Hindawi Publishing Corporation
Discrete Dynamics in Nature and Society
Volume 2012, Article ID 865075, 18 pages
doi:10.1155/2012/865075

Research Article

Modeling and Analysis of Peer-to-Peer Botnets

Liping Feng,[1, 2] Xiaofeng Liao,[1] Qi Han,[1] and Lipeng Song[3]

[1] *State Key Laboratory of Power Transmission Equipment and System Security,*
College of Computer Science, Chongqing University, Chongqing 400044, China
[2] *Department of Computer Science and Technology, Xinzhou Normal University,*
Shanxi 034000, Xinzhou, China
[3] *Department of Computer Science and Technology, North University of China,*
Shanxi 030051, Taiyuan, China

Correspondence should be addressed to Liping Feng, fenglp@yeah.net

Received 23 July 2012; Revised 28 September 2012; Accepted 28 September 2012

Academic Editor: Xiaofan Yang

Peer-to-Peer (P2P) botnets have emerged as one of the most serious threats to Internet security. To effectively eliminate P2P botnets, in this paper, the authors present two novel dynamical models to portray the process of formation of P2P botnets, one of which is called microlevel model, the other is called macrolevel model. Also, the stability of equilibria is investigated along with the analysis of how to prevent the P2P botnet. Furthermore, by analyzing the relationship between infection rate and the proportion of the hosts with countermeasures, we obtain the mathematical expressions of effective immune regions and depict their numerical simulations. Finally, numerical simulations verify the correctness of mathematical analysis. Our results can provide the guidance for security practitioners to defend and eliminate P2P botnet at a cost-effective way.

1. Introduction

A botnet is a network of thousands (or more) of compromised hosts under the control of a botnetmaster, which usually recruits new vulnerable computers by running all kinds of malicious software (malware), such as Trojan horses, worms, computer viruses, and so forth [1]. For a variety of nefarious purposes, a botnetmaster who operates a botnet controls remotely those zombie computers to pursuit various malicious activities, such as distributed denial-of-service attacks (DDoS), email spam, password cracking, and so forth [2]. Botnets have been turned out one of the most serious threat to Internet [3].

To effectively fight against botnets, researchers have endeavored to explore working mechanisms of botnets from different perspectives in the past few years (see [4–11]). These existing researches provide perfect insight into detection and elimination of botnets. Aiming at describing the dynamical characteristics of botnets, Dagon et al. [12] constructed a Susceptible-Infective-Recovered (SIR) model, which took into account the effect of time and location on malware spread dynamics. The model accurately characterizes the population growth of a botnet. Considering the interactions among botnets, Song et al. [1] presented the interaction game model among botnets to investigate the effect of the cooperation and the competition on the number of botnet individuals.

Most previous botnets as shown in Figure 1 use Internet relay chat (IRC) as a form of communication for centralized command and control (C&C) structure. Botnets based on C&C structure are easily checked and cracked by defenders; as well as the threats of botnets can be mitigated and eliminated if the central of C&C is unavailable [13]. In comparison, Peer-to-Peer (P2P) betnets as shown in Figure 2 employing a distributed command-and-control structure are more robust and more difficult for the security community to defend. Thus, P2P botnets, such as Trojan.Peacomm, Storm botnet [14], have emerged and gradually escalated in recent years. The threats of P2P botnets to Internet security have drawn widespread attention. Reference [15] presented a stochastic model of Storm Worm P2P botnet to examine how different factors, such as the removal rate and the initial infection rate, impact the total propagation bots. Kolesnichenko et al. developed a mean-field model to analyze P2P botnet behaviors [16]. In their seminal work, Yan et al. [17] mathematically elaborated the performance of a new type of P2P botnet—AntBot from perspectives of reachability, resilience to pollution and scalability. They also developed a P2P botnet simulator to evaluate the effectiveness of analysis. Furthermore, the authors suggested some potential defense schemes for defenders to effectively disrupt AntBot operations.

For security workers to be better prepared for potentially destructive P2P botnets, it is necessary for them to understand deeply factors that influence the formation of P2P botnets. Against this backdrop, in this paper, we utilize mathematical modeling method to investigate how immunizations affect the dynamical actions of P2P botnets. Our key contributions are summarized as follows: (i) we propose novel dynamical models which reflect the formation of P2P botnets; (ii) we derive mathematically the feasible region of immunization and depict their numerical simulations; (iii) we suggest a probable immune method for researchers and security professionals.

The remainder of the paper is organized as follows. Section 2 elaborates modeling mechanism. In Section 3, we derive the equilibria of models and prove their stabilities. In Section 4, we get the mathematical expressions of immune feasible regions and obtain the results of numerical simulations. In Section 5, we depict the numerical simulations to verify conclusions of Section 4. Section 6 concludes this paper with some conclusions.

2. Modeling P2P Botnets

Considering bot candidates and the network a botnet attaches itself to, we roughly divide P2P botnets into three categories [18]: (i) Parasite P2P botnet, in which all bot members are chosen from an existing P2P network; (ii) Leaching P2P botnet, which is a botnet that bot candidates are from vulnerable hosts throughout the Internet, but they will join in and depend on an existing P2P network; (iii) Bot-only P2P botnet, which refers to a botnet that occurs in an unattached network, and there are no nonmalignant peers except bots.

For parasite P2P botnet, once a vulnerable host is compromised by botnet malware, it will directly become a bot member and serve for the botmaster without further joining the botnet. Up to this trait, in Section 2.1, we present a deterministic mathematical model named

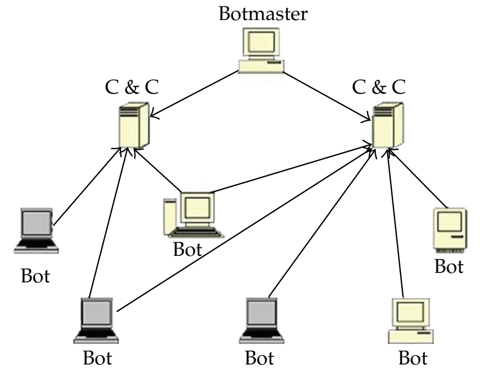


Figure 1: Centralized botnet [18].

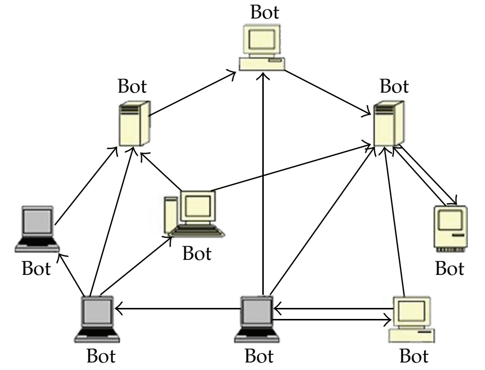


Figure 2: P2P botnet [18].

"microlevel model" to reflect its dynamical features. However, many botmasters extend their scales to the whole Internet to recruit new zombies because the scale of *parasite botnet* is limited by the number of peers in an existing P2P network. For constructing this type P2P botnet, there are two steps: the first step is trying to infect new vulnerable hosts throughout the whole Internet, and the second step is new compromised hosts joining into network and connecting with other bots. In Section 2.2, we use a novel mathematical model, which we call "macrolevel model" to characterize their dynamical actions.

2.1. The Microlevel Model

In this subsection, we employ the classical SIR model, which has been widely used by many researchers to study Internet malware propagation [19–24], to characterize the dynamical behavior of *parasite P2P botnets*. Let $\widehat{S}(t), \widehat{I}(t)$, and $\widehat{R}(t)$ be the numbers of hosts at time t in stats S, I, and R, respectively. Let $\widehat{N}$ be the total number of hosts in a P2P network and be relatively stable, then we have

$$\widehat{S}(t) + \widehat{I}(t) + \widehat{R}(t) = \widehat{N}. \tag{2.1}$$

That is, given a P2P network with a total of $\widehat{N}$ hosts, any host in the network will be at a state of either $\widehat{S}$, $\widehat{I}$, or $\widehat{R}$, and the sum of all hosts in these states equals $\widehat{N}$. In addition, unlike the traditional *SIR* model, our model includes the impact of real-time immunization to virus propagation.

As a result, the model we employ is as follows:

$$
\begin{aligned}
\frac{d\widehat{S}(t)}{dt} &= \widehat{\mu}\widehat{N} - \widehat{\beta}\frac{\widehat{I}(t)\widehat{S}(t)}{\widehat{N}} - \left(\widehat{\mu} + \widehat{r}_s\right)\widehat{S}(t), \\
\frac{d\widehat{I}(t)}{dt} &= \widehat{\beta}\frac{\widehat{I}(t)\widehat{S}(t)}{\widehat{N}} - \left(\widehat{\mu} + \widehat{r}_i\right)\widehat{I}(t), \\
\frac{d\widehat{R}(t)}{dt} &= \widehat{r}_s\widehat{S}(t) + \widehat{r}_i\widehat{I}(t) - \widehat{\mu}\widehat{R}(t),
\end{aligned}
\tag{2.2}
$$

where $\widehat{\mu}$ is the replacement rate of the hosts per hours; $\widehat{\beta}$ is infection rate per hour; $\widehat{r}_s$ is the state transition rate from $\widehat{S}$ to $\widehat{R}$ due to real-time immune measures; $\widehat{r}_i$ is the recovery rate from infected state $\widehat{I}$ to $\widehat{R}$ due to antivirus measures. It is easy to verify that the positive cone R_+^3 is a positive invariant set with respect to system (2.2), where $R_+^3 = \{(\widehat{S}, \widehat{I}, \widehat{R}) \in R^3 : \widehat{S} > 0, \widehat{I} > 0, \widehat{R} > 0\}$.

In what follows, we consider the effect of immunization on computer virus propagation in the P2P network. In reality, it is reasonable for us to assume that some hosts have immune measures, others have not. Hence, in our model the total hosts can be partitioned into two subclasses: immune and no immune hosts. Let f be the proportion of the hosts with immune measures $(0 \leq f \leq 1)$. We make a simple assumption that immunization has no effect on the infected time. So, we need only to change infection rate $\widehat{\beta}$. Let $\widehat{\beta}_1$ be the proportion of hosts with immune measures infected by infective hosts, and let $\widehat{\beta}_2$ $(\widehat{\beta}_1 \leq \widehat{\beta}_2)$ be the proportion of hosts without immune measures infected by infective hosts. Therefore rewrite infection rate $\widehat{\beta}$ as

$$
\overline{\beta} = f\widehat{\beta}_1 + (1 - f)\widehat{\beta}_2. \tag{2.3}
$$

Hence, the new differential equation model can be expressed as follows:

$$
\begin{aligned}
\frac{d\widehat{S}(t)}{dt} &= \widehat{\mu}\widehat{N} - \overline{\beta}\frac{\widehat{I}(t)\widehat{S}(t)}{\widehat{N}} - \left(\widehat{\mu} + \widehat{r}_s\right)\widehat{S}(t), \\
\frac{d\widehat{I}(t)}{dt} &= \overline{\beta}\frac{\widehat{I}(t)\widehat{S}(t)}{\widehat{N}} - \left(\widehat{\mu} + \widehat{r}_i\right)\widehat{I}(t), \\
\frac{d\widehat{R}(t)}{dt} &= \widehat{r}_s\widehat{S}(t) + \widehat{r}_i\widehat{I}(t) - \widehat{\mu}\widehat{R}(t).
\end{aligned}
\tag{2.4}
$$

2.2. The Macrolevel Model

In this subsection, we use a two-stage *SIR* model to depict the dynamical action of *leeching P2P botnets*, in which botmasters recruit new bots from the whole Internet. The model monitors the four populations of susceptible (S), stage-1-infected (I_1) hosts that are compromised but not connect with other bots, and stage-2-infected (I_2) hosts that are indeed bots and recovered (R). We assume that the number of hosts on Internet is relatively stable, which is often adopted in other existing efforts [25, 26]. Let N be the total number of hosts on Internet. Then our model can be formulated as follows:

$$\begin{aligned}
\frac{dS(t)}{dt} &= \mu N - (\alpha_1 I_1(t) + \alpha_2 I_2(t))\frac{S(t)}{N} - (\mu + r_s)S(t),\\
\frac{dI_1(t)}{dt} &= (\alpha_1 I_1(t) + \alpha_2 I_2(t))\frac{S(t)}{N} - (\mu + r_1 + \delta)I_1(t),\\
\frac{dI_2(t)}{dt} &= \delta I_1(t) - (\mu + r_2)I_2(t),\\
\frac{dR(t)}{dt} &= r_s S(t) + r_1 I_1(t) + r_2 I_2(t) - \mu R(t),
\end{aligned} \tag{2.5}$$

where μ is the replacement rate of the hosts per hours, α_1 and α_2 is infection rate per hour, respectively, and r_s is the state transition rate from S to R due to real-time immune measures, r_i $(i = 1, 2)$ is the recovery rate from infected state I_1 and I_2 due to antivirus measures, respectively.

It is easy to verify the positive cone R_+^4 that is a positive invariant set with respect to system (2.5), where $R_+^4 = \{(S, I_1, I_2, R) \in R^4 : S > 0, I_1 > 0, I_2 > 0, R > 0, S(t) + I_1(t) + I_2(t) + R(t) = N\}$.

In what follows, we analyze the effect of immunization on dynamical characteristics of P2P botnets. Let g be the proportion of the hosts that have immune measures $(0 \leq g \leq 1)$. We make a simple assumption that immunization has no effect on the infected time. So, we need only to change infection rate α_1 and α_2. Let α_{11} be the proportion of hosts with immune measures in S state infected by infective hosts I_1; let α_{21} be the proportion of hosts with immune measures in S state infected by infective hosts I_2; let α_{12} $(\alpha_{11} \leq \alpha_{12})$ be the proportion of hosts without immune measures in S state infected by infective hosts I_1, and let α_{22} $(\alpha_{21} \leq \alpha_{22})$ be the proportion of hosts without immune measures in S state infected by infective hosts I_2. Therefore rewrite infection rate α_1 and α_2 as

$$\begin{aligned}
\overline{\alpha}_1 &= g\alpha_{11} + (1 - g)\alpha_{12},\\
\overline{\alpha}_2 &= g\alpha_{21} + (1 - g)\alpha_{22}.
\end{aligned} \tag{2.6}$$

Hence, the new macrolevel differential equation model is

$$\begin{aligned}
\frac{dS(t)}{dt} &= \mu N - (\overline{\alpha}_1 I_1(t) + \overline{\alpha}_2 I_2(t))\frac{S(t)}{N} - (\mu + r_s)S(t),\\
\frac{dI_1(t)}{dt} &= (\overline{\alpha}_1 I_1(t) + \overline{\alpha}_2 I_2(t))\frac{S(t)}{N} - (\mu + r_1 + \delta)I_1(t),\\
\frac{dI_2(t)}{dt} &= \delta I_1(t) - (\mu + r_2)I_2(t),\\
\frac{dR(t)}{dt} &= r_s S(t) + r_1 I_1(t) + r_2 I_2(t) - \mu R(t).
\end{aligned} \tag{2.7}$$

3. Model Analysis

To achieve the effective region of f and g, we first obtain the stable equilibria for systems (2.4) and (2.7).

3.1. *The Microlevel Model Analysis*

In this subsection, we will solve the equilibria of system (2.4) and investigate their stability.

The first two equations in system (2.4) do not depend on the third equation, and therefore this equation may be omitted without loss of generality. Hence, system (2.4) can be rewritten as

$$\begin{aligned}\frac{d\widehat{S}(t)}{dt} &= \widehat{\mu}\widehat{N} - \overline{\beta}\frac{\widehat{I}(t)\widehat{S}(t)}{\widehat{N}} - (\widehat{\mu} + \widehat{r}_s)\widehat{S}(t),\\ \frac{d\widehat{I}(t)}{dt} &= \overline{\beta}\frac{\widehat{I}(t)\widehat{S}(t)}{\widehat{N}} - (\widehat{\mu} + \widehat{r}_i)\widehat{I}(t).\end{aligned} \tag{3.1}$$

Now, we analyze system (3.1) by finding its equalibria. Steady states of system (3.1) satisfy the following equation:

$$\frac{d\widehat{S}(t)}{dt} = \frac{d\widehat{I}(t)}{dt} = 0. \tag{3.2}$$

Solving the system (3.2), we can conclude that system (3.1) always has a virus-free equilibrium (DFE) $E_0 = (\widehat{\mu}\widehat{N}/(\widehat{\mu} + \widehat{r}_s), 0)$. Furthermore, define

$$\widehat{R}_0 = \frac{\overline{\beta}\widehat{\mu}}{(\widehat{\mu} + \widehat{r}_s)(\widehat{\mu} + \widehat{r}_i)}. \tag{3.3}$$

$\widehat{R}_0$ is called the basic reproduction number. If $\widehat{R}_0 > 1$, then system (3.1) has a virus-epidemic equilibrium $E_1 = (\widehat{S}_1, \widehat{I}_1) = (((\widehat{\mu} + \widehat{r}_i)/\overline{\beta})\widehat{N}, (\mu\overline{\beta} - (\widehat{\mu} + \widehat{r}_s)(\widehat{\mu} + \widehat{r}_i)/\overline{\beta}(\widehat{\mu} + \widehat{r}_i))\widehat{N})$.

Lemma 3.1. *DFE E_0 is locally asymptotically stable when $\widehat{R}_0 < 1$ and unstable when $\widehat{R}_0 > 1$.*

Proof. The characteristic equation of system (3.1) near E_0 is

$$\det\begin{pmatrix} -(\widehat{\mu} + \widehat{r}_s) - \lambda & -\dfrac{\overline{\beta}\widehat{\mu}}{\widehat{\mu} + \widehat{r}_s} \\ 0 & \dfrac{\overline{\beta}\widehat{\mu} - (\widehat{r}_i + \widehat{\mu})(\widehat{\mu} + \widehat{r}_s)}{\widehat{\mu} + \widehat{r}_s} - \lambda \end{pmatrix} = 0. \tag{3.4}$$

Solving (3.4), we can get $\lambda_1 = -(\widehat{\mu} + \widehat{r}_s)$, $\lambda_2 = (\overline{\beta}\widehat{\mu} - (\widehat{r}_i + \widehat{\mu})(\widehat{\mu} + \widehat{r}_s))/(\widehat{\mu} + \widehat{r}_s) \equiv (\widehat{r}_i + \widehat{\mu})(\widehat{R}_0 - 1)$. Obviously, DFE is locally asymptotically stable when $\widehat{R}_0 < 1$ and unstable when $\widehat{R}_0 > 1$. □

Further, we have the following theorem.

Theorem 3.2. *DFE E_0 is global asymptotically stable if $\widehat{R}_0 \le 1$.*

Proof. Learn from the first equation of system (3.1)

$$\dot{\widehat{S}}(t) \le \widehat{\mu}\widehat{N} - \left(\widehat{\mu} + \widehat{r}_s\right)\widehat{S}(t). \tag{3.5}$$

Thus,

$$\widehat{S}(t) \le \frac{\widehat{\mu}\widehat{N}}{\widehat{\mu} + \widehat{r}_s} + \left(\widehat{S}(0) - \frac{\widehat{\mu}N}{\widehat{\mu} + \widehat{r}_s}\right) \exp\left[-\left(\widehat{\mu} + \widehat{r}_s\right)t\right]. \tag{3.6}$$

When $t \rightarrow \infty$, one can get

$$\widehat{S}(t) \le \frac{\widehat{\mu}\widehat{N}}{\widehat{\mu} + \widehat{r}_s}. \tag{3.7}$$

We choose Lyapunov function to be the form

$$V(t) = \widehat{I}(t). \tag{3.8}$$

The time derivative of $V(t)$ along system (3.1) is given by

$$\dot{V}(t) = \dot{\widehat{I}}(t) = \overline{\beta}\frac{\widehat{I}(t)\widehat{S}(t)}{\widehat{N}} - \left(\widehat{\mu} + \widehat{r}_i\right)\widehat{I}(t) \le \left[\overline{\beta}\frac{\widehat{\mu}}{\widehat{\mu} + \widehat{r}_s} - \left(\widehat{\mu} + \widehat{r}_i\right)\right]\widehat{I}(t) = \left(\widehat{\mu} + \widehat{r}_i\right)\left(\widehat{R}_0 - 1\right) \le 0. \tag{3.9}$$

The theorem is proven. □

Next, we will analyze the stability of virus-epidemic equilibrium E_1 of system (3.1).

Theorem 3.3. *If $\widehat{R}_0 > 1$, then the virus-epidemic equilibrium E_1 of system* (3.1) *is locally asymptotically stable.*

Proof. The characteristic equation of system (3.1) at E_1 is given by

$$\det\begin{pmatrix} -\dfrac{\overline{\beta}\widehat{I}_1}{\widehat{N}} - \left(\widehat{\mu} + \widehat{r}_s\right) - \lambda & -\dfrac{\overline{\beta}\widehat{S}_1}{\widehat{N}} \\ \dfrac{\overline{\beta}\widehat{I}_1}{\widehat{N}} & \dfrac{\overline{\beta}\widehat{S}_1}{\widehat{N}} - \left(\widehat{\mu} + \widehat{r}_i\right) - \lambda \end{pmatrix} = 0, \tag{3.10}$$

which equals

$$\lambda^2 + a\lambda + b = 0, \tag{3.11}$$

where $a = (\widehat{\mu} + \widehat{r}_s)\widehat{R}_0$, $b = (\widehat{\mu} + \widehat{r}_s)(\widehat{\mu} + \widehat{r}_i)(\widehat{R}_0 - 1) + \widehat{r}_s(1 - \widehat{\mu})$. Obviously, in accordance with the relationship between roots and coefficients of quadratic equation, all eigenvalues of (3.11) have negative real parts. Thus, E_1 is locally asymptotically stable when $\widehat{R}_0 > 1$. □

Theorem 3.4. *If $\widehat{R}_0 > 1$, then the virus-epidemic equilibrium E_1 is globally asymptotically stable.*

Proof. Consider the following Lypunov function [26]

$$V = \int_{\widehat{S}_1}^{\widehat{S}} \frac{x - \widehat{s}_1}{x}\,dx + \int_{\widehat{I}_1}^{\widehat{I}} \frac{x - \widehat{I}_1}{x}\,dx, \tag{3.12}$$

which is always positive in R_+^2. Moreover, the function satisfies

$$\begin{aligned}\dot{V} &= \frac{\widehat{S} - \widehat{S}_1}{\widehat{S}}\widehat{S}' + \frac{\widehat{I} - \widehat{I}_1}{\widehat{I}}\widehat{I}' = \left(1 - \frac{\widehat{S}_1}{\widehat{S}}\right)\left[\widehat{\mu}\widehat{N} - \widehat{\beta}\frac{\widehat{I}\widehat{S}}{\widehat{N}} - (\widehat{\mu} + \widehat{r}_s)\widehat{S}\right] \\ &\quad + \left(1 - \frac{\widehat{I}_1}{\widehat{I}}\right)\left[\widehat{\beta}\frac{\widehat{I}\widehat{S}}{\widehat{N}} - (\widehat{\mu} + \widehat{r}_i)\widehat{I}\right] = -\widehat{\mu}\frac{\widehat{S}}{\widehat{S}_1}\left(\frac{\widehat{S}_1}{\widehat{S}} - 1\right)^2 \leq 0.\end{aligned} \tag{3.13}$$

Thus, we prove that the endemic equilibrium E_1 is globally asymptotically stable. □

3.2. The Macrolevel Model Analysis

In this subsection, we will solve the equilibria of system (2.7) and investigate their stability.

The first two equations in system (2.7) do not depend on the third equation, and therefore this equation may be omitted without loss of generality. Hence, system (2.7) can be rewritten as

$$\begin{aligned}\frac{dS(t)}{dt} &= \mu N - (\overline{\alpha}_1 I_1(t) + \overline{\alpha}_2 I_2(t))\frac{S(t)}{N} - (\mu + r_s)S(t), \\ \frac{dI_1(t)}{dt} &= (\overline{\alpha}_1 I_1(t) + \overline{\alpha}_2 I_2(t))\frac{S(t)}{N} - (\mu + r_1 + \delta)I_1(t), \\ \frac{dI_2(t)}{dt} &= \delta I_1(t) - (\mu + r_2)I_2(t).\end{aligned} \tag{3.14}$$

The equalibria of system (3.14) are determined by setting $dS(t)/dt = dI_1(t)/dt = dI_2(t)/dt = 0$. There is always a virus-free equilibrium (DFE) $Q_0 = ((\mu/(\mu + r_s))N, 0, 0)$. Furthermore, define

$$R_0 = \frac{\mu[\overline{\alpha}_1(\mu + r_2) + \overline{\alpha}_2\delta]}{(\delta + \mu + r_1)(\mu + r_s)(\mu + r_2)}. \tag{3.15}$$

If $R_0 > 1$, system (3.14) has a virus-epidemic equilibrium $Q_1 = (S^*, I_1^*, I_2^*)$, where

$$S^* = \frac{(\delta+\mu+r_1)(\mu+r_2)}{\overline{\alpha}_1(\mu+r_2)+\overline{\alpha}_2\delta}N, \qquad I_1^* = \frac{(\mu+r_2)(\mu+r_s)}{\overline{\alpha}_1(\mu+r_2)+\overline{\alpha}_2\delta}(R_0-1)N,$$
$$I_2^* = \frac{\delta(\mu+r_s)}{\overline{\alpha}_1(\mu+r_2)+\overline{\alpha}_2\delta}(R_0-1)N. \tag{3.16}$$

Lemma 3.5. *DFE Q_0 of system* (3.14) *is locally asymptotically stable when $R_0 < 1$ and unstable when $R_0 > 1$.*

Proof. The characteristic equation of system (3.14) near DFE Q_0 can be written as follows:

$$\det\begin{pmatrix} -(\mu+r_s)-\lambda & -\dfrac{\overline{\alpha}_1\mu}{\mu+r_s} & -\dfrac{\overline{\alpha}_2\mu}{\mu+r_s} \\ 0 & \dfrac{\overline{\alpha}_1\mu-(\delta+r_1+\mu)(\mu+r_s)}{\mu+r_s}-\lambda & \dfrac{\overline{\alpha}_2\mu}{\mu+r_s} \\ 0 & \delta & -(\mu+r_2)-\lambda \end{pmatrix} = 0. \tag{3.17}$$

The above equation has a negative real part characteristic root $\lambda = -(\mu + r_s)$ and roots of

$$[-(\mu+r_s)-\lambda]\left(\lambda^2+c\lambda+d\right)=0, \tag{3.18}$$

where $c = \mu + r_2 - (\overline{\alpha}_1\mu/(\mu + r_s)) + \delta + \mu + r_1,\ d = (\mu + r_2)(\delta + \mu + r_1)(1 - R_0)$.

It is easy to verify that c is always positive. Obviously, when $R_0 < 1$, d is positive. In accordance with the relationship between roots and coefficients of quadratic equation, there are no positive real roots of (3.18). Hence, DFE Q_0 of system (3.14) is locally asymptotically stable when $R_0 < 1$ and unstable when $R_0 > 1$. □

Further, the following theorem holds.

Theorem 3.6. *DFE Q_0 of system* (3.14) *is global asymptotically stable if $R_0 \le 1$.*

Proof. From the first equation of system (3.14), we obtain

$$\dot{S}(t) \le \mu N - (\mu + r_s)S(t). \tag{3.19}$$

Thus,

$$S(t) \le \frac{\mu N}{\mu+r_s} + \left(S(0) - \frac{\mu N}{\mu+r_s}\right)\exp[-(\mu+r_s)t]. \tag{3.20}$$

When $t \rightarrow \infty$, we have

$$S(t) \leq \frac{\mu}{\mu + r_s} N. \tag{3.21}$$

Consider the Lyapunov function

$$V(I_1, I_2) = (\mu + r_2) I_1 + \frac{\mu \overline{\alpha}_2}{\mu + r_s} I_2, \tag{3.22}$$

which is always positive in R_+^2 where $R_+^2 = \{(I_1, I_2) \in R^2 : I_1 > 0, I_2 > 0\}$. Moreover, in the case of system (3.14), the function satisfies

$$\begin{aligned}
\dot{V}(I_1, I_2) &= (\mu + r_2)(\overline{\alpha}_1 I_1 + \overline{\alpha}_2 I_2) \frac{S}{N} - (\mu + r_2)(\mu + r_1 + \delta) I_1 + \frac{\mu \overline{\alpha}_2 \delta}{\mu + r_s} I_1 - \frac{\mu \overline{\alpha}_2 (\mu + r_2)}{\mu + r_s} I_2 \\
&\leq (\mu + r_2)(\overline{\alpha}_1 I_1 + \overline{\alpha}_2 I_2) \frac{\mu}{\mu + r_s} - (\mu + r_2)(\mu + r_1 + \delta) I_1 + \frac{\mu \overline{\alpha}_2 \delta}{\mu + r_s} I_1 - \frac{\mu \overline{\alpha}_2 (\mu + r_2)}{\mu + r_s} I_2 \\
&= \frac{\mu [\overline{\alpha}_1 (\mu + r_2) + \overline{\alpha}_2 \delta] - (\mu + r_2)(\mu + r_1 + \delta)(\mu + r_s)}{\mu + r_s} I_1 \\
&= (\mu + r_2)(\mu + r_1 + \delta)(R_0 - 1) I_1. \\
&\leq 0
\end{aligned} \tag{3.23}$$

So, the DFE Q_0 is globally attractive. Combining Lemma 3.5, we have DFE Q_0 is globally asymptotically stable. □

Next, we will analyze the stability of virus-epidemic equilibrium Q_1 of system (3.14). The characteristic equation of system (3.14) near endemic equilibrium Q_1 is given by

$$\det \begin{pmatrix} -(\overline{\alpha}_1 I_1^* + \overline{\alpha}_2 I_2^*) - (\mu + r_s) - \lambda & -\overline{\alpha}_1 S_1 & -\overline{\alpha}_2 S_1 \\ \overline{\alpha}_1 I_1^* + \overline{\alpha}_2 I_2^* & \overline{\alpha}_1 S - (\mu + r_1 + \delta) & \overline{\alpha}_2 S_1 \\ 0 & \delta & -(\mu + r_2) - \lambda \end{pmatrix} = 0, \tag{3.24}$$

which corresponds to

$$\begin{aligned}
&\lambda^3 + (g_3 + g_5 + g_6 - g_7)\lambda^2 + (g_3 g_5 + g_3 g_6 + g_5 g_6 - g_3 g_7 - g_4 S^* - g_6 g_7 + g_1 g_7)\lambda \\
&\quad + g_3 g_5 g_6 - g_3 g_7 g_6 - g_4 g_6 S^* + g_1 g_3 g_7 + g_4 g_1 S^* = 0,
\end{aligned} \tag{3.25}$$

where $g_1 = \overline{\alpha}_1 I_1^* + \overline{\alpha}_2 I_2^*$, $g_2 = \mu + r_s$, $g_3 = \mu + r_2$, $g_4 = \overline{\alpha}_2 \delta$, $g_5 = \mu + r_1 + \delta$, $g_6 = \overline{\alpha}_1 I_1^* + \overline{\alpha}_2 I_2^* + \mu + r_s$, $g_7 = \overline{\alpha}_1 S^*$.

According to Hurwitz criteria

$$\begin{aligned} H_1 &= g_3 + g_5 + g_6 - g_7 \\ &= 3\mu + r_1 + r_2 + r_s + \delta + \overline{\alpha}_1 I_1^* + \overline{\alpha}_1 I_2^* - \overline{\alpha}_1 S^* \\ &> 2\mu + r_2 + r_s + \overline{\alpha}_1 I_1^* + \overline{\alpha}_1 I_2^* \\ &> 0, \end{aligned} \tag{3.26}$$

$$\begin{aligned} H_2 = {} & (g_3 + g_5 + g_6 - g_7)(g_3 g_5 + g_3 g_6 + g_5 g_6 - g_3 g_7 - g_4 S^* - g_6 g_7 + g_1 g_7) \\ & - (g_3 g_5 g_6 - g_3 g_7 g_6 - g_4 g_6 S^* + g_1 g_3 g_7 + g_4 g_1 S^*), \\ H_3 = {} & (g_3 g_5 g_6 - g_3 g_7 g_6 - g_4 g_6 S^* + g_1 g_3 g_7 + g_4 g_1 S^*) H_2. \end{aligned}$$

Hence, we can get the following theorem.

Theorem 3.7. *Let $R_0 > 1$. if $H_2 > 0$ and $H_3 > 0$ hold, then the virus-epidemic equilibrium Q_1 of system* (3.14) *is locally asymptotically stable.*

4. Control Strategies of P2P Botnets

Theorems 3.2 and 3.6 indicate that P2P botnets will be eliminated if reasonable antivirus strategies are taken (represented by the formulations of $\widehat{R}_0$ and R_0). Here, we will investigate effective methods eliminating P2P botnets by deriving the feasible region of f and g.

First, we derive the feasible region of f. Substituting (2.3) into (3.3), we have

$$\widehat{R}_0 = \frac{\widehat{\mu}\left[f\widehat{\beta}_1 + (1-f)\widehat{\beta}_2\right]}{(\widehat{\mu} + \widehat{r}_s)(\widehat{\mu} + \widehat{r}_i)}. \tag{4.1}$$

According to the meaning of $\widehat{R}_0$, we can quantify the lower limit for an effective immunity f. When $\widehat{R}_0 = 1$, it is easy to get

$$f_e = \frac{(\widehat{\mu} + \widehat{r}_s)(\widehat{\mu} + \widehat{r}_i) - \widehat{\beta}_2\widehat{\mu}}{\left(\widehat{\beta}_1 - \widehat{\beta}_2\right)\widehat{\mu}}. \tag{4.2}$$

We define the “immune effective region” f as follows

$$0 \le f_e < f \le 1. \tag{4.3}$$

Corollary 4.1. *If $0 < f_e < 1$ and f satisfies $f_e < f \le 1$, then it is possible to eliminate botnets within P2P networks. Otherwise, if $f_e > 1$ or $f_e > f$, then immunization can only reduce the scale of P2P botnets.*

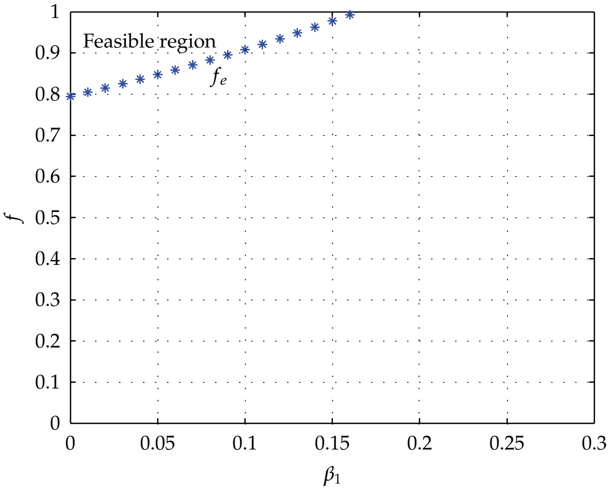


Figure 3: The theoretical immune feasible region f.

Similarly, one will get the feasible region of g. Substituting (2.6) into (3.15), one can obtain

$$R_0 = \frac{\mu\{[g\alpha_{11} + (1-g)\alpha_{12}](\mu + r_2) + \delta[g\alpha_{21} + (1-g)\alpha_{22}]\}}{(\delta + \mu + r_1)(\mu + r_s)(\mu + r_2)}. \tag{4.4}$$

According to the meaning of R_0, one can quantify the lower limit for an effective immunization g. When $R_0 = 1$, one has

$$g_e = \frac{(\mu + r_2)(\mu + r_s)(\delta + \mu + r_1) - \mu[(\mu + r_2)\alpha_{12} + \delta\alpha_{22}]}{\mu[(\mu + r_2)(\alpha_{11} - \alpha_{12}) + \delta(\alpha_{21} - \alpha_{22})]}. \tag{4.5}$$

Define "immune effective region" g as follows.

$$0 \leq g_e < g \leq 1. \tag{4.6}$$

Corollary 4.2. *If $0 < g_e < 1$ and g satisfies $g_e < g \leq 1$, then it is possible to eliminate P2P botnets on Internet. Otherwise, if $g_e > 1$ or $g_e > g$, then immunization can only reduce the scale of P2P botnets.*

The numerical solution of f_e obtained from (4.2) is plotted with different value of β_1 and fixed values of $\mu = 2.28 \times 10^{-4}$, $\beta_2 = 0.8$, $\widehat{r}_s = 0.0059$, and $\widehat{r}_i = 0.0059$ in Figure 3. Similarly, Figure 4 depicts the numerical solution of g_e obtained from (4.5) with different value of α_{21} and fixed values of $\mu = 2.28 \times 10^{-4}$, $\delta = 0.5$, $r_s = 0.015$, $r_1 = 0.0059, r_2 = 0.0059, \alpha_{12} = 0.5, \alpha_{11} = 0.1$, and $\alpha_{22} = 0.7$.

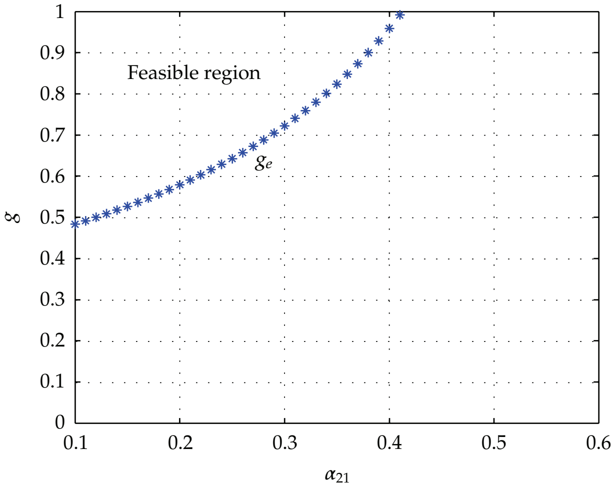


Figure 4: The theoretical immune feasible region g.

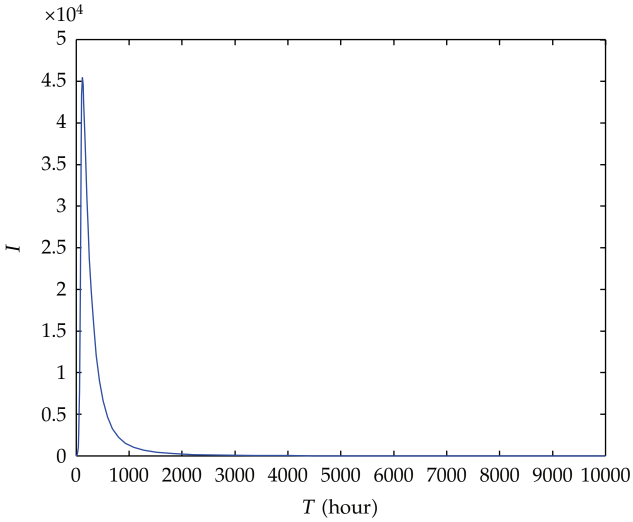


Figure 5: The virus propagation result when $f > f_e$.

5. Numerical Simulations

To validate the accuracy of f_e obtained from (4.2), we simulate system (2.4) with the following parameters: $N = 100000$, $\mu = 2.28E-4$, $\beta_2 = 0.8$, $r_s = 0.0059$, $r_i = 0.0059$, $\beta_1 = 0.1$, and (i) $f = 0.95$, where $f > f_e = 0.9079$; (ii) $f = 0.6$, where $f < f_e = 0.9079$. Initial values are set to $S(0) = 99998, I(0) = 10$, and $R(0) = 0$, respectively. Figures 5 and 6 show the simulation results with the above two sets of parameters, respectively, which are consistent with theoretical prediction.

Similarly, we verify the accuracy of g_e obtained from (4.5) by simulating system (2.7). The following parameter values are adopted: $\mu = 2.28E-4$, $\alpha_{11} = 0.1$, $\alpha_{12} = 0.5$, $\alpha_{21} = 0.3$, $\alpha_{22} = 0.7$, $\delta = 0.5$, $r_s = 0.015$, $r_1 = r_2 = 0.0059$, and (i) $g = 0.9$, where $g > g_e = 0.7221$;

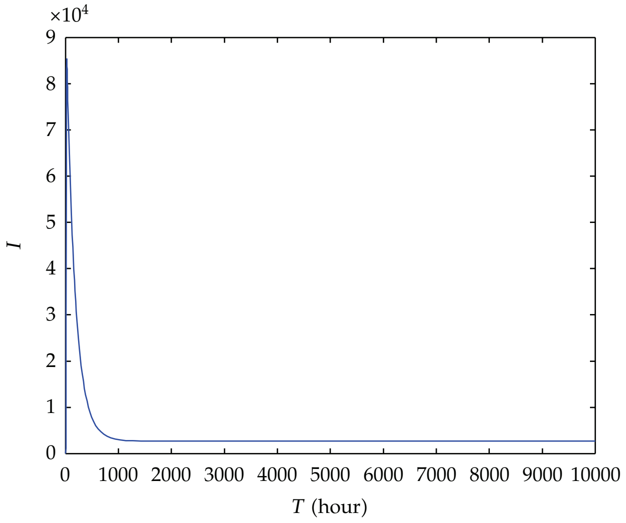


Figure 6: The virus propagation result when $f < f_e$.

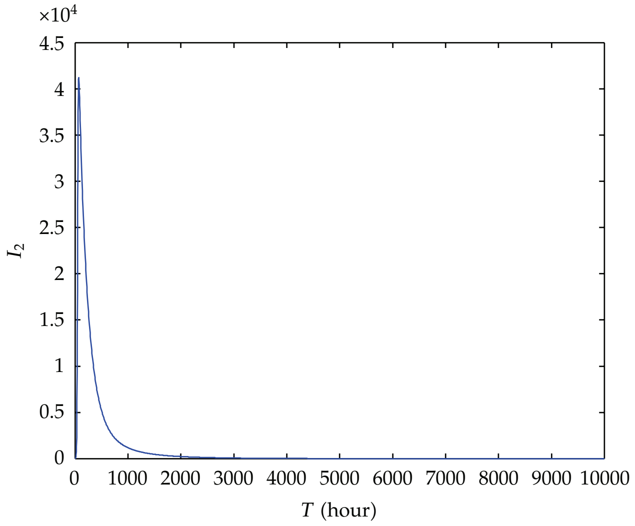


Figure 7: The result of virus propagation when $g > g_e$.

(ii) $g = 0.2$, where $g < g_e = 0.7221$. Initial values are set to $S(0) = 99996, I_1(0) = 2, I_2(0) = 2$, and $R(0) = 0$, respectively. Simulation results in Figures 7 and 8 are consistent with theoretical prediction.

For investigating the effect of different replacement rate $\widehat{\mu}$ on f, we depict simulation results of f_e in Figure 9, in which we set $\widehat{\mu} = 1.14E-4,\ 2.28\times10^{-4}, 3.42E-4$, and $4.57E-4$, that is, replacement time is one year, nine months, a half year, and three months. Other parameters are the same to Figure 3.

Similarly, for investigating the effect of μ on g, we set $\mu = 1.14E-4,\ 2.28\times10^{-4}, 3.42E-4$, and $4.57E-4$; other parameters are the same to Figure 4. The simulation result is depicted in Figure 10.

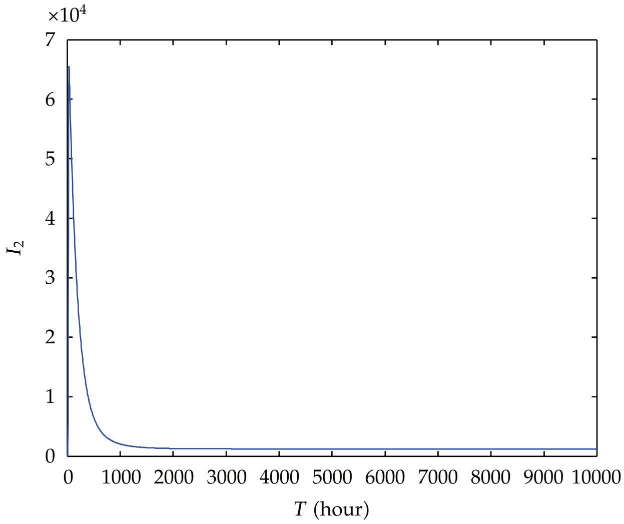


Figure 8: The result of virus propagation when $g < g_e$.

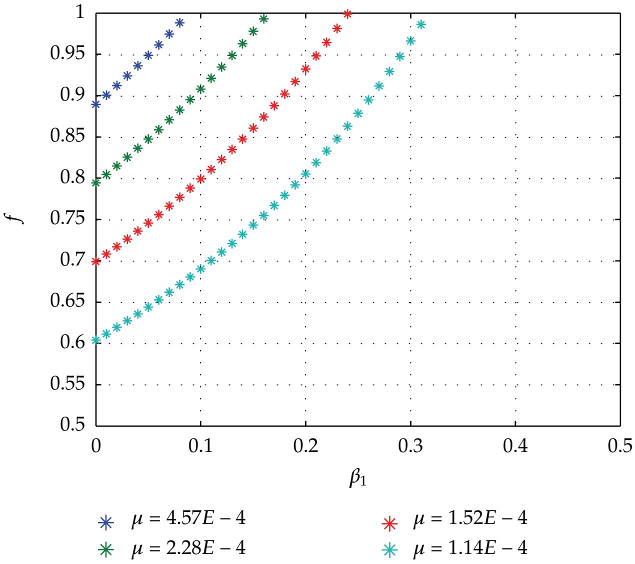


Figure 9: The effect of different μ on f_e.

Figures 9 and 10 reflect the fact that decreasing the replacement rate of computers can enhance the effectiveness of immunizations. This finding contributes to management and maintenance of networks at a cost-effective way.

6. Conclusions

As a kind of new form of botnets, P2P botnets have attracted considerable attention. In this paper, the authors explore two novel dynamical models. The first is a micro-level model

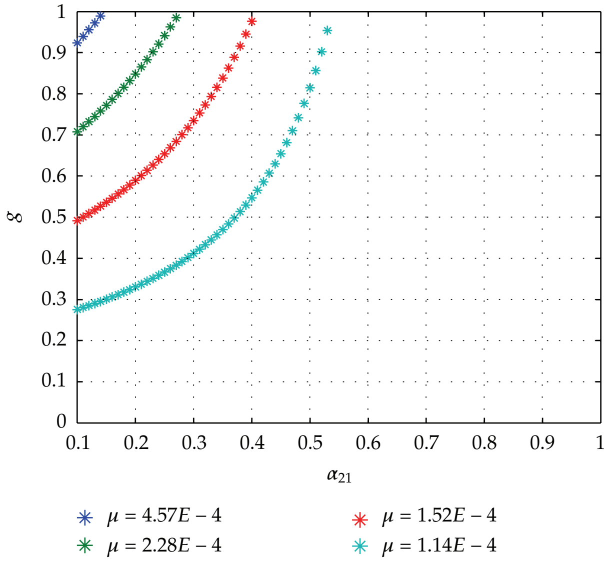


Figure 10: The effect of different μ on g_e.

which describes the dynamical behavior of *Parasite P2P botnets*. The Second is the macro-level model which characterizes the dynamical action of *Leaching P2P botnet*. Throughout the paper, we focus on the effect of immunization on dynamics of P2P botnets. Through detailed mathematical analysis, the feasible region of immunization has been derived. In addition, we simulate the feasible region of immunization by using different parameter values. Furthermore, the correctness of feasible region has been verified.

The thresholds of immunizations have demonstrated that antivirus strategies have great influence on the dynamics of P2P botnets. More specifically, in feasible regions of immunizations, the spread of computer viruses will be stopped, and the botnet will be cracked. In contrary, immune measures merely decrease the scale of hosts infected by computer viruses, and the botnet will survive. In addition, our results also show that the replacement rate of computers will affect the threshold of immunizations.

Our investigations can provide insight on the effectiveness of various antivirus measures (e.g., antivirus products and user education). According to the thresholds of (4.2) and (4.5), secure organizations can make cost-effective countermeasures to work well in practice. Our study is only limited to unstructured P2P networks, such as Gnutella. Taken a step further, our models are adapted to topology-independent malware, such as file-sharing worms, viruses, Trojans, and so on. In the future, we will concentrate our attentions on the propagation model of topology-aware malware.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 60973114, Grant 61170249, and Grant 61003247, in part by the Natural Science Foundation project of CQCSTC under Grant 2009BA2024, and in part by the State Key

Laboratory of Power Transmission Equipment and System Security and New Technology, Chongqing University, under Grant 2007DA10512711206.

References

[1] L. P. Song, Z. Jin, and G. Q. Sun, "Modeling and analyzing of botnet interactions," *Physica A*, vol. 390, no. 2, pp. 347–358, 2011.

[2] W. F. Zhang and C. Jin, "The research on approaches for botnet detection," *Energy Procedia*, vol. 13, pp. 9726–9732, 2011.

[3] "Symantec Internet Security Threat Report," 2011, http://www.symantec.com/threatreport/topic.jsp?id=threatreport.

[4] A. K. Seewald and W. N. Gansterer, "On the detection and identification of botnets," *Computers and Security*, vol. 29, no. 1, pp. 45–58, 2010.

[5] C. Elliott, "Botnets: to what extent are they a threat to information security?" *Information Security Technical Report*, vol. 15, no. 3, pp. 79–103, 2010.

[6] W. Lu, G. Rammidi, and A. A. Ghorbani, "Clustering botnet communication traffic based on n-gram feature selection," *Computer Communications*, vol. 34, no. 3, pp. 502–514, 2011.

[7] J. Rrushi, E. Mokhtari, and A. A. Ghorbani, "Estimating botnet virulence within mathematical models of botnet propagation dynamics," *Computer & Security*, vol. 30, pp. 791–802, 2011.

[8] G. P. Schaffer, "Worms and viruses and botnets, Oh My!: rational responses to emerging internet threats," *IEEE Security and Privacy*, vol. 4, no. 3, pp. 52–58, 2006.

[9] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security and Privacy*, vol. 1, no. 4, pp. 33–39, 2003.

[10] G. Goth, "Fast-moving Zombies: botnets stay a step ahead of the fixes," *IEEE Internet Computing*, vol. 11, no. 2, pp. 7–9, 2007.

[11] P. Barford and V. Yegneswaran, "An inside look at botnets," *Malware Detection*, vol. 27, pp. 171–191, 2007.

[12] D. Dagon, C. C. Zou, and W. K. Lee, "Modeling botnet propagation using time and zones," in *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS' 06)*, 2006.

[13] J. B. Grizzard, V. Sharma, C. Nunnery, and B. B. H. Kang, "Peer-to-peer botnet: overview and case study," in *Proceedings of the 1st conference on First Workshop on Hot Topics in understanding Botnets*, pp. 1–8, 2007.

[14] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, "Measurements and mitigation of peer-to-peer-based botnets: a case study on storm eorm," in *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, 2008.

[15] E. Van Ruitenbeek and W. H. Sanders, "Modeling peer-to-peer botnets," in *Proceedings of the 5th International Conference on the Quantitative Evaluation of Systems (QEST '08)*, pp. 307–316, September 2008.

[16] A. Kolesnichenko, A. Remke, P. T. 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.

[17] G. Yan, D. T. Ha, and S. Eidenbenz, "AntBot: anti-pollution peer-to-peer botnets," *Computer Networks*, vol. 55, no. 8, pp. 1941–1956, 2011.

[18] P. Wang, B. Aslam, and C. C. Zou, *Peer-to-Peer Botnets: The Next Generation of Botnet Attacks*, School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, Fla, USA, 2010.

[19] J. G. Ren, X. F. Yang, Q. Y. Zhu, L. X. Yang, and C. M. Zhang, "A novel computer virus model and its dynamics," *Nonlinear Analysis: Real World Applications*, vol. 13, no. 1, pp. 376–384, 2012.

[20] Q. Y. Zhu, X. F. Yang, L. X. Yang, and C. M. Zhang, "Optimal control of computer virus under a delayed model," *Applied Mathematics and Computation*, vol. 218, no. 23, pp. 11613–11619, 2012.

[21] L. P. Feng, X. F. Liao, H. Q. Li, and Q. Han, "Hopf bifurcation analysis of a delayed viral infection model in computer networks," *Mathematics and Computer Modeling*, vol. 56, pp. 167–179, 2012.

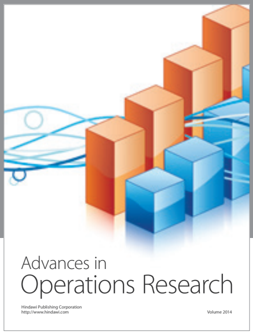
[22] L. X. Yang and X. F. Yang, "Propagation behavior of virus code in the situation that infected computers are connected to the Internet with possible probability," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 693695, 13 pages, 2012.

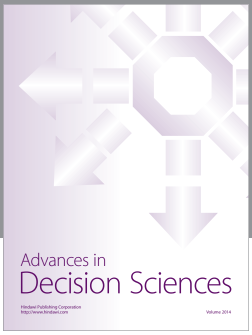
[23] X. F. Yang and L. X. Yang, "Towards the epidemiological modeling of computer viruses," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 259671, 2012.

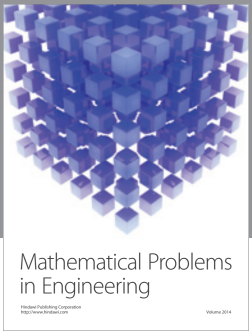
[24] Q. Y. Zhu, X. F. Yang, and J. G. Ren, "Modeling and analysis of the spread of computer virus," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, pp. 5117–5124, 2012.

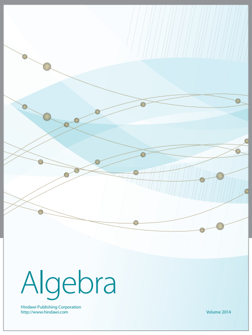
[25] C. Q. Gan, X. F. Yang, W. P. Liu, Q. Y. Zhu, and X. L. Zhang, "Propagation of computer virus under human intervention: a dynamical model," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 106950, 8 pages, 2012.

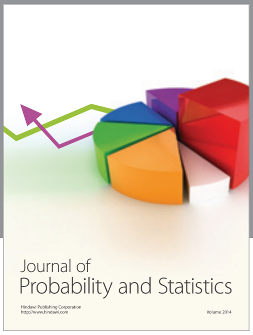
[26] H. Yuan and G. Q. Chen, "Network virus-epidemic model with the point-to-group information propagation," *Applied Mathematics and Computation*, vol. 206, no. 1, pp. 357–367, 2008.


Advances in
Operations Research

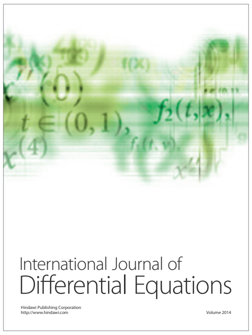

Advances in
Decision Sciences

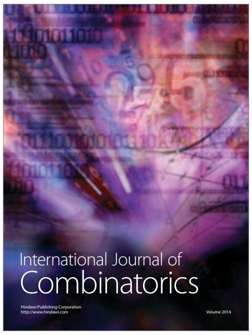

Mathematical Problems
in Engineering

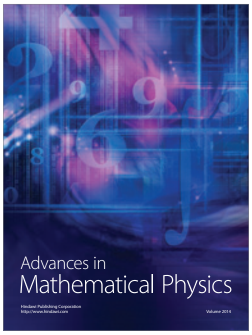

Algebra

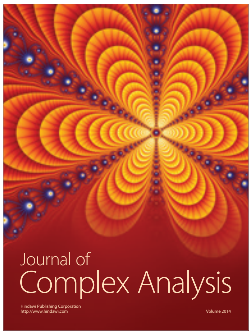

Journal of
Probability and Statistics

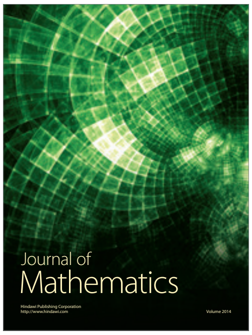
The Scientific
World Journal

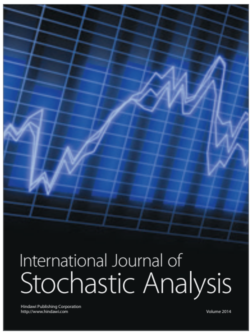

International Journal of
Differential Equations

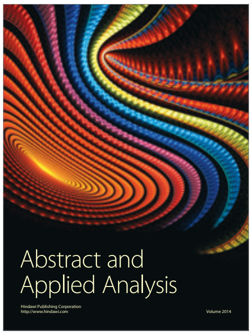

International Journal of
Combinatorics

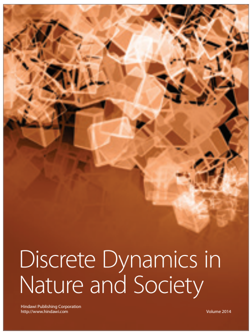

Advances in
Mathematical Physics

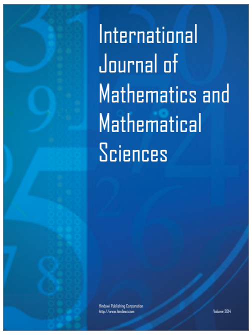

Journal of
Complex Analysis


Journal of
Mathematics


International Journal of
Stochastic Analysis

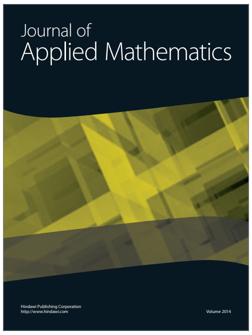

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


Journal of
Applied Mathematics

Journal of
Optimization