

Research Article

Modeling Peer-to-Peer Botnet on Scale-Free Network

Liping Feng,¹ Hongbin Wang,¹ Qi Han,² Qingshan Zhao,¹ and Lipeng Song³

¹ Department of Computer Science and Technology, Xinzhou Teachers University, Xinzhou 034000, China

² School of Electronic and Information Engineering, Chongqing University of Science and Technology, Chongqing 401331, China

³ Department of Computer Science and Technology, North University of China, Taiyuan 030051, China

Correspondence should be addressed to Lipeng Song; slp880@gmail.com

Received 23 January 2014; Accepted 27 March 2014; Published 23 April 2014

Academic Editor: Yun Kang

Copyright © 2014 Liping Feng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-to-peer (P2P) botnets have emerged as one of the serious threats to Internet security. To prevent effectively P2P botnet, in this paper, a mathematical model which combines the scale-free trait of Internet with the formation of P2P botnet is presented. Explicit mathematical analysis demonstrates that the model has a globally stable endemic equilibrium when infection rate is greater than a critical value. Meanwhile, we find that, in scale-free network, the critical value is very little. Hence, it is unrealistic to completely dispel the P2P botnet. Numerical simulations show that one can take effective countermeasures to reduce the scale of P2P botnet or delay its outbreak. Our findings can provide meaningful instruction to network security management.

1. Introduction

A botnet is a network of thousands of compromised computers (bots) under the control of botmaster, which usually recruits new vulnerable computers by running all kinds of malicious software, such as Trojan horses, worms, and computer viruses [1]. For nefarious profits, the botnetmaster which operates a botnet manipulates remotely zombie computers to work on various malicious activities, such as distributed denial-of-service attacks (DDoS), email spam, and password cracking. Nowadays, botnets have become one of the most serious threats to Internet.

According to operating mechanism of botnets, there are two kinds of botnets. One is the traditional botnet using Internet relay chat (IRC) as a form of communication for centralized command and control (C&C) structure (see Figure 1 [2]). The other is peer-to-peer botnet utilizing a distributed command-and-control structure (see Figure 2 [2]). Traditional botnets are easily checked and cracked by defenders, and the threats of botnets can be mitigated and eliminated if the central of C&C is unavailable [3]. By contrast, P2P botnets employing a decentralized command-and-control structure are more robust and are much harder for security community to dismantle [4]. Therefore, P2P botnets, such as Trojan.Peach and Storm botnet [5], have

emerged and gradually escalated in recent years. Moreover, P2P botnets are increasingly sophisticated and thus their potential damage is much greater than traditional botnets. Further, the potential for more damage exists in the future.

Therefore, threats of P2P botnets to Internet security have drawn widespread attention [6–12]. Yan et al. [6] mathematically analyzed the performance of Antbot—a new type of P2P botnets—from the perspectives of resilience, reachability, and scalability, and the authors developed a distributed P2P botnet simulator to evaluate the effectiveness of Antbot against pollution-based mitigation in practice. Kolesnichenko et al. [7] developed the mean-field model to analyze behaviors of P2P botnet and compared it with simulations obtained from the Mobius tool (a software tool for modeling the behavior of complex systems). Results show that the mean-field method is much faster than simulation for predicting the behavior of P2P botnet. van Ruitenbeek and Sanders [8] 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. To be well prepared for future botnet attacks, Wang et al. [9] studied advanced botnet attack techniques that could be developed by botmasters in the future and proposed the design of an advanced hybrid P2P botnet. Results show that a honeypot, in computer terminology, is a trap set to detect, deflect, or,

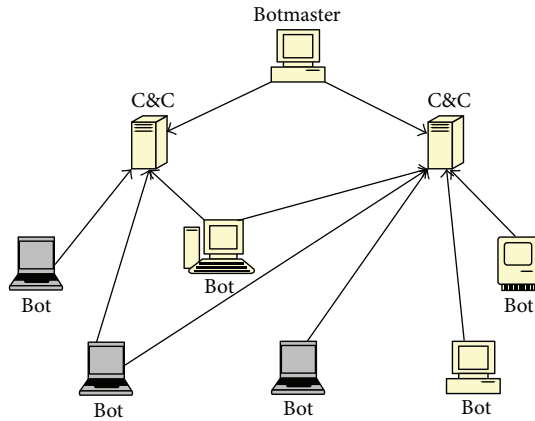


FIGURE 1: Centralized botnet.

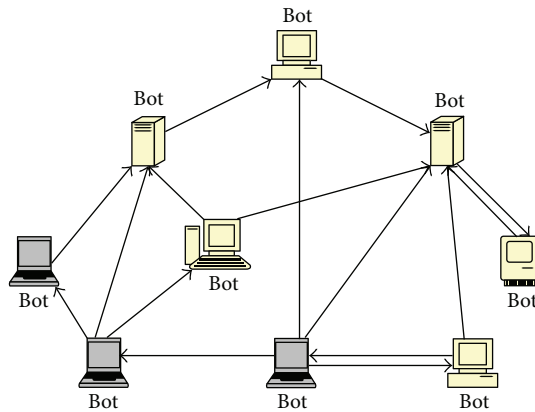


FIGURE 2: P2P botnet.

in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers—play an important role to defend against an advanced botnet.

Nevertheless, few people studied the dynamical behaviors of P2P botnets. In [7], the authors proposed a mean-field model of P2P botnet, but the model has not been analyzed mathematically. In fact, explicit mathematical analysis contributes to understand deeply the prevalent characteristics of P2P botnet. Aiming at describing the dynamics of P2P botnets in a more effective way, in this paper, we employ the dynamical model of computer worms, which has been widely used by many researchers to study Internet malware propagation [13–22]. As many botnets are created by computer worms [23], it is reasonable to describe the prevalence of P2P botnets with the model of worm propagation. In addition, by analyzing data from real computer virus epidemics, the authors [24] pointed out the importance of incorporating the peculiar topology of scale-free network in the theoretical description of computer worm propagation. In biological epidemic areas, there is much valuable research which considers the effect

of complex network on pathophoresis [25, 26]. However, we have not seen the report which considers the effect of complex network on prevalence of P2P botnet. Hence, it is necessary to examine the effect of the topology of the network on the propagation of P2P botnet.

In this paper, the dynamics of *leaching P2P botnets* are investigated. In a *leaching P2P botnet*, botmasters recruit new zombies on the Internet. For constructing this kind of P2P botnet, there are two steps: the first step is trying to infect new vulnerable hosts throughout the Internet, and the second step is newly compromised hosts joining the botnet and connecting with other bots [2]. In SF network, taking into account the heterogeneity induced by the hosts with different degree k , we divide the hosts into different states where the hosts in each state have the same degree k .

2. The Model

To model the propagation of the P2P botnet on the Internet, we assume that the total number of nodes on Internet is a constant N . Each node changes over time among four states: susceptible (S), exposed (E), infected (I), and recovered (R) due to the spread of computer worm. We describe these four states in detail as follows.

- (1) Susceptible (S): a node has the software vulnerability that the bot program can exploit.
- (2) Exposed (E): a node has been infected by the bot program, but it has not become a member of P2P botnet.
- (3) Infected (I): a node is a formal member of P2P botnet, which means the node can infect its neighbors with the bot program.
- (4) Removed (R): a node has installed a detection tool that can identify and remove the bot program, or a node has installed a software patch to eliminate the node vulnerability exploited by the bot program.

There are five state transitions among these four states.

- (1) Propagating the bot program: nodes in the “susceptible” state will change to the “exposed” state with the infection rate β .
- (2) Joining the P2P botnet from exposed state: nodes in the “exposed” state will join the P2P botnet under the control of the botmaster and change to “infected” state at the proportion δ .
- (3) Immunizing nodes from susceptible state: nodes in the “susceptible” state will change to the “recovered” state at the proportion r_s if corresponding nodes take countermeasures, for example, antivirus software, patching, firewall, and intrusion detection system (IDS). The immune rate is affected by many factors, for example, user vigilance.
- (4) Immunizing nodes from exposed state: nodes in the “exposed” state will change to the “recovered” state at the proportion r_1 if corresponding nodes take antivirus countermeasures.

- (5) Immunizing nodes from infected state: nodes in the “infected” state will change to the “recovered” state at the proportion r_2 if corresponding nodes take antivirus countermeasures.

Let $S_k(t)$, $E_k(t)$, $I_k(t)$, and $R_k(t)$ be the number of degree k in states S , E , I , and R at time t , respectively. Then one has

$$S_k(t) + E_k(t) + I_k(t) + R_k(t) = N. \tag{1}$$

The dynamic equations can be written as

$$\begin{aligned} \frac{dS_k(t)}{dt} &= \mu - \alpha k \theta (I(t)) S_k(t) - (\mu + r_s) S_k(t), \\ \frac{dE_k(t)}{dt} &= \alpha k \theta (I(t)) S_k(t) - (\mu + r_1 + \delta) E_k(t), \\ \frac{dI_k(t)}{dt} &= \delta E_k(t) - (\mu + r_2) I_k(t), \\ \frac{dR_k(t)}{dt} &= r_s S_k(t) + r_1 E_k(t) + r_2 I_k(t) - \mu R_k(t), \end{aligned} \tag{2}$$

where the probability $0 \leq \theta(I(t)) \leq 1$ describes a link pointing to an infected host, which satisfies the relation

$$\theta(I(t)) = \frac{1}{\langle k \rangle} \sum_k k P(k) I_k(t), \tag{3}$$

and $I(t) = \sum_k P(k) I_k$ is the density of infected hosts in the whole network at time t ; $P(k)$ is a degree distribution. Other parameters can be explained as follows. μ is the replacement rate of the hosts per hour; α is infection rate per hour; r_s is the state transition rate from S_k to R_k due to immune measures; r_i ($i = 1, 2$) is the recovery rate from exposed state E_k and infected state I_k , respectively; and δ is transition rate from E_k to I_k .

3. Model Analysis

In this subsection, we solve the equilibria of system (2) and investigate their stability.

The first three equations in system (2) do not depend on the fourth equation, and, therefore, this equation may be omitted without loss of generality. Hence, system (2) can be rewritten as

$$\begin{aligned} \frac{dS_k(t)}{dt} &= \mu - \alpha k \theta (I(t)) S_k(t) - (\mu + r_s) S_k(t), \\ \frac{dE_k(t)}{dt} &= \alpha k \theta (I(t)) S_k(t) - (\mu + r_1 + \delta) E_k(t), \\ \frac{dI_k(t)}{dt} &= \delta E_k(t) - (\mu + r_2) I_k(t). \end{aligned} \tag{4}$$

The equilibria of system (7) are determined by setting

$$\begin{aligned} \mu - \alpha k \theta (I(t)) S_k(t) - (\mu + r_s) S_k(t) &= 0, \\ \alpha k \theta (I(t)) S_k(t) - (\mu + r_1 + \delta) E_k(t) &= 0, \\ \delta E_k(t) - (\mu + r_2) I_k(t) &= 0. \end{aligned} \tag{5}$$

There is always a disease-free equilibrium (DFE) $Q_0 = (\mu/(\mu + r_s), 0, 0)$. Furthermore, solving the endemic equilibrium of (5), one can obtain $Q_1 = (S_k^*, E_k^*, I_k^*)$, where

$$\begin{aligned} S_k^* &= \frac{\mu}{\alpha k \theta + \mu + r_s}, \\ E_k^* &= \frac{\mu \alpha k \theta}{(\alpha k \theta + \mu + r_s) (\mu + r_1 + \delta)}, \\ I_k^* &= \frac{\delta \mu \alpha k \theta}{(\alpha k \theta + \mu + r_s) (\mu + r_1 + \delta) (\mu + r_2)}. \end{aligned} \tag{6}$$

Substituting I_k^* into (3), we have

$$\begin{aligned} \theta &= \frac{1}{\langle k \rangle} \sum_k k P(k) I_k(t) \\ &= \frac{1}{\langle k \rangle} \sum_k k P(k) \frac{\delta \mu \alpha k \theta}{(\alpha k \theta + \mu + r_s) (\mu + r_1 + \delta) (\mu + r_2)}. \end{aligned} \tag{7}$$

Obviously, if the endemic equilibrium exists, there must be $0 < \theta \leq 1$. That is, it must satisfy

$$\begin{aligned} \frac{d}{d\theta} \left[\frac{1}{\langle k \rangle} \sum_k k P(k) \frac{\delta \mu \alpha k \theta}{(\alpha k \theta + \mu + r_s) (\mu + r_1 + \delta) (\mu + r_2)} \right] \Big|_{\theta=0} \\ \geq 1, \end{aligned} \tag{8}$$

and it equals

$$\begin{aligned} \frac{1}{\langle k \rangle} \sum_k k P(k) \left\{ (\delta \mu \alpha k (\mu + r_1 + \delta) (\mu + r_2) (\alpha k \theta + \mu + r_s) \right. \\ \left. - (\mu + r_1 + \delta) (\mu + r_2) \delta \mu \alpha^2 k^2 \theta) \right. \\ \left. \times ((\alpha k \theta + \mu + r_s) (\mu + r_1 + \delta) (\mu + r_2))^{-1} \right\} \Big|_{\theta=0} \\ \geq 1. \end{aligned} \tag{9}$$

Let α_c be the minimum value of α satisfying the above inequality. Then,

$$\frac{\delta \mu \alpha_c}{\langle k \rangle (\mu + r_s) (\mu + r_1 + \delta) (\mu + r_2)} \sum_k k^2 P(k) = 1; \tag{10}$$

that is

$$\frac{\langle k^2 \rangle \delta \mu \alpha_c}{\langle k \rangle (\mu + r_s) (\mu + r_1 + \delta) (\mu + r_2)} = 1, \tag{11}$$

where $\langle k^2 \rangle = \sum_k k^2 P(k)$.

Hence,

$$\alpha_c = \frac{\langle k \rangle (\mu + r_s) (\mu + r_1 + \delta) (\mu + r_2)}{\langle k^2 \rangle \delta \mu}. \tag{12}$$

Summarizing the above analysis, one can get the following theorem.

Theorem 1. If $\alpha < \alpha_c$, then system (4) has only one free-equilibrium Q_0 ; if $\alpha > \alpha_c$, then system (4) has endemic-equilibrium Q^* except Q_0 .

In what follows, the endemic-equilibrium point Q^* will be analyzed.

The Jacobian matrix of system (4) at Q^* is

$$J = \begin{pmatrix} -\alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) I_k^* & 0 & \alpha k S_k^* \frac{1}{\langle k \rangle} \sum_k kP(k) \\ \alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) I_k^* & -(\mu + \gamma_1 + \delta) & \alpha k S_k^* \frac{1}{\langle k \rangle} \sum_k kP(k) \\ 0 & \delta & -(\mu + \gamma_2) \end{pmatrix}, \tag{13}$$

and the associated characteristic equation is

$$\lambda^3 + a\lambda^2 + b\lambda + c = 0, \tag{14}$$

where

$$\begin{aligned} a &= \mu + r_1 + \delta + \mu + r_2 + \alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) I_k^*, \\ b &= (\mu + r_1 + \delta)(\mu + r_2) - \delta \alpha k S_k^* \frac{1}{\langle k \rangle} \sum_k kP(k) \\ &\quad + \left(\alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) I_k^* + \mu + r_s \right) (r_1 + \delta + 2\mu + r_2), \\ c &= \left(\alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) I_k^* + \mu + r_s \right) (\mu + r_1 + \delta)(\mu + r_2) \\ &\quad - \left(\delta \alpha k S_k^* \frac{1}{\langle k \rangle} \sum_k kP(k) \right) \\ &\quad \times \left(\alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) I_k^* + \mu + r_s + \alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) \right). \end{aligned} \tag{15}$$

According to Hurwitz criteria [27],

$$\begin{aligned} H_1 &= \mu + r_1 + \delta + \mu + r_2 + \alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) I_k^* > 0, \\ H_2 &= H_1 b - c, \quad H_3 = H_2 c. \end{aligned} \tag{16}$$

Hence, one can obtain the following lemmas.

Lemma 2. For system (4), if $H_2 > 0$ and $H_3 > 0$ hold, then the endemic-equilibrium Q^* is locally asymptotically stable.

For depicting the globally asymptotical stability of Q^* , firstly, one can introduce three preliminary results.

Lemma 3 (see [28, 29]). Suppose that the initial relative infected density $0 < I_k(0) < 1$ satisfies $\sum_k kP(k)I_k(0) > 0$. Then, for all $t > 0$, the solution of system (4) satisfies $0 < \theta(I(t)) < 1$ and $0 < I_k(t) < 1$.

Proposition 4 (see [28, 29]). Suppose that the solution $I_k(t)$ of system (4) satisfies $\limsup_{t \rightarrow \infty} I_k \leq U_k$ and $\liminf_{t \rightarrow \infty} I_k \geq \ell_k$, where $U_k \geq 0$ and $\ell_k \geq 0$. Then,

$$\begin{aligned} \limsup_{t \rightarrow \infty} I_k &\leq \left(\alpha \delta \mu k \frac{1}{\langle k \rangle} \sum_k kP(k) U_k \right) \\ &\quad \times \left((\mu + r_1 + \delta)(\mu + r_2) \right. \\ &\quad \left. \times \left(\mu + r_s + \alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) U_k \right) \right)^{-1}, \\ \liminf_{t \rightarrow \infty} I_k &\geq \left(\alpha \delta \mu k \frac{1}{\langle k \rangle} \sum_k kP(k) \ell_k \right) \\ &\quad \times \left((\mu + r_1 + \delta)(\mu + r_2) \right. \\ &\quad \left. \times \left(\mu + r_s + \alpha k \frac{1}{\langle k \rangle} \sum_k kP(k) U_k \right) \right)^{-1}. \end{aligned} \tag{17}$$

Proposition 5 (see [28, 29]). Suppose that the initial relative infected densities $0 < I_k(0) < 1$ satisfy $\alpha > \alpha_c$ and $\sum_k kP(k)I_k(0) > 0$. Then, the solution of system (4) satisfies $\lim_{t \rightarrow \infty} \inf \theta(I(t)) > 0$ and $\lim_{t \rightarrow \infty} \inf I_k(t) > 0$.

The proofs of the above conclusions are similar to those presented in [28, 29]. Here, we will omit them.

Next, main results will be presented.

Lemma 6. Suppose that the initial relative infected densities $0 < I_k(0) < 1$ satisfy $\alpha > \alpha_c$ and $\sum_k kP(k)I_k(0) > 0$. Then, the solution of system (4) satisfies $\lim_{t \rightarrow \infty} I_k(t) = I_k$, $\lim_{t \rightarrow \infty} E_k(t) = E_k$, and $\lim_{t \rightarrow \infty} S_k(t) = S_k$, where $I_1, I_2, I_3, \dots, I_n$ ($E_1, E_2, E_3, \dots, E_n; S_1, S_2, S_3, \dots, S_n$) are the unique nonzero stationary points of system (4).

The proof is completed in the appendix

Combining Lemma 2 with Lemma 6, one can conclude the following conclusion.

Theorem 7. If the endemic-equilibrium Q^* exists, then it is globally asymptotically stable.

4. Numerical Analysis and Control Strategies

4.1. Numerical Examples. In this subsection we present the results of numerical experiments investigating the effectiveness of theoretic analysis. In order to observe the effects of parameters on transmission process, we use system (4) to simulate the evolution behavior of P2P botnet for given parameters on SF network with $\langle k \rangle = 8$ and $N = 100000$. Here, we set the parameter values of system (4) which are, respectively, $\mu = 0.01$, $r_s = 0.01$, $r_1 = 0.06$, $r_2 = 0.06$, and $\delta = 0.6$. By calculation, one can obtain $\alpha_c = 1.49 \times 10^{-5}$.

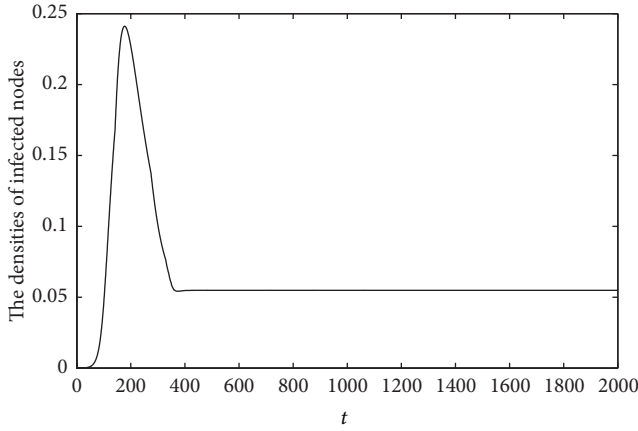


FIGURE 3: The density of infected nodes with parameters $\mu = 0.01$, $r_s = 0.01$, $r_1 = 0.06$, $r_2 = 0.06$, $\alpha = 0.005 > \alpha_c$, $\langle k \rangle = 8$, and $N = 100000$.

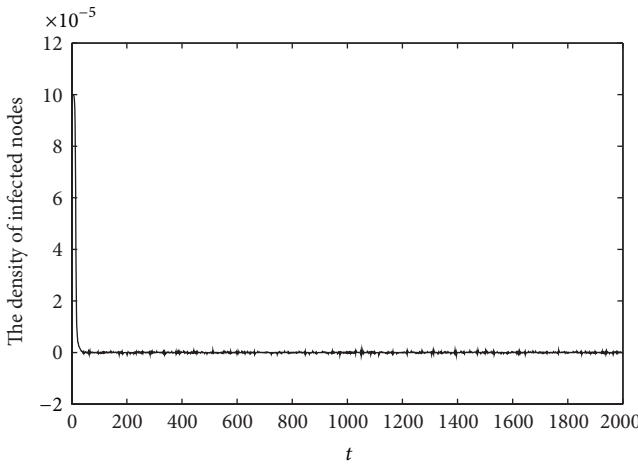


FIGURE 4: The density of infected nodes with parameters $\mu = 0.01$, $r_s = 0.01$, $r_1 = 0.06$, $r_2 = 0.06$, $\alpha = 1.5 \times 10^{-8} < \alpha_c$, $\langle k \rangle = 8$, and $N = 100000$.

Figures 3 and 4 show the simulation results with $\alpha = 0.005 > \alpha_c$ and $\alpha = 1.5 \times 10^{-6} < \alpha_c$, respectively, which are consistent with theoretical analysis.

From the conclusion of Theorem 7, we learn that it is necessary for eliminating P2P botnet on the Internet to let $\alpha < \alpha_c$ by corresponding countermeasures. Meanwhile, the simulation results show that the critical value of infection α_c is very little, and this means that it is difficult to destroy completely the P2P botnet in reality.

4.2. Control Strategies. In what follows, we consider mainly the effect of the real-time immune measurement and antivirus software on the scale of the P2P botnet.

- (i) For fixed model parameters, $\mu = 0.01$, $r_1 = 0.06$, $r_2 = 0.06$, $\delta = 0.6$, and $\alpha = 0.005$, we investigate the effect of different real-time immunity (r_s) on the scale of P2P botnet. Simulation result is depicted in Figure 5. From Figure 5, it can be observed that enhancing

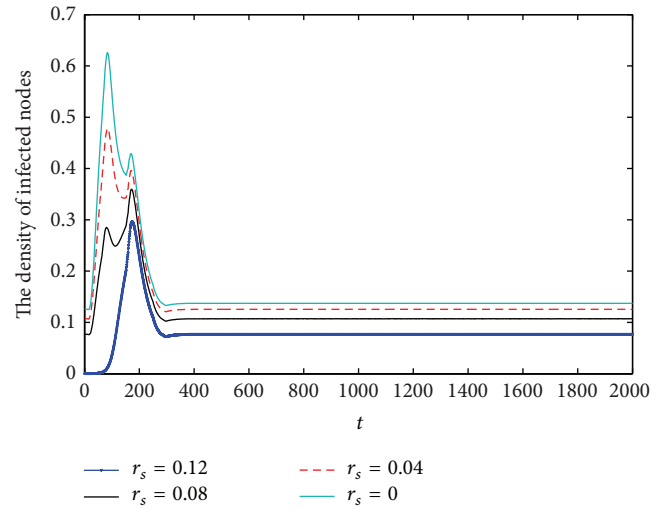


FIGURE 5: An illustration of the impact of real-time immune measure (r_s) on the density of infected nodes.

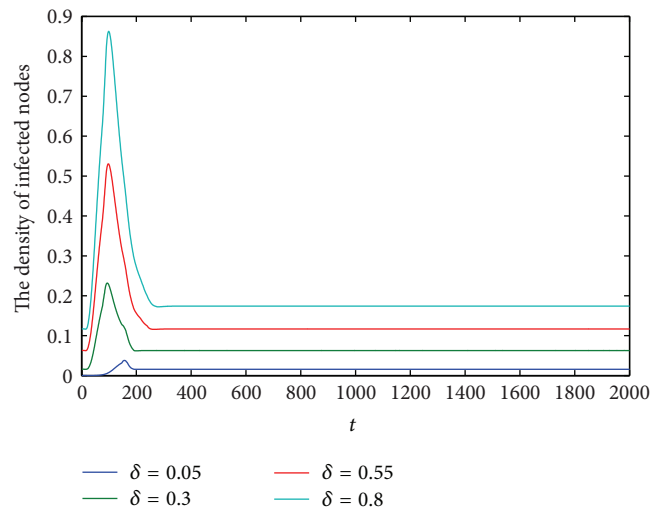


FIGURE 6: An illustration of the impact of antivirus software (δ) on the density of infected nodes.

real-time immune measures contributes to reduce the scale of P2P botnet and delay its outbreak. Hence, it is strongly advised that network users should install patches for bugs in time and update antivirus software to the latest version.

- (ii) For fixed model parameters, $\mu = 0.01$, $r_1 = 0.06$, $r_2 = 0.06$, $r_s = 0.01$, and $\alpha = 0.005$, we investigate the effect of antivirus software (δ) on the scale of P2P botnet. Simulation results are depicted in Figure 6. The profile of Figure 6 demonstrates that the larger percent conversion from E to I there is, the bigger scale a P2P botnet has. Thus, it is proposed that malware is killed when the node is infected by the bot program but does not join botnet.

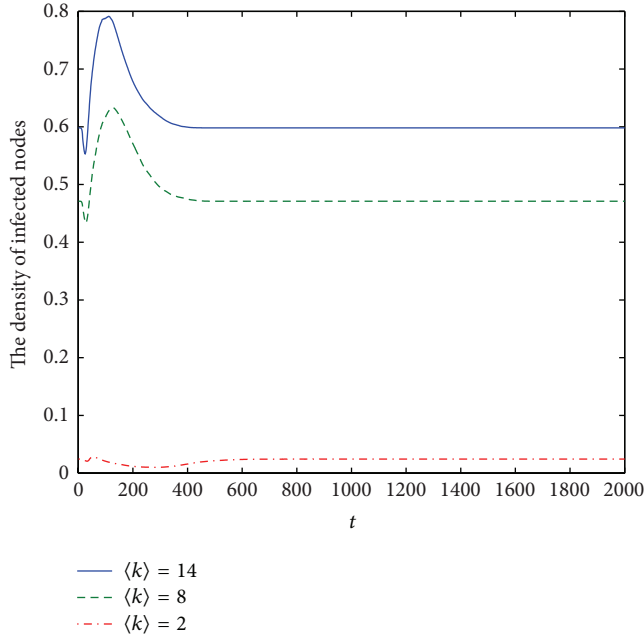


FIGURE 7: An illustration of the impact of average degree ($\langle k \rangle$) on the density of infected nodes.

Additionally, the effect of average degree $\langle k \rangle$ on prevalent behavior of P2P botnet is depicted in Figure 7. From Figure 7, we find that the scale of P2P botnet will increase when $\langle k \rangle$ becomes larger. So decreasing the average degree of network can also control the massive outbreak of P2P botnet.

5. Conclusions

As a new kind of attack platform to network security, P2P botnets have attracted considerable attention. Research is necessary to fully understand the threat and prepare to defend against it. To better exploit the spreading behavior of P2P botnet, in this paper, we present a mathematical model of creation of P2P botnet, which combines the scale-free character of Internet with the formation trait of P2P botnet. Hence, the model can portrait more accurately the dynamical features of P2P botnet propagation. Theoretical analysis shows that the model has a globally stable endemic equilibrium. The influence of some parameters to the scale of P2P botnet has been investigated. Simulation results demonstrate that it is difficult to destroy completely the P2P botnet in reality. This is the reason that many malwares saturate to a very low level of persistence [30]. However, Figures 6 and 7 show that we can reduce the scale of P2P botnet and delay its outbreak by efficient countermeasures, such as real-time immunity or autorunning of antivirus software.

The dynamical model we present could be extended to study the growth possibilities of P2P botnets in future work. The model is also possible to predict how botnetmasters could create more potent and aggressive botnets. Such predictions could ultimately be useful to antimalware developers as well.

Appendix

Proof of Lemma 6. Substituting (3) into I_k^* , we can obtain

$$I_k^* = \left(\alpha \delta \mu k \frac{1}{\langle k \rangle} \sum_k k P(k) I_k \right) \times \left((\mu + r_1 + \delta)(\mu + r_2) \times \left(\mu + r_s + \alpha k \frac{1}{\langle k \rangle} \sum_k k P(k) I_k \right) \right)^{-1}. \quad (\text{A.1})$$

Let $U_k^{(1)} = 1$, and define the following sequence:

$$U_k^{(m+1)} = \left(\alpha \delta \mu k \frac{1}{\langle k \rangle} \sum_k k P(k) U_k^{(m)} \right) \times \left((\mu + r_1 + \delta)(\mu + r_2) \times \left(\mu + r_s + \alpha k \frac{1}{\langle k \rangle} \sum_k k P(k) U_k^{(m)} \right) \right)^{-1}. \quad (\text{A.2})$$

Then, according to Lemma 3, for $1 \leq k \leq n$, $\lim_{t \rightarrow \infty} \sup I_k(t) \leq 1 = U_k^{(1)}$. By applying Proposition 4, we obtain

$$\lim_{t \rightarrow \infty} \sup I_k(t) \leq U_k^{(m)}, \quad 0 \leq k \leq n, \quad m = 1, 2, \dots \quad (\text{A.3})$$

In what follows, consider the convergence of the sequence defined in (A.2). By (A.2), for all k , $U_k^{(2)} \leq 1 = U_k^{(1)}$. If for all k , $U_k^{(m+1)} \leq U_k^{(m)}$, then it is easy to obtain $U_k^{(m+2)} \leq U_k^{(m+1)}$.

By induction, for all k , the sequence $U_k^{(m)}$ is decreasing, so its limit exists, denoted by $U_k = \lim_{m \rightarrow \infty} U_k^{(m)}$. Then it is easy to show that $U_k = \lim_{t \rightarrow \infty} \sup I_k(t) \leq U_k$.

On the other hand, substituting (A.1) into (3), we can get the following equation:

$$\theta(t) = \frac{1}{\langle k \rangle} \sum_k k P(k) I_k = \frac{1}{\langle k \rangle} \sum_k k P(k) \left(\alpha \delta \mu k \frac{1}{\langle k \rangle} \sum_k k P(k) I_k \right) \times \left((\mu + r_1 + \delta)(\mu + r_2) \times \left(\mu + r_s + \alpha k \frac{1}{\langle k \rangle} \sum_k k P(k) I_k \right) \right)^{-1}. \quad (\text{A.4})$$

From (7), $\theta = F(\theta)$, so by letting $\tilde{h}(x) = F(x) - x$, one can obtain that $\tilde{h}(0) = 0$ and $\tilde{h}'(0) > 0$. By the definition of derivative, if $x > 0$ is sufficiently small, then $\tilde{h}(x) > \tilde{h}(0) = 0$.

According to Proposition 5, we can take $\ell_k^{(1)}$ such that, for all $k, 0 < \ell_k^{(1)} < \lim_{t \rightarrow \infty} \inf I_k(t)$.

Let

$$x = \frac{1}{\langle k \rangle} \sum_k kP(k) \ell_k^{(1)}, \quad \tilde{h} \left(\frac{1}{\langle k \rangle} \sum_k kP(k) \ell_k^{(1)} \right) > 0; \tag{A.5}$$

we have

$$\frac{1}{\langle k \rangle} \sum_k kP(k) \ell_k^{(2)} > \frac{1}{\langle k \rangle} \sum_k kP(k) \ell_k^{(1)}. \tag{A.6}$$

If for all $k, \ell_k^{(m+1)} > \ell_k^{(m)}$, it is easy to obtain $\ell_k^{(m+2)} > \ell_k^{(m+1)}$.

Thus, by induction, for each k , the sequence $\ell_k^{(m)}$ is increasing, so its limit exists, denoted by $\ell_k = \lim_{m \rightarrow \infty} \ell_k^{(m)}$. Thus, it is easy to verify that $\ell_k < \lim_{t \rightarrow \infty} \inf I_k(t)$.

Both U_k and ℓ_k are positive stationary points of system (4). Therefore, by the uniqueness of the positive stationary point of the differential equation, we have $U_k = \ell_k = I_k$ and $I_k \leq \lim_{t \rightarrow \infty} \inf I_k(t) \leq \lim_{t \rightarrow \infty} \sup I_k(t) \leq I_k, 1 \leq k \leq n$; that is, $\lim_{t \rightarrow \infty} I_k(t) = I_k$.

Substituting I_k into (5), we will obtain $\lim_{t \rightarrow \infty} E_k(t) = E_k$ and $\lim_{t \rightarrow \infty} S_k(t) = S_k$.

Lemma 6 is proven. \square

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61379125), Program for Basic Research of Shan'xi Province (2012011015-3), Higher School of Science and Technology Innovation Project of Shan'xi Province (2013148), Key Construction Disciplines of Xinzhou Teachers University (ZDXK201204, XK201307), Research Project of Chongqing University of Science and Technology (CK2013B15), and Research Program of Chongqing Municipal Education Commission (KJ131401).

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] 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.
 [3] 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 Workshop on Hot Topics in Understanding Botnets*, pp. 1–8, 2007.
 [4] Q. T. Han, W. Q. Yu, Y. Y. Zhang, and Z. W. Zhao, "Modeling and evaluating of typical advanced peer-to-peer botnet," *Performance Evaluation*, vol. 72, pp. 1–15, 2014.

[5] 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 worm," in *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, 2008.
 [6] 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.
 [7] 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," in *Computer Performance Engineering*, vol. 6977, pp. 133–147, 2011.
 [8] 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.
 [9] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 2, pp. 113–127, 2010.
 [10] 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.
 [11] H. L. Jiang and X. X. L. Shao, "Detecting P2P botnets by discovering flow dependency in C&C traffic," in *Peer-To-Peer Networking and Applications*, pp. 1–12, 2012.
 [12] M. Khosroshahy, M. K. Ali, and D. Y. Qiu, "The SIC botnet lifecycle model: a step beyond traditional epidemiological models," *Computer Networks*, vol. 57, pp. 404–421, 2013.
 [13] X. Han, Y.-H. Li, L.-P. Feng, and L.-P. Song, "Influence of removable devices' heterouse on the propagation of malware," *Abstract and Applied Analysis*, vol. 2013, Article ID 296940, 6 pages, 2013.
 [14] Y. Li, J. Pan, L. Song, and Z. Jin, "The influence of user protection behaviors on the control of internet worm propagation," *Abstract and Applied Analysis*, vol. 2013, Article ID 531781, 13 pages, 2013.
 [15] L.-P. Song, X. Han, D.-M. Liu, and Z. Jin, "Adaptive human behavior in a two-worm interaction model," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 828246, 13 pages, 2012.
 [16] L.-P. Song, Z. Jin, G.-Q. Sun, J. Zhang, and X. Han, "Influence of removable devices on computer worms: dynamic analysis and control strategies," *Computers & Mathematics with Applications*, vol. 61, no. 7, pp. 1823–1829, 2011.
 [17] L.-X. Yang and X. Yang, "Propagation behavior of virus codes in the situation that infected computers are connected to the internet with positive probability," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 693695, 13 pages, 2012.
 [18] Q. Zhu, X. Yang, L.-X. Yang, and X. Zhang, "A mixing propagation model of computer viruses and countermeasures," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1433–1441, 2013.
 [19] Q. Zhu, X. Yang, and J. Ren, "Modeling and analysis of the spread of computer virus," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 5117–5124, 2012.
 [20] Q. Zhu, X. Yang, L.-X. Yang, and C. Zhang, "Optimal control of computer virus under a delayed model," *Applied Mathematics and Computation*, vol. 218, no. 23, pp. 11613–11619, 2012.
 [21] L.-X. Yang and X. Yang, "The effect of infected external computers on the spread of viruses: a compartment modeling study," *Physica A*, vol. 392, no. 24, pp. 6523–6535, 2013.

- [22] L.-X. Yang and X. Yang, "The spread of computer viruses over a reduced scale-free network," *Physica A*, vol. 396, pp. 173–184, 2014.
- [23] 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.
- [24] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: structure and dynamics," *Physics Reports*, vol. 424, no. 4-5, pp. 175–308, 2006.
- [25] Y. Moreno, R. Pastor-Satorras, and A. Vespignani, "Epidemic outbreaks in complex heterogeneous networks," *The European Physical Journal B: Condensed Matter and Complex Systems*, vol. 26, no. 4, pp. 521–529, 2002.
- [26] R. Yang, B.-H. Wang, J. Ren et al., "Epidemic spreading on heterogeneous networks with identical infectivity," *Physics Letters A*, vol. 364, no. 3-4, pp. 189–193, 2007.
- [27] R. C. Robinson, *An introduction to Dynamical Systems: Continuous and Discrete*, Pearson Prentice Hall, Upper Saddle River, NJ, USA, 2004.
- [28] L. Wang and G.-Z. Dai, "Global stability of virus spreading in complex heterogeneous networks," *SIAM Journal on Applied Mathematics*, vol. 68, no. 5, pp. 1495–1502, 2008.
- [29] M. Yang, X. C. Fu, and Q. C. Wu, "Global stability of SIS epidemic model with infective medium on complex networks," *Journal of Systems Engineering*, vol. 25, pp. 767–772, 2011 (Chinese).
- [30] J. O. Kephart, G. B. Sorkin, D. M. Chess, and S. R. White, "Fighting computer viruses," *Scientific American*, vol. 277, no. 5, pp. 88–93, 1997.