An Analysis of Worm Dynamics with Honeypot Feedback in Scale-Free Networks

Jiali Xue, Jianguo Ren*, Liping Feng and Lei Wang

***Abstract*—Scale-free networks' complex topology makes them an ideal target for worm attacks. Research has demonstrated that honeypot technology holds enormous promise for resolving worm-related problems. In this paper, we propose a novel propagation model based on honeypot feedback, namely H-SAIR. After capturing the virus successfully, the honeypot collects assault behaviors, analyzes attack paths, generates immunity information, and provides immune feedback to adjacent nodes to promote active protection. First, we introduce honeypot node H and affected node A based on the SIR model. Then, we use dynamics analysis to compute the model's propagation threshold R_0, proving the global stability of the disease-free equilibrium P_0 and the existence of the endemic equilibrium P^*. Finally, the experimental results indicate that when R_0 is less than 1, the H-SAIR model effectively constrains the spread of worms. With the increase in feedback rate, the containment effect will become stronger. Meanwhile, we can effectively control the spread of worms by strategically placing enough honeypots at hub sites, thereby maintaining network security.**

***Index Terms*—worms; honeypots; feedback mechanisms; scale-free networks; stability analysis**

I. Introduction

THE rapid development of information technology has exacerbated network security issues, making it the focus of social attention. Currently, the Internet is extensively utilized across several domains, including teleconferencing, entertainment, and e-commerce, facilitating the transfer of information beyond the constraints of information and space. Nevertheless, the widespread use of the internet concurrently results in the continual enhancement and evolution of network viruses. Network security faces a significant threat from worms [1]. It is a type of malware capable of rapid propagation and self-replication that can quickly infect numerous hosts, leading to significant issues such as network paralysis, system crashes, and data loss [2]. Consequently, more and more scholars gradually pay attention to the important topic of network security. Therefore, studying the worm propagation process can facilitate the implementation of more targeted defense strategies, which is critical for network security [3], [4].

Currently, researchers have demonstrated scale-free characteristics in many real networks, such as the Internet, power grid, and World Wide Web [5], [6]. Scale-free networks have a highly complex network topology, and the degrees of nodes obey a power-law distribution $P(k) \sim k^{-r}, r \in (2,3]$ (where r is the power exponent). This means that most nodes have low degrees while a few nodes have very high degrees, creating a big difference between core and periphery nodes [7]-[9]. Due to the complexity of scale-free networks, passive security defense strategies are not always effective. As a result, honeypots, which are an active security defense mechanism, have become an important tool in combating viruses [10]. Honeypots are beneficial for detection, attack, or disruption and can be deployed in different locations within the network [11].

Fig. 1 shows the deployment blueprint for honeypots. Honeypot systems are typically deployed in external networks to safeguard real servers or hosts, effectively blocking attacks from external viruses. Implementing vulnerable honeypots within internal networks to attract virus attacks for analysis can enhance the defense capabilities of actual hosts and strengthen their defensive capabilities.

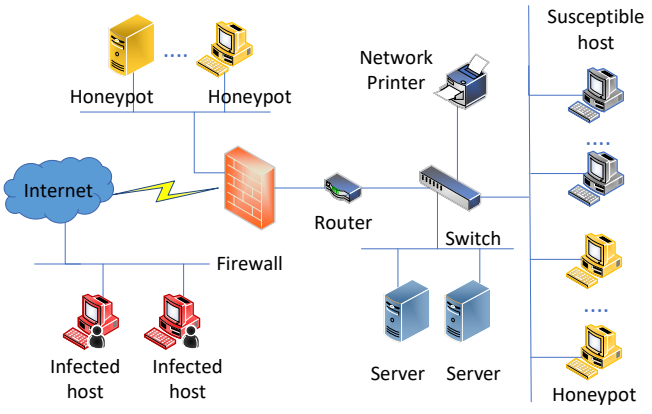

Fig. 1. The deployment blueprint for the honeypots in the network

Recent research indicates that honeypot technology has significant potential for addressing worm-related issues. However, the role of honeypots in transmitting immunization information to the periphery for prevention and control has not been sufficiently examined. In this paper, we will analyze the trapping and feedback mechanisms of honeypots on worms, and propose an active defense model to better

Manuscript received June 13, 2024; revised November 21, 2024.

This work was supported in part by the National Science Foundation of Shanxi Province under Grant 202203021211116, and the National Science Foundation of Jiangsu Province under Grant BK20241960.

Jiali Xue is a postgraduate student in the College of Computer Science and Technology at Jiangsu Normal University, Xuzhou 221116, China. (e-mail: 2020220575@jsnu.edu.cn).

Jianguo Ren is an associate professor at the College of Computer Science and Technology at Jiangsu Normal University, Xuzhou 221116, China. (e-mail: jsnucs1119@163.com).

Liping Feng is a teacher in the Department of Computer Science at Xinzhou Teacher University, Xinzhou 034000, China. (e-mail: fenglp@yeah.net).

Wang Lei is an engineer in the Hydrology Bureau of Yishu-Si Water Resources Management Bureau, Xuzhou 221116, China. (e-mail: 23165155@qq.com).

understand the dynamics of virus propagation in scale-free networks. It will also investigate the influence of the placement and quantity of deployed honeypots on virus spread, aiming to formulate a scientific and effective virus defense strategy.

This paper assumes that after a worm attack, the honeypots deployed in the network adopt a "wide-in, tight-out" strategy [25] and will not become a new source of infection. We can refer to common devices in the network as common nodes, and we can refer to honeypot devices as honeypot nodes.

II. Related Work

In recent years, the widespread use of the Internet has greatly improved people's knowledge of the world, but the problem of network security has become increasingly serious. The dynamics of network virus propagation have become a widely researched topic among many experts [12]-[15], revealing the patterns of virus transmission, analyzing the development trend, and then proposing targeted defense measures.

Regarding the defense of worms, it has been studied by the related literature, and significant progress has been made. In Refs. [16], [17], Gan and Kim et al. proposed a "vaccination" strategy for patching vulnerabilities or updating systems in nodes during the virus propagation process, prompting susceptible nodes to enter a recovery state early. In Refs. [18], [19], Xiao and Dong et al. proposed a propagation model that includes an isolation state to isolate infected nodes and reduce virus spread. The results showed that "vaccination" and isolation can effectively inhibit virus transmission. However, these defense strategies have a certain time lag and cannot resist virus attacks in time.

To address this challenge, the public has recommended using honeypot technology as a proactive security measure. In Ref. [20], Qin proposed a ransomware monitoring method based on distributed honeypot technology. Honeypot transformed into a security service through port mapping, covering all intranet network segments and safeguarding the terminal security of enterprises. In Ref. [21], Hu introduced the design principles and architecture of a virtual honeynet, successfully implementing a closed virtual honeynet that ultimately demonstrated its practicality, reliability, and stability. In Ref. [22], Negi introduced a method for intrusion detection and defense in cloud security, utilizing a honeypot network. This approach employed cloud-based honeypots consistent with cloud frameworks, aiding in monitoring malicious attacks and protecting the cloud environment. In Ref. [23], Li designed and implemented a honeynet architecture specifically for the industrial control field, combining virtualization technology, honeynet architecture, and industrial systems to alter the asymmetric situation of network attacks and defense games. The aforementioned literature demonstrates the value of honeypots in defending against virus attacks.

Existing studies have focused on the design of honeypot technology in various domains, while theoretical research is still in its infancy. In Ref. [24], Ren created a model of compartments within a scale-free network and studied the interaction between virus propagation and honeynets, concluding that honeypots with smaller power-law indices are more effective in capturing virus samples. In Ref. [25], Na proposed a worm propagation model for distributed honeypots based on a two-factor model, considering the characteristics of honeypots and scale-free networks in a distributed environment, and investigated the virus propagation patterns. In Ref. [26], Fu suggested a malware propagation model with immunization and isolation as defenses in two layers of complex networks (industrial control networks and honeynets). It studied the impact of average degree and power-law exponents on virus propagation in two layers of complex networks and revealed the relationship between virus propagation and honeynet effectiveness.

All the above studies share a common issue: they only focused on the honeytrap's role in capturing viruses within scale-free networks, while neglecting the significance of honeypots in feedbacking immune information to other nodes in the network after capturing the virus. Additionally, they did not consider the impact of honeypot deployment sites on virus defense. In this paper, we introduce a worm defense model that utilizes honeypot feedback mechanisms in a scale-free network, named H-SAIR.

The primary contributions of this article are as follows:

1)We add the affected state node *A* into the classical SIR model to further distinguish the stage of the virus infection. Considering the role of honeypots against worms, we introduce honeypot susceptible node S^h and honeypot infected node I^h to create a new propagation model, named H-SAIR.

2)We perform dynamic analysis of the model, calculating the propagation threshold R_0, disease-free equilibrium P_0, and endemic equilibrium P^* associated with the node degree *k*. We also prove the stability and uniqueness of the equilibrium point.

3)Numerical simulations using MATLAB verify the validity of the theory and show the propagation dynamics of the worms in a scale-free network. We compare the containment effects of different models on worms, explore the influence of different parameters on virus propagation, study the importance of honeypot's number and deployment location, and propose practical measures to contain the spread of the virus.

III. The H-SAIR Model

Worms probe the network for groups of susceptible hosts and launch attacks on hosts with system vulnerabilities. Once the virus enters the system, it will use system resources for self-replication and preparation, but infection symptoms will not immediately appear. At this point, the susceptible nodes have not yet been fully infected, so they are referred to as $A\ (affected)$ nodes in this paper. Therefore, based on the classical SIR model, we consider including A node before the infected state. We distinguish the stages of host infection in detail to enhance our analysis of the virus propagation process.

In this paper, the spread of the worm follows the state transition process of $S \rightarrow A \rightarrow I \rightarrow R$. The workflow of the worm is described in the Algorithm 1:

Algorithm1: The process of worms' attack and propagation.

repeat
  begin
    Worms probe vulnerable hosts.
    Generate an IP address.
    Send a TCP/SYN-ACK packet to hosts randomly.
    if *the SYN-ACK packet is received* **then**
      Complete the three-way handshake;
      Establish a connection with the target host;
      Acquire the control of the target host successfully;
      Send malicious codes to affected hosts for infection.
    else if *the SYN-ACK packet isn't received* **then**
      Back to step 5.
    end
    Worms perform on-site processing and replicate themselves.
    Generate copies, and repeats the above steps.
  end
  return infection status.
until $N(I_k^p)$ *and* $N(S_k^h)$ *are both empty.*

In this paper, we focus on the feedback mechanism of honeypots in controlling worms in scale-free networks. The degree of nodes in this network follows a power-law distribution $P(k) \sim k^{-r}, r \in (2,3]$ (where r is the power exponent), and the average degree of nodes is $< k >= \sum_{k=1}^{\Delta} kP(k)$, where Δ represents the maximum degree of nodes in the network. The model categorizes all nodes into six states, referred to as $S_k^p, A_k^p, I_k^p, R_k^p, S_k^h, I_k^h$. The common node density $N_k^p(t)$ and the honeypot node density $N_k^h(t)$ must satisfy the following conditions:

$$N_k^p(t) = S_k^p(t) + A_k^p(t) + I_k^p(t) + R_k^p(t)$$
$$N_k^h(t) = S_k^h(t) + I_k^h(t)$$

The parameters are defined as shown in Table I:

TABLE I
DEFINITION OF PARAMETERS AND VARIABLES

Parameters /Variables	Definition
d_1	Probability of a new honeypot node joining the network per unit time
μ_1	Probability of a honeypot node moving out of network per unit time
γ	Infection rate of worms to honeypot-susceptible nodes
ω	Removal rate of worms from infected nodes
d	Probability of a common node joining the network per unit time
μ	Probability of a common node moving out of network per unit time
β	Infection rate of worms to susceptible nodes
ξ	Feedback rate of honeypot-infected nodes
ψ	Probability of affected nodes transforming into infected nodes
S_k^h	Density of honeypot-susceptible nodes with degree k
I_k^h	Density of honeypot-infected nodes with degree k
S_k^p	Density of susceptible nodes with degree k
A_k^p	Density of affected nodes with degree k
I_k^p	Density of infected nodes with degree k
R_k^p	Density of recovered nodes with degree k
Θ^h	Probability that other nodes in the network communicate with honeypot-infected nodes
Θ^p	Probability that other nodes in the network communicate with infected nodes

The network is equipped with deceptive information and exploitable vulnerabilities for each honeypot node, allowing it to actively lure worms into launching attacks. Honeypot nodes monitor worm's attack behavior, then provide generated immune information to common nodes. These nodes can detect and patch security vulnerabilities in time, thus effectively preventing potential virus attacks. The infected nodes and honeypot-infected nodes communicate with other nodes in the network with probabilities of Θ^p and Θ^h, respectively, and interact with each other.

$$\begin{aligned}\Theta^p(t) &= \frac{1}{< k >}[1 \times P(1)I_1^p + \cdots + \Delta \times P(\Delta)I_\Delta^p] \\ &= \frac{1}{< k >}\sum_{k=1}^{\Delta} kP(k)I_k^p\end{aligned} \tag{1}$$

$$\begin{aligned}\Theta^h(t) &= \frac{1}{< k >}[1 \times P(1)I_1^h + \cdots + \Delta \times P(\Delta)I_\Delta^h] \\ &= \frac{1}{< k >}\sum_{k=1}^{\Delta} kP(k)I_k^h\end{aligned} \tag{2}$$

In the following, we utilize Algorithm 2 to describe trapping and feedback mechanisms for honeypots:

Algorithm2: Honeypot trapping and feedback mechanisms.

Input: Susceptible Nodes S_k^p, Infected Nodes I_k^p, Honeypot-susceptible Nodes S_k^h

Output: Affected Nodes A_k^p, Recovered Nodes R_k^p, Honeypot-infected Nodes I_k^h

begin
  Deploy honeypots to lure worms into attacking.
  foreach $I_k^p \in N(I^p)$ **do**
    Scan the susceptible nodes, and obtain the control of the target nodes successfully.
    foreach $S_k^h \in N(S^h)$ **do**
      if *honeypot captured the virus successfully* **then**
        Honeypot-susceptible nodes convert to

honeypot-infected nodes;
The firewall intercepts the data packets in and out of the honeypots;
Data transponders dump data messages;
Intercept all system logs through honeypots;
Extract useful data using protocol analysis, behavioral analysis, profiling, etc.
Analyze the infection behavior of worms and prepare immunization codes.
else if *honeypot not catching the worms* **then**
if *worms infected susceptible nodes* **then**
The state of common nodes transforms into: $S_k^p \rightarrow A_k^p \rightarrow I_k^p \rightarrow R_k^p$.
else
No nodes were infected.
end
end
end
end
foreach $I_k^h \in N(I^h)$ **do**
Scan the network, interact with common nodes;
Feedback immunization codes for susceptible nodes;
Common nodes (S_k^p, A_k^p, I_k^p) convert to recovered nodes R_k^p.
end
return recovered nodes R_k^p;
end

The state transition relationship of the H-SAIR model is shown in Fig. 2, where the circular boxes represent the states of the nodes, and the arrows indicate the direction of node state transitions.

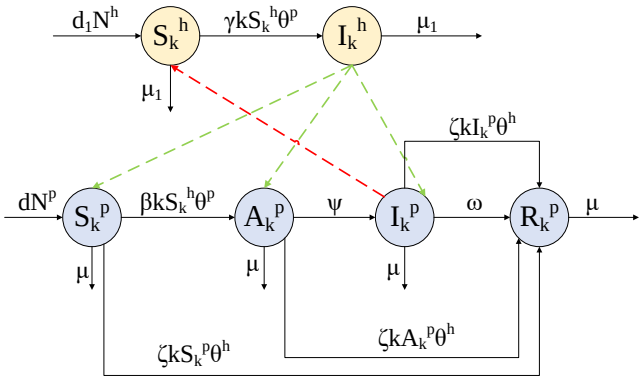

Fig. 2. Schematic diagram of model state transformation

The transformational relationships between the states are as follows:

1) $S_k^p \rightarrow A_k^p$: Worms exploit system vulnerabilities in susceptible nodes to launch attacks, gain control, and then transform into affected nodes.

2) $A_k^p \rightarrow I_k^p$: Worms transmit the primary program to affected nodes, causing it to become completely infected, and subsequently transform into infected nodes.

3) $I_k^p \rightarrow R_k^p$: Infected nodes update the virus database to install patches and remove worms.

4) $S_k^p \rightarrow R_k^p$: Susceptible nodes receive the immune information, which is fed back from the honeypot-infected nodes, and thus become recovered.

5) $A_k^p \rightarrow R_k^p$: Affected nodes receive the immune information, which is fed back from the honeypot-infected nodes, and thus become recovered.

6) $S_k^h \rightarrow I_k^h$: Honeypot-susceptible nodes get attacked by worms or interact with infected nodes, resulting in infection and its transformation into honeypot-infected nodes.

7) $I_k^p \rightarrow S_k^h$: Worms replicate themselves at infected nodes to infect other computer systems, while honeypot-susceptible nodes actively induce worm intrusion.

8) $I_k^h \rightarrow S_k^p(A_k^p, I_k^p)$: Honeypot-infected nodes generate immune information by analyzing the virus's attack behavior and feeding it back to the common nodes (susceptible nodes, affected nodes, recovered nodes).

Therefore, the probability of susceptible nodes with degree k become infected is $1-(1-\beta\Theta^p)^k \approx \beta k\Theta^p$, the probability of honeypot-susceptible nodes with degree k become infected is $1-(1-\gamma\Theta^p)^k \approx \gamma k\Theta^p$, and the probability of honeypot-infected nodes of degree k deal in feedback is $1-(1-\xi\Theta^h)^k \approx \xi k\Theta^h$.

According to the states transition relationships in Fig. 2, its differential dynamics equation can be expressed as:

$$\begin{cases} \frac{dS_k^p}{dt} = dN_k^p - \beta k S_k^p \Theta^p - \xi k S_k^p \Theta^h - \mu S_k^p \\ \frac{dA_k^p}{dt} = \beta k S_k^p \Theta^p - \xi k A_k^p \Theta^h - \psi A_k^p - \mu A_k^p \\ \frac{dI_k^p}{dt} = \psi A_k^p - \omega I_k^p - \xi k I_k^p \Theta^h - \mu I_k^p \\ \frac{dR_k^p}{dt} = \xi k \Theta^h (S_k^p + A_k^p + I_k^p) + \omega I_k^p - \mu R_k^p \\ \frac{dS_k^h}{dt} = d_1 N_k^h - \gamma k S_k^h \Theta^p - \mu_1 S_k^h \\ \frac{dI_k^h}{dt} = \gamma k S_k^h \Theta^p - \mu_1 I_k^h (k = 1,2,3,\ldots,\Delta) \end{cases} \tag{3}$$

In particularly, it follows from

$$N^p(t) = S^p(t) + A^p(t) + I^p(t) + R^p(t)$$

$$= \sum_{k=1}^{\Delta} [S_k^p(t) + A_k^p(t) + I_k^p(t)]$$

$$N^h(t) = S^h(t) + I^h(t) = \sum_{k=1}^{\Delta} [S_k^h(t) + I_k^h(t)]$$

It can be calculated as follows:

$$\frac{dN_k^p}{d\,t} = dN^p \text{ - } \mu N_k^p, \lim_{t\to\infty} N_k^p = \frac{dN^p}{\mu}$$

$$\frac{dN_k^h}{d\,t} = d_1 N^h \text{ - } \mu_1 N_k^h, \lim_{t\to\infty} N_k^h = \frac{dN^h}{\mu}$$

Simplification of Eq. (3) yields the following sub-equation, referred to as Model I:

$$\begin{cases} \dfrac{dS_k^p}{dt} = dN_k^p \text{ - } \beta k S_k^p \Theta^p \text{ - } \xi k S_k^p \Theta^h \text{ - } \mu S_k^p \\ \dfrac{dA_k^p}{dt} = \beta k S_k^p \Theta^p \text{ - } \xi k A_k^p \Theta^h \text{ - } \psi A_k^p \text{ - } \mu A_k^p \\ \dfrac{dI_k^p}{dt} = \psi A_k^p \text{ - } \omega I_k^p \text{ - } \xi k I_k^p \Theta^h \text{ - } \mu I_k^p \\ \dfrac{dI_k^h}{dt} = \gamma k(\dfrac{d_1 N_k^h}{\mu_1} \text{ - } I_k^h)\Theta^p \text{ - } \mu_1 I_k^h (k = 1 \ldots \Delta) \end{cases} \quad (4)$$

The feasible domain of Model I is denoted by Ω:

$$\Omega = [(S_k^p, A_k^p, I_k^p, I_k^h) \in R_+^4 : S_k^p + A_k^p + I_k^p \le \frac{dN^p}{\mu},$$

$$I_k^h \le \frac{d_1 N^h}{\mu_1}, S_k^p, A_k^p, I_k^p, I_k^h \ge 0, k = 1,2,3,\ldots,\Delta)]$$

This set is a positive-invariant set for Model I.

There exists a unique disease-free equilibrium P_0 for Model I.

$$P_0 = (S_{0k}^p, A_{0k}^p, I_{0k}^p, I_{0k}^h)^T = (\frac{dN^p}{\mu}, 0, 0, 0)^T$$

Let $x = (x_1, x_2, \ldots x_{3\Delta})^T = (A_{0k}^p, I_{0k}^p, I_{0k}^h)^T$, Model I can be written as $\frac{dx}{dt} = F(x) \text{ - } V(x)$.

$$F(x) = \begin{pmatrix} \beta k S_k^p \Theta^p \\ 0 \\ \gamma k S_k^h \Theta^p \end{pmatrix}$$

$$V(x) = \begin{pmatrix} \xi\, k A_k^p \Theta^h + \psi A_k^p + \mu A_k^p \\ \omega I_k^p + \xi\, k I_k^p \Theta^h + \mu I_k^p \text{ - } \psi A_k^p \\ \mu_1 I_k^h \end{pmatrix}$$

Next, we solve the Jacobian matrix for $F(x)$ and $V(x)$ separately, yielding the following results:

$$F(P_0) = \left(\frac{\partial \vartheta}{\partial x_i}\right)_{3\Delta\times 3\Delta} = \begin{pmatrix} 0 & \beta\, k S_k^p \dfrac{\partial \Theta^p}{\partial I_k^p} & 0 \\ 0 & 0 & 0 \\ 0 & \gamma\, k S_k^h \dfrac{\partial \Theta^p}{\partial I_k^p} & 0 \end{pmatrix}$$

$$V(P_0) = \left(\frac{\partial \nu}{\partial x_i}\right)_{3\Delta\times 3\Delta} = \begin{pmatrix} \xi k \Theta^h + \psi + \mu & 0 & \xi k A_k^p \dfrac{\partial \Theta^h}{\partial I_k^h} \\ \text{-}\psi & \omega + \xi k \Theta^h + \mu & \xi k I_k^p \dfrac{\partial \Theta^h}{\partial I_k^h} \\ 0 & 0 & \mu_1 \end{pmatrix}$$

We use the next-generation matrix method to calculate the basic regeneration number $R_0 = \rho(FV^{-1})$, which is the propagation threshold value for the Model I related to the disease-free equilibrium P_0.

$$\begin{aligned} \rho(FV^{-1}) &= \frac{\psi\beta k S_k^p}{(\psi+\mu)(\omega+\mu)} \cdot \frac{\partial \Theta^p}{\partial I_k^p} \\ &= \frac{\psi\beta}{(\psi+\mu)(\omega+\mu)} \cdot \frac{dN^p}{\mu} \cdot \frac{1}{< k >} \times \\ &\quad \left[\begin{pmatrix} 1 \\ 2 \\ \vdots \\ \Delta \end{pmatrix} \times (1 \times P(1)\ 2 \times P(2) \cdots \Delta \times P(\Delta))\right] \\ &= \frac{\psi\beta dN^p}{(\psi+\mu)(\omega+\mu)\mu} \cdot \frac{1}{< k >} \cdot \sum_{k=1}^{\Delta} k^2 P(k) \end{aligned} \quad (5)$$

$$R_0 = \frac{\psi\beta}{(\psi+\mu)(\omega+\mu)} \cdot \frac{dN^p}{\mu} \cdot \frac{1}{< k >} \cdot \sum_{k=1}^{\Delta} k^2 P(k) \quad (6)$$

IV. The Stability Analysis

In this section, we focus on proving the local and global stability of disease-free equilibrium P_0, as well as the existence and uniqueness of endemic equilibrium P^*.

A. Local Stability of Disease-Free Equilibrium

Lemma 1. When $R_0 < 1$, the disease-free equilibrium P_0 is locally asymptotically stable within the feasible domain; instead, when $R_0 > 1$, P_0 is unstable within the feasible domain.

Proof. The Jacobian matrix of the Model I at the disease-free equilibrium P_0 is

$$J(P_0)_{4\Delta\times 4\Delta} = \begin{pmatrix} J_{11} & \cdots & J_{1\Delta} \\ \vdots & \ddots & \vdots \\ J_{\Delta 1} & \cdots & J_{\Delta\Delta} \end{pmatrix} \quad (7)$$

The characteristic polynomial associated with the matrix is:

$$\begin{aligned} &(\lambda+\mu)^{\Delta} \cdot (\lambda+\mu_1)^{\Delta} \cdot (\lambda+\psi+\mu)^{\Delta\text{-}1} \cdot (\lambda+\omega+\mu)^{\Delta\text{-}1} \\ &\times[(\lambda+\psi+\mu)(\lambda+\omega+\mu) \text{ - } \frac{\psi\beta dN^p}{\mu < k >} \sum_{k=1}^{\Delta} k^2 P(k)] = 0 \end{aligned} \quad (8)$$

In Eq. (8), there exist Δ repeated characteristic roots $-\mu < 0$ and $-\mu_1 < 0$, $(\Delta - 1)$ repeated characteristic roots $-\psi - \mu < 0$ and $-\omega - \mu < 0$, and two characteristic roots in the equation:

$$(\lambda + \psi + \mu)(\lambda + \omega + \mu) - \frac{\psi\beta dN^p}{\mu < k >} \times \sum_{k=1}^{\Delta} k^2 P(k) = 0$$

Let $a = \psi + \mu, b = \omega + \mu, m = \frac{\psi\beta dN^p}{\mu < k >} \sum_{k=1}^{\Delta} k^2 P(k)$, then the equation can be reformulated as $(\lambda + a)(\lambda + b) - m = 0$, and its characteristic root can be calculated for $\lambda = \frac{-(a+b) \pm \sqrt{(a+b)^2 - 4(ab - m)}}{2 \times 1}$. Where $\lambda_1 < 0$, $\lambda_2 = \frac{-(a+b) + \sqrt{(a+b)^2 - 4(ab - m)}}{2 \times 1}$. According to $R_0 < 1$, it can be calculated that $\lambda_2 < 0$. Thus, when $R_0 < 1$, the disease-free equilibrium P_0 of Model I is locally asymptotically stable, when $R_0 > 1$, $\lambda_2 > 0$, the disease-free equilibrium P_0 is unstable.

B.Global Stability of Disease-Free Equilibrium

Lemma 2. When $R_0 < 1$, the disease-free equilibrium P_0 is globally asymptotically stable within the feasible domain; instead, when $R_0 > 1$, P_0 is unstable in the feasible domain.

Proof. Create the subsequent Lyapunov function [27]:

$$L(A_k^p, I_k^p) = \psi A_k^p + (\xi k\Theta^h + \psi + \mu) I_k^p \tag{9}$$

According to Model I, the full derivative of $L(A_k^p, I_k^p)$ is

$$\begin{aligned}
L' &= \psi(\beta k S_k^p \Theta^p - \xi k A_k^p \Theta^h - \psi A_k^p - \mu A_k^p) \\
&\quad + (\xi k\Theta^h + \psi + \mu)(\psi A_k^p - \omega I_k^p - \mu I_k^p - \xi k I_k^p \Theta^h) \\
&= \psi[\beta k S_k^p \Theta^p - (\xi k\Theta^h + \psi + \mu) A_k^p] \\
&\quad + (\xi k\Theta^h + \psi + \mu)[\psi A_k^p - (\omega + \mu + \xi k\Theta^h) I_k^p] \\
&= \psi\beta k S_k^p \Theta^p - (\xi k\Theta^h + \psi + \mu)(\omega + \mu + \xi k\Theta^h) I_k^p \\
&\leq \psi\beta k S_k^p \Theta^p - (\psi + \mu)(\omega + \mu) I_k^p \\
&= \psi\beta k \frac{dN^p}{\mu < k >} \sum_{k=1}^{\Delta} k P(k) I_k^p - (\psi + \mu)(\omega + \mu) I_k^p \\
&= [\frac{\psi\beta}{(\psi + \mu)(\omega + \mu)} \frac{dN^p}{\mu < k >} \sum_{k=1}^{\Delta} k^2 P(k) I_k^p - 1] I_k^p \\
&= (R_0 - 1) I_k^p < 0
\end{aligned} \tag{10}$$

We can compute $L' < 0$ when $R_0 < 1$. By the $Lasalle$ invariant principle, we demonstrate Lemma 2.

C.Existence of Endemic Equilibrium

We solve the endemic equilibrium P^* by the following differential equation:

$$\begin{cases}
dN_k^p - \beta k S_{*k}^p \Theta^p - \xi k S_{*k}^p \Theta^h - \mu S_{*k}^p = 0 \\
\beta k S_{*k}^p \Theta^p - \xi k A_{*k}^p \Theta^h - \psi A_{*k}^p - \mu A_{*k}^p = 0 \\
\psi A_{*k}^p - \omega I_{*k}^p - \xi k I_{*k}^p \Theta^h - \mu I_{*k}^p = 0 \\
\gamma k(\frac{d_1 N_k^h}{\mu_1} - I_{*k}^h)\Theta^p - \mu_1 I_{*k}^h = 0
\end{cases} \tag{11}$$

Assuming Θ^h and Θ^p to be constants, the endemic equilibrium P^* of Model I is

$$P^* = (S_{*k}^p, A_{*k}^p, I_{*k}^p, I_{*k}^h)^T \tag{12}$$

The calculation results are as follows:

$$\begin{cases}
S_{*k}^p = \dfrac{dN^p}{\beta k\Theta_*^p + \xi k\Theta_*^h + \mu} \\
A_{*k}^p = \dfrac{dN^p \beta k\Theta_*^p}{(\xi k\Theta_*^h + \psi + \mu)(\beta k\Theta_*^p + \xi k\Theta_*^h + \mu)} \\
I_{*k}^p = \dfrac{dN^p \beta k\psi\Theta_*^p}{(\omega + \mu + \xi k\Theta_*^h)(\xi k\Theta_*^h + \psi + \mu)} \\
\qquad \times \dfrac{1}{(\beta k\Theta_*^p + \xi k\Theta_*^h + \mu)} \\
R_{*k}^p = \dfrac{\xi k\Theta_*^h (S_{*k}^p + A_{*k}^p + I_{*k}^p) + \omega I_{*k}^p}{\mu} \\
I_{*k}^h = \dfrac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k\Theta_*^p + \mu_1)}
\end{cases}$$

Using Eq. (1), (2), we can calculate as follows:

$$\begin{aligned}
\Theta_*^h &= \frac{1}{< k >} \sum_{k=1}^{\Delta} k P(k) I_k^h \\
&= \frac{1}{< k >} \sum_{k=1}^{\Delta} k P(k) \frac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k\Theta_*^p + \mu_1)}
\end{aligned} \tag{13}$$

$$\begin{aligned}
\Theta_*^p &= \frac{1}{< k >} \sum_{k=1}^{\Delta} k P(k) I_k^p \\
&= \frac{1}{< k >} \sum_{k=1}^{\Delta} k P(k) \times \frac{dN^p \beta k\psi\Theta_*^p}{(\omega + \mu + \xi k\Theta_*^h)} \times \\
&\quad \frac{1}{(\xi k\Theta_*^h + \psi + \mu)(\beta k\Theta_*^p + \xi k\Theta_*^h + \mu)} \\
&= \frac{1}{< k >} \sum_{k=1}^{\Delta} k P(k) \frac{dN^p \beta k\psi\Theta_*^p}{H(\Theta_*^p)}
\end{aligned} \tag{14}$$

Let $H(\Theta_*^p) = (\omega + \mu + \xi k\Theta_*^h)(\xi k\Theta_*^h + \psi + \mu)(\beta k\Theta_*^p + \xi \times k\Theta_*^h + \mu)$. According to Eq. (14), We can obtain:

$$H(\Theta_*^p) = (\omega + \mu + \xi k \frac{1}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k \Theta_*^p + \mu_1)}) \times (\frac{\xi k}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k \Theta_*^p + \mu_1)} + \psi + \mu) \times (\beta k \Theta_*^p + \xi k \frac{1}{< k >} \times \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k \Theta_*^p + \mu_1)} + \mu)$$

Next, we generate the self-consistent equation $f(\Theta_*^p)$.

$$f(\Theta_*^p) = \frac{1}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{dN^p \beta k \psi \Theta_*^p}{H(\Theta_*^p)} \tag{15}$$

If there exists a unique nontrivial solution to the equation, it must satisfy the following condition:

$$\left. \frac{df(\Theta_*^p)}{d\Theta_*^p} \right|_{\Theta_*^p = 0} > 1$$

$$\frac{df(\Theta_*^p)}{d\Theta_*^p} = \frac{1}{< k >} \sum_{k=1}^{\Delta} kP(k) \cdot \frac{dN^p \beta k \psi [H(\Theta_*^p) - \Theta_*^p \times H'(\Theta_*^p)]}{H(\Theta_*^p)^2} \tag{16}$$

Let

$$c = (\omega + \mu + \xi k \frac{1}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k \Theta_*^p + \mu_1)})$$

$$e = (\xi k \frac{1}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k \Theta_*^p + \mu_1)} + \psi + \mu)$$

$$g = (\beta k \Theta_*^p + \frac{\xi k}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h \Theta_*^p}{\mu_1(\gamma k \Theta_*^p + \mu_1)} + \mu)$$

We can calculate as follows:

$$H'(\Theta_*^p) = \frac{e \cdot g \cdot \xi k}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h}{\mu_1} \frac{\mu_1}{(\gamma k \Theta_*^p + \mu_1)^2} + \frac{c \cdot g \cdot \xi k}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h}{\mu_1} \frac{\mu_1}{(\gamma k \Theta_*^p + \mu_1)^2} + c \cdot e \cdot [\beta k + \frac{\xi k}{< k >} \sum_{k=1}^{\Delta} kP(k) \frac{\gamma k d_1 N^h \mu_1}{\mu_1(\gamma k \Theta_*^p + \mu_1)^2}] \tag{17}$$

According to $\left. \frac{df(\Theta_*^p)}{d\Theta_*^p} \right|_{\Theta_*^p = 0} = R_0$, it can be shown that at that time $R_0 > 1$, and there is $\left. \frac{df(\Theta_*^p)}{d\Theta_*^p} \right|_{\Theta_*^p = 0} > 1$. As a result, there is one positive endemic equilibrium P^* for Model I.

V. Simulation Results

We perform the numerical simulation with a given scale-free network, assuming all system parameters are constant. Considering a total of 10,000 nodes in the network, the experiment is conducted in a scale-free network following a power-law distribution with an exponent of 2.17 and a maximum node degree of 300. The average degree of this network is calculated to be 5.99. We keep the basic parameters for the following experiments unchanged: set $\beta = 0.2$, $\psi = 0.35$, $\omega = 0.15$, $d = 0.00015$, $\mu = 0.00015$, $\gamma = 0.4$, $\xi = 0.001$, $d_1 = 0.0025$, and $\mu_1 = 0.0025$. Additionally, select 10 initial infected nodes and 50 initial honeypot nodes.

A. Comparison of Different Models

In this paper, we propose the H-SAIR model, which builds upon the aforementioned literature [24] and further describes the stages of virus infection by incorporating the affected state (*A*). Consider the ability of honeypots to capture viruses and their mechanism for feedback immune information. The study [24] investigated the compartmental modeling of viral spread and honeypot interaction. Based on the literature, we create the H-SIR model and specify it as Model II, using the following differential equation:

$$\begin{cases} \frac{dS_k^p}{dt} = dN_k^p - \beta k S_k^p \Theta^p - \xi S_k^p \Theta^h - \mu S_k^p \\ \frac{dI_k^p}{dt} = \beta k S_k^p \Theta^p - \omega I_k^p - \mu I_k^p \\ \frac{dI_k^h}{dt} = \gamma k (\frac{d_1 N_k^h}{\mu_1} - I_k^h) \Theta^p - \mu_1 I_k^h (k = 1 \ldots \Delta) \end{cases} \tag{18}$$

The propagation threshold $R_0 = 0.1139 < 1$ for both Model I and Model II. Model II only considers the immune feedback of honeypots on susceptible nodes in the network, ignoring the affected state in the pre-infection stage and missing the global prevention process.

Figs. 3 and 4 show the evolution of different state nodes over time in Model II, while Figs. 5 and 6 depict the evolution of different state nodes over time in Model I. Both models exhibit similar overall trends in worm propagation; in the early stages of the system, the virus continuously scans and attacks, infecting honeypots and susceptible nodes in a short period of time.

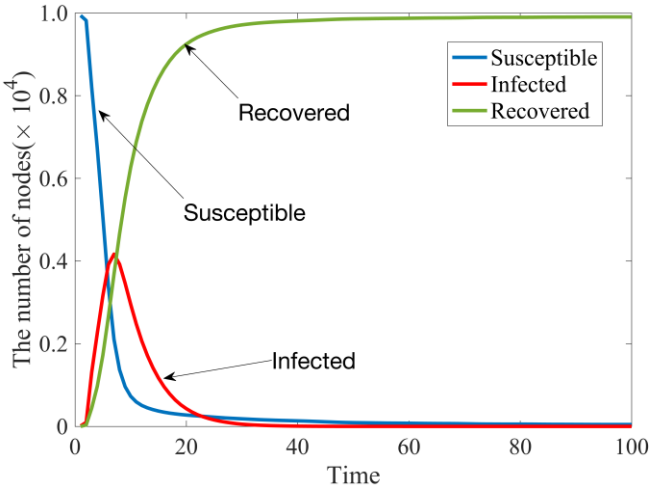

Fig. 3. Evolution of the H-SIR model's system

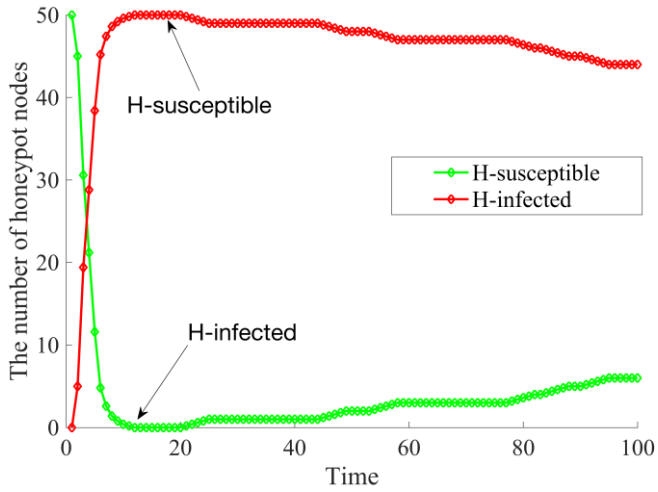

Fig. 4. Honeypot evolution over time in the H-SIR model

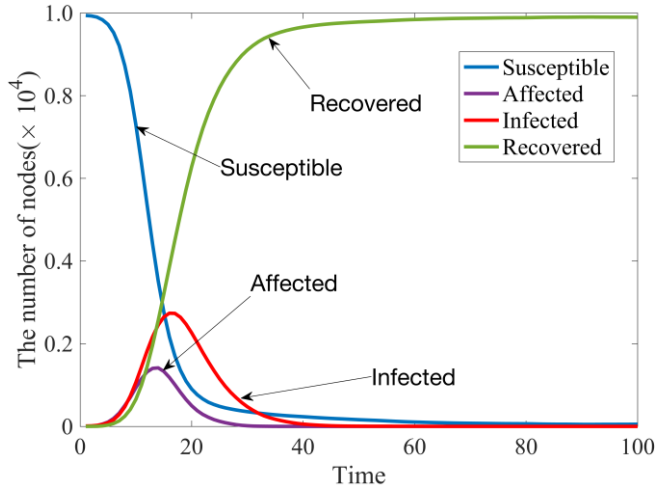

Fig. 5. Evolution of the H-SAIR model's system

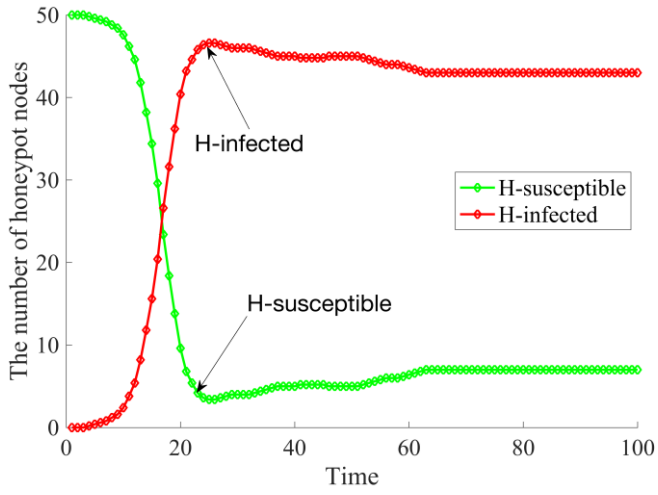

Fig. 6. Honeypot evolution over time in the H-SAIR model

The trend of the curve in the figure indicates that the number of infected nodes increases rapidly in the early stages. Subsequently, the honeypot-infected nodes interact with common nodes, providing feedback on immune information, thus achieving an early immune effect. After reaching its peak, the number of infected nodes gradually decreases until it tends to zero. When compared to Fig. 3, the peak of infected nodes in Fig. 5 decreases by 34.39%. Additionally, compared to Fig. 4, the honeypot utilization in Fig. 6 has also decreased. It can be observed that the immunization of the global by H-SAIR model can effectively reduce the number of virus-infected nodes while reducing the consumption of honeypot resources. Compared to Model II, the H-SAIR model proposed in this paper can better control the spread of the virus in the pre-infection stage.

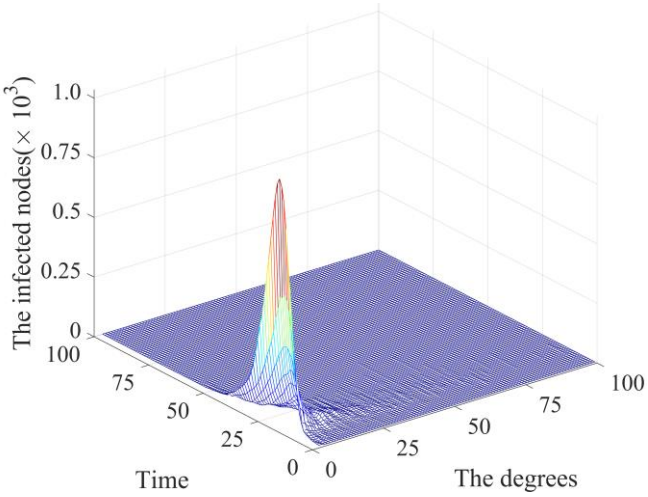

Fig. 7. The number of infected nodes versus degree and time

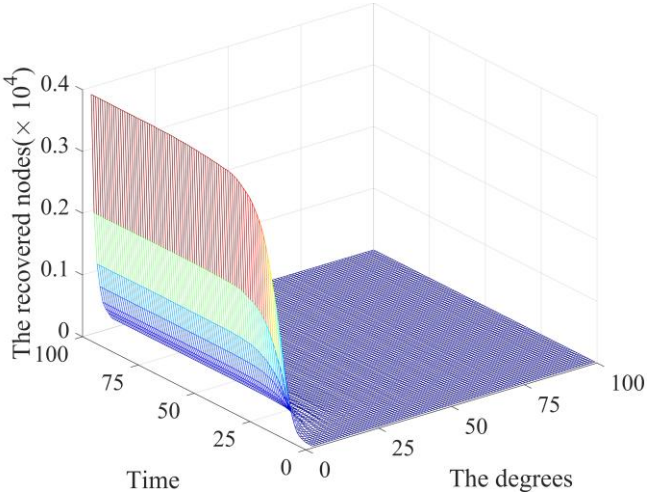

Fig. 8. The number of recovered nodes versus degree and time

Figs. 7 and 8 depict the relationship between the number of infected and recovered nodes and the degree of nodes in the network (k) and time (t), respectively. The infected nodes are primarily those with lower degrees, consistent with the characteristics of power-law distribution in the scale-free network. Over time, the worm will ultimately disappear, leading to a stable equilibrium within the system, thus verifying Lemma 1.

B.Comparison of Parameters

This section examines the impact of important parameters (β, γ, ξ) on infected nodes over time and provides the corresponding defense measures.

1)Parameter β

To study the effect of infection rate β on viral propagation, Fig. 9 shows the variation of the number of infected nodes over time with values of 0.2, 0.4, and 0.6.

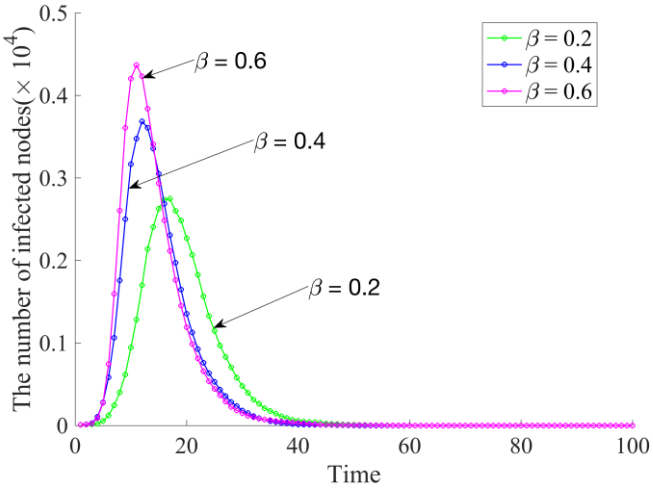

Fig. 9. The number of infected nodes over time at different β

Fig. 9 shows that a lower worm infection rate β is associated with a reduced number of nodes in the infected condition and an earlier peak time. Compared to the values of β being 0.4 and 0.6, setting the parameter β to 0.2 results in a decrease of 25.39% and 37.05% in the peak number of infected nodes.

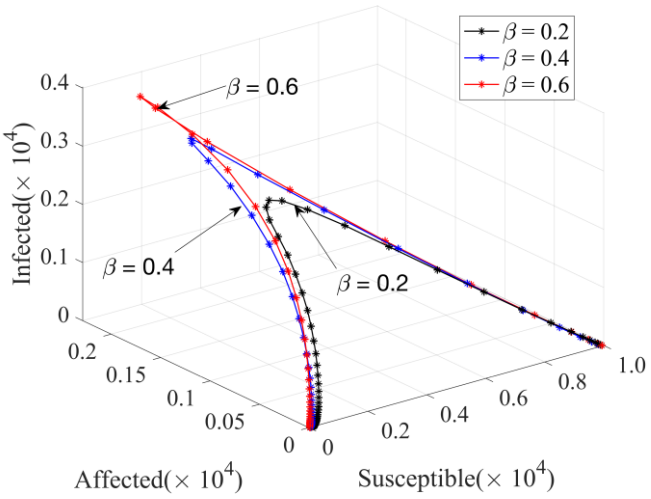

Fig. 10. Phase diagram of (S, A, I) at different β

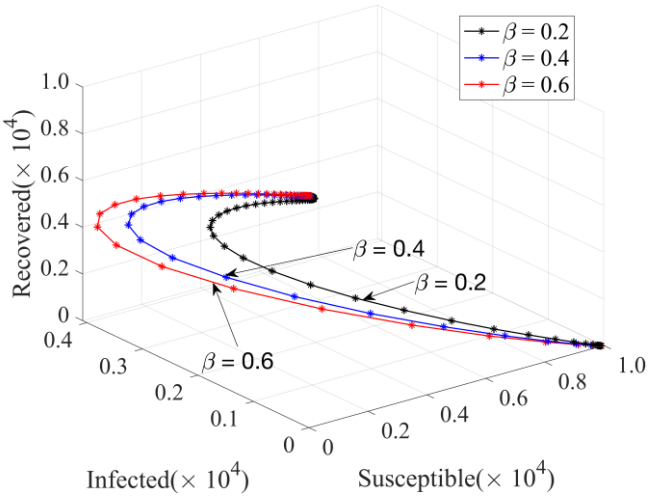

Fig. 11. Phase diagram of (S, I, R) at different β

Figs. 10 and 11 illustrate the phase diagrams for (Susceptible, Affected, Infected) and (Susceptible, Infected, Recovered) at different values of the parameter β, respectively. Despite the varying values of parameter β, the basic regeneration number follows to $R_0 < 1$.

For this reason, using an Intrusion Detection System (IDS) to detect known worm signatures, using a firewall to block unnecessary traffic, and implementing Distributed Denial of Service (DDoS) protection can effectively reduce the infection rate β. These measures can enhance network resilience and prevent worms' propagation.

2)Parameter γ

Fig. 12 shows the variation of the number of infected nodes over time when the honeypot infection rate γ takes values of 0.1, 0.4, and 0.9. The values of the γ are different, but the basic regeneration number $R_0 < 1$ remains constant. Fig. 12 indicates that as the honeypot infection rate γ increases, the number of infected nodes reaches a smaller peak. This suggests that honeypots are more effective in luring worms, and due to the virus prioritizing attacking them, they can better control the spread of the virus.

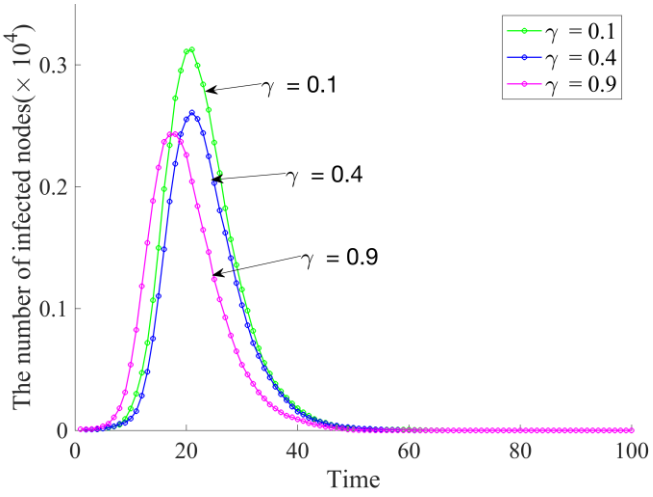

Fig. 12. The number of infected nodes over time at different γ

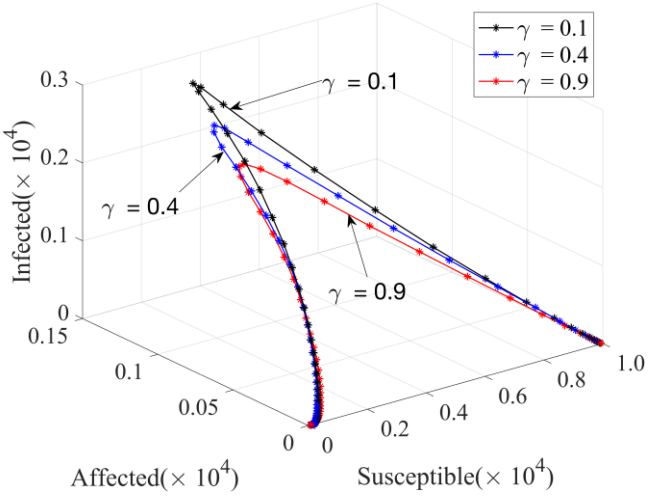

Fig. 13. Phase diagram of (S, A, I) at different γ

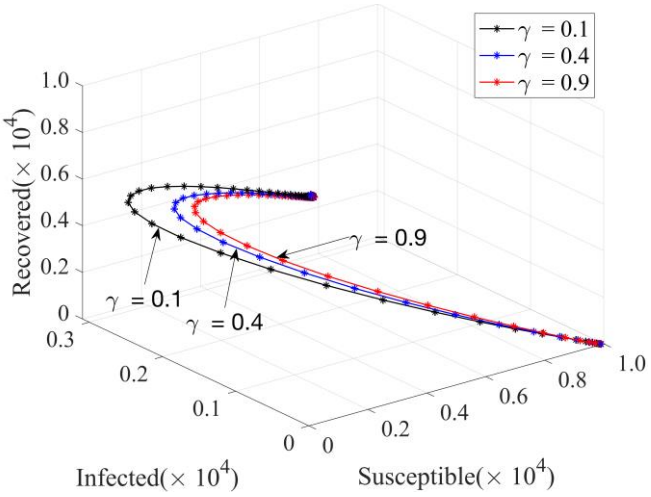

Fig. 14. Phase diagram of (S, I, R) at different γ

Figs. 13 and 14 show the phase diagrams for (Susceptible, Affected, Infected) and (Susceptible, Infected, Recovered) at different values of parameter γ. The number of infected nodes decreases with the increase of parameter γ.

Therefore, increasing the honeypot infection rate γ can control the spread of worms. If necessary, honeypots can replicate real environments, implement popular services and applications, and utilize public IP addresses, thereby enhancing the likelihood of the honeypot becoming targeted.

3)Parameter ξ

In this paper, we propose a honeypot feedback mechanism, in which the honeypot feeds back immune information to the common nodes after capturing worms successfully. Fig. 15 shows the variation of the number of infected nodes over time when the feedback rate ξ takes values of 0, 0.001, 0.003, and 0.005. Figs. 16 and 17 show the phase diagrams for (Susceptible, Affected, Infected) and (Affected, Infected, Recovered) at different values of ξ, respectively. At this point, the basic regeneration number $R_0 < 1$.

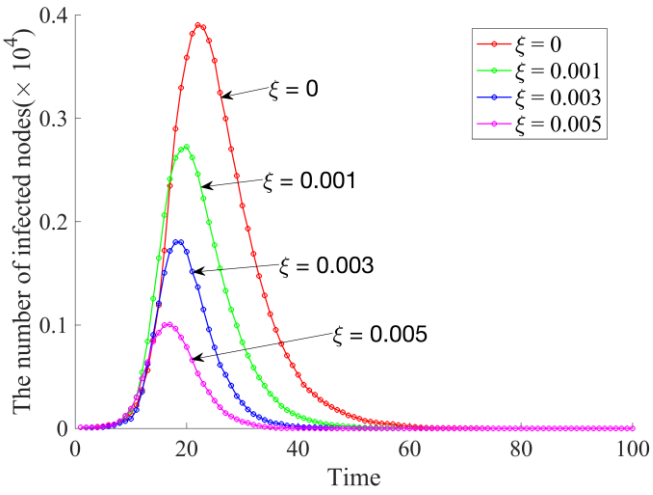

Fig. 15. The number of infected nodes over time at different ξ

As shown in Fig. 15, if $\xi = 0$, the honeypot will not communicate with common nodes and cannot provide immune information. If it only improves its own anti-virus capabilities, it cannot effectively inhibit virus propagation.

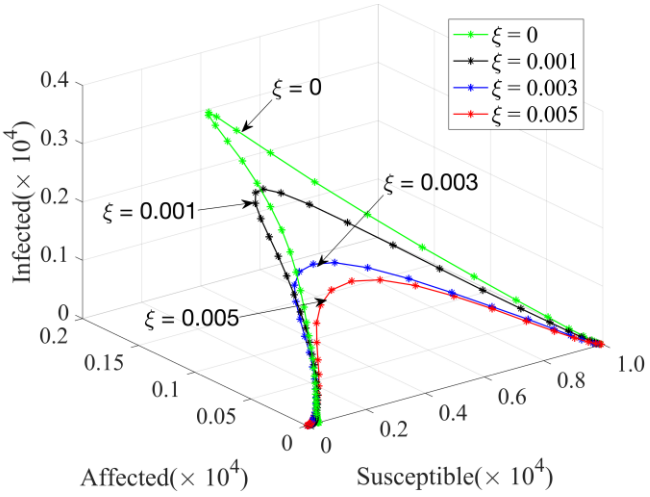

Fig. 16. Phase diagram of (S, A, I) at different ξ

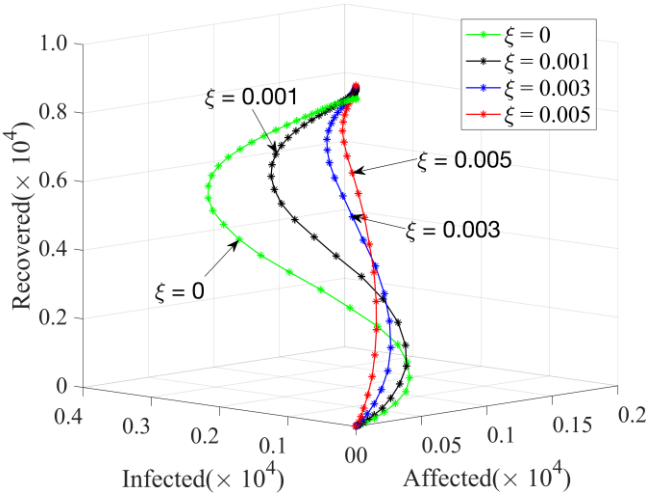

Fig. 17. Phase diagram of (A, I, R) at different ξ

As can be seen from the above graphs, with the increase of the feedback rate ξ, on the one hand, the number of infected nodes can decrease earlier and faster until it tends to zero; on the other hand, the peak of infected nodes is much smaller than when $\xi = 0$. Compared to $\xi = 0$, regardless of the feedback rate ξ, the network can reach a stable state more quickly. Therefore, increasing the feedback rate ξ can enhance the overall immunity of the system, which plays a crucial role in containing the spread of worm propagation in the network.

The experimental results indicate that (β, γ, ξ) significantly influences the spread of worms. The number of infected nodes is directly related to the infection rate β and inversely related to the honeypot infection rate γ and feedback rate ξ. Consequently, it is necessary to enhance the network's virus resistance capability while increasing the attractiveness of honeypots to viruses. Additionally, improving the mechanism for honeypot feedback on immune information is crucial.

C.Comparison of Honeypot Deployments

Since the degrees of nodes in a scale-free network follow a power-law distribution. If a worm launches an attack on the hub nodes, the network will be highly vulnerable. Next, we

deploy the honeypots at different locations within the scale-free network with an initial number of 0, 50, and 100 nodes.

Fig. 18 shows the variation of infected nodes when the honeypot deployment location is randomly selected. Figs. 19 and 20 show the phase diagrams for (Susceptible, Infected, H-infected) and (Affected, Infected, H-infected), respectively. In the following, honeypot-infected will be referred to simply as H-infected.

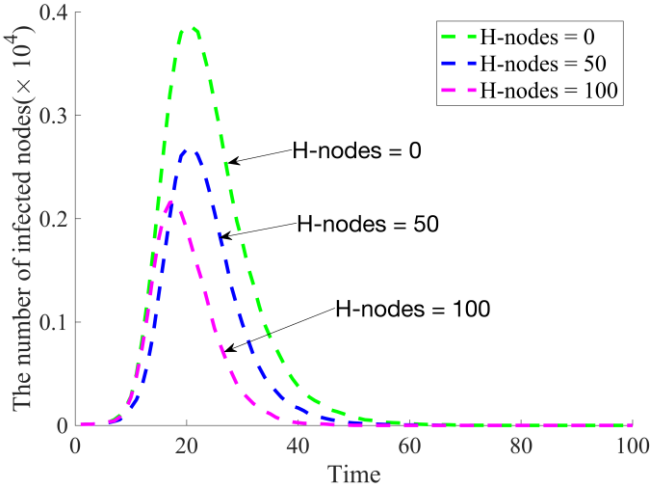

Fig. 18. Number of infected nodes over time at random locations

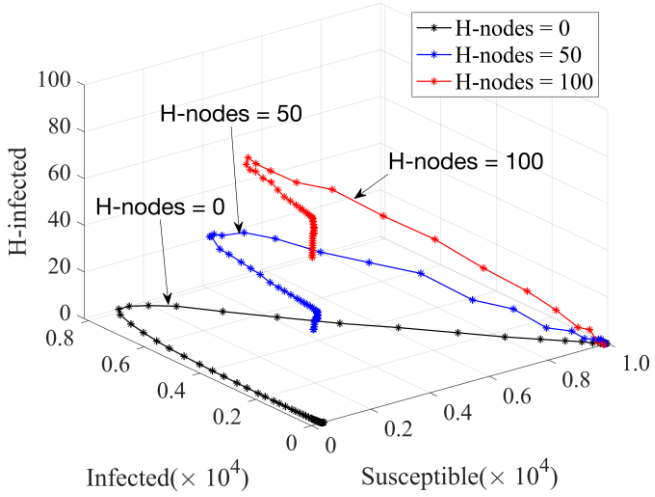

Fig. 19. Phase diagram of (S, I, H-infected) at random locations

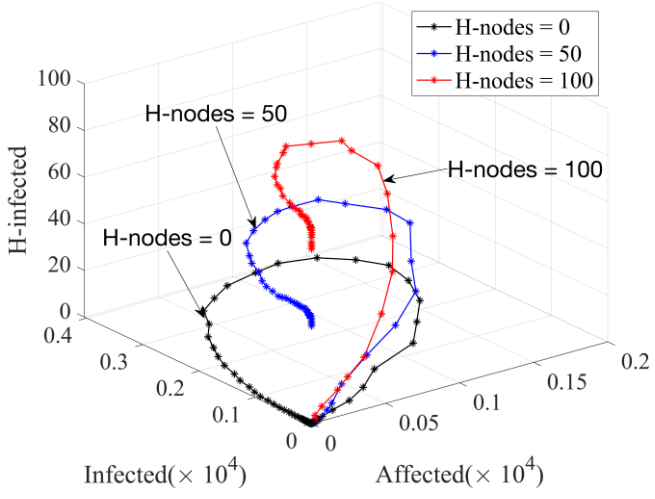

Fig. 20. Phase diagram of (A, I, H-infected) at random locations

Fig. 21 shows the variation of infected nodes when the honeypot is deployed at the hub location. Figs. 22 and 23 show the phase diagrams for (Susceptible, Infected, H-infected) and (Affected, Infected, H-infected), respectively.

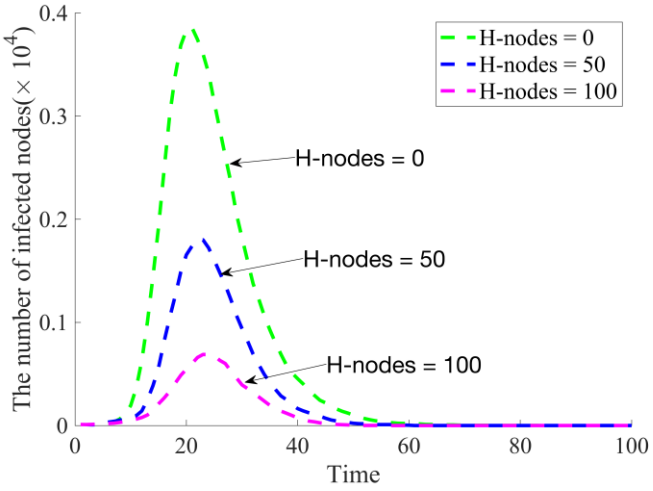

Fig. 21. Number of infected nodes over time at hub locations

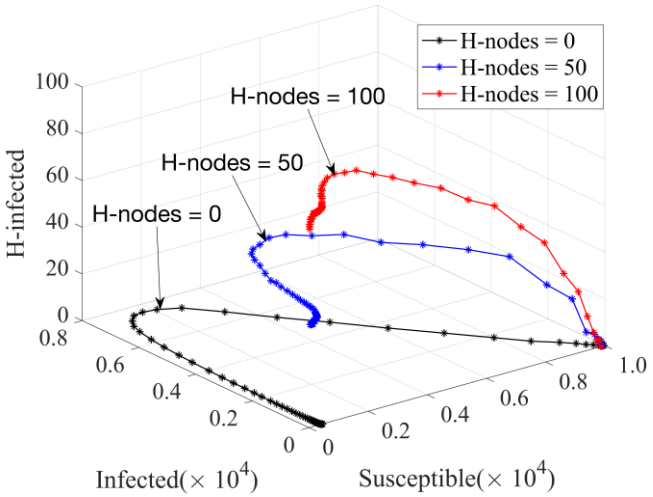

Fig. 22. Phase diagram of (S, I, H-infected) at hub locations

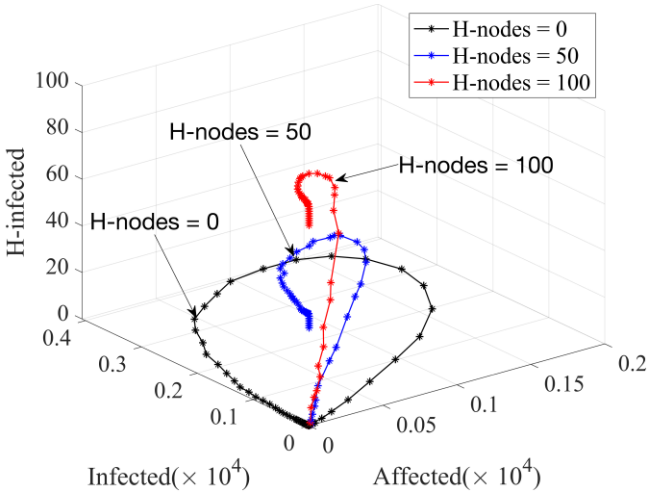

Fig. 23. Phase diagram of (A, I, H-infected) at hub locations

Figs. 18 and 21 indicate that increasing the number of deployed honeypots can reduce the number of infected nodes and control the spread of the virus, compared to the state

without any deployed honeypots (H-nodes=0) in the network. Comparing Fig. 18 with Fig. 21, it is observed that when the total number of honeypots remains constant, honeypots deployed in hub positions perform better in terms of trapping and feedback. Regardless of whether the number of honeypots is 50 or 100, deploying them in hub locations results in a lower peak of infected nodes compared to random locations.

The above experimental results show that the location and number of deployed honeypots are crucial in controlling the spread of worms. Therefore, if the capital and labor costs permit, it is important to deploy a sufficient number of honeypots in central and hotspot locations within a network. In the meantime, the honeypots should play the role of feeding back immune information to effectively enhance the network's security defenses.

D.Further Discussion

On the basis of experiment b above, we further discuss the interaction between the parameters through sensitivity analysis. It is easy to know that R_0 and I_*^p are affected by the infection rate β, the removal rate ω, the honeypot infection rate γ, and the feedback rate ξ. Therefore, the partial derivatives of the infected node I_*^p are obtained, respectively. As we know:

$$\begin{aligned} I_*^p &= \sum_{k=1}^{\Delta} I_{*k}^p(t) \\ &= \sum_{k=1}^{\Delta} \frac{dN^p \beta k \psi \Theta_*^p}{(\omega+\mu+\xi k\Theta_*^h)(\psi+\mu+\xi k\Theta_*^h)} \\ &\times \frac{1}{(\mu+\beta k\Theta_*^p+\xi k\Theta_*^h)} \end{aligned} \tag{19}$$

Let $n = dN^p k\psi\Theta_*^p$, $x = \omega+\mu+\xi k\Theta_*^h$, $y = \psi+\mu+\xi k\Theta_*^h$, $z = \mu+\beta k\Theta_*^p+\xi k\Theta_*^h$, and combine Eq. (13), we can obtain:

$$\frac{\partial I_*^p}{\partial \beta} = \sum_{k=1}^{\Delta} \frac{n\cdot(\xi k\Theta_*^h+\mu)}{x\cdot y\cdot z^2} > 0$$

$$\frac{\partial I_*^p}{\partial \omega} = -\sum_{k=1}^{\Delta} \frac{n\cdot\beta}{x^2\cdot y\cdot z} < 0$$

$$\frac{\partial I_*^p}{\partial \xi} = -\sum_{k=1}^{\Delta} \frac{n\cdot\beta k\Theta_*^p(yz+xz+xy)}{x^2\cdot y^2\cdot z^2} < 0$$

$$\frac{\partial I_*^p}{\partial \Theta_*^h} = -\sum_{k=1}^{\Delta} \frac{n\cdot\beta\xi k(yz+xz+xy)}{x^2\cdot y^2\cdot z^2} < 0$$

$$\frac{\partial \Theta_*^h}{\partial \gamma} = \frac{1}{<k>}\sum_{k=1}^{\Delta} kP(k)\frac{kd_1N^h\Theta_*^p}{(\gamma k\Theta_*^p+\mu_1)^2} > 0$$

According to $\frac{\partial I_*^p}{\partial \gamma} = \frac{\partial I_*^p}{\partial \Theta_*^h}\times\frac{\partial \Theta_*^h}{\partial \gamma}$, $\frac{\partial I_*^p}{\partial \gamma} < 0$. It can be inferred that the number of infected nodes in virus propagation increases monotonically with parameter β, and decreases monotonically with parameters ω, γ, and ξ.

Fig. 24 shows the sensitivity surface of infection rate β, removal rate ω, and the peak of infected nodes. As the infection rate β increases, the peak of infected nodes also increases. On the contrary, as the removal rate of ω increases, the peak of infected nodes gradually decreases.

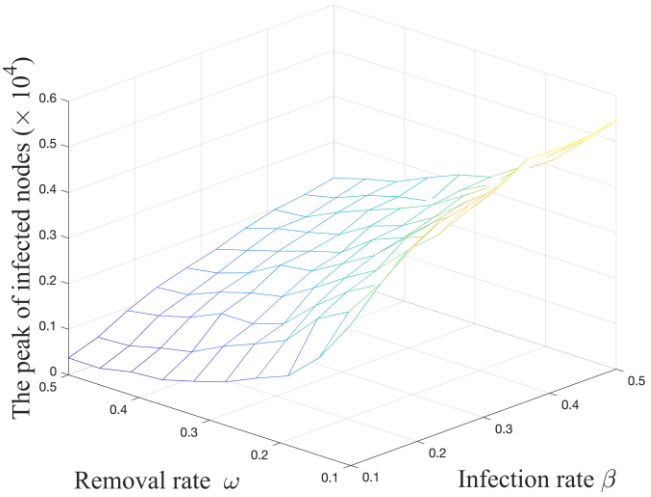

Fig. 24. Sensitivity surface of β, ω and the peak of infected nodes

Fig. 25 shows the sensitivity surface of honeypot infection rate γ, feedback rate ξ, and infection nodes peak. It can be seen that with the increase of the honeypot infection rate γ, the peak of infected nodes decreases. Similarly, as the feedback rate ξ increases, the peak of infected nodes decreases.

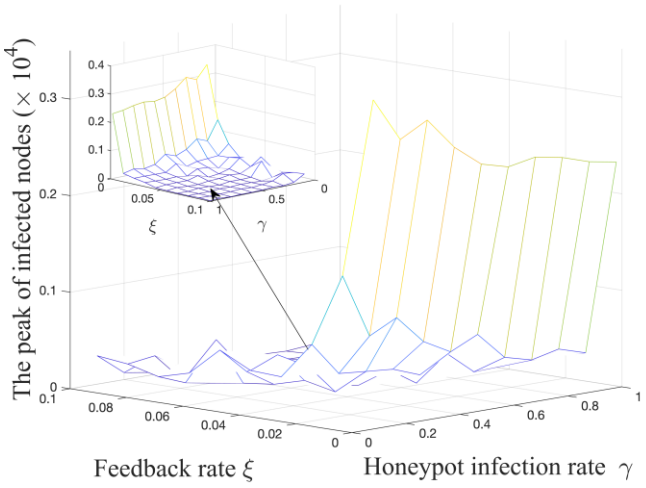

Fig. 25. Sensitivity surface of γ, ξ and the peak of infected nodes

Therefore, it is crucial to reduce the infection rate while improving the removal rate, honeypot infection rate, and feedback rate in order to control the spread of worms. For instance, running an older or vulnerable operating system on honeypots, installing known vulnerabilities, using weak passwords, or storing sensitive data. Additionally, depending on the severity of the threat, the most important immunization information should be fed back first, which can effectively control the scale of the spread of worms.

VI. Conclusion

This paper introduces a feedback mechanism based on the honeypot-captured worms and proposes a new model, named H-SAIR. The honeypot can proactively identify potential risks and transmit immune information to common nodes, effectively preventing worm propagation. We analyze the stability of the equilibrium points and demonstrate the feasibility of the H-SAIR model.

We simulate the propagation model of worms under the honeypot feedback mechanism using MATLAB, and analyze the influence of critical parameters (β , γ , ξ) on the number of infected nodes. Compared with the original H-SIR model, the H-SAIR model proposed in this paper can better control the virus transmission. Additionally, we simulate the deployment locations and quantities of honeypots in the network. The results indicate that in a scale-free network, appropriately deploying a sufficient number of honeypots at hub locations can significantly inhibit virus spread, thereby enhancing network security.

Deploying numerous honeypot servers on the actual network necessitates consideration of various issues, including capital expenditure, labor costs, network bandwidth, and security risks. The paper primarily discusses theoretical proofs and simulations to validate the effectiveness of honeypot defenses against worms. As a result, in the next step, we will conduct a further examination of the practical utility of honeypots in real networks, aiming to derive findings that accurately reflect the actual circumstances.

References

[1] Y. Wang, S. Wen, Y. Xiang, W. Zhou, "Modeling the Propagation of Worms in Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 942-960, 2014.

[2] ChukwuNonso H. Nwokoye, Ikechukwu I. Umeh, Njideka N. Mbeledogu, and Vincent O. S. Okeke, "Scan-Based Worms: The Impact of IPV4 Address Space on Epidemic Computer Network Models," *Engineering Letters*, vol. 29, no.2, pp611-623, 2021.

[3] M. Jingyi, "Network worm prevention countermeasure discussion," *Computer Programming Skills & Maintenance*, no. 4, pp. 168-169+175, 2020.

[4] W. Dongfang, J. Jie, "Big Data Era of Computer Network Information Security and Protection Strategy Study," *Wireless Internet Science and Technology*, vol. 24, pp. 40-41, 2015.

[5] Z. Dongyu, H. Fujun, C. Jun, "Robustness analysis of power system based on a complex network," *Power System Protection and Control*, vol. 49, no. 1, pp. 72-80, 2021.

[6] M.-K. Awais, J. Nadeem, "Computationally efficient topology optimization of scale-free IoT networks," *Computer Communications*, vol. 185, no. 1, pp. 1-12, 2022.

[7] X. Chunxia, J. Guoping, X. Lingling, "Propagation Model of Email Worm-virus Based on Heterogeneous Networks," *Computer Technology and Development*, vol. 26, no. 1, pp. 90-96, 2016.

[8] G. Zhihong, Q. Yujuan, J. Xiaowei, "Virus propagation dynamic model and stability on complex networks," *Journal of Huazhong University of Science and Technology(Natural Science Edition)*, vol. 39, no. 1, pp. 114-117, 2011.

[9] Wenxiao Yin, Benzhen Guo, Hailong Hu, Yanhong Hu, and Qiang Li, "The Research on WSNs Scale-free Topology for Prolonging Network Lifetime," *Engineering Letters*, vol. 29, no.1, pp238-243, 2021.

[10] J. Zhaopeng, F. Binxing, L. Chaoge, L. Qixu, L. Jianbao, "Survey on cyber deception," *Journal on Communications*, vol. 38, no. 12, pp. 128-143, 2017.

[11] S. Leyi, L. Yang, M. Mengfei, "Latest Research Progress of Honeypot Technology," *Journal of Electronics & Information Technology*, vol. 41, no. 2, pp. 498-508, 2019.

[12] Jian Ding, Tao Zhao, Zhigang Liu, and Qiong Guo, "Stability and Bifurcation Analysis of A Delayed Worm Propagation Model in Mobile Internet," *IAENG International Journal of Computer Science*, vol. 47, no.3, pp533-539, 2020.

[13] J.-S. Valdez, P. Guevara, J. Audelo, G. Delgado, "Numerical Approaching of SIR Epidemic Model for Propagation of Computer Worms," *IEEE Latin America Transactions*, vol. 13, no. 10, pp. 3452-3460, 2015.

[14] R. Wang, Y. Xue, "Stability analysis and optimal control of worm propagation model with saturated incidence rate," *Computers & Security*, vol. 125, p. 103063, 2013.

[15] W. Gang, L. Shiwei, H. Xin, "Network virus spreading SEIORS model and its stability under escape mechanism," *Journal of Harbin Institute of Technology*, vol. 51, no. 5, pp. 131-137, 2019.

[16] C. Gan, X. Yang, W. Liu, Q. Zhu, "A propagation model of computer virus with nonlinear vaccination probability," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 92-100, 2014.

[17] K.-S. Kim, M.-M. Ibrahim, I.-H. Jung, S. Kim, "Mathematical analysis of the effectiveness of control strategies to prevent the autorun virus transmission propagation," *Applied Mathematics and Computation*, vol. 371, p. 124955, 2020.

[18] X. Xiao, P. Fu, C. Dou, Q. Li, G. Hu, S. Xia, "Design and analysis of SEIQR worm propagation model in mobile internet," *Communications in Nonlinear Science and Numerical Simulation*, vol. 43, pp. 341-350, 2017.

[19] N.-P. Dong, H.-V. Long, N.-T.-K. Son, "The dynamical behaviors of fractional-order SE1E2IQR epidemic model for malware propagation on Wireless Sensor Network," *Communications in Nonlinear Science and Numerical Simulation*, vol. 11, p. 106428, 2022.

[20] Q. Yujie, "Ransom worm virus monitoring method based on distributed honeypot technology," *Cyber Security And Data Governance*, vol. 37, no. 9, pp. 45-48, 2018.

[21] H. Yizhao, W. Zhen, A. Li, "Design and Realization of a Virtual Honeynet System," *Computer Engineering & Science*, vol. 31, no. 8, pp. 21-23, 2009.

[22] P.-S. Negi, A. Garg, R. Lal, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2020.

[23] L. Zhengda, Z. Chengsheng, "Design and implementation of honeynet based on honeypot for industrial control system," *Cyber Security And Data Governance*, vol. 39, no. 8, pp. 21-26+32, 2020.

[24] J. Ren, Y. Xu, "A compartmental model to explore the interplay between virus epidemics and honeynet potency," *Applied Mathematical Modelling*, vol. 59, pp. 86-99, 2018.

[25] N. Risa, Z. Xianfeng, "Study of worm propagation model based on distributed honeynet," *Application Research of Computers*, vol. 26, no. 9, pp. 3512-3515, 2009.

[26] Q. Fu, Y. Yao, C. Sheng, W. Yang, "Interplay Between Malware Epidemics and Honeynet Potency in Industrial Control System Network," *IEEE Access*, vol. 8, pp. 81582-81593, 2020.

[27] X. Yuan, Y. Xue, M. Liu, "Global stability of an SIR model with two susceptible groups on complex networks," *Chaos, Solitons & Fractals*, vol. 59, pp. 42-50, 2014.