Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 2851677, 14 pages
https://doi.org/10.1155/2022/2851677

Research Article

Modeling and Analysis in Peer-To-Peer Botnet with Virtual Patching and Quarantine Strategy

Wei Yang,[1] Qiang Fu,[2] Yu Yao,[3,4] and Wei Sun[3]

[1]*Software College, Northeastern University, Shenyang, China*
[2]*College of Computer Science and Technology, Shenyang University of Chemical Technology, Shenyang, China*
[3]*College of Computer Science and Engineering, Northeastern University, Shenyang, China*
[4]*Engineering Research Center of Security Technology of Complex Network System, Ministry of Education, Shenyang, China*

Correspondence should be addressed to Qiang Fu; qiang.fu@outlook.com

Received 11 October 2021; Revised 6 July 2022; Accepted 8 October 2022; Published 29 October 2022

Academic Editor: Abdul Qadeer Khan

Botnets, especially peer-to-peer (P2P) botnets have become the root because of many Internet attacks recently. To effectively suppress P2P botnets, quarantine and virtual patching strategy are proposed and two dynamical models (SIIQR model and SIIQPR model) are given based on the SIIR model. The two models can examine the impact of different containment strategies on the growth of the P2P botnets. In addition, the stability of equilibrium is investigated and the basic reproduction number is obtained, which governs whether or not P2P botnets are extinct. The virtual patching strategy and quarantine strategy can effectively contain the propagation of the P2P botnets. Numerical and simulation results show the effectiveness of our models, larger infected rate, and larger deploying rate of virtual patching can control the number of infected hosts more effectively.

1. Introduction

1.1. Motivation. The peer-to-peer (P2P) botnet is a new generation of self-organizing botnet that has replaced the old centralized IRC/HTTP (Internet Relay Chat/Hyper Text Transfer Protocol)-based botnet to avoid a single point of failure and avoid detection during command and control (C&C) connection [1]. A P2P botnet adopts a decentralized architecture using an overlay network exchanging command and control data between the bot-masters and the bots. A bot-master in P2P botnet recruits new vulnerable hosts (bots) to run malicious software by all kinds of attacking techniques such as Trojan, worms, and virus [2]. A host in P2P botnet can act as a bot-master and a bot, which makes the detection of P2P botnet even more difficult and the effect of P2P botnet more harmful [3, 4]. P2P botnets, such as Peacomm, Storm botnet [5], Waledac botnet [6], Miner botnet [7], Kelihos botnet [8], and Zero Access botnet [9] have emerged and gradually escalated in recent years.

Threats of P2P botnets to the Internet security have drawn widespread attention by researchers. Some traditional epidemic models of infectious diseases were used to describe the propagation of P2P botnet. Kolesnichenko et al. develop the mean-field model to analyse behaviours of P2P botnet and compared it with simulations obtained from the Mobius tool [10]. Sanders et al. develop a stochastic model of P2P botnet to examine how different factors impact the total propagation bots which provides insight on possible defence tactics [11]. Feng et al. use dynamical models to portray the process of formation of P2P botnets in micro- and macro-level and also propose a mathematical model that combines the scale-free trait of Internet with the formation of P2P botnet presented [12, 13]. Even though there are quite a few ways to evade the attacks, there is a crucial need for one which can turn table on attacker by using active approach. Virtual patching is a very suitable solution, and the effect of virtual patching on the P2P botnet also need to be studied.

Virtual patching is a remediation technique using in the network security field. Virtual patching gives a temporary protection for the vulnerable hosts to survive the spanning time of updating the software or releasing the new patching of application. If a vulnerability is identified, the customer

most likely will not be able to modify the source code themselves and have to wait for an official patch to be released, it means that an officially supported patch may not be available for an extended period of time. Virtual patching is the process of creating and implementing a temporary policy that is used to mitigate exploitation risks associated with the discovery of new security vulnerabilities [14]. It eliminates the potential threat of application or system security loopholes being identified and exploited by hackers.

1.2. Related Works. To effectively fight against P2P botnets, some research results achieved mainly on the detection of P2P botnet. Su et al. propose an effective framework by integrating SDN and machine learning to detect and categorize P2P network traffics, which can automatically analyse network traffic and flexibly change flow entries in OpenFlow switches through the SDN controller [15]. Yang and Wang extract the data packet size and the symmetric intervals in flow according to the concept of graphic symmetry. They combine with flow information entropy and session features to detect the P2P botnet and get a high detection accuracy [16]. Dehkordi and Sadeghiyan propose an effective node-removal method against P2P botnets [17]. Xing et al. propose an unstructured P2P botnet detection framework based on SAW community discovery [18]. Zhuang and Chang propose an enhanced PeerHunter, a network-flow level community behaviour analysis based system, to detect P2P botnets [19]. Khan et al. propose a hybrid technique to detect botnets based on P2P traffic similarity [20]. As the development of botnets, P2P botnets are more robust and difficult for security community to defend.

Although most of previous works can offer useful insight into the propagation and detection of the P2P botnet, some of them ignore or fail to discuss the effect of containment strategies to the P2P botnets. In the past decades, some traditional epidemic models of infectious diseases are used to describe the propagation of Internet worms [21], Lloyd and May put forward a point that the spreading process of computer viruses is similar to the spreading model of human infectious diseases [22]. Then, the SIS model [23] and SIR model [24] have been proposed later inspired by human infectious disease. Dynamic quarantine is one of the common containment strategy of Internet worm and first proposed by Zou et al. [25]. Dynamic quarantine is an active defence method and a host is quarantined whenever its behaviour looks suspicious by blocking traffic on its anomaly port. The quarantined host will be released after a short time, and the experiment has proved that the dynamic quarantine will raise a worm's epidemic threshold, which will reduce the chance for a worm to spread out. Chen studies the effectiveness of partial quarantine for simple epidemics and derive the critical threshold for networks to have herd immunity [26]. Fan presents a study on modeling the propagation of P2P worms under quarantine using logic matrix [27]. Yao et al. model and analyse the quarantine strategy with time delay and variable infection rate [28]. Martín del Rey et al. propose a malware propagation model based on random complex networks, it is based on individuals and described by cellular automata [29]. Sheng et al. study the spread of industrial viruses with intelligent honeynet model [30]. Liu et al. study the characteristics of key nodes in complex networks [31]. Sardar et al. propose and analyse a conceptual mathematical model for the tumor-immune interaction [32]. Masood et al. develop an autonomous epidemic virus model to depict the transmission of malicious computer code in active networks with preexisting immunity and quarantine as effective control strategies [33]. However, the topology and the node equipment of the ICS network are quite different with that in the P2P botnets. The topology of the ICS network is approximately regarded as a power law distribution, and it is mainly composed of PLCs and honeypots. Therefore, the epidemic dynamic is quite different in the two networks. However, the effectiveness of P2P botnet quarantine has not yet been studied in detail.

In this paper, according to the life cycle of P2P botnet, a P2P botnet model called Susceptible-Infected-Infected-Recovered (SIIR) model is proposed to reflect the formation of P2P botnets. On this basis, two mathematical models (SIIQR, SIIQPR) are proposed and analysed with quarantine strategy and virtual patching, respectively. The bot-free equilibrium point is analysed and the basic reproduction number is derived to quantify the guideline for effective defence of P2P botnets. The simulation and numerical experiments are conducted to verify the correctness and effectiveness of our models. Through the comparative experiments, the model with both quarantine strategy and virtual patching can restrain the propagation of the P2P botnets the best, and for the SIIQPR model, larger infected rate that the bot-masters recruit new hosts and larger deploying rate of virtual patching can control the number of infected hosts more effectively. The paper can give effective strategy into predicting and restraining of the P2P botnet.

The rest of the paper is organized as follows. In Section 2, the propagation models of P2P botnet are presented combining the P2P botnet formation process and the dynamic quarantine and virtual patching strategy. Section 3 analyses the stability of equilibrium and obtained the basic reproduction number. In Section 4, the numerical analysis and simulation experiments of our models are carried out. Section 5 summarized the paper with some future directions.

2. Model Formulation

The life cycle of the P2P botnet consists of four primary phases, namely, initial infection, peer propagation, secondary injection, and attack [34, 35]. Initial infection phase: bot code is created through different technologies such as web downloads, vulnerability exploitation, e-mail attachments, automatic scanning, and traditional file-based viruses inserted into users' computers [36]. Bot code is a program that performs user-centric tasks automatically without any interaction with a user. The vulnerable end-user computer that running bot code is called bot-master. Peer propagation phase: the bot-master tries to connect with other vulnerable hosts based on its own hard-coded

peer list to select P2P bot candidates. Secondary injection phase: the new bots download the latest update of the bot code through the C&C channel, which will update it for future tasks. All the updated bots form a network called P2P botnet. Attack phase: finally, the bot initiates malicious activities such as spam or phishing emails, distributed denial-of-service (DDoS) attacks, stealing information, and scanning activities.

In the peer propagation phase, there are three ways for a bot-master to recruits new hosts. Therefore, P2P botnet can be classified into three category: parasite P2P botnet, leaching P2P botnet, and bot-only P2P botnet. In addition, the P2P botnet (such as Sinit) uses a random scan method to find other interactive bots, this leads to a very weak connection of the constructed P2P botnet. So the topology of the P2P botnets is approximately regarded as a random distribution. To enhance readability and facilitate understanding, some definitions are given as follows which explain the meaning of some concepts involved in this paper.

Definition 1. Parasite P2P botnet is a botnet in which bots are chosen from an existing P2P network.

Definition 2. Leaching P2P botnet is a botnet in which bot-masters recruit new bots from vulnerable hosts throughout the whole Internet, but they will join in and depend on an existing P2P network.

Definition 3. Bot-only P2P botnet is a botnet that occurs in an unattached network, and there are no nonmalignant peers except bots.

In this paper, we focus on talking about the leaching P2P botnet, which is a typical kind of P2P botnet and can best reflect the characteristics of P2P network.

2.1. SIIR Model. According to the life cycle of the P2P Botnet, we can consider the propagation process of the leaching P2P botnet as a two-step process. Step one, an infected host (bot-master) try to infect the new susceptible hosts (bots) throughout the whole Internet. Step two, the new compromised hosts join into the P2P network and connect with other bots. So a two-phase SIR model is employed to describe the dynamic behaviour of leaching P2P botnet, which is called SIIR model. The proposed model can describe the spreading behaviour of leaching P2P botnet more realistically in this paper.

In the model, there are four kinds of hosts: susceptible hosts (S), stage-1-infected hosts ($I1$), stage-2-infected hosts ($I2$), and recovered hosts (R). Stage-1-infected hosts ($I1$) are compromised hosts but not connected with other bots. In Stage-1-infected hosts ($I1$), no abnormal traffic is generated because there are no interaction with other bots and the stage-1-infected hosts are hard to be detected. Stage-2-infected hosts ($I2$) are indeed bots that joins the P2P network and do attack activities. If the stage-2-infected hosts carry on the attack activities, they can be detected and recovered.

Considering that the hosts on the Internet will dynamically join and leave the P2P network, the birth rate and the death rate μ are added to model this process, but not all the newly joined hosts will become bots in P2P botnet. If the hosts are patched, even if they just joined the network, they will directly be immune to the attack. The probability of a newly added node being patched is $1 - p$, the rest of newly joined hosts will become susceptible hosts.

β is the infected rate that represented the probability in the process of susceptible hosts and are selected as bot-masters. ρ is the infected rate that the bot-masters recruit new hosts on the Internet. γ is the recovered rate of the infected hosts. The state transition diagram of the SIIR model is shown in Figure 1.

The total number of hosts on the Internet is assumed relatively stable. We have the following equation:

$$N = S(t) + I_1(t) + I_2(t) + R(t). \tag{1}$$

Let $S(t)$, $I_1(t)$, $I_2(t)$, and $R(t)$ be the number of hosts in leaching P2P botnets at time t in state S, I_1, I_2, and R, respectively. And the propagation model of leaching P2P botnets can be represented with the following equation:

$$\begin{cases} \dfrac{\mathrm{d}S}{\mathrm{d}t} = p\mu N - \mu S(t) - \beta S(t)\left[I_1(t) + I_2(t)\right], \\ \dfrac{\mathrm{d}I_1}{\mathrm{d}t} = \beta S(t)\left[I_1(t) + I_2(t)\right] - (\rho + \mu) I_1(t), \\ \dfrac{\mathrm{d}I_2}{\mathrm{d}t} = \rho I_1(t) - (\mu + \gamma) I_2(t), \\ \dfrac{\mathrm{d}R}{\mathrm{d}t} = (1 - p)\mu N + \gamma I_2(t) - \mu R(t). \end{cases} \tag{2}$$

2.2. SIIQR Model. In order to study the effectiveness of quarantine in P2P botnet, SIIQR model is established to model the dynamic quarantine process and analyse the dynamic quarantine effect. Only when hosts in the stage-2-infected hosts (I_2) state, they will carry out the attack and show suspicious behaviour. A host is quarantined by blocking traffic on its anomaly port whenever its behaviour looks suspicious. The dynamic quarantine will be released after a short time, even if the host has not been inspected by security staff yet.

The dynamic quarantine is a compensation method that can tolerate higher false alarm rate of P2P botnet detection. A falsely quarantined healthy host will only be quarantined for a short time, thus its normal activities will not be interfered too much. The state transition diagram of the SIIQR model is shown in Figure 2.

σ is the quarantine rate that depends on the performance parameter of the misuse intrusion detection system. δ is the transition rate from state Q to state R. Let $Q(t)$ be the number of the state Q hosts at time t. The propagation model of leaching P2P botnets combining dynamic quarantine methods is shown as follows:

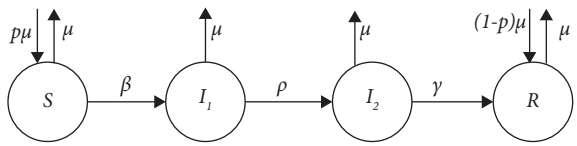

Figure 1: The state transition diagram of the SIIR model.

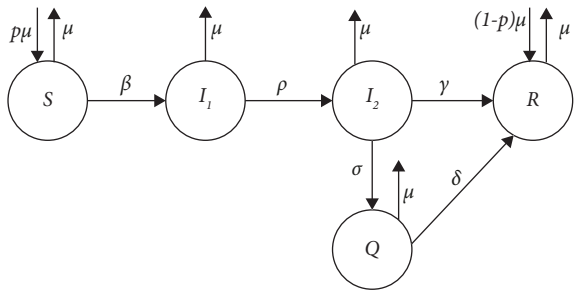

Figure 2: The state transition diagram of the SIIQR model.

$$\begin{cases} \dfrac{dS}{dt} = p\mu N - \mu S(t) - \beta S(t)\left[I_1(t) + I_2(t)\right], \\ \dfrac{dI_1}{dt} = \beta S(t)\left[I_1(t) + I_2(t)\right] - (\rho + \mu) I_1(t), \\ \dfrac{dI_2}{dt} = \rho I_1(t) - (\sigma + \gamma + \mu) I_2(t), \\ \dfrac{dQ}{dt} = \sigma I_2(t) - (\mu + \delta) Q(t), \\ \dfrac{dR}{dt} = \gamma I_2(t) + \delta Q(t) + (1 - p)\mu N - \mu R(t). \end{cases} \tag{3}$$

2.3. SIIQPR Model. The dynamic quarantine strategy is used for unknown cyber attacks and is carried out when the hosts exhibit a suspicious behaviour. Virtual patching is a policy for an intermediary device (i.e., firewall) that is able to identify and block attempts to exploit a specific vulnerability. Virtual patching strategy is used for known attack behaviour and it gives a temporary protection for the vulnerable hosts to survive the spanning time of updating the software or releasing the new patching of application.

The workflow of virtual patching consists of the following phases: preparation phase, identification phase, analysis phase, virtual patch creation phase, implementation/testing phase. The preparation phase need to setup the virtual patching processes and framework prior to actually having to deal with an identified vulnerability. The identification phase occurs when a vulnerability of Internet host is aware. Then, we need to expedite the implementation of virtual patches through the analysis, creation, implementation, and testing.

The virtual patching is often deployed on the firewall. Once the virtual patching is ready, the firewall will analyse transactions and intercepts attacks in transit, the malicious traffic will never reach the hosts. The effect of virtual patching is that the specific attacks will not be implemented even if the hosts are still susceptible. So a new state called P state (virtual patched state) is added to reflect the process of configuring virtual patches on firewall. The P state is completely different from the R state. The hosts in P state are still susceptible, but the vulnerability exploited attempt does not succeed. The hosts in R state are patched up and cannot be infected.

The virtual patching strategy will mainly affect the propagation of P2P botnet if it is in initial infection phase and peer propagation phase. In initial infection phase, the bot code cannot be inserted into the susceptible hosts for virtual patching. However, the susceptible hosts and the stage-1-infected hosts can be virtual patched. It is assumed that the deploying rate of virtual patching on the Internet is α_1 and α_2, respectively.

In peer propagation phase, the bot-masters cannot connect with other bots by using the specified vulnerability. Some of the bot-masters lost the ability to recruit new bots, therefore the state transition of the stage-1-infected hosts is from state I_1 to state P. The state transition diagram of the *SIIQPR* model is shown in Figure 3.

$P(t)$ is the number of virtual patched hosts at time t, and the propagation model of leaching P2P botnets combining dynamic quarantine and virtual patching methods is shown as follows:

$$\begin{cases} \dfrac{dS}{dt} = p\mu N - (\mu + \alpha_1) S(t) - \beta S(t)\left[I_1(t) + I_2(t)\right], \\ \dfrac{dP}{dt} = \alpha_1 S(t) + \alpha_2 I_1(t) - (\omega + \mu) P(t), \\ \dfrac{dI_1}{dt} = \beta S(t)\left[I_1(t) + I_2(t)\right] - (\alpha_2 + \rho + \mu) I_1(t), \\ \dfrac{dI_2}{dt} = \rho I_1(t) - (\sigma + \gamma + \mu) I_2(t), \\ \dfrac{dQ}{dt} = \sigma I_2(t) - (\mu + \delta) Q(t), \\ \dfrac{dR}{dt} = (1 - p)\mu N + \gamma I_2(t) + \delta Q(t) + \omega P(t) - \mu R(t). \end{cases} \tag{4}$$

3. Equilibrium and Stability

In this section, the dynamical behaviour of systems (2)–(4) proposed in Section 2 is studied here. A general formal study to obtain the reproduction number and stability properties of equilibrium points is proposed and formally discussed [37]. In addition, epidemic dynamics on complex networks has been studied with the methods

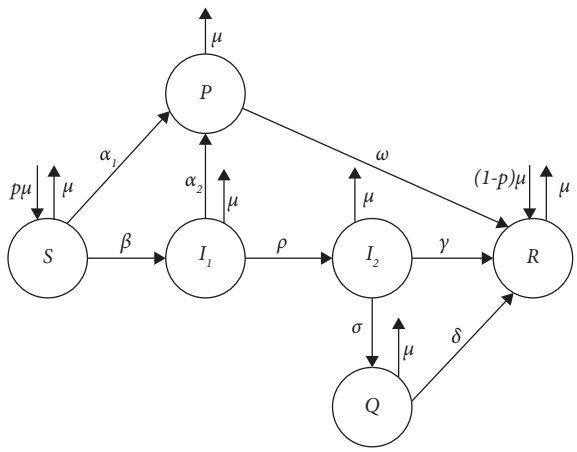

Figure 3: The state transition diagram of the SIIQPR model.

of the mathematical models and computational methods [38, 39, 40]. Based on these studies, the equilibrium and the basic reproduction number of system (2)–(4) are analysed.

3.1. Bot-Free Equilibrium of SIIR Model. Bot-free equilibrium means that the malware becomes extinct, system (2) can be rewritten as follows:

$$\begin{cases} \dfrac{\mathrm{d}S}{\mathrm{d}t} = p\mu N - \mu S(t) - \beta S(t)\left[I_1(t) + I_2(t)\right], \\ \dfrac{\mathrm{d}I_1}{\mathrm{d}t} = \beta S(t)\left[I_1(t) + I_2(t)\right] - (\rho + \mu) I_1(t), \\ \dfrac{\mathrm{d}I_2}{\mathrm{d}t} = \rho I_1(t) - (\mu + \gamma) I_2(t). \end{cases} \tag{5}$$

Let $I_1(t) = I_2(t) = 0$, the bot-free equilibrium (BFE) $E^*(S^*, I_1^*, I_2^*)$ can be obtained, that is, $S^* = pN$, $I_1^* = I_2^* = 0$. Therefore, we can obtain the following theorem.

Theorem 1. *BFE E^* of system (2) is locally asymptotically stable when $R_0 < 1$ and unstable when $R_0 > 1$, where*

$$\begin{aligned} R_0 &= \frac{p\beta N(\mu + \gamma + \rho)}{(\rho + \mu)(\mu + \gamma)} \\ &= \frac{\beta S^*(\mu + \gamma + \rho)}{(\rho + \mu)(\mu + \gamma)}. \end{aligned} \tag{6}$$

Proof. The characteristic equation of system (5) can be written as follows:

$$\det\begin{pmatrix} \lambda + \mu & \beta S^* & \beta S^* \\ 0 & \lambda - \beta S^* + (\rho + \mu) & -\beta S^* \\ 0 & \rho & \lambda + (\mu + \gamma) \end{pmatrix} = 0. \tag{7}$$

Table 1: Parameters for disease-free equilibrium.

Parameter	Value
N	1000000
β	0.00000008
μ	0.0005
p	0.2
γ	0.06
δ	0.0000001
σ	0.008
ω	0.00000008

Equation (5) has one negative real part characteristic root $\lambda = -\mu$ and roots of $(\lambda + \mu)(\lambda^2 + c\lambda + d) = 0$, where

$$\begin{aligned} c &= \rho + 2\mu + \gamma - \beta S^*, \\ d &= (\rho + \mu)(\mu + \gamma) - \beta S^*(\mu + \gamma + \rho). \end{aligned} \tag{8}$$

Obviously, when $R_0 < 1$, d is positive and $\mu + \gamma > \beta S^*(\mu + \gamma + \rho)/(\rho + \mu)$.

Thus, $c = \rho + 2\mu + \gamma - \beta S^* > u + r - \beta S^* > 0$ and $d > 0$. According to the Routh-Hurwitz criteria, the bot-free equilibrium point $E^*(S^*, I_1^*, I_2^*)$ is stable if and only if all of the characteristic values are negative. Hence the BFE E^* of system (5) is locally asymptotically stable when $R_0 < 1$ and unstable when $R_0 > 1$. □

3.2. Bot-Free Equilibrium of SIIQR Model. Let $N = S(t) + I_1(t) + I_2(t) + Q(t) + R(t)$ in system (3), therefore system (3) can be rewritten as follows:

$$\begin{cases} \dfrac{dS}{dt} = p\mu N - \mu S(t) - \beta S(t)\left[I_1(t) + I_2(t)\right], \\ \dfrac{dI_1}{dt} = \beta S(t)\left[I_1(t) + I_2(t)\right] - (\rho + \mu) I_1(t), \\ \dfrac{dI_2}{dt} = \rho I_1(t) - (\sigma + \gamma + \mu) I_2(t), \\ \dfrac{dQ}{dt} = \sigma I_2(t) - (\mu + \delta) Q(t). \end{cases} \tag{9}$$

If $I_1(t) = I_2(t) = 0$, the bot-free equilibrium (BFE) $E^*(S^*, I_1^*, I_2^*, Q^*)$ can be obtained, that is $S^* = pN$, $I_1^* = I_2^* == Q^* = 0$.

Theorem 2. *BFE E^* of system (9) is locally asymptotically stable when $R_0 < 1$ and unstable when $R_0 > 1$.*

$$\begin{aligned} R_0 &= \frac{p\beta N(\mu + \gamma + \sigma + \rho)}{(\rho + \mu)(\mu + \gamma + \sigma)} \\ &= \frac{\beta S^*(\mu + \gamma + \sigma + \rho)}{(\rho + \mu)(\mu + \gamma + \sigma)}. \end{aligned} \tag{10}$$

Proof. The characteristic equation of system (9) can be written as follows:

$$\det\begin{pmatrix} \lambda+\mu & \beta S^* & \beta S^* & 0 \\ 0 & \lambda-\beta S^*+(\rho+\mu) & -\beta S^* & 0 \\ 0 & -\rho & \lambda+(\mu+\gamma+\sigma) & 0 \\ 0 & 0 & \sigma & \lambda+(\mu+\delta) \end{pmatrix}=0. \tag{11}$$

Equation (11) has two negative real part characteristic roots $\lambda_1=-\mu,\lambda_2=-(\mu+\delta)$ and roots of $(\lambda+\mu)(\lambda^2+c\lambda+d)(\lambda+\mu+\delta)=0$, where

$$\begin{aligned} c&=\rho+2\mu+\gamma+\sigma-\beta S^*,\\ d&=(\rho+\mu)(\mu+\gamma+\sigma)-\beta S^*(\mu+\gamma+\sigma+\rho). \end{aligned} \tag{12}$$

Obviously, when $R_0<1$, $\mu+\rho>\beta S^*(\mu+\gamma+\rho+\sigma)/(\mu+\gamma+\sigma)>\beta S^*$ and the polynomial d is positive. Thus, $d>0$ and $c=\rho+2\mu+\gamma-\beta S^*>u+\rho-\beta S^*>0$. According to the Routh-Hurwitz criteria, the bot-free equilibrium point $E^*(S^*,I_1^*,I_2^*,Q^*)$ is stable if and only if all the characteristic values are negative. Then, the BFE E^* of system (9) is locally asymptotically stable when $R_0<1$ and unstable when $R_0>1$. □

3.3. Bot-Free Equilibrium of SIIQPR Model. Similar with the two models above, SIIQPR model has a bot-free equilibrium. Let $N=S(t)+I_1(t)+I_2(t)+Q(t)+P(t)+R(t)$ in system (9), then system (9) can be rewritten as follows:

$$\begin{cases} \dfrac{\mathrm{d}S}{\mathrm{d}t}=p\mu N-(\mu+\alpha_1)S(t)-\beta S(t)[I_1(t)+I_2(t)],\\ \dfrac{\mathrm{d}P}{\mathrm{d}t}=\alpha_1 S(t)+\alpha_2 I_1(t)-(\omega+\mu)(t),\\ \dfrac{\mathrm{d}I_1}{\mathrm{d}t}=\beta S(t)[I_1(t)+I_2(t)]-(\alpha_2+\rho+\mu)I_1(t),\\ \dfrac{\mathrm{d}I_2}{\mathrm{d}t}=\rho I_1(t)-(\sigma+\gamma+\mu)I_2(t),\\ \dfrac{\mathrm{d}Q}{\mathrm{d}t}=\sigma I_2(t)-(\mu+\delta)Q(t). \end{cases} \tag{13}$$

Similarly, let $I_1(t)=I_2(t)=0$ the bot-free equilibrium (BFE) $E^*(S^*,I_1^*,I_2^*,Q^*,P^*)$ can be obtained, that is $S^*=p\mu N/\mu+\alpha_1$, $I_1^*=0$, $I_2^*=0$, $Q^*=0$, $P^*=p\mu N\alpha_1/(\mu+\omega)(\alpha_1+\omega)$.

Theorem 3. *BFE E^* of system (13) is locally asymptotically stable when $R_0<1$ and unstable when $R_0>1$.*

$$\begin{aligned} R_0&=\frac{\beta S^*(\mu+\gamma+\sigma+\rho)}{(\rho+\mu+\alpha_2)(\mu+\gamma+\sigma)}\\ &=\frac{pN\mu\beta(\mu+\gamma+\sigma+\rho)}{(\rho+\mu+\alpha_2)(\mu+\gamma+\sigma)(\mu+\alpha_1)}. \end{aligned} \tag{14}$$

Proof. The characteristic equation of system (13) can be written as follows:

$$\det\begin{pmatrix} \lambda+(\mu+\alpha_1) & 0 & \beta S^* & \beta S^* & 0 \\ -\alpha_1 & \lambda+(\mu+\omega) & \alpha_2 & 0 & 0 \\ 0 & 0 & \lambda+(\alpha_2+\rho+\mu-\beta S^*) & \beta S^* & 0 \\ 0 & 0 & -\rho & \lambda+(\mu+\gamma+\sigma) & 0 \\ 0 & 0 & 0 & \sigma & \lambda+(\mu+\delta) \end{pmatrix}=0. \tag{15}$$

Equation (15) has two negative real part characteristic roots $\lambda_1=-(\mu+\alpha_1),\lambda_2=-(\mu+\omega),\lambda_3=-(\mu+\delta)$ and roots of $(\lambda+\mu+\alpha_1)(\lambda+\mu+\omega)(\lambda+\mu+\delta)(\lambda^2+c\lambda+d)=0$, where

$$\begin{aligned} c&=\rho+2\mu+\gamma+\sigma+\alpha_2-\beta S^*,\\ d&=(\rho+\alpha_2+\mu)(\mu+\gamma+\sigma)-\beta S^*(\mu+\gamma+\sigma+\rho), \end{aligned} \tag{16}$$

When $R_0<1,\rho+\alpha_2+\mu>\beta S^*(\mu+\gamma+\rho+\sigma)/(\mu+\gamma+\sigma)>\beta S^*$ and the polynomial d is positive. Thus, $d>0$ and $c=\rho+\alpha_2+2\mu+\gamma+\sigma-\beta S^*>\rho+\alpha_2+\mu-\beta S^*>0$. According to the Routh-Hurwitz criteria, the bot-free equilibrium point $E^*(S^*,I_1^*,I_2^*,Q^*,P^*)$ is stable if and only if all the characteristic values are negative, the BFE E^* of system (13) is locally asymptotically stable when $R_0<1$ and unstable when $R_0>1$. Then, we analyse the global behaviours of the bot-free equilibrium. For system (13), the set

$$\Omega\equiv\{y=\{y_1,y_2,\ldots,y_n\}\in R_+^n:\ 0\le y_i\le 1,\quad i=1,\ldots,n\}, \tag{17}$$

is positive invariant.

For all $t>0$, $y_i(t)\ge 0$, where $i=1,\ldots,n$, and the initial value $y(0)\in\Omega$. Besides, there would exist $k_0\in\{1,\ldots,n\}$ and $t_0>0$, such that $y_{k_0}(t_0)=0$. To ensure the generality, let $y_i=i_i$ and $t^*=\inf\{t>0,\quad i_i(t)=0\}$. It follows from system (13).

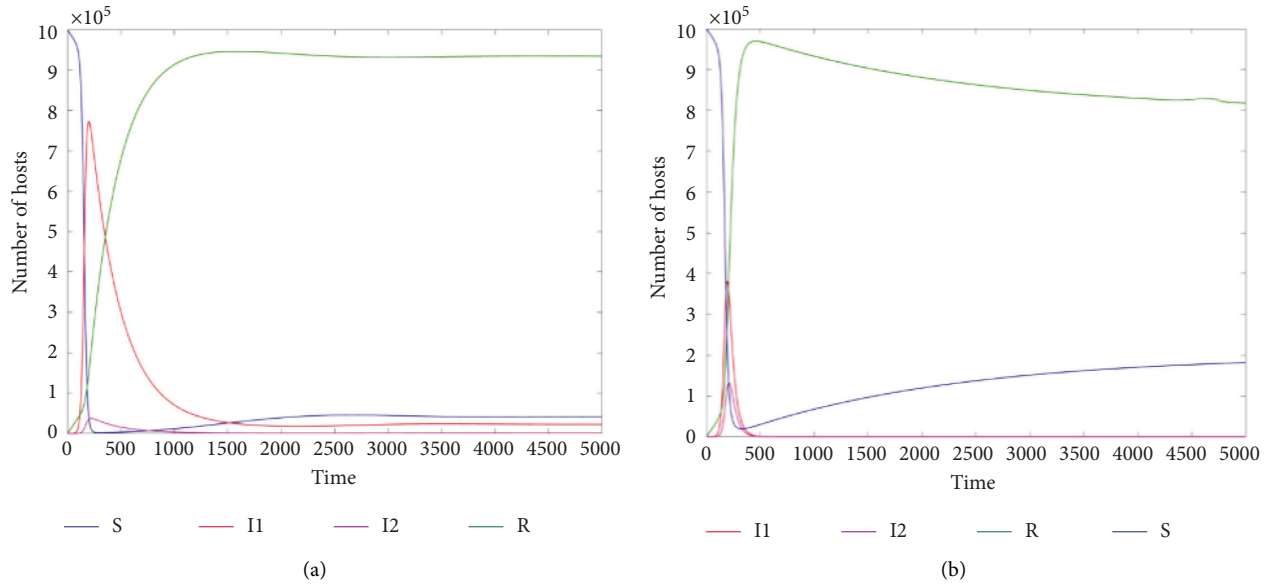

Figure 4: The numerical results of SIIR model. (a): $R_0 > 1$. (b): $R_0 < 1$.

$$\frac{\mathrm{d}i_i(t^*)}{\mathrm{d}t} = \beta i_0 I_1(t^*) > 0. \tag{18}$$

However, the definition of t^* yields $\mathrm{d}i(t^*)/\mathrm{d}t \le 0$, which leads to a contradiction. Then, based on Theorem 3.2 in the work of Zhao et al. [41], we derive the global stability of the disease-free equilibrium of system (13). □

Lemma 1. *For a constant differential autonomous system*

$$\frac{\mathrm{d}y(t)}{\mathrm{d}t} = f(y), \tag{19}$$

where $y \in R^n$ and $f: R_+^n \longrightarrow R^n$ is a continuous differential map. The following conditions are assumed.

(1) f is cooperative in R, that is, for $\forall y \in R_+^n$ and i, $j = 1, 2, \ldots, n$, if $i \neq j$, then $\partial f_i/\partial x_j \ge 0$. Meanwhile, $Df(y) = (\partial f_i/\partial x_j)_{1 \le i,\ j \le n}$ is irreducible for $\forall y \in R_+^n$;

(2) $f(0) = 0$ and for all $y \in R_+^n$, if $y_i = 0$, then $f_i(y) \ge 0$, $i = 1, 2, \ldots, n$;

Then, the following result is obtained:

If $s(Df(0)) = \max\{\mathrm{Re}\lambda; \det(\lambda - Df(0))\} \le 0$, $y = 0$ is globally asymptotically stable in R_+^n.

Theorem 4. *If $R_0 \le 1$, the disease-free equilibrium is globally asymptotically stable in Ω;*

Proof. Obviously, the function $f: \Omega \longrightarrow R^n$ is continuously differential and $f(0) = 0$, $f_i(y) \ge 0$ for all $y \in \Omega$ with $y_i = 0, i = 1, 2, \ldots, n$. In addition, $\partial f_i/\partial y_j \ge 0$ for $y \in \Omega, i \neq j$. Thus, the function f is a cooperative system. Particularly, for all $y \in \Omega$, $Df = (\partial f_i/\partial y_j)_{1 \le i,\ j \le n}$ is irreducible; and for any $\varepsilon \in (0, 1)$ and $y \in \Omega$, $f_i(\varepsilon y) \ge \varepsilon f_i(y)$ with $i = 1, 2, \ldots, n$. It implies that f is strictly sublinear in Ω. So the proof is completed by applying Lemma 1. □

4. Applications

In this section, numerical experiments of the models we proposed are conducted to verify our derivation, and some dynamical properties of our model are showed. In our experiments, the performance metrics is the equilibrium with different R_0, and simulation experiments can prove this from the dynamics of the system, the fit of the two curves (numerical curves and simulation curves) can confirm the reliability of the experiments. In addition, simulation results are presented to verify the actual behaviour in P2P botnet. It is worth noting that the birth rate and the death rate are considered in our experiments. To obtain the spread of worm in a large-scale network, the vulnerable population is assumed $N = 1{,}000{,}000$ in our experiments. In Table 1, the values of several parameters are listed, and these values are invariable in this paper.

4.1. Performance of the SIIR Model. To validate the accuracy of obtained from SIIR model, the parameters for disease-free equilibrium are listed in Table 1, and the following parameters are set: (a) $\rho = 0.003$, where $R_0 = 4.79 > 1$, and (b) $\rho = 0.023$, where $R_0 = 0.93 < 1$. The numerical and simulation results are shown in Figures 4 and 5, respectively.

In Figure 4(a), the number of the infected hosts is not zero when the system becomes stable, whereas the number of the infected hosts Figure 4(b) is zero. Thus, the correctness of the bot-free equilibrium of SIIR model is verified. When we take the actual situation into consideration, the basic reproduction number is usually larger than 1, which means the P2P botnets should be controlled by the corresponding containment strategies. In Figure 5, simulation results are presented to verify the actual behaviour of malware propagation in P2P botnet. The solid curves are numerical results and the imaginary curves are simulation results. It is

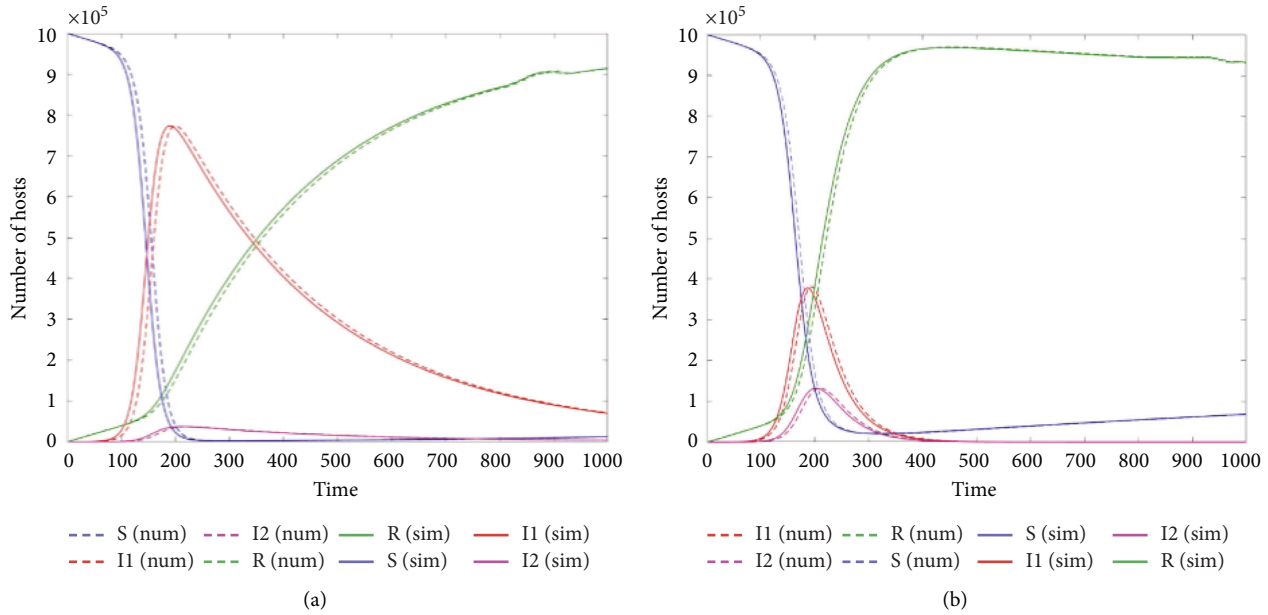

Figure 5: The simulation results of SIIR model. (a): $R_0 > 1$. (b): $R_0 < 1$.

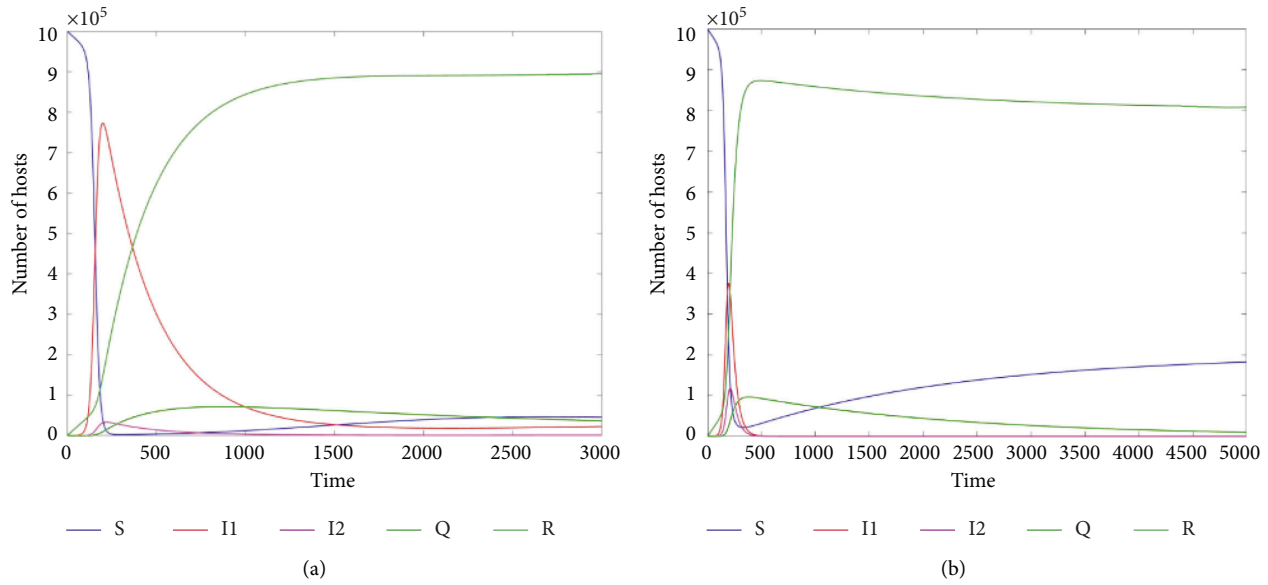

Figure 6: The numerical results of SIIQR model. (a): $R_0 > 1$. (b): $R_0 < 1$.

obviously to find that the simulation curves match the numerical curves well. The small difference does not affect the validity of our results.

4.2. Performance of the SIIQR Model. For the SIIQR model, $\delta = 0.0000001$ is the transition rate from state Q to state R. $\sigma = 0.008$ is the quarantine ratio that the stage-2-infected hosts are quarantined by the misuse detection system, and other parameters for disease-free equilibrium are listed in Table 1. To validate the accuracy of R_0 obtained from SIIQR model, the following parameters are set: (a) $\rho = 0.003$, where $R_0 = 4.73 > 1$, (b) $\rho = 0.023$, where $R_0 = 0.86 < 1$, and other parameters are not changed. The numerical and simulation results are shown in Figures 6 and 7, respectively.

In Figure 6, the bot-free and endemic equilibrium is showed, and Theorem 2 is verified as well, namely BFE E^* of the system is locally asymptotically stable when $R_0 < 1$ and unstable when $R_0 > 1$. In Figure 7, simulation results are presented to verify the actual behaviour of malware propagation. The same as Figure 4, the solid curves are numerical results and the imaginary curves are simulation results. Similarly, the simulation curves match the numerical curves well.

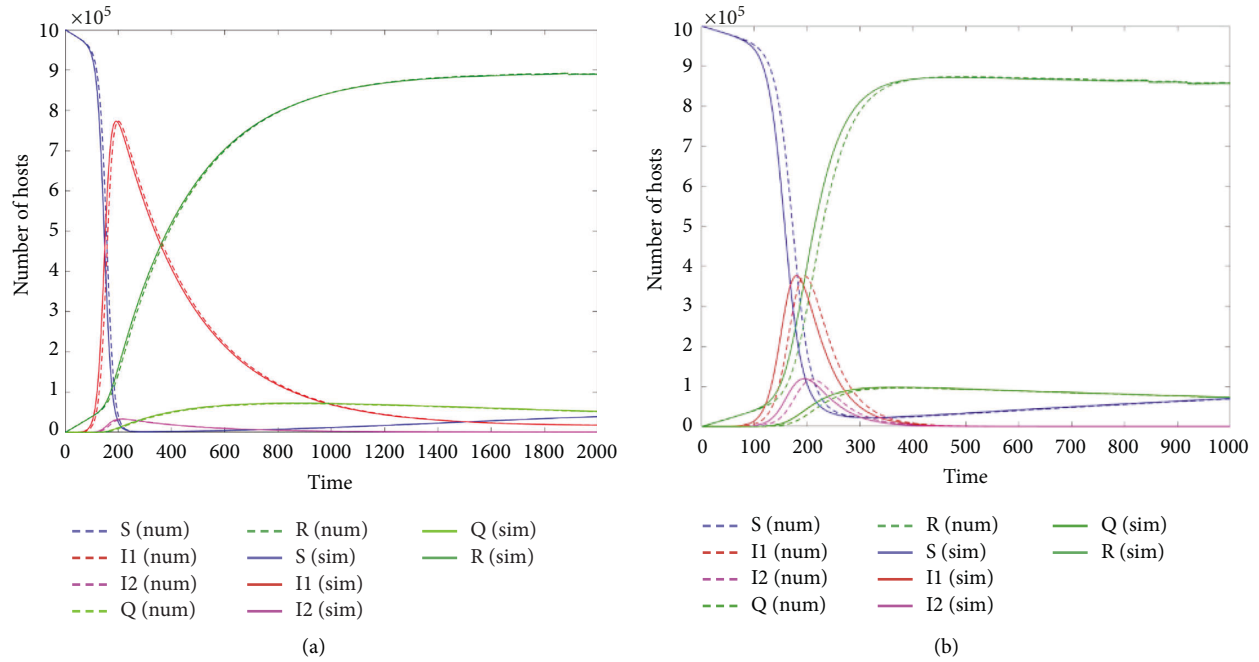

Figure 7: The simulation results of SIIQR model. (a): $R_0 > 1$. (b): $R_0 < 1$.

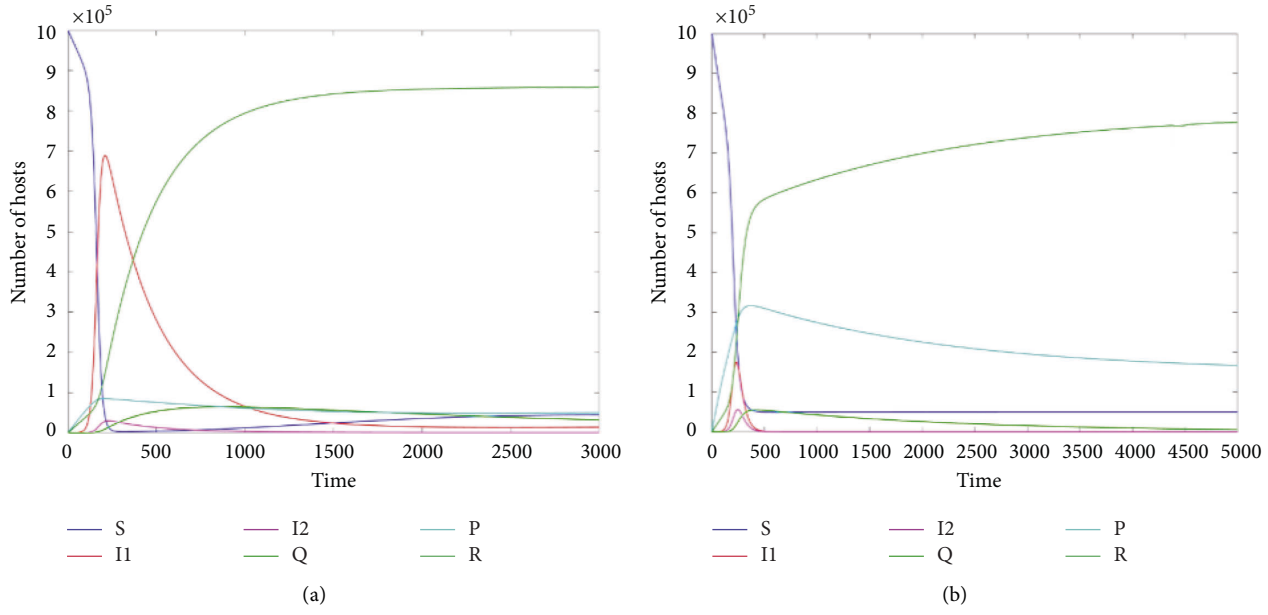

Figure 8: The numerical results of SIIQPR model. (a): $R_0 > 1$. (b): $R_0 < 1$.

4.3. Performance of the SIIQPR Model. In this subsection, (a): $\alpha_1 = 0.0006$, $\alpha_2 = 0.00001$, $\rho = 0.003$, the basic reproduction number $R_0 > 1$, (b): $\alpha_1 = 0.0015$, $\alpha_2 = 0.0035$, $\rho = 0.023$ the basic reproduction number $R_0 > 1$. α_1 and α_2 are the temporarily patching rates by virtual patching strategy, respectively. And $\omega = 0.00000005$ is the rate that the P hosts turn into state R patched by the real patching, other parameters for disease-free equilibrium are listed in Table 1. Under the above parameters, numerical and simulation experiments on the SIIPQR model is conducted and the results are shown in Figures 8 and 9.

Figure 8 shows the results of the numerical curves including bot-free and endemic equilibrium. Figure 9 shows a tiny distinction between the simulation and numerical experiments. The effect of the virtual patching strategy is verified. The good matches between the simulation and numerical experiments verify that the SIIQPR model can describe the P2P botnets well. And the result shows that the

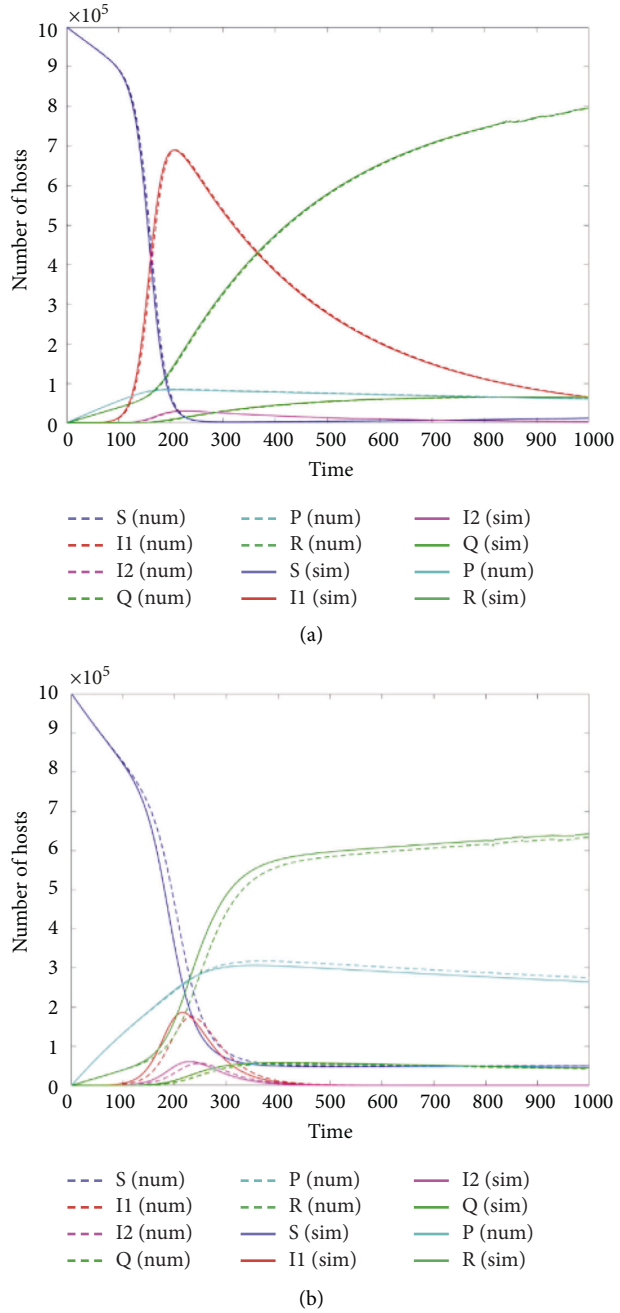

Figure 9: The simulation results of SIIQPR model. (a): $R_0 > 1$. (b): $R_0 < 1$.

virtual patching strategy can effectively control the P2P botnets.

In order to appraise the effectiveness of the virtual patching strategy, comparisons have been made among the three models, SIIR model, SIIQR model, and SIIQPR model. The tendencies of worm propagation from three models are shown in Figure 10.

All the infected hosts in the three models will die out for the reason that their basic reproduction numbers are $R_0 < 1$. In Figure 10, solid curves are the number of I_1 hosts, and the dashed curves are the number of I_2 hosts. Blue, red, and green curves represent SIIR, SIIQR, and SIIQPR models, respectively. The number of infected hosts can show the effect of the models. As Figure 10 shows, the number of infected hosts in SIIQPR model (green lines) is the minimum. So the SIIQPR is the best one. Comparing SIIR model with SIIQR model, Figure 9 shows that the number of I_2 hosts only drop a little while the number of I_1 hosts almost changes just a little. It demonstrates that one and only quarantine strategy is not effective to inhibit worms propagation. After adopting both the virtual patching and quarantine strategy, the number of I_1 hosts and I_2 hosts is

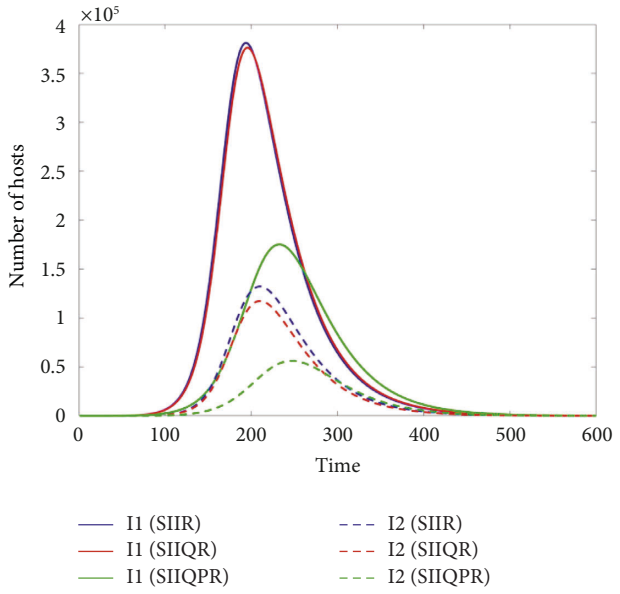

Figure 10: Comparison of infected hosts of three models.

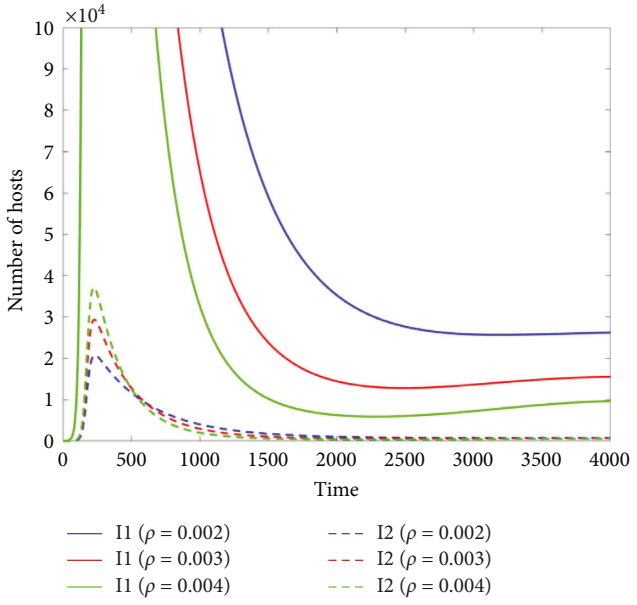

Figure 11: Comparison of infected hosts with different parameter ρ in SIIQPR model.

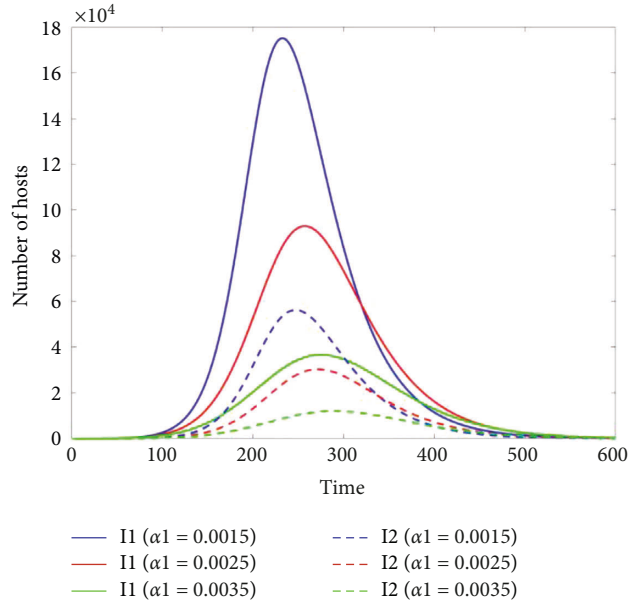

Figure 12: Comparison of infected hosts with different parameter α_1 in SIIQPR model.

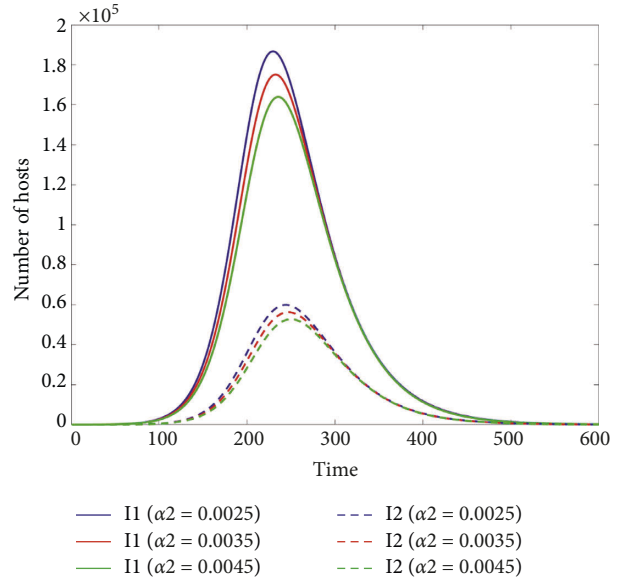

Figure 13: Comparison with different deploying rate of virtual patching α_2 in SIIQPR model.

effectively controlled. The excellent effect SIIQPR model is demonstrated. In addition, the parameters ρ and α_1 is analysed based on the SIIQPR model.

When $R_0 > 1$, the parameter ρ is set $\rho = 0.002$, $\rho = 0.003$, and $\rho = 0.004$. Figure 11 shows the comparison of the infected hosts with different parameter ρ in the SIIQPR model. Similar with Figure 9, the number of I_1 and I_2 hosts are compared. It is obviously to find that the number of I_1 hosts is fewer with larger parameter ρ. And the I_2 hosts is opposite of this. Because of the range of hosts' number, the difference is not showed very clearly.

When $R_0 < 1$, the parameter α_1 is set $\alpha_1 = 0.0015$, $\alpha_1 = 0.0025$, and $\alpha_1 = 0.0035$. Figure 12 shows the comparison of the infected hosts with different parameter α_1 in the SIIQPR model. It is obviously that the number of I_1 and I_2 hosts is lower with larger parameter α_1. It demonstrates that larger parameters ρ and α_1 can control the number of infected hosts more effectively. In addition, the influence of deploying rate of virtual patching α_2 and quarantine rate σ are discussed in Figures 13 and 14, respectively. As we see, the difference of the curves with different α_2 and σ is not very prominent. This illustrates that controlling the deploying

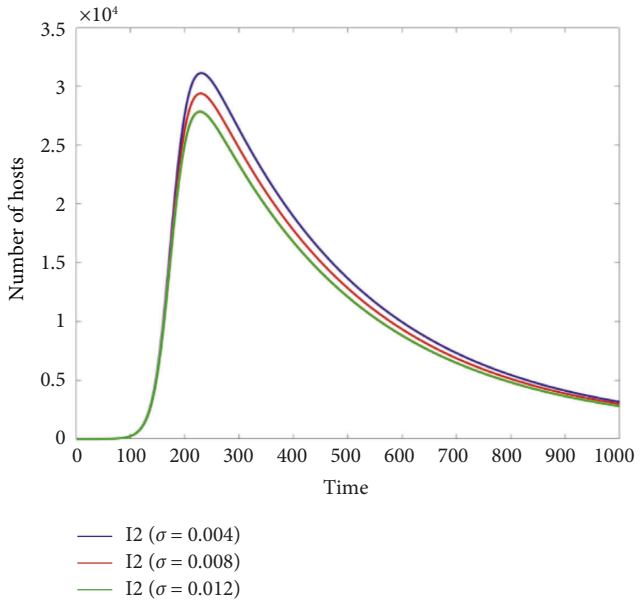

Figure 14: Comparison of infected hosts with different quarantine rate σ in SIIQPR model.

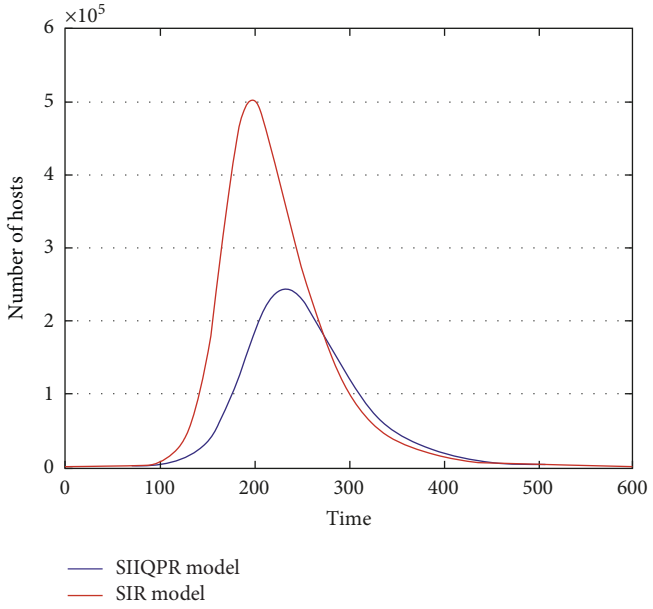

Figure 15: Comparison of infected hosts between SIIQPR model and SIR model.

rate of virtual patching α_1 and infected rate ρ is more efficient to suppress the P2P botnet.

It is easy to confirm that SIIQPR model works better in Figure 15. When the system reach bot-free equilibrium, the number of infected hosts in SIR model is much larger than that in SIIQPR model. Based on the experiment results and analysis above, the virtual patching strategy is effective on protecting the susceptible hosts and the constant quarantine strategy is not sufficient in controlling the worm propagation. Our models can describe the dynamic behaviour of P2P botnets accurately.

5. Conclusion

P2P botnets have attracted considerable attention. The containment strategy of the propagation of P2P botnets is an important topic. The virtual patching strategy and quarantine strategy are effective measures to ensure network security. This paper explores two novel dynamical models to examine the different containment strategies impacting on the propagation of the P2P botnets. The first is SIIQR model which describes the dynamical behaviour of P2P botnets under quarantine strategy. The second is the SIIQPR model which describes the dynamical behaviour of P2P botnets under quarantine strategy and virtual patching. Through the detailed mathematical analysis, the stability of equilibrium is investigated and the basic reproduction number is obtained, which governs whether or not P2P botnets are extinct. Numerical and simulation experiments show the dynamics of the models, and the birth rate and the death rate are considered in the experiments. Furthermore, the effect of virtual patching is showed and the influence of parameters ρ, σ, α_1, and α_2 is analysed as well in SIIQPR model, and we find that controlling the deploying rate of virtual patching α_1 and infected rate ρ is more efficient to suppress the P2P botnet. In a word, the analysis and experiment results verify that the virtual patching strategy and quarantine strategy can effectively contain the propagation of the P2P botnets. This paper provides a new insight to the containment strategy of P2P botnets.

Data Availability

We have no data supporting the results.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Applied Basic Research Program of Liaoning Province under Grant no. 2022JH2/101300240.

References

[1] P. Wang, B. Aslam, and C. C. Zou, "Peer-to-Peer botnets," in *Handbook of Information and Communication Security*, P. Stavroulakis and M. Stamp, Eds., pp. 335–350, Springer Press, Berlin, Germany, 2010.

[2] W. Ye and K. Cho, "P2P and P2P botnet traffic classification in two stages," *Soft Computing*, vol. 21, no. 5, pp. 1315–1326, 2015.

[3] M. Alauthaman, N. Aslam, L. Zhang, R. Alasem, and M. A. Hossain, "A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks," *Neural Computing & Applications*, vol. 29, no. 11, pp. 991–1004, 2016.

[4] S. K. Tetarave, S. Tripathy, E. Kalaimannan, C. John, and A. Srivastava, "A routing table poisoning model for peer-to-peer (P2P) botnets," *IEEE Access*, vol. 7, pp. 67983–67995, 2019.

[5] T. Holz, M. Steiner, and F. Dahl, "Measurements and mitigation of peer-to-peer-based botnets: a case study on Storm worm," *LEET*, vol. 8, pp. 1–9, 2008.

[6] D. Jang, M. Kim, and H. Jung, "Analysis of HTTP2P botnet: case study waledac," in *Proceedings of the IEEE 9th Malaysia International Conference on Communications (MICC)*, pp. 409–412, Kuala Lumpur, December 2009.

[7] D. Plohmann and E. Gerhards-Padilla, "Case study of the miner botnet," in *Proceedings of the 2012 4th International Conference on Cyber Conflict*, pp. 1–16, Tallinn, June 2012.

[8] M. Kerkers, J. J. Santanna, and A. Sperotto, "Characterisation of the Kelihos," in *Proceedings of the International Conference on Autonomous Infrastructure*, Berlin, Heidelberg, June 2014.

[9] M. Cheenu, "A review of zero access peer-to-peer botnet," *International Journal of Computer Trends and Technology*, vol. 12, 2014.

[10] A. Kolesnichenko, A. Remke, P. T. de Boer, and B. R. Haverkort, "Comparison of the mean-field approach and simulation in a peer-to-peer botnet case study," *Computer Performance Engineering*, vol. 6977, pp. 133–147, 2011.

[11] E. V. Ruitenbeek and W. H. Sanders, "Modeling peer-to-peer botnets," in *Proceedings of the 2008 Fifth International Conference on Quantitative Evaluation of Systems*, pp. 307–316, Saint-Malo, France, September 2008.

[12] L. Feng, X. Liao, Q. Han, and L. Song, "Modeling and analysis of peer-to-peer botnets," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 865075, 18 pages, 2012.

[13] L. Feng, H. Wang, and Q. Han, "Modeling peer-to-peer botnet on scale-free network," *Abstract and Applied Analysis*, vol. 8, 2014.

[14] Y. Yao, W. Sun, S. Li, and F. X. Gao, "Virtual patching containment strategy of Internet worm modeling and analysis," *Applied Mechanics and Materials*, vol. 380-384, pp. 2216–2220, 2013.

[15] S. C. Su, Y. R. Chen, and S. C. Tsai, "Detecting P2P botnet in software defined networks," *Security and Communication Networks*, vol. 13, 2018.

[16] Z. Yang and B. Wang, "A feature extraction method for P2P botnet detection using graphic symmetry concept," *Symmetry*, vol. 11, no. 3, p. 326, 2019.

[17] M. J. Dehkordi and B. Sadeghiyan, "An effective node-removal method against P2P botnets," *Computer Networks*, vol. 182, Article ID 107488, 2020.

[18] Y. Xing, H. Shu, F. Kang, and H. Zhao, "Peertrap: an unstructured P2P botnet detection framework based on SAW community discovery," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9900396, 18 pages, 2022.

[19] D. Zhuang and J. M. Chang, "Enhanced PeerHunter: detecting peer-to-peer botnets through network-flow level community behavior analysis," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1485–1500, 2019.

[20] R. U. Khan, X. Zhang, R. Kumar, A. Sharif, N. A. Golilarz, and M Alazab, "An adaptive multi-layer botnet detection technique using machine learning classifiers," *Applied Sciences*, vol. 9, no. 11, p. 2375, 2019.

[21] S. Staniford, V. Paxson, and N. Weaver, "How to own the Internet in your spare time," in *Proceedings of the The 11th Usenix Security Symposium*, pp. 149–169, CA, USA, August 2002.

[22] A. L. Lloyd and R. M. May, "Epidemiology: how viruses spread among computers and people," *Science*, vol. 292, no. 5520, pp. 1316-1317, 2001.

[23] J. C. Martin, L. L. Burge III, J. I. Gill, A. N. Washington, and M. Alfred, "Modelling the spread of mobile malware," *International Journal of Computer Aided Engineering and Technology*, vol. 2, no. 1, pp. 3–14, 2010.

[24] S. H. Qing and W. P. Wen, "A survey and trends on Internet worms," *Computers & Security*, vol. 24, no. 4, pp. 334–346, 2005.

[25] C. C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling and analysis under dynamic quarantine defense," in *Proceedings of the 2003 ACM workshop*, pp. 51–60, DC, USA, October 2003.

[26] T. M. Chen and N. Jamil, "Effectiveness of quarantine in worm epidemics," in *Proceedings of the 2006 IEEE International Conference on Communications*, pp. 2142–2147, Istanbul, Turkey, June 2006.

[27] X. Fan and Y. Xiang, "Modeling the propagation of Peer-to-Peer worms under quarantine," in *Proceedings of the 2010 IEEE Network Operations and Management Symposium*, pp. 942–945, Osaka, Japan, April 2010.

[28] Y. Yao, Q. Fu, and W. Yang, "An epidemic model of computer worms with time delay and variable infection rate," *Security and Communication Networks*, vol. 11, 2018.

[29] A. Martín del Rey, G. Hernández, A. Bustos Tabernero, and A. Queiruga Dios, "Advanced malware propagation on random complex networks," *Neurocomputing*, vol. 423, no. 29, pp. 689–696, 2021.

[30] C. Sheng, Y. Yao, Q. Fu, W. Yang, and Y. Liu, "Study on the intelligent honeynet model for containing the spread of industrial viruses," *Computers & Security*, vol. 111, Article ID 102460, 2021.

[31] H. Liu, X. Xu, J. A. Lu, G. Chen, and Z. Zeng, "Optimizing pinning control of complex dynamical networks based on spectral properties of grounded laplacian matrices," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 786–796, 2021.

[32] M. Sardar, S. Khajanchi, S. Biswas, S. F. Abdelwahab, and K. S. Nisar, "Exploring the dynamics of a tumor-immune interplay with time delay," *Alexandria Engineering Journal*, vol. 60, no. 5, pp. 4875–4888, 2021.

[33] Z. Masood, K. Majeed, R. Samar, and M. A. Z. Raja, "Design of epidemic computer virus model with effect of quarantine in the presence of immunity," *Fundamenta Informaticae*, vol. 161, no. 3, pp. 249–273, 2018.

[34] P. Wang, B. Aslam, and C. C. Zou, "Peer-to-Peer botnets: the next generation of botnet attacks," *Electrical Engineering*, vol. 25, 2010.

[35] J. B. Grizzard, V. Sharma, and C. Nunnery, "Peer-to-peer botnets: overview and case study," in *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, p. 1, MA, USA, April 2007.

[36] Lurhq Threat Intelligence Group, "Sinit P2P trojan analysis," 2003, http://www.secureworks.com/research/threats/sinit.

[37] M. De la Sen, R. Nistal, S. Alonso-Quesada, and A. Ibeas, "Some formal results on positivity, stability, and endemic steady-state attainability based on linear algebraic tools for a class of epidemic models with eventual incommensurate delays," *Discrete Dynamics in Nature and Society*, vol. 2019, Article ID 8959681, 22 pages, 2019.

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

[39] M. J. Keeling and K. T. Eames, "Networks and epidemic models," *Journal of The Royal Society Interface*, vol. 2, no. 4, pp. 295–307, 2005.

[40] C. Castellano and R. Pastor-Satorras, "Competing activation mechanisms in epidemics on networks," *Scientific Reports*, vol. 2, no. 1, pp. 371–376, 2012.

[41] X. Zhao and J. Zhu, "Global asymptotic behavior in some cooperative systems of functional differential equations," *Canadian Applied Mathematics Quarterly*, vol. 4, no. 4, pp. 421–444, 1996.

[42] C. Rossow, D. Andriesse, and T. Werner, "P2PWNED: modeling and evaluating the resilience of peer-to-peer botnets," *IT-Information Technology*, vol. 54, pp. 64–70, 2012.