–5682, 2000.

[17] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, 2001.

[18] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Physical Review A*, vol. 63, no. 6, Article ID 066117, 2001.

[19] J. Liu and T. Zhang, "Epidemic spreading of an SEIRS model in scale-free networks," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 8, pp. 3375–3384, 2011.

[20] R. Olinky and L. Stone, "Unexpected epidemic thresholds in heterogeneous networks: the role of disease transmission," *Physical Review A*, vol. 70, no. 3, Article ID 030902, 2004.

[21] J. Joo and J. L. Lebowitz, "Behavior of susceptible-infected-susceptible epidemics on heterogeneous networks with saturation," *Physical Review A*, vol. 69, no. 6, Article ID 066105, 2004.

[22] M. Yang, Z. Zhang, L. Qiang, and G. Zhang, "An SLBRS model with vertical transmission of computer virus over the internet," *Discrete Dynamics in Nature and Society*, vol. 2012, no. 12, pp. 341–379, 2012.

[23] Z. Zhang and H. Yang, "Stability and hopf bifurcation for a delayed SLBRS computer virus model," *The Scientific World Journal*, vol. 2014, no. 08, Article ID 373171, 6 pages, 2014.

[24] P. A. Naik, "Global dynamics of a fractional-order SIR epidemic model with memory," *International Journal of Biomathematics*, vol. 13, no. 08, Article ID 2050071, 2020.

[25] A. Ahmad, M. Farman, P. A. Naik, N. Zafar, A. Akgul, and M. U. Saleem, "Modeling and numerical investigation of fractional-order bovine babesiosis disease," *Numerical Methods for Partial Differential Equations*, vol. 37, no. 3, pp. 1946–1964, 2021.

[26] W. Tang, Y. J. Liu, Y. L. Chen, Y. X. Yang, and X. X. Niu, "SLBRS: network virus propagation model based on safety entropy," *Applied Soft Computing*, vol. 97, Article ID 106784, 2020.

[27] H. Sun, H. Li, and Z. Zhu, "Dynamics of an SIRS epidemic models with periodic infection rates on a scale-free networks," *Journal of Biological Systems*, vol. 30, no. 03, pp. 673–693, 2022.

[28] M. B. Ghori, P. A. Naik, J. Zu, Z. Eskandari, and M. Naik, "Global dynamics and bifurcation analysis of a fractional-order SEIR epidemic model with saturation incidence rate," *Mathematical Methods in the Applied Sciences*, vol. 45, no. 7, pp. 3665–3688, 2022.

[29] Y. Okabe and A. Shudo, "Spread of variants of epidemic disease based on the microscopic numerical simulations on networks," *Scientific Reports*, vol. 12, no. 1, pp. 523–529, 2022.

[30] R. Pastor-Satorras and A. Vespignani, "Epidemics and immunization in scale-free networks," *Handbook of Graphs and Networks*, vol. 15, pp. 111–130, 2002.

[31] W. J. Bai, T. Zhou, and B. H. Wang, "Immunization of susceptible-infected model on scale-free networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 384, no. 2, pp. 656–662, 2007.

[32] N. Masuda, "Immunization of networks with community structure," *New Journal of Physics*, vol. 11, no. 12, Article ID 123018, 2009.

[33] H. Zhang and X. Fu, "Spreading of epidemics on scale-free networks with nonlinear infectivity," *Nonlinear Analysis: Theory, Methods & Applications*, vol. 70, no. 9, pp. 3273–3278, 2009.

[34] Q. C. Wu, X. C. Fu, Z. Jin, and M. Small, "Influence of dynamic immunization on epidemic spreading in networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 419, pp. 566–574, 2015.

[35] C. Buono and L. A. Braunstein, "Immunization strategy for epidemic spreading on multilayer networks," *EPL*, vol. 109, no. 2, Article ID 26001, 2015.

[36] L. X. Yang, M. Draief, and X. Yang, "The optimal dynamic immunization under a controlled heterogeneous node-based SIRS model," *Physica A: Statistical Mechanics and Its Applications*, vol. 450, pp. 403–415, 2016.

[37] J. Cao, Y. Wang, A. Alofi, A. Al-Mazrooei, and A. Elaiw, "Global stability of an epidemic model with carrier state in heterogeneous networks," *IMA Journal of Applied Mathematics*, vol. 80, no. 4, pp. 1025–1048, 2015.

[38] G. Liu, Z. Tan, Z. Liang, H. J. Chen, and X. J. Zhong, "Fractional optimal control for malware propagation in the internet of underwater Things," *IEEE Internet of Things Journal*, vol. 11, 2023.

[39] Y. Q. Yang, G. Y. Liu, Z. W. Liang, H. J. Chen, L. H. Zhu, and X. J. Zhong, "Hybrid control for malware propagation in rechargeable WUSN and WASN: from knowledge-driven to data-driven," *Chaos, Solitons & Fractals*, vol. 173, Article ID 113703, 2023.

[40] T. Alamo, D. G Reina, P. Millán Gata, V. M. Preciado, and G. Giordano, "Data-driven methods for present and future pandemics: monitoring, modelling and managing," *Annual Reviews in Control*, vol. 52, pp. 448–464, 2021.

[41] L. L. Xia, Y. R. Song, C. C. Li, and G. P. Jiang, "Improved targeted immunization strategies based on two rounds of selection," *Physica A: Statistical Mechanics and Its Applications*, vol. 496, pp. 540–547, 2018.

[42] T. Li and Y. Guo, "Optimal control and cost-effectiveness analysis of a new COVID-19 model for Omicron strain," *Physica A: Statistical Mechanics and Its Applications*, vol. 606, no. 3, Article ID 128134, 2022.

[43] Y. Guo and T. Li, "Fractional-order modeling and optimal control of a new online game addiction model based on real data," *Communications in Nonlinear Science and Numerical Simulation*, vol. 121, no. 8, Article ID 107221, 2023.

[44] T. Li and Y. Guo, "Modeling and optimal control of mutated COVID-19 (Delta strain) with imperfect vaccination," *Chaos, Solitons & Fractals*, vol. 156, Article ID 111825, 2022.

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