Applied Mathematics & Information Sciences
An International Journal

Optimal Attack Strategies in a Dynamic Botnet Defense Model

Y. Shang

Institute for Cyber Security, University of Texas at San Antonio, Texas 78249, USA

Received: Received Jul 8, 2011; Revised Oct. 4, 2011; Accepted Oct. 6, 2011
Published online: 1 January 2012

Abstract: Since the number of compromised computers, or botnet, continues to grow, the cyber security problem has become increasingly important and challenging to both academic researchers and industry practitioners. A respect to combat botnet propagation is to understand the attacker's behaviors based on the whole operation of a system that can be modeled with population models used in epidemiological studies. In this paper, we treat the interaction between the botnet herder and the defender group as a modified SIS epidemic model with external entrance and allowing computers of undetected states. Based on optimal control theory, we derive the optimal strategy of the botnet herder as a feedback on the rate of infection under given levels of entrance and defense. The obtained optimal policies dynamically evolve with time and offer useful insights for ultimately solving the botnet defense problem.

Keywords: Botnet defense, virus epidemics, epidemic models, dynamic programming, optimal control.

1. Introduction

Nowadays national security, social harmony, and economic progress largely rely on the use of cyberspace. Despite the considerable efforts made by researchers over the last two decades, the cyber security problem is not well understood and far from being completely solved. Botnets are emerging threat with hundreds of millions of computers infected [1,2]. They are networks of computers infected with malwares that allow cybercriminals or botnet herders to control the infected computers remotely without the user's knowledge. According to the study of [3], more than thirty percent of all computers connected to the Internet are infected bots and controlled by attackers.

In this paper, we focus on the economic aspects of botnet activity and suggest effective attack strategies of the botnet herder (rather than defense strategies by the defender) capitalizing on the theory of dynamic programming and optimal control. Understanding the attack policies can in turn lead to useful insights for defending cyberspace, and guide the design of effective defense strategies. We characterize the interaction between the attacker, i.e., botnet herder, and the defender group as a modified SIS epidemic model with immigration or external entrance, in which a computer's state may be either susceptible or infectious. The size of the system in question is thus increasing and we allow the presence of computers of undetected states, both of which are highly desirable in the real-life networks.

In our framework, the goal of a botnet herder is to minimize his cost by intensifying his intrusion in a network of computers. We define botnet herder's optimal attack policy as the solution to a cost minimization control problem under fixed levels of defense and entrance. Our result indicates that it is optimal for the botnet herder to reduce his percentage of invasion in the network when the percentage of infected hosts is over some threshold. The reason is that once the percentage of infection passes the steady-state level, the opportunity cost of getting caught or traced surpasses the size benefits of the operation cost. On the other hand, the botnet herder should make full attack effort to pursue his economic profits when the percentage of infected hosts is below some threshold. We would like to point out that these thresholds change with time, thus providing essentially dynamical optimal strategies.

Recently, some researchers have combined the epidemic model with optimal control and game-like modeling to capture interdependent security decisions; see e.g. [4–7]. These prior works are conceptually or spiritually relevant to the present study. The work [4] provides a

* Corresponding author: e-mail: shylmath@hotmail.com

game theoretical framework to model the interaction between the botnet herder and the defender group in a fixed population system. Unlike our situation, the percentage of infected computers, evolving according to an SIS model, is solely used to describe the network dynamics. Under a given level of network defense, [7] addresses the botnet defense business as a result of profit maximization decision making and investigates the deterrent effect of the uncertainty presented by honeypots. The authors in [6] investigate a network of interconnected agents' decisions about whether to invest some amount to self-protect and deploy security solutions which decrease the probability of contagion. However, they assign the transition probability of states of computers rather than employ the epidemic evolutionary process directly. The work [5] develops one-shot games between botnet herders and defenders and analyzes botnet herder's attack coordinations as well as defender's security defense decisions. Multiple Nash equilibria are derived in [5] under different conditions. Relevant work of contact transmission model and some features in our epidemic dynamics are compared in Section 2.

The rest of the paper is organized as follows. In Section 2 we present our botnet defense model. The optimal strategies of botnet herder under fixed levels of entrance and network defense are analyzed in Section 3. The proof of main result is deferred to Section 4. We conclude our paper and suggest some possible future directions in Section 5.

2. Botnet defense model

The standard model used in the study of virus and worm propagation is called the contact process or the epidemic model [8]. In the classical SIS model, the status of a node (i.e. host or computer) is either infectious or susceptible. A host recovered from a worm immediately becomes susceptible again. This is plausible in the context of cyber security because an antivirus software scan a computer regularly, and each time a computer is infected it remains so until the next scan by the antivirus software. Another reason is that a computer may be subject to several vulnerabilities, so it is still vulnerable when recovered from one virus.

We now introduce a modified deterministic SIS dynamic system which characterizes the growth of networks as well as the botnet herder's strategies. Let $x(t)$ and $y(t)$ denote the percentages of infectious and susceptible hosts at time t, respectively. The dynamical process $\{(x(t), y(t)); t \geq 0\}$ is initiated by value $(x(0), y(0)) = (x_0, y_0)$ with

$$x_0 + y_0 = a \in (0, 1] \tag{1}$$

(which we will explain later) and is described by the following set of differential equations:

$$\frac{\mathrm{d}y(t)}{\mathrm{d}t} = -cv(x(t), y(t))y(t) \tag{2}$$

$$\begin{aligned} &-\beta x(t)y(t) + \gamma x(t) + \mu(1 - y(t)) \\ \frac{\mathrm{d}x(t)}{\mathrm{d}t} &= cv(x(t), y(t))y(t) \\ &+\beta x(t)y(t) - \gamma x(t) - \mu x(t) \end{aligned} \tag{3}$$

where $c \geq 0$ is the average attack successful rate, $v(x, y) \in [0, 1]$ is the attack effort intensity, $\beta \geq 0$ is the average number of transmissions possible from a given infectious host in each period, $\gamma \geq 0$ is the recovery rate and $\mu \geq 0$ is the entrance rate of external hosts.

This model encodes several remarkable features and we elaborate on them in the sequel.

1. The susceptible hosts outside the network continuously join with constant rate μ, which accounts for the last term in Equation (3). Hence, the size of the network is increasing. Most of the existing work concerning the spread of computer viruses only treat the closed population, c.f. [9,10,5–7,11,12]. However, this feature is desirable in the practical setting since new computers get access to the Internet as times goes on [13]. In addition, each host in the network regularly recovered from the vulnerabilities by, for example, reinstalling the system, which explains the last term in Equation (2). This sort of birth-death process has been proposed in epidemiology and is known as the SIR epidemics with demography [15,14]. However, the population in that case fluctuates around a fixed value due to the fact that infected agents are finally removed from the system, which is in contrast to our case.

2. In (1), the initial value is assumed to be $a \in (0, 1]$, since the susceptible hosts are usually not well defined at the beginning of an epidemic. Generally, we have $x(t) + y(t) \leq 1$ rather than the commonly used requirement $x(t) + y(t) = 1$ for $t \geq 0$. By doing so, we allow undetected (or uncategorized) hosts to exist in the network, which is also highly appealing in reality.

Solving the systems (2) and (3) with initial value (1) yields $x(t) + y(t) = 1 - (1 - a)e^{-\mu t}$. Thereby, we have $x(t) + y(t)$ tends to 1 increasingly as $t \to \infty$. In other words, the percentage of uncategorized hosts is reducing as time goes on. If $a = 1$, then $x(t) + y(t) \equiv 1$. Note that in case of $a < 1$ the network dynamics can not be described by only using that of $x(t)$ as in [4].

3. The term $cv(x(t), y(t))y(t)$ in Equations (2) and (3) depicts the increment of percentage of infectious hosts resulting from botnet herder's direct attack effort rather than contagion. $v(x, y)$ is the attack effort intensity, the botnet herder's control, indicating how aggressively the botnet herder exerts his intrusion. On the other hand, the authors in [5] assume that the attacker has the control of successful attack rate, which is tantamount to set $c = 1$ and $v(x, y) \equiv p$, a constant probability of successful attack.

3. Optimal strategies under fixed levels of entrance and defense

In this section, we solve the botnet herder's best response when facing fixed levels of entrance μ and defense γ.

Let $k > 0$ be the per unit time cost associated with botnet herder's attack effort. Denote by $f(x)$ the botnet herder's cost function with $f'(x) < 0$ and $f''(x) > 0$. We refer the reader to [4,6] for the reason of this assumption. The total cost of attack effort per unit time is given by $kv(x,y)$, which is the extra penalty cost from increasing probability of getting caught due to the increasing severity of attack. The botnet herder's objective is to minimize the discounted total cost (operation cost plus effort cost) with a constant discount rate $r > 0$ over an infinite time horizon [4,16]:

$$\inf_v \Big\{ J_{x,y}(v) = \int_0^\infty e^{-rt}(f(x) + kv(x,y))\mathrm{d}t \Big\}, \quad 0 \le v(x,y) \le 1. \tag{4}$$

To solve the minimization problem, we form the current value Hamiltonian associated with (4) by

$$\begin{aligned} H(x,y,v,p,q) = f(x) + kv + p(cvy \\ +\beta xy - \gamma x - \mu x) \\ +q(-cvy - \beta xy \\ +\gamma x + \mu(1-y)), \end{aligned} \tag{5}$$

where $p = p(t)$ and $q = q(t)$ are the botnet herder's marginal costs at time t. The optimal control, $\hat{v}(x,y)$, is obtained by minimizing the Hamiltonian H. Since the Hamiltonian is linear in v, the optimal control takes the following bang-bang and (a possible) singular form

$$\hat{v}(x,y) = 1_{[H_v<0]} + u1_{[H_v=0]} \tag{6}$$

with some $0 < u < 1$ to be determined and $H_v = \partial H/\partial v = k + cy(p-q)$. When $H_v = 0$ and stays at this value, the botnet herder exerts an intermediate attack effort u. This phase is called singular.

The adjoint equations are shown to be given by

$$\begin{aligned} \dot{p} = -H_x + rp = -f'(x) - p\beta y \\ +p\gamma + p\mu + q\beta y - q\gamma + rp, \end{aligned} \tag{7}$$

$$\begin{aligned} \dot{q} = -H_y + rq = -pcv - p\beta x \\ +qcv + q\beta x + q\mu + rq. \end{aligned} \tag{8}$$

Substituting (2), (7) and (8) into $\dot{H}_v = c\dot{y}(p-q) + cy(\dot{p} - \dot{q})$, and equating $\dot{H}_v$ and H_v to zero, we obtain

$$f'(x) = \frac{k}{cy}\Big(\beta y - \gamma - \frac{\gamma x}{y} - \frac{\mu}{y} - r\Big). \tag{9}$$

We may solve (9) in conjunction with $x + y = b \in [a,1]$ for the steady state percentage of infected computers, $x^* = x^*(b)$ and $y^* = y^*(b) = b - x^*$, two functions of b. The optimal control $\hat{v}(x,y)$ in this singular region is a b-dependent rate and found by solving $\dot{x} = \dot{y} = 0$ at x^* and y^*:

$$\hat{v}(x^*,y^*) = u = -\frac{\beta x^* y^* - (\gamma+\mu)x^*}{cy^*}. \tag{10}$$

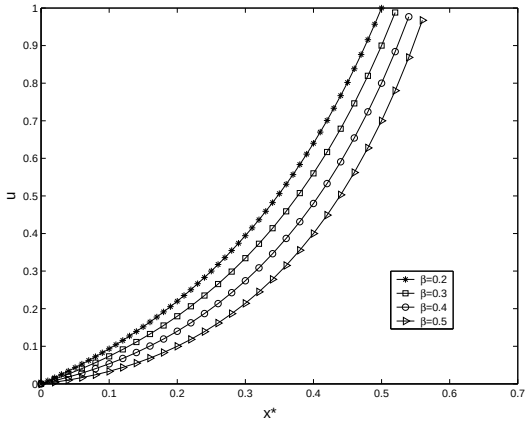

Figure 1 Optimal strategy in the singular region as a feedback on different infection rates β.

Theorem 1.*Suppose $\mu+\gamma > \beta$, $f'(x) < 0$, $f''(x) > 0$ and $f'(0) < -\frac{k(r+\gamma+\mu-\beta a)}{ca}$. For each $b \in [a,1]$, we assume $cy^* + \beta x^* y^* - \gamma x^* - \mu x^* > 0$. Then the optimal feedback of the botnet herder is given by*

$$\hat{v}(x,y) = \begin{cases} 1, & x < x^*, \\ u, & x = x^*, \\ 0, & x > x^*, \end{cases} \tag{11}$$

where $u = -\frac{\beta x^* y^* - (\gamma+\mu)x^*}{cy^*}$, *and* $x^* < \frac{\sqrt{(c+\gamma+\mu-b\beta)^2 + 4\beta cb} - (c+\gamma+\mu-b\beta)}{2\beta}$.

See Section 4.

From the above result we can see that the most effective strategies of the botnet herder implicitly depend on the total percentage of infectious and susceptible hosts, $x(t) + y(t)$, at time t. Therefore, Theorem 3.1 indicates that the optimal attack strategies for the botnet herder is essentially dynamical, which is in contrast to those time-invariant strategies derived in fixed network size [4–7].

Set $a = 1$ (therefore $b = 1$). The singular region, $x = x^*$, has the additional property that the values of the control and the state variables are constant in this region; that is, it exhibits a steady-state property. Let $c = 0.5$ and $\gamma + \mu = 0.6$. We plot the optimal control u as a function of (possible) x^* in Fig. 3.1 for different values of infection rate, β.

4. Proof of Theorem 3.1

We first establish two lemmas.

Lemma 1.*Suppose that the assumptions of Theorem 3.1 hold. Set*

$$F(x,y) = f'(x)cy + k\Big(r - \beta y + \gamma + \frac{\gamma x}{y} + \frac{\mu}{y}\Big). \tag{12}$$

Then there exits a unique pair $(x^*(b), y^*(b))$ *such that* $F(x^*, y^*) = 0$ *and* $x^* + y^* = b$ *for each* $b \in [a, 1]$.

Let $F(x) := F(x, b-x)$. Hence, we have $F(b) = +\infty$ and $F(0) < 0$ by (12). Since $f'(x) < 0$ and $f''(x) > 0$, we get $F'(x) = c(f''(x)(b-x) - f'(x)) + k\beta + \frac{kb\gamma + k\mu}{(b-x)^2} > 0$. The result then follows.

Lemma 2.*Suppose the assumptions of Theorem 3.1 hold. Then we have* $x^* < \frac{\sqrt{(c+\gamma+\mu-b\beta)^2+4\beta cb}-(c+\gamma+\mu-b\beta)}{2\beta}$, *which is a solution to a long-run steady state,* $\dot{x} = 0$ *with* $v(x, y) = 1$ *and* $x + y = b$.

There is only one zero for $G(x, y) := cy + \beta xy - \gamma x - \mu x$ with $y = b - x \in (0, b)$, which is at $x = \frac{\sqrt{(c+\gamma+\mu-b\beta)^2+4\beta cb}-(c+\gamma+\mu-b\beta)}{2\beta}$. The proof concludes from the assumptions in Theorem 3.1.

Proof of Theorem 3.1. As in [4], we use dynamic programming arguments to obtain the optimal control trajectories. It is well known that if the value function is smooth, the corresponding feedback leads to an optimal solution [16]. The botnet herder's value function is defined as

$$\begin{aligned}\phi(x, y) \ &: = \inf_v \Big\{ J_{x,y}(v) \\ &= \int_0^\infty e^{-rt}(f(x) + kv(x, y))\mathrm{d}t \Big\}.\end{aligned}$$

The corresponding Bellman equation (e.g. [17]) is

$$\begin{aligned} r\phi(x, y) &= \inf_v \{f(x) + kv + \phi_x(x, y)\dot{x}\} \\ &= \inf_v \{f(x) + kv + \phi_x(x, y) \\ &\quad (cvy + \beta xy - \gamma x - \mu x)\} \\ &= \inf_v H(x, y, v, \phi_x(x, y), 0) \\ &= \inf_v H(x, y, v, p, 0), \end{aligned}$$

where $p = \phi_x(x, y) := \partial\phi(x, y)/\partial x$.

From (6) we know the optimal control $\hat{v}$ takes the form

$$\hat{v}(x, y) = 1_{[k+pcy<0]} + u1_{[k+pcy=0]},$$

and then we may express the Hamiltonian as

$$\begin{aligned} H(x, y, v, p, 0) &= f(x) + p(\beta xy \\ &\quad -\gamma x - \mu x) - (k + pcy)^-, \end{aligned}$$

where $z(x, y)^- = -z(x, y)1_{[z<0]}$. Consequently, we get

$$\begin{aligned} r\phi(x, y) &= f(x) + \phi_x(x, y)(\beta xy - \gamma x \\ &\quad -\mu x) - (k + \phi_x(x, y)cy)^-. \end{aligned} \tag{13}$$

Set $z(x, y) = k + \phi_x(x, y)cy$, and we have $z_x(x, y) = c\phi_{xx}(x, y)y$. By utilizing (**??**), we derive that

$$\begin{aligned} &z_x(x, y) + z(x, y)\frac{r - \beta y + \gamma + \mu}{(\beta x + c1_{[z(x,y)<0]})y - \gamma x - \mu x} \\ &+ \frac{f'(x)cy + k(r - \beta y + \gamma + \mu)}{(\beta x + c1_{[z(x,y)<0]})y - \gamma x - \mu x} = 0. \end{aligned} \tag{14}$$

If $z(x, y) < 0$, by (12) and (14) we obtain

$$\begin{aligned} &\frac{d}{dx}\left(z(x, y)e^{-\int_0^x \frac{r-\beta y+\gamma+\mu}{(\beta\xi+c)y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\right) \\ &+ \frac{F(x, y) - k\big(\frac{\gamma x}{y} + \frac{\mu(1-y)}{y}\big)}{(\beta x + c)y - \gamma x - \mu x} e^{-\int_0^x \frac{r-\beta y+\gamma+\mu}{(\beta\xi+c)y-\gamma\xi-\mu\xi}\mathrm{d}\xi} = 0. \end{aligned} \tag{15}$$

If $z(x, y) > 0$, by (12) and (14) we obtain

$$\begin{aligned} &\frac{\mathrm{d}}{\mathrm{d}x}\Big(z(x, y)e^{\int_x^1 \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\Big) \\ &+ \frac{F(x, y) - k\big(\frac{\gamma x}{y} + \frac{\mu(1-y)}{y}\big)}{\beta xy - \gamma x - \mu x} e^{\int_x^1 \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi} = 0. \end{aligned}$$

For $x^* < x < 1$, by (16) we set

$$\begin{aligned} &z(x, y)e^{\int_x^1 \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi} + \int_{x^*}^x \frac{F(\eta, y) - k\big(\frac{\gamma\eta}{y} + \frac{\mu(1-y)}{y}\big)}{\beta\eta y - \gamma\eta - \mu\eta} \\ &\times e^{\int_\eta^1 \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\mathrm{d}\eta = 0. \end{aligned}$$

Therefore,

$$\begin{aligned} z(x, y) = &-\int_{x^*}^x \frac{F(\eta, y) - k\big(\frac{\gamma\eta}{y} + \frac{\mu(1-y)}{y}\big)}{\beta\eta y - \gamma\eta - \mu\eta} \\ &\times e^{\int_\eta^x \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\mathrm{d}\eta. \end{aligned} \tag{16}$$

It is clear that $z(x, y) > 0$. Now we want to verify that $z(x, y)$ also satisfies the boundary condition for $z(x, y) \to k$ as $y \to 0$. We rewrite (16) using integration by part and (12) as

$$\begin{aligned} z(x, y) = &\ k - ke^{\int_{x^*}^x \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi} \\ &- \int_{x^*}^x \frac{f'(\eta)cy}{\beta\eta y - \gamma\eta - \mu\eta} e^{\int_\eta^x \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\mathrm{d}\eta. \end{aligned}$$

The fact that $e^{\int_\eta^x \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi} \le \frac{y}{b-\eta}$ and

$$\Big|\int_{x^*}^x \frac{f'(\eta)cy}{\beta\eta y - \gamma\eta - \mu\eta} e^{\int_\eta^x \frac{r-\beta y+\gamma+\mu}{\beta\xi y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\mathrm{d}\eta\Big| \le Cy(x - x^*)$$

for some constant C imply the boundary condition at $y = 0$.

For $0 < x < x^*$, by (15) we set

$$\begin{aligned} &-z(x, y)e^{-\int_0^x \frac{r-\beta y+\gamma+\mu}{(\beta\xi+c)y-\gamma\xi-\mu\xi}\mathrm{d}\xi} \\ &+ \int_x^{x^*} \frac{F(\eta, y) - k\big(\frac{\gamma\eta}{y} + \frac{\mu(1-y)}{y}\big)}{(\beta\eta + c)y - \gamma\eta - \mu\eta} \\ &\times e^{-\int_0^\eta \frac{r-\beta y+\gamma+\mu}{(\beta\xi+c)y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\mathrm{d}\eta = 0. \end{aligned}$$

Accordingly,

$$z(x, y) = \int_x^{x^*} \frac{F(\eta, y) - k\big(\frac{\gamma\eta}{y} + \frac{\mu(1-y)}{y}\big)}{(\beta\eta + c)y - \gamma\eta - \mu\eta} \tag{17}$$

$$\times e^{-\int_x^\eta \frac{r-\beta y+\gamma+\mu}{(\beta\xi+c)y-\gamma\xi-\mu\xi}\mathrm{d}\xi}\mathrm{d}\eta,$$

and $z(x,y)<0$ by the assumptions in Theorem 3.1.

For $x = x^*$, we have $y = b - x^* = y^*$ and $z(x^*,y^*) = 0$. By Lemma 4.1, (x^*,y^*) is uniquely defined, and Lemma 4.2 implies $x^* < \frac{\sqrt{(c+\gamma+\mu-b\beta)^2+4\beta cb}-(c+\gamma+\mu-b\beta)}{2\beta}$. By setting $\dot{x}|_{x=x^*,y=y^*} = \dot{y}|_{x=x^*,y=y^*} = 0$, we obtained the optimal control as

$$\hat{v} = u = -\frac{\beta x^* y^* - (\gamma+\mu)x^*}{cy^*}.$$

Thereby, we have got the optimal feedback of the botnet herder

$$\hat{v}(x,y) = \begin{cases} 1, & x < x^*, \\ u, & x = x^*, \\ 0, & x > x^*, \end{cases}$$

as desired.

5. Conclusion and future work

In this paper, we employ optimal control methods to analyze the botnet business between the botnet herder and defender group and suggest feasible attack policies. The dynamics of hosts evolve according to a modified SIS epidemic model allowing external entrance. For given levels of network defense and entrance, we obtain the botnet herder's optimal strategy as a feedback on the rate of infection. Our analysis of network epidemiology model is of both conceptual value and practical interest. One interesting future direction would be the stochastic extension (c.f. [14]), since botnet evolution is an inherently stochastic phenomenon and subjects to many random disturbances. To capture the infection process between different hosts, heterogeneous models [14] are preferable.

Acknowledgement

The author is grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir, Proc. Cybersecurity Applications & Technology Conference for Homeland Security, 299 (2009).
[2] P. Wang, B. Aslam and C.C. Zou, In: Handbook of Information and Communication Security, P. Stavroulakis and M. Stamp (Eds.), 335 (Springer, New York, 2010).
[3] C. Wüest, http://www.symantec.com/business/theme.jsp?themeid=threatreport, (2010).
[4] A. Bensoussan, M. Kantarcioglu and C. Hoe, http://www.utdallas.edu/~mxk055100 /publications/botnet-defense-game.pdf
[5] N. Fultz and J. Grossklags, LNCS **5628**, 167 (2009).
[6] M. Lelarge, Proc. 47th Annual Allerton Conference on Communication, Control, and Computing, 1353 (2009).
[7] Z. Li, Q. Liao and A. Striegel, In: Managing Information Risk and the Economics of Security, M.E. Johnson (Ed.), 245 (Springer, New York, 2009).
[8] O. Diekmann and J.A.P. Heesterbeek, Mathematical Epidemiology of Infectious Disease (John Wiley & Sons, Chichester, 2000).
[9] N. Berger, C. Borgs, J.T. Chayes and A. Saberi, Proc. 16th Annual ACM-SIAM Symposium on Discrete Algorithms, 301 (2005).
[10] F. Cohen, Computer and Security **6**, 22 (1987).
[11] J.R.C. Piqueira and V.O. Araujo, Applied Mathematics and Computation **213**, 355 (2009).
[12] Y. Shang, Rep. Math. Phys. **67**, 255 (2011).
[13] M. Faloutsos, P. Faloutsos and C. Faloutsos, Proc. ACM SIGCOMM Conference, 251 (1999).
[14] T. Britton, Math Biosci. **225**, 24 (2010).
[15] I. Nåsell, J. R. Statist. Soc. B **61**, 309 (1999).
[16] D.P. Bertsekas, Dynamic Programming and Optimal Control Vol 1 (Athena Scientific, Nashua, 2005).
[17] D. Yeung and L. Petrosyan, Cooperative Stochastic Differential Games (Springer, New York, 2006).

Yilun Shang is a postdoctoral fellow in the University of Texas at San Antonio, USA. His research fields are random graph theory, structure and dynamics of complex networks, percolation theory and cyber security. In June 2010, he obtained a Ph.D. at the Department of Mathematics, Shanghai Jiao Tong University, China. He has published more than 20 papers in international peer reviewed journals.