RESEARCH ON VIRUS PROPAGATION MODELS IN CLOUD NETWORKS

Yanjing LI[1]

Traditional virus propagation models exhibit notable limitations when describing viral spread in cloud networks, particularly in their passive treatment of external factors, ignorance of network dynamics, and oversimplified immunization strategies. To address these gaps, this paper proposes an improved Healthy-Susceptible-Infected-Recovered (HSIR) propagation model tailored to cloud environments, which extends the classic SIR model by partitioning the susceptible class according to node neighborhood infection status. The model explicitly incorporates the elastic topology of cloud networks, proactive containment mechanisms, and the time delay between outbreak detection and immunization deployment. Theoretical analysis and numerical simulations demonstrate that the HSIR model can accurately characterize virus propagation dynamics in real cloud networks. This work provides a reliable theoretical basis for understanding and controlling viral spread in cloud infrastructures.

Keywords: virus propagation model; cloud network; immunization strategy; network dynamics; time delay

1. Introduction

Amid accelerating advances in cloud computing, cloud networks have emerged as a core infrastructure in the information age, providing unprecedented convenience for data storage, processing, and sharing. However, the openness and inherent dynamism of cloud environments also create favorable conditions for computer virus propagation. Viruses can spread rapidly in such environments, seriously threatening the security and stability of cloud networks. While traditional virus propagation models, such as SIS and SIR, have been widely applied to characterize virus spread in static networks, they encounter notable limitations when extended to dynamic cloud scenarios. Specifically, cloud networks are marked by highly dynamic topology, frequent node joining and leaving, and intricate external environmental influences on node states. These factors collectively prevent traditional models from accurately capturing the real process of virus propagation.

To address these critical limitations, this study proposes an infectious-dynamics model specifically designed for cloud environments. By integrating the

[1] Associate Professor, Dept. of Information Engineering, Shijiazhuang University of Applied Technology, China, e-mail: 532465444@qq.com

dynamic characteristics of cloud networks and the inherent complexity of virus propagation, this model aims to offer new insights and effective methods for understanding and controlling virus spread in cloud infrastructures. Overall, this research fills the gap in virus propagation modeling for cloud environments and provides an essential theoretical foundation for developing robust security and virus-control strategies.

2. Related Work

Computer viruses are so named due to their similarity to biological viruses. This analogy inspires researchers to model computer virus propagation using biological virus transmission models [1-4]. Kephart and White [5,6] first introduced epidemic dynamics and put forward the SIS framework, which has two states: susceptible and infected nodes. Considering that infected nodes in computer networks can recover, J Kim [7] extended the SIS model to the SIR model by adding a recovered node state, laying a foundation for subsequent research.

As research has advanced, many scholars have refined virus propagation models and verified their stability [8-10]. For instance: Hui Cao et al. devised a malware-spread framework that incorporates age-structure, loss of acquired immunity, and delays. Their rigorous mathematical analysis revealed the impact of age-structure and delays on model stability [11]. Vladislav Taynitskiy et al. integrated two epidemic models to propose the SWIRS model [12]. They studied the conditions for outbreak and derived the structure of best-response defense tactics. Within cyber-physical settings, Zhenhua Yu et al. introduced the SEI2RS framework featuring heterogeneous infection rates and investigated the presence and stability of steady-state solutions [13]. References [14-16] also proposed various virus propagation models and corresponding optimization and control strategies. Some researchers have studied virus propagation models in different network types, such as wireless sensor networks [17-20], mobile internet [21], and email networks [22], and analyzed their stability. In recent years, with the widespread application of cloud computing, research on virus propagation and security modeling oriented to dynamic cloud networks has gradually become a hot topic. A series of improved models and analytical methods have been proposed to adapt to the characteristics of cloud scenarios [23-27].

However, most existing models overlook the impact of external environmental factors on network node state changes. In cloud environments, the dynamic joining and leaving of nodes significantly affect virus propagation. Cloud networks are highly dynamic, with frequent node changes, which traditional virus propagation models fail to accurately describe. Therefore, this paper proposes an extended HSIR propagation model for cloud environments, which refines the susceptible state by introducing a topological partition of node infection risk. It

factors in the dynamic cloud environment, incorporates immunization tactics, and captures the delay separating viral spread from defense deployment. The goal is to more realistically reflect the virus propagation process in actual cloud environments.

3. Key Technologies and Methods

3.1 The HSIR Model with Injection Immunization Strategy

This study focuses on the propagation process of a single virus in a cloud network. The network nodes are partitioned into four mutually exclusive and exhaustive states: Healthy (H), Susceptible (S), Infected (I), and Recovered (R). The definitions and transition rules are as follows:

H (Healthy, non-immunized): Nodes that are uninfected, unimmunized, and currently have no infected neighbors. A healthy node cannot be directly infected; it first transitions into a susceptible node only when at least one of its neighboring nodes is already infected.

S (Susceptible): Nodes that are uninfected, non-immunized, and have at least one infected neighbor. Susceptible nodes are vulnerable to infection and may transition to the infected state with a certain probability per unit time.

I (Infected): Nodes that are actively infected and capable of spreading the virus to neighboring nodes.

R (Recovered/immunized): Nodes that have been immunized (via vaccination or defense mechanisms) and gain permanent immunity. Nodes in H, S, and I states can all be immunized and directly transition to the R state, which cannot be reinfected.

Key Definitions:

Definition 1 (Infection Rate, α): The probability that a susceptible node becomes infected per unit time upon contact with infected neighbors.

Definition 2 (Immunization Rate, ρ): The sum of the probabilities per unit time that uninfected nodes (healthy and susceptible) and infected nodes transition to the recovered state, i.e., $\rho = \gamma + \omega + \delta$, where γ, ω, and δ denote the probabilities per unit time that a healthy node, a susceptible node, and an infected node transition to the recovered state, respectively.

Definition 3 (Immunization Delay, π): The time lag between the detection of virus activity and the formal deployment of immunization strategies.

Definition 4 (Initial Condition, t=0): At the start of virus propagation, only a very small number of nodes are randomly selected as initial infected nodes such that $I(0) \ll N$. All direct neighbors of these infected nodes are set as susceptible nodes, and the remaining nodes are healthy. No nodes are immunized at the initial moment ($R(0)=0$). The node conservation relation $H(0)+S(0)+I(0)+R(0)=N$ holds.

Definition 5(Single-contact Infection Probability, β): Per-contact transmission likelihood between network nodes.

Definition 6 (Neighbor Contact Quantity, $C(N)$): Per-time contacts from an infectious host to its susceptible peers in the network.

Assumption 1: Nodes become infected instantaneously, i.e., the intra-node infection process is neglected, and the time required for the virus to transmit from an infected node to a neighboring node is fixed and is referred to as one unit time.

Assumption 2: The cloud network is modeled at the logical layer, focusing on node connectivity rather than physical hardware details.

Assumption 3: The virus remains active throughout the propagation process. In each unit time, an infected node spreads the virus to its neighboring nodes. While the infection rate differs across virus types, it remains constant for a single virus during propagation.

State transitions are depicted in Fig. 1.

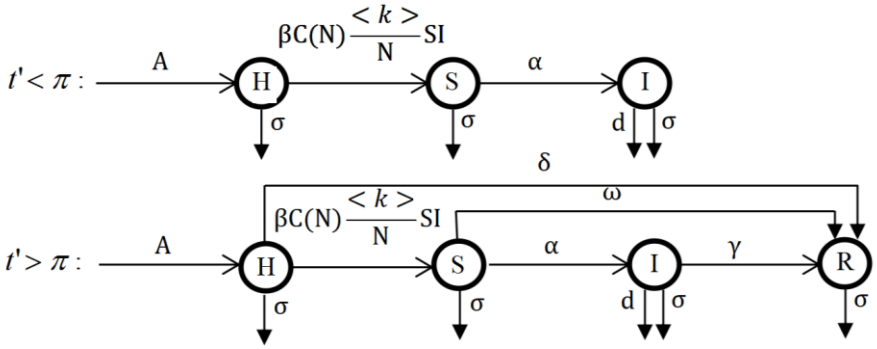


Fig. 1. HSIR Virus Propagation Model

When the immunization strategy has not been introduced (i.e., $t' < \pi$), the virus spreads freely due to the absence of immunization, resulting in an unrestricted and rapid rise in infections. Once the immunization strategy is implemented (i.e., $t' > \pi$), both the virus and the immunization strategy propagate within the network.

Set N as the initial fleet size of the cloud network. Let A represent the influx of new nodes per unit time. $\beta C(N)$ gives the contact rate, formed by multiplying the per-time contacts from an infectious host to its susceptible peers, $C(N)$, by the per-contact transmission likelihood, β. Thus, $\beta C(N)\frac{< k >}{N}SI$ denotes the probability of healthy nodes transitioning to susceptible per unit time. α gives the per-time-unit infection likelihood for susceptible hosts. γ measures the rate at which infected hosts gain immunity per unit interval. ω quantifies the per-time-unit immunization likelihood for susceptible hosts. δ denotes the per-time-unit immunization likelihood for healthy hosts. σ denotes the fraction of hosts departing each time unit, while d indicates the share eliminated by infection.

Before immunization deployment ($t'<\pi$), no immunization is activated. Only Healthy (H), Susceptible (S), and Infected (I) states exist. The system is:

$$\begin{cases} \dfrac{dH(t)}{dt} = \dfrac{A}{\sigma} - \beta C(N)\dfrac{< k >}{N} H(t)S(t)I(t) - \sigma H(t) \\ \dfrac{dS(t)}{dt} = \beta C(N)\dfrac{< k >}{N} H(t)S(t)I(t) - \sigma S(t) - aS(t) \\ \dfrac{dI(t)}{dt} = aS(t) - \sigma I(t) - dI(t) \end{cases} \tag{1}$$

For $t' > \pi$, the HSIR propagation system is described by these differential equations:

$$\begin{cases} \dfrac{\mathrm{d}H(t)}{dt} = \dfrac{A}{\sigma} - \beta C(N)\dfrac{< k >}{N} H(t)S(t)I(t) - \delta H(t) - \sigma H(t) \\ \dfrac{dS(t)}{dt} = \beta C(N)\dfrac{< k >}{N} H(t)S(t)I(t) - \omega S(t) - \alpha S(t) - \sigma S(t) \\ \dfrac{dI(t)}{dt} = \alpha S(t) - \gamma I(t) - dI(t) - \sigma I(t) \\ \dfrac{dR(t)}{dt} = \gamma I(t) + \omega S(t) + \delta H(t) - \sigma R(t) \end{cases} \tag{2}$$

The theoretical analysis and steady-state results in this work focus on the post-immunization regime ($t'>\pi$), while the numerical simulations consider the full time domain including both ($t'<\pi$) and ($t'>\pi$) phases.

Initially, for $t'>\pi$, the fleet size equals N, $H(t) + S(t) + I(t) + R(t) = N$ i.e., .

$H(t)$ counts healthy, non-vaccinated hosts; $S(t)$ denotes susceptible individuals; $I(t)$ tallies infections; and $R(t)$ records recoveries. The term $\beta C(N)\dfrac{< k >}{N} H(t)S(t)I(t)$ reflects the neighborhood-dependent infection condition in cloud networks.

Let $\sigma dt = d\tau$, $\beta_1 = \dfrac{\beta C(N) < k >}{\sigma N}$, $\delta_1 = \dfrac{\delta}{\sigma}, \omega_1 = \dfrac{\omega}{\sigma}, \alpha_1 = \dfrac{\alpha}{\sigma}, d_1 = \dfrac{d}{\sigma}$, $\gamma_1 = \dfrac{\gamma}{\sigma}$.

Then we have:

$$\begin{cases} \dfrac{dH(t)}{d\tau} = \dfrac{A}{\sigma} - \beta_1 H(t)S(t)I(t) - \delta_1 H(t) - H(t) \\ \dfrac{dS(t)}{d\tau} = \beta_1 H(t)S(t)I(t) - \omega_1 S(t) - \alpha_1 S(t) - S(t) \\ \dfrac{dI(t)}{d\tau} = \alpha_1 S(t) - \gamma_1 I(t) - d_1 I(t) - I(t) \\ \dfrac{dR(t)}{d\tau} = \gamma_1 I(t) + \omega_1 S(t) + \delta_1 H(t) - R(t) \end{cases} \tag{3}$$

This system is equivalent to system (1). $N(t)$ satisfies the following differential equation:

$$\frac{dN(t)}{dt} = \frac{dH(t)}{dt} + \frac{dS(t)}{dt} + \frac{dI(t)}{dt} + \frac{dR(t)}{dt} = \frac{A}{\sigma} - N - d_1 I(t).$$

Replacing variable H with variable N, we obtain:

$$\begin{cases} \dfrac{dS(t)}{d\tau} = \beta_1 H(t)S(t)I(t) - P_1 S(t) \\ \dfrac{dI(t)}{d\tau} = \alpha_1 S(t) - P_2 I(t) \\ \dfrac{dR(t)}{d\tau} = \gamma_1 I(t) + \omega_1 S(t) + \delta_1 H(t) - R(t) \\ \dfrac{dN(t)}{d\tau} = \dfrac{A}{\sigma} - N(t) - d_1 I(t) \end{cases} \tag{4}$$

Where $P_1 = \omega_1 + \alpha_1 + 1$ and $P_2 = \gamma_1 + d_1 + 1$ System (4) is equivalent to Systems (2) and (3). Thus, we can study System (4) to understand Systems (2) and (3). From a biological perspective, we study System (4) within $M = \left\{ (H,S,I,R) \in R_+^4 : 0 \le S + I + R \le N \le \dfrac{A}{\sigma} \right\}$. Given the practical meaning of System (4), all initial values lie within M, making M the largest positive invariant set for System (4).

3.2 Equilibrium Points and Stability Proof

Next, we derive the steady-state solutions and confirm their stability.

Set the right-hand sides of the four differential equations in system (3) to zero:

$$\frac{A}{\sigma} - \beta_1 H(t)S(t)I(t) - \delta_1 H(t) - H(t) = 0 \tag{5}$$

$$\beta_1 H(t)S(t)I(t) - P_1 S(t) = 0 \tag{6}$$

$$\alpha_1 S(t) - P_2 I(t) = 0 \tag{7}$$

$$\gamma_1 I(t) + \omega_1 S(t) + \delta_1 H(t) - R(t) = 0 \tag{8}$$

$$\text{Also, } \frac{A}{\sigma} - N(t) - d_1 I(t) = 0 \tag{9}$$

From formulas (5), (6), (7), (8) and (9), we can obtain the following:

$$\begin{cases} H^* = \dfrac{A\alpha_1\sigma d_1^{\,2}}{\beta_1 P_2 (A-\sigma N)^2 + (\delta_1+1)\alpha_1\sigma d_1^{\,2}} \\ S^* = \dfrac{P_2(A-\sigma N)}{\sigma\alpha_1 d_1} \\ I^* = \dfrac{A-\sigma N}{\sigma d_1} \\ R^* = \gamma_1 I^* + \omega_1 S^* + \delta_1 H^* \end{cases} \tag{10}$$

Where $P_1 = \alpha_1 + \omega_1 + 1$ and $P_2 = \gamma_1 + d_1 + 1$ Inserting the expressions for S and I into equation (6) yields:

$$\frac{P_2}{\alpha_1\sigma d_1}\left(\frac{A\alpha_1\beta_1 d_1(A-\sigma N)}{\beta_1 P_2(A-\sigma N)^2 + (\delta_1+1)\alpha_1\sigma d_1^{\,2}} - P_1\right)(A-\sigma N) = 0 \tag{11}$$

Let:

$$F(N) = \frac{P_2}{\alpha_1\sigma d_1}\left(\frac{A\alpha_1\beta_1 d_1(A-\sigma N)}{\beta_1 P_2(A-\sigma N)^2 + (\delta_1+1)\alpha_1\sigma d_1^{\,2}} - P_1\right) \tag{12}$$

Via (11), system (4) invariably admits an infection-free steady state within $\left(0, \frac{A}{\sigma}\right)$. Given that $N = \frac{A}{\sigma}$, the infection-free steady state is

$$P^0 = \left(\frac{A}{\sigma(\delta_1+1)}, 0, 0, \frac{A\delta_1}{\sigma(\delta_1+1)}\right).$$

Given that:

$$F\left(\frac{A}{\sigma}\right) = -\frac{P_1 P_2}{\alpha_1\sigma d_1} < 0 \tag{13}$$

$$F(0) = \frac{P_1 P_2}{\alpha_1\sigma d_1}\left(\frac{A\alpha_1\beta_1 d_1(A-\sigma N)}{P_1[\beta_1 P_2(A-\sigma N)^2 + (\delta_1+1)\alpha_1\sigma d_1^{\,2}]} - 1\right) = \frac{P_1 P_2}{\sigma d_1\alpha_1}(R_0 - 1) \tag{14}$$

The threshold of system (4) is $R_0 = \dfrac{A\alpha_1\beta_1 d_1(A-\sigma N)}{P_1[\beta_1 P_2(A-\sigma N)^2 + (\delta_1+1)\alpha_1\sigma d_1^{\,2}]}$.

Note that R_0 depends on the total node count N, which varies with node arrivals and departures. In this paper, R_0 is treated as an approximate constant threshold under the assumption that N remains near its equilibrium state. This approximation is reasonable for stable cloud networks with mild node dynamics.

When $R_0 > 1$, $F(N)$ is monotonically decreasing. Since $F(0) > 0$ and $F\left(\frac{A}{\sigma}\right) < 0$, there is a unique positive root of $F(N)=0$ within the interval $\left(0, \frac{A}{\sigma}\right)$ his means that system (4) has a unique endemic equilibrium point $P^*(H^*, S^*, I^*, R^*)$ where the values of H^*, S^*, I^*, and R^* follow from (10).

Theorem 1: When $R_0 \le 1$ P^0 is globally asymptotically stable within M; when $R_0 > 1$, P^0 loses stability.

Proof: When $R_0 \le 1$, we choose the Lyapunov function

$$V = \alpha_1 S + P_1 I \tag{15}$$

Then,

$$\begin{aligned} V'|_{System(3)} &= \beta_1\alpha_1 H(t)S(t)I(t) - \alpha_1 P_1 S(t) + \alpha_1 P_1 S(t) - P_1 P_2 I(t) \\ &= \left[\beta_1\alpha_1 H(t)S(t) - P_1 P_2\right] I(t) \\ &= P_1 P_2 \left(\frac{A\alpha_1\beta_1 d_1 (A - \sigma N)}{P_1[\beta_1 P_2 (A - \sigma N)^2 + (\delta_1 + 1)\alpha_1 \sigma d_1^{\,2}]} - 1 \right) I(t) \\ &= P_1 P_2 (R_0 - 1) I(t) \end{aligned}$$

Thus, when $R_0 \le 1$, it follows that $V' \le 0$. Moreover, $V' = 0$ if and only if $I(t)=0$ or $R_0 = 1$. Let $M = \{(H, S, I, R) \mid V' = 0\}$, then the largest positive invariant set in M is the singleton set $\{P^0\}$. Hence, per Theorem 1, P^0 becomes globally stable for $R_0 \le 1$. $R_0 > 1$, we $V' > 0$, implyinP^0at is unstable.

Theorem 2: For $R_0 >$ lystem (4) admits a single endemic steady state P^* that remains locally stable.

Proof: The Jacobian matrix corresponding to System (4), when evaluated at point $P^* = (S^*, I^*, R^*, N^*)$, reads:

$$\begin{pmatrix} \beta_1 H^* I^* - P_1 & \beta_1 H^* S^* & 0 & 0 \\ \alpha_1 & -P_2 & 0 & 0 \\ \omega_1 & \gamma_1 & -1 & 0 \\ 0 & -d_1 & 0 & -1 \end{pmatrix}$$

Its characteristic equation reads $\lambda E - J(P^*) = 0$ with E denoting the identity. Reduction of the equation yields:

$$(\lambda+1)^2[(\lambda+P_1-\beta_1 H^* I^*)(\lambda+P_2)-\alpha_1\beta_1 H^* S^*]=0$$

which can be further reduced to: $(\lambda+1)^2[\lambda^2+\alpha_1\lambda+\alpha_2]=0$

Here, $\alpha_1=P_1+P_2-\beta_1 H^* I^*$, $\alpha_2=P_2(P_1-\beta_1 H^* I^*)-\alpha_1\beta_1 H^* S^*$.

Given that:

$$\begin{aligned}P_1-\beta_1 H^* I^*-\alpha_1\beta_1 H^* S^* &= P_1-\beta_1 H^*\left(\frac{A-\sigma N}{\sigma d_1}-\alpha_1\times\frac{P_2(A-\sigma N)}{\sigma\alpha_1 d_1}\right)\\ &= P_1-\beta_1 H^* I^*(1-P_2)\\ &= P_1-\beta_1 H^* I^*(1-\gamma_1-d_1-1)\\ &= P_1+\beta_1 H^* I^*(\gamma_1+d_1)>0\end{aligned}$$

It follows that:

$$a_1=P_1+P_2-\beta_1 H^* I^*>0;$$

$$\begin{aligned}a_2 &= P_2(P_1-\beta_1 H^* I^*)-\alpha_1\beta_1 H^* S^*\\ &= (\gamma_1+d_1)(P_1-\beta_1 H^* I^*)+P_1-\beta_1 H^* I^*-\alpha_1\beta_1 H^* S^*>0\end{aligned}$$

Thus:

$$\Delta_1=a_1>0$$

$$\Delta_2=\begin{vmatrix}a_1 & a_3\\ a_0 & a_2\end{vmatrix}=a_1 a_2>0$$

The Hurwitz test verifies that P remains locally stable. Hence, $R_0=\dfrac{A\alpha_1\beta_1 d_1(A-\sigma N)}{P_1[\beta_1 P_2(A-\sigma N)^2+(\delta_1+1)\alpha_1\sigma d_1^{\,2}]}$ marks the immunity threshold of the HSIR framework. For $R_0<1$, infection dies out and the system settles at the disease-free state. When $R_0>1$, the disease persists, and the system stabilizes at the endemic equilibrium point.

4. Simulation and Analysis

4.1 Simulation Configuration

To ensure the reproducibility of experiments, this section explicitly presents the simulation settings and parameter values. The simulation is implemented on a discrete-event simulation platform, supporting elastic cloud topology, dynamic node join-leave, and state transition rules. All parameters are consistent with the HSIR model assumptions in Section 3 and refer to typical configurations of medium-scale cloud environments.

(1) Basic network settings

Total initial logical nodes: N=5000.

Node composition: computing nodes (40%), storage nodes (35%), network nodes (25%).

Initial conditions: I(0)=2 (randomly network nodes), R(0)=0; susceptible nodes are direct neighbors of infected nodes, and the rest are healthy.

(2) Infection-related parameters

Infection rate: $\alpha=0.08$.

Average node degree: $<k> = 8$.

(3) Immunization-related parameters

Immunization rate: $\rho\in[0.01, 0.50]$.

Sub-immunization rates: $\gamma=0.3\rho$, $\omega=0.5\rho$, $\delta=0.2\rho$, satisfying $\rho=\gamma+\omega+\delta$.

Immunization delay: $\pi=5$ time units.

(4) Node dynamic parameters

New node arrival rate: A=15 per unit time.

Normal node departure rate: $\sigma=0.003$.

Infection-induced node elimination rate: d=0.001.

(5) Simulation setup

Baseline scenario: $\rho=0$ (no proactive immunization).

Simulation duration: 100 time units.

Time step: 1 unit.

4.2 Simulation Results and Analysis

The simulation environment replicates a real cloud infrastructure with the above configuration. Network nodes have the highest external connectivity and serve as high-risk entry points due to frequent interactions with external systems. As illustrated in Fig. 2, the infection dynamics exhibit a three-stage evolutionary trend over time: exponential growth, peak formation, and stable convergence.

(1) Exponential Growth Stage (t=0-18 time units)

The number of infected nodes increased rapidly from 2 to approximately 1,100. During this stage, a sufficient number of susceptible nodes were present, and frequent data interactions occurred among edge nodes. Viruses propagated rapidly through inter-node communication links, demonstrating a typical exponential growth trend.

(2) Peak Formation Stage (t=18-20 time units)

The growth rate of infected nodes gradually decelerated, reaching a peak of approximately 1,200 at t=20. The population of susceptible nodes decreased significantly during this period. Meanwhile, some infected nodes transitioned to a recovered state due to built-in protection mechanisms (e.g., default firewalls). The combined effect of these two factors contributed to the slowdown in the growth of infected nodes.

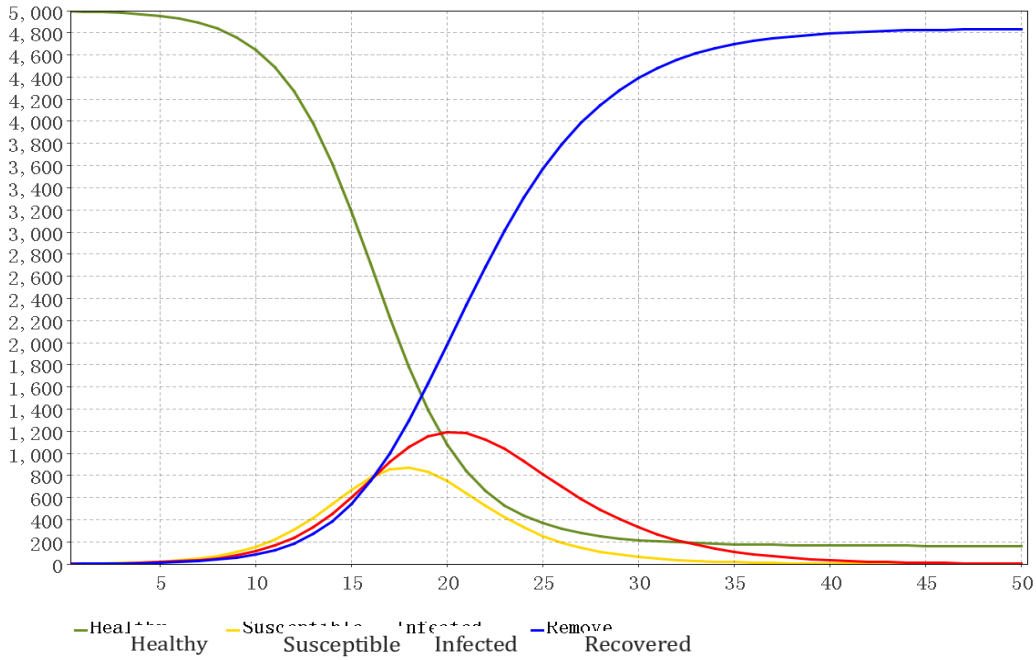


Fig. 2. Virus propagation in cloud networks

(3) Stable Convergence Stage (t>20 time units)

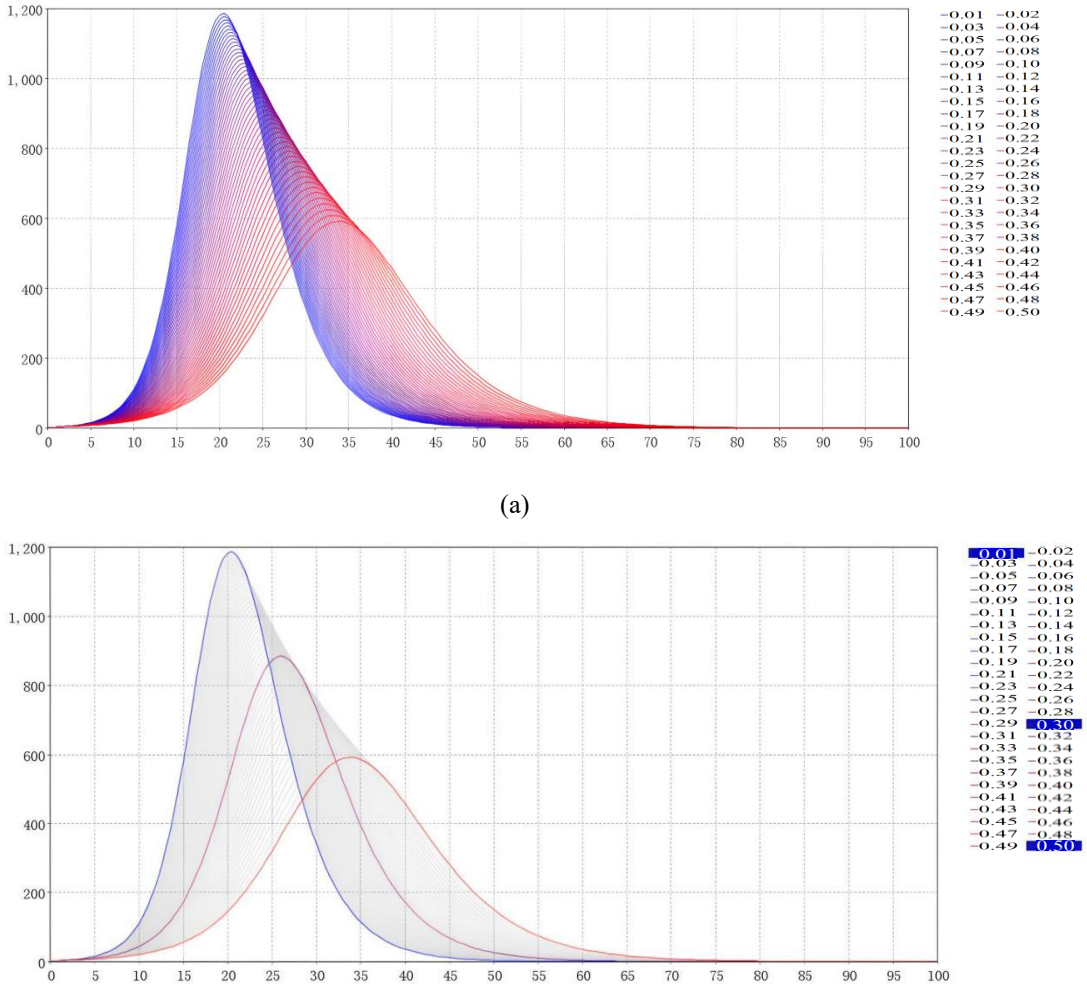
The number of infected nodes gradually declined from the peak and eventually stabilized, attaining a dynamic equilibrium. At this stage, the rate of new infections was essentially balanced by the speed at which infected nodes were recovering.

To evaluate the efficacy of immunization strategies, we conduct 50 groups of simulations with immunization rates uniformly ranging from 1% to 50%. In each group, immunized nodes are randomly distributed across all three node types to ensure generalizability, with all other parameters maintained as specified in Section 4.1. The outcomes of the simulation are depicted in Fig. 3(a).

The immunization rate significantly influenced two key viral transmission metrics: the final infection scale and the time to peak infection. Multi-gradient simulations revealed the following patterns:

Negative correlation between final infection scale and immunization rate: In Fig. 3(b), it can be observed that when the immunization rate was 1%, the quantity of infected nodes at the end was roughly 1190. This value is close to the 1200-node baseline in the non-immunization case, suggesting that the viral spread was hardly curbed. When the immunization rate increased to 10%, the number of infected nodes decreased to 1000, representing a 15.9% reduction compared to the 1% immunization rate, indicating that the inhibitory effect of immunization began

to emerge initially. At 30% immunization, the number of infected nodes decreased to 870, representing a 26.9% reduction compared to the 1% immunization rate. At 50% immunization, infected nodes dropped to 590, a 50.8% reduction relative to the non-immunization scenario. This occurs because higher immunization rates preemptively confer immunity to more susceptible nodes, disrupting viral transmission paths.



(a)

(b)

Fig. 3. Impact of different immunization rates on Infections and Peak.

Positive correlation between time to peak infection and immunization rate: At 1% immunization, the infection peak occurred at t=21, which is similar to the non-immunized scenario (t=20). At 10% immunization, the infection peak occurred at t=22; at 30% immunization, the peak was delayed to t=27; at 50% immunization,

it was further delayed to t=33. This delay arises because immunization reduces viral transmission efficiency, extending the time required for the virus to reach its maximum spread.

These patterns are consistent with real cloud security practices. Increasing antivirus coverage (i.e., a higher immunization rate) reduces the final infection scale and delays the infection peak, providing valuable time for security response. This confirms the practical validity of the simulation results.

5. Discussion

As evidenced by our simulations, the HSIR model is applicable to dynamic cloud networks because it captures three critical elements: node dynamics, immunization strategies, and the infection-to-immunization time lag. Leveraging the model's properties and simulation-derived patterns, the following targeted prevention and control measures are proposed:

(1) Establishing a dynamic node immunization admission-exit mechanism

Cloud nodes are frequently added and removed. Traditional SIS/SIR models assume a fixed node count, failing to accurately model such dynamics. By accounting for node dynamics, the HSIR model yields a truer-to-life depiction of how infections propagate through the cloud network. Building on this, the prevention and control measures can be designed as follows:

•**Node admission:** Implement an "immunize-before-online" protocol, including full-system virus scanning, prior installation of cloud-aware antivirus tools, and assignment of dynamic security levels utilizing HSIR risk predictions (e.g., flagging high-risk nodes and enhancing their port protection).

•**Node exit:** Enforce a "virus cleanup-log upload" procedure to eliminate residual malware and upload infection histories to a cloud security log center. This data supports ongoing HSIR model parameter updates and prediction refinement.

(2) Implementing a hierarchical immunization strategy

Unlike the SIS model, the HSIR model supports both reactive (post-infection) and preventive immunization, aligning better with real-world cloud security needs. Consistent with the simulation pattern—higher immunization rates improve containment effectiveness—a tiered strategy is recommended under resource constraints:

Divide the cloud network into two zones:

•**Core zone:** Contains database and critical computing nodes. Apply a high immunization rate (30%–50%)—simulations show 30% reduces final infections by 26.9%, while 50% reduces them by 50.8%. Given that there is a significant order-of-magnitude gap between the losses caused by core node failures and non-core node failures, the resource cost of high immunization is justified. These ranges are illustrative examples only.

•**Non-core zone:** Includes network forwarding and temporary storage nodes. Use a basic immunization rate (5%–20%)—the non-core zone's large node count makes this rate optimal for balancing containment effectiveness and resource consumption. These values are purely illustrative and require practical calibration.

(3) Building a predictive immunization activation mechanism

SIR/SIRS models fail to account for the immunization lag, while the HSIR model accurately captures the lag characteristic of "detecting infections first and then initiating prevention and control" in real-world scenarios by introducing an "immunization delay parameter" (π, i.e., the time difference between viral propagation and the implementation of immunization strategies). Building on this, a predictive activation mechanism can be designed:

•**Trend prediction:** Embed the HSIR model into a transmission prediction module. Input current counts of infected/susceptible nodes and node dynamics parameters to forecast infection scale over the next 10~15 time units.

•**Threshold triggering:** Two levels of early warning thresholds are established as illustrative examples. If infections are predicted to exceed an example threshold of 500 at t+5, a basic immunization response is activated (increasing the immunization rate of the non-core zone by an example increment of 5% and that of the core zone by an example increment of 3%); if infections are predicted to exceed an example threshold of 800 at t+5, an emergency immunization protocol is implemented (increasing the immunization rate of both the non-core zone and the core zone by an example increment of 10%). These values are purely illustrative examples and must be calibrated per deployment. This mechanism leverages the model's predictive capability to shift defense from passive response to active defense, effectively offsetting the risks posed by immunization delays.

6. Conclusions

Traditional virus propagation models are passive and struggle to adapt to dynamic network environments due to their failure to adequately consider state-node number changes and other external factors. Cloud networks, as large-scale, distributed, and dynamically changing complex networks, have dynamic node numbers and complex virus propagation processes, making it difficult for traditional models to accurately describe virus propagation. Herein, we introduce the HSIR framework—a new propagation paradigm for cloud environments. It jointly captures cloud-network elasticity, proactive defense deployment, and the delay separating malware spread from countermeasure deployment. Through rigorous mathematical analysis, we identify the model's equilibrium points and prove their stability. We also determine the epidemic propagation threshold of the model. Numerical tests validate the performance of the HSIR model, demonstrating

its ability to faithfully capture malware dynamics across cloud infrastructures. In conclusion, the HSIR model provides a more accurate and practical theoretical framework for the investigation of virus propagation in cloud networks, providing a solid theoretical foundation for developing security and virus - control strategies in cloud networks.

REFERENCES

[1] *Madhusudanan, V, and R. Geetha*. "Dynamics of Epidemic Computer Virus Spreading Model with Delays." Wireless Personal Communications 115.3(2020):-.

[2] Chinebu, Titus, et al. "Epidemic Model and Mathematical Study of Impact of Vaccination for the Control of Malware in Computer Network." Journal of Advances in Mathematics and Computer Science ,2021.

[3] Upadhyay, Kumar Singh, Prerna. "Modeling and control of computer virus attack on a targeted network." Physica, A. Statistical mechanics and its applications 538(2020).

[4] Del Rey, A. Martin, R. C. Vara, and S. R. Gonzalez. "A computational propagation model for malware based on the SIR classic model." Neurocomputing, 2022.

[5] JO Kephart, SR White. Directed-graph epidemiological models of computer viruses: Proceedings of the 1991 IEEE Symposium on Security and Privacy, Oarkland, CA, USA, 20-22, 1991.

[6] JO Kephart, SR White. Measuring and modeling computer virus prevalence: Proceedings of the 1993 IEEE Symposium on Security and Privacy, Oarkland, CA, USA, 20-22, 1993[C].

[7] J Kim, S Radhakrishnan, SK Dhall, et al. Measurement and analysis of worm propagation on Internet network topology: Computer Communications and Networks, 2004.

[8] Liu, Min , et al. "An Epidemic Model with Two Impulses for the Propagation of Malware in Heterogeneous Wireless Sensor Networks." Chinese of Journal Electronics[J]. 34.4(2025):1357-1374.

[9] Wu, Guowen , et al. "STSIR: An individual-group game-based model for disclosing virus spread in Social Internet of Things." Journal of network and computer applications[J].(2023).

[10] J. L. Wang, L. Zhong and X. X. Chang, "SEIQRS model analysis and optimal control with two delays," PLOS ONE, 20(2025): e0319417.

[11] Cao, Hui, et al. "The Dynamical Analysis of Computer Viruses Model with Age Structure and Delay." Discrete Dynamics in Nature and Society 2021(2021).

[12] Taynitskiy V, Gubar E, Fedyanin D, et al. Optimal Control of Joint Multi-Virus Infection and Information Spreading[J]. 2020.DOI:10.48550/arXiv.2007.09745.

[13] Yu, Zhenhua, et al. "SEI 2 RS malware propagation model considering two infection rates in cyber–physical systems." Physica A: Statistical Mechanics and its Applications 597(2022):127207-.

[14] Derya Avcı, Fatma Soytürk. “Optimal control strategies for a computer network under virus threat”. Journal of Computational and Applied Mathematics[J].419(2023).

[15] Beyza Billur İskender Eroğlu, Dilara Yapışkan. “Comparative analysis on fractional optimal control of an SLBS model”. Journal of Computational and Applied Mathematics[J].421 (2023).

[16] Kim, Kwang Su, et al. "Mathematical analysis of the effectiveness of control strategies to prevent the autorun virus transmission propagation." Applied Mathematics and Computation 371(2020).

[17] Zhou, Haiping, S. Shen, and J. Liu. "Malware propagation model in wireless sensor networks under attack–defense confrontation." Computer Communications 162(2020):51-58.

[18] Batista F K, Angel Martín del Rey, Queiruga-Dios A. A New Individual-Based Model to Simulate Malware Propagation in Wireless Sensor Networks[J]. 2020.DOI:10.3390/math8030410.
[19] Liu, Guiyun, et al. "Dynamical Analysis and Optimal Control for a SEIR Model Based on Virus Mutation in WSNs." Mathematics 9(2021).
[20] A, Nguyen Phuong Dong, H. V. L. B. C, and N. L. G. D. "The fuzzy fractional SIQR model of computer virus propagation in wireless sensor network using Caputo Atangana–Baleanu derivatives." Fuzzy Sets and Systems (2021).
[21] Ding, Jian, et al. "Stability and Bifurcation Analysis of A Delayed Worm Propagation Model in Mobile Internet." IAENG Internaitonal journal of computer science 3 Pt.2(2020):47.
[22] Xie, Boli, and M. Liu. "Dynamics Stability and Optimal Control of Virus Propagation Based on the E-Mail Network." IEEE Access[J]. 9(2021):32449-32456.
[23] Alavizadeh, Hooman, et al. "Social network botnet attack mitigation model for cloud." Computer Networks[J]. c(2025):111160.
[24] LongZhenyue, et al. "A Transformer-based network intrusion detection approach for cloud security." Journal of Cloud Computing[J]. 13(2024).
[25] Kirubavathi, G., et al. "Detection and mitigation of TCP-based DDoS attacks in cloud environments using a self-attention and intersample attention transformer model." The Journal of Supercomputing[J]. 81.3(2025):1-42.
[26] Rout, Chinmayee, S. Sethi, and R. K. Sahoo. "FSEGM: feature selection and ensemble generative model for adaptive cloud security." Journal of Cloud Computing[J].15.1(2026):6.
[27] Bouleghlimat, Imene, S. Boudouda, and S. Hacini. "LSPP: a leakage-resilient security approach for a cloud-assisted big data." The Journal of Supercomputing[J]. 81.1(2025):1-39.