Canad. Math. Bull. Vol. **56** (3), 2013 pp. 621–629
http://dx.doi.org/10.4153/CMB-2012-007-2
© Canadian Mathematical Society 2012

Optimal Control Strategies for Virus Spreading in Inhomogeneous Epidemic Dynamics

Yilun Shang

Abstract. In this paper, we study the spread of virus/worm in computer networks with a view to addressing cyber security problems. Epidemic models have been applied extensively to model the propagation of computer viruses, which characterize the fact that infected machines may spread malware to other hosts connected to the network. In our framework, the dynamics of hosts evolves according to a modified inhomogeneous Susceptible-Infectious-Susceptible (SIS) epidemic model with time-varying transmission rate and recovery rate. The infection of computers is subject to direct attack as well as propagation among hosts. Based on optimal control theory, optimal attack strategies are provided by minimizing the cost (equivalently maximizing the profit) of the attacker. We present a threshold function of the fraction of infectious hosts, which captures the dynamically evolving strategies of the attacker and reflects the persistence of virus spreading. Moreover, our results indicate that if the infectivity of a computer worm is low and the computers are installed with antivirus software with high reliability, the intensity of attacks incurred will likely be low. This agrees with our intuition.

1 Introduction

The cyber security problem has become increasingly important as cyber attacks continue to grow in number, scope and severity [5]. Computer viruses and botnets (zombie networks) are global threats with hundreds of millions of computers infected [1]. Theoretical modeling of computer worm epidemic dynamics is a significant problem that has attracted many studies. In this paper, we consider the economic aspects of botnet activity and suggest optimal attack strategies for the attackers (*e.g.*, hackers, botnet herders, etc.) based on dynamic programming and optimal control theory. Understanding the attack strategies taken by the botnet herder in depth may be instrumental in the effective design of security and defense measures.

We characterize the interaction between the attacker and the defender group (network/computer users) as a modified inhomogeneous SIS epidemic model with time dependent transmission and recovery rates, in which a computer's state may be either susceptible or infectious. The infection of computers is subject to direct attack as well as propagation among hosts. In our framework, the attacker's goal is to minimize his cost by intensifying his intrusion in a network of computers. We define attacker's optimal attack strategy as the solution to a cost minimization control problem with a deterministic population. The optimal strategy is obtained as a feedback on the rates of transmission (infection) and recovery. We predict that it is optimal for the attacker

Received by the editors November 18, 2010; revised December 14, 2011.
Published electronically March 24, 2012.
AMS subject classification: **49J15**, 92D30.
Keywords: computer virus, epidemic dynamics, optimal control, network security.

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

to reduce his attack effort (*e.g.*, the spread of malicious programs) when the fraction of infected hosts is over some threshold function. This threshold function hinges on the rates of infection and recovery, and may change over time. On the other hand, the attacker should apply a full attack effort to pursue his economic profit when the fraction of infected hosts is below the threshold function. As a byproduct, our result indicates that if the infectivity of a computer worm is low and the computers are equipped with reliable defense systems, the intensity of attacks incurred will likely be low (see the discussion in Section 3). This phenomenon is intuitively plausible and we shall establish a theoretical proof here.

Recently some researchers have combined the epidemic dynamics with optimal control and game-like modeling to capture interdependent security decisions, *e.g.*, in [4], [11], [13], [14], [17], [23]. We briefly review the prior work that is conceptually or spiritually relevant as follows. The work [4] provides a game theoretical framework to model the interaction between the botnet herder and the defender group in a deterministic population system. Unlike our scenario, the transmission rate and recovery rate of the system are assumed to be constants. Thus, the optimal strategy obtained there does not vary with respect to time. Under a given level of network defense in terms of recovery rate, [14] analyzes the virus propagation business as a result of profit maximization decision making and investigates the deterrent effect of the uncertainty presented by virtual honeypots. For more details on honeypots techniques, we refer the reader to the monograph [16]. Optimal adaptive defense against worm infection is discussed in [23], where cost is introduced by false positives and false negatives of the detection systems. The authors in [13] address a scenario of 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 fixed transition probabilities of states of computers rather than employing the epidemic evolutionary process directly. For a different purpose, the work [11] develops one-shot games between attackers and defenders and investigates attacker coordination as well as the defender's security defense decisions. Multiple Nash equilibria are derived under different conditions. Also in [17], the author examines the effective attack strategies when the virus spreads into a population with immigrants. However, in all the above-mentioned works, only time invariant transmission and recovery rates are treated.

The rest of the paper is organized as follows. In Section 2, we present our inhomogeneous SIS model. The optimal strategies of the attacker are analyzed in Section 3. In Section 4, we give the proof of the main result. We finally conclude the paper in Section 5.

2 The Inhomogeneous SIS Model

Most existing models employed in the study of computer virus and worm propagation are adapted from the so-called contact processes or epidemic models [9], [10], [15]. In the typical Susceptible-Infectious-Susceptible (SIS) model, the state of a node (*i.e.*, host or computer) at a given time is either infectious or susceptible. A host recovered from a worm immediately becomes susceptible again. This reflects the fact that antivirus software scans a computer regularly and each time a computer is

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

infected it remains so until the next scan by the antivirus software [5]. Another reason is that a computer may be subject to several vulnerabilities, so it is still vulnerable when recovered from one virus.

Let $x(t)$ and $y(t)$ denote the infectious and susceptible fractions of the hosts at time t, respectively. One point to mention here is that in mathematical epidemiology conventions the definitions of $x(t)$ and $y(t)$ are reverse compared with the above ones. The dynamical process $\{x(t), y(t); t \geq 0\}$ is initiated by $\big(x(0), y(0)\big) = (x_0, y_0)$ with $x_0 + y_0 = 1$ and expressed by the following set of differential equations:

$$\frac{\mathrm{d}y(t)}{\mathrm{d}t} = -cv\big(x(t), y(t)\big)\, y(t) - \beta(t)x(t)y(t) + \gamma(t)x(t) \tag{2.1}$$

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = cv\big(x(t), y(t)\big)\, y(t) + \beta(t)x(t)y(t) - \gamma(t)x(t) \tag{2.2}$$

where $c > 0$ is the average attack success rate, $v(x, y) \in [0, 1]$ is the attack effort intensity of the botnet herder, $\beta(t) > 0$ is the average number of infecting transmissions possible from a given infectious host in each period, and $\gamma(t) > 0$ is the recovery rate. Note that the transmission rate $\beta(t)$ and the recovery rate $\gamma(t)$ may vary from time to time, which accommodate realistic scenarios. The infection of computers occurs from both the direct attack (the first term on the right-hand side of (2.2)) and the spreading among hosts (the second term on the right-hand side of (2.2)). Although similar inhomogeneous epidemic models have been proposed in recent studies [3], [18], [20], [21], they focus on statistical aspects and parameter estimation for epidemic dynamics.

From (2.1) and (2.2) we get $\mathrm{d}x/\mathrm{d}t + \mathrm{d}y/\mathrm{d}t = 0$; therefore the initial values yield $x(t) + y(t) = 1$ for $t \geq 0$. We may describe the above dynamical system solely by the equation of $x(t)$ as

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = cv\big(x(t)\big)\big(1 - x(t)\big) + \beta(t)x(t)\big(1 - x(t)\big) - \gamma(t)x(t). \tag{2.3}$$

Here, the term $cv\big(x(t)\big)$ in (2.3) depicts the increment of the fraction of infectious computers resulting from direct attack rather than contagion (*cf.* [4]). The attacker's control, $v(x)$, indicates how aggressively the attacker exerts his intrusion. By contrast, the authors in [11] assume that the attacker contains the successful attack rate to a fixed level, which is equivalent to $c = 1$ and $v(x) \equiv p$, a constant probability of successful attack.

3 The Optimal Attack Strategies

In this section, we deal with the attacker's optimal strategy in light of the time varying transmission rate $\beta(t)$ and recovery rate $\gamma(t)$. For ease of notation, in what follows we sometimes suppress the argument t as $\beta = \beta(t)$, $\gamma = \gamma(t)$ and $x = x(t)$, *etc.*

Let $k > 0$ be the per unit time cost associated with the attacker's effort. Let $f(x)$ represent the attacker's cost function with $f'(x) < 0$ and $f''(x) > 0$. This assumption is borne out in, *e.g.*, [4], [13] and implies that the operational cost of the attacker

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

decreases at a decreasing rate as the number of infected computers increases. The total cost of attack effort per unit time is given by $kv(x)$, which is the extra penalty cost from increasing probability of getting caught due to the increasing severity of attack. The attacker'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 scale [6]:

$$\inf_{v}\left\{ J_x(v) = \int_0^{\infty} e^{-rt}\big(f(x) + kv(x)\big)\, \mathrm{d}t \right\}, \quad 0 \le v(x) \le 1. \tag{3.1}$$

To solve the minimization problem, we write the current value Hamiltonian associated with (3.1) by

$$H(x, v, p) = f(x) + kv + p\big(cv(1-x) + \beta x(1-x) - \gamma x\big), \tag{3.2}$$

where $p = p(t)$ is the attacker's marginal cost at time t. The optimal control, $\hat{v}(x)$, 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

$$\hat{v}(x) = 1_{[H_v<0]} + u1_{[H_v=0]} \tag{3.3}$$

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

The adjoint equations are shown to be given by

$$\dot{p} = -H_x + rp = -f'(x) + \big(cv + \beta(2x-1) + \gamma + r\big)\, p. \tag{3.4}$$

Substituting (2.3) and (3.4) into $\dot{H}_v = c\dot{p}(1-x) - cp\dot{x}$, and equating $\dot{H}_v$ and H_v to zero, we obtain

$$f'(x) = \frac{k}{c(1-x)}\left(\beta(1-x) - \frac{\gamma}{1-x} - r\right). \tag{3.5}$$

We may solve (3.5) for the steady state percentage of infected computers, $x^* = x^*(t)$. The optimal control $\hat{v}(x)$ in this singular region is a time-dependent rate and found by solving $\dot{x} = 0$ at x^*:

$$\hat{v}(x^*) = u = -\frac{\beta x^*(1-x^*) - \gamma x^*}{c(1-x^*)}. \tag{3.6}$$

Our main result is given as follows.

Theorem 3.1 *Suppose that* $\gamma(t) > \beta(t) > 0$, $\big(\beta(t)x^*(t) + c\big)\big(1 - x^*(t)\big) - \gamma(t)x^*(t) > 0$ *and* $f'(0) < -k\big(r+\gamma(t)-\beta(t)\big)\big/c$ *for all* $t \ge 0$. *Recall that* $f'(x) < 0$ *and* $f''(x) > 0$. *Then the optimal response of the attacker is given by*

$$\hat{v}(x) = \begin{cases} 1, & x < x^*(t), \\ u, & x = x^*(t), \\ 0, & x > x^*(t), \end{cases} \tag{3.7}$$

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

where

$$u = u(t) = -\frac{\beta(t)x^*(t)\big(1 - x^*(t)\big) - \gamma(t)x^*(t)}{c\big(1 - x^*(t)\big)},$$

and

$$x^*(t) < \frac{\sqrt{\big(c + \gamma(t) - \beta(t)\big)^2 + 4\beta(t)c} - \big(c + \gamma(t) - \beta(t)\big)}{2\beta(t)}.$$

Furthermore, the threshold $x^*(t)$ is non-decreasing when $\beta(t)$ is non-decreasing and $\gamma(t)$ is non-increasing; $x^*(t)$ is non-increasing when $\beta(t)$ is non-increasing and $\gamma(t)$ is non-decreasing. The monotonicity of $x^*(t)$ is strict when either $\beta(t)$ or $\gamma(t)$ is strictly monotonic at time instant t. This is illustrated in Table 1.

$x^*(t)$		$\beta(t)$		
		↗	↘	→
$\gamma(t)$	↗	ID	↘	↘
	↘	↗	ID	↗
	→	↗	↘	→

Table 1: Monotonicity of the threshold $x^*(t)$ with respect to the monotonicity of $\beta(t)$ and $\gamma(t)$. Here, "ID" means "indefinite".

Theorem 3.1 indicates that if the fraction of infectious hosts $x(t) < x^*(t)$, then it is optimal for the attacker to enhance the infection in the network by applying full attack effort. If $x(t) > x^*(t)$, it is optimal to reduce the percentage of invasion in the network by exerting zero attack effort. If $x(t) = x^*(t)$, then an intermediate attack effort $u(t)$ would be optimal, in light of the assumptions given here. In addition, the correlations between rates $\beta(t)$, $\gamma(t)$ and the threshold, $x^*(t)$, imply that if a virus or bot is liable to transmit and the defense mechanism of computers is weak, they are then highly prone to be attacked by the botnet herder. On the other hand, if the infectivity of a computer worm is low and the computers are equipped with reliable defense systems, the risk of suffering from intensive attacks will likely be reduced. The reason is that when the threshold x^* increases, the size benefits of the operation cost are apt to overwhelm the opportunity cost of getting caught or traced. Therefore, the attacker would exert full effort. This phenomenon has been observed in the recent study of the dormant Confiker botnet [12].

4 Proof of Theorem 3.1

We will proceed in a similar reasoning with [4]. We first establish two useful lemmas.

Lemma 4.1 *Suppose the assumptions of Theorem 3.1 hold. Set*

$$F(x,t) = f'(x)c(1-x) + k\Big(r - \beta(t)(1-x) + \frac{\gamma(t)}{1-x}\Big). \tag{4.1}$$

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

Then for all $t \geq 0$ there exits a unique $x^* = x^*(t)$ such that $F(x^*, t) = 0$. Moreover, Table 1 in Theorem 3.1 holds.

Proof For $t \geq 0$ we have $F(1,t) = +\infty$ and $F(0,t) < 0$ by (4.1). Since $f'(x) < 0$ and $f''(x) > 0$, we get $F_x(x,t) = c\big(f''(x)(1-x) - f'(x)\big) + k\beta(t) + \frac{k\gamma(t)}{(1-x)^2} > 0$. Note that $f'(x) < 0$ by assumption, the results then follow as per straightforward arguments. ■

Lemma 4.2 *Suppose the assumptions of Theorem 3.1 hold. Then for $t \geq 0$ we have*

$$x^*(t) < \frac{\sqrt{\big(c+\gamma(t)-\beta(t)\big)^2 + 4\beta(t)c} - \big(c+\gamma(t)-\beta(t)\big)}{2\beta(t)},$$

which is a solution to a long-run steady state, $\dot{x} = 0$ with $v(x) = 1$.

Proof There is only one zero for $G(x,t) := \big(\beta(t)x+c\big)(1-x) - \gamma(t)x$ with $x \in (0,1)$, which is at

$$x(t) = \frac{\sqrt{(c+\gamma(t)-\beta(t))^2 + 4\beta(t)c} - (c+\gamma(t)-\beta(t))}{2\beta(t)}.$$

The proof concludes from the assumptions in Theorem 3.1. ■

Proof of Theorem 3.1 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 [6]. The attacker's value function is defined as

$$\phi(x) := \inf_v \left\{ J_x(v) = \int_0^\infty e^{-rt}\big(f(x) + kv(x)\big)\,\mathrm{d}t \right\}.$$

The corresponding Bellman equation (*e.g.*, [22]) is

$$\begin{aligned} r\phi(x) &= \inf_v \{ f(x) + kv + \phi'(x)\dot{x} \} \\ &= \inf_v \big\{ f(x) + kv + \phi'(x)\big(cv(1-x) + \beta x(1-x) - \gamma x\big) \big\} \\ &= \inf_v H\big(x, v, \phi'(x)\big) \\ &= \inf_v H(x, v, p), \end{aligned}$$

where $p := \phi'(x)$.

From (3.3) we know that the optimal control $\hat{v}$ takes the form

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

and then we may express the Hamiltonian as

$$H(x,v,p) = f(x) + p\big(\beta x(1-x) - \gamma x - \mu x\big) - \big(k + pc(1-x)\big)^-,$$

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

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

$$r\phi(x) = f(x) + \phi'(x)(\beta x(1-x) - \gamma x) - \big(k + \phi'(x)c(1-x)\big)^-. \tag{4.2}$$

Set $z(x,t) = k + \phi'(x)c(1-x)$, and we have $z'(x,t) = c\big(\phi''(x)(1-x) - \phi'(x)\big)$. By utilizing (4.2), we derive that

$$z_x(x,t) + z(x,t)\frac{r - \beta(1-x) + \frac{\gamma}{1-x}}{(\beta x + c1_{[z(x,t)<0]})(1-x) - \gamma x} + \frac{F(x,t)}{(\beta x + c1_{[z(x,t)<0]})(1-x) - \gamma x} = 0. \tag{4.3}$$

If $z(x,t) < 0$, by (4.1) and (4.3) we obtain

$$\frac{\mathrm{d}}{\mathrm{d}x}\Big(z(x,t)e^{-\int_0^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi+c)(1-\xi)-\gamma\xi}\mathrm{d}\xi}\Big) + \frac{F(x,t)}{(\beta x + c)(1-x) - \gamma x}e^{-\int_0^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi+c)(1-\xi)-\gamma\xi}\mathrm{d}\xi} = 0. \tag{4.4}$$

If $z(x,t) > 0$, by (4.1) and (4.3) we have

$$\frac{\mathrm{d}}{\mathrm{d}x}\Big(z(x,t)e^{\int_x^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi}\Big) + \frac{F(x,t)}{\beta x(1-x) - \gamma x}e^{\int_x^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi} = 0. \tag{4.5}$$

For $x^* < x < 1$, involving (4.5) we set

$$z(x,t)e^{\int_x^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi} + \int_{x^*}^x \frac{F(\eta,t)}{\beta\eta(1-\eta) - \gamma\eta}e^{\int_\eta^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi}\mathrm{d}\eta = 0.$$

Hence,

$$z(x,t) = -\int_{x^*}^x \frac{F(\eta,t)}{\beta\eta(1-\eta) - \gamma\eta}e^{\int_\eta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi}\mathrm{d}\eta. \tag{4.6}$$

It is clear that $z(x,t) > 0$ for $t \geq 0$. Now we need to verify that $z(x,t)$ also satisfies the boundary condition for $z(x,t) \to k$ as $x \to 1$. We rewrite (4.6) using integration by parts and (4.1) as

$$z(x,t) = k - ke^{\int_{x^*}^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi} - \int_{x^*}^x \frac{f'(\eta)c(1-\eta)}{\beta\eta(1-\eta) - \gamma\eta}e^{\int_\eta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi}\mathrm{d}\eta.$$

The fact that $e^{\int_\eta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi} \leq \frac{1-x}{1-\eta}$ and $\big|\int_{x^*}^x \frac{f'(\eta)c(1-\eta)}{\beta\eta(1-\eta)-\gamma\eta}e^{\int_\eta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{\beta\xi(1-\xi)-\gamma\xi}\mathrm{d}\xi}\mathrm{d}\eta\big| \leq C(1-x)(x-x^*)$ for some constant C imply the boundary condition at $x = 1$.

For $0 < x < x^*$, by using (4.4) we set

$$-z(x,t)e^{-\int_0^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi+c)(1-\xi)-\gamma\xi}\mathrm{d}\xi} + \int_x^{x^*} \frac{F(\eta,t)}{(\beta\eta + c)(1-\eta) - \gamma\eta}e^{-\int_0^\eta \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi+c)(1-\xi)-\gamma\xi}\mathrm{d}\xi}\mathrm{d}\eta = 0.$$

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

Accordingly,

$$z(x,t)=\int_x^{x^*}\frac{F(\eta,t)}{(\beta\eta+c)(1-\eta)-\gamma\eta}e^{-\int_x^\eta\frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi+c)(1-\xi)-\gamma\xi}\,\mathrm{d}\xi}\,\mathrm{d}\eta, \tag{4.7}$$

and $z(x,t)<0$ for $t\geq 0$ by the assumptions in Theorem 3.1.

For $x=x^*(t)$, we have $z(x^*,t)=0$. It follows from Lemma 4.1 that x^* is uniquely defined, and Lemma 4.2 implies

$$x^*(t)<\frac{\sqrt{\big(c+\gamma(t)-\beta(t)\big)^2+4\beta(t)c}-\big(c+\gamma(t)-\beta(t)\big)}{2\beta(t)}.$$

By setting $\dot{x}|_{x=x^*}=0$, we obtained the optimal control as

$$\hat{v}=u(t)=-\frac{\beta(t)x^*(t)\big(1-x^*(t)\big)-\gamma(t)x^*(t)}{c\big(1-x^*(t)\big)}.$$

Thereby, we have obtained the optimal feedback of the attacker

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

as desired. ■

5 Conclusion

In this paper, we investigate the spread of virus in computer networks based on optimal control theory. We move a step further by exploring models that accommodate practical situations where the rates of infection and recovery may change over time, which capture the fact that attack and defense are under dynamical adjustment. Optimal attack strategies are provided by minimizing the cost function of the attacker. Understanding the optimal strategies taken by the attacker may offer some guidelines for the network society on how to cope with the cybercriminals. One interesting future direction would be to incorporate randomness into the model [7], since virus propagation is an inherently stochastic phenomenon and subjects to many random disturbances.

Restriction on the topology of the spreading networks is not explicitly stated in the current work. Realizing the fact that different hosts may have different infection capabilities due to their different degrees, finding the optimal strategies over general (directed) network topologies [19] is another interesting problem. To capture the infection process between different hosts, multi-type models [2], [3], [8] would certainly be appealing.

Finally, we mention that the present study is meant to investigate analytical characterizations of attack-defense dynamics while assuming certain parameter values are observed by drawing on empirical data or expert knowledge.

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press

Acknowledgments The author wishes to thank the referee whose detailed comments and suggestions helped improve the paper significantly. The author is grateful to the editor Professor Jianhong Wu for helpful comments.

References

[1] M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir, *A survey of botnet technology and defenses.* In: Proc. Cybersecurity Applications & Technology Conference For Homeland Security (CATCH '09), Washington, DC, March 2009, 299–304.
[2] F. Ball, D. Mollison and G. Scalia-Tomba, *Epidemics with two levels of mixing.* Ann. Appl. Prob. **7**(1997), 46–89. http://dx.doi.org/10.1214/aoap/1034625252
[3] F. Ball, D. Sirl and P. Trapman, *Analysis of a stochastic SIR epidemic on a random network incorporating household structure.* Math. Biosci. **224**(2010), 53–73. http://dx.doi.org/10.1016/j.mbs.2009.12.003
[4] A. Bensoussan, M. Kantarcioglu and C. Hoe, *A game-theoretical approach for finding optimal strategies in a botnet defense model.* In: Proc. GameSec '10, Berlin, Germany, 2010, 135–148.
[5] N. Berger, C. Borgs, J. T. Chayes and A. Saberi, *On the spread of viruses on the internet.* In: Proc. 16th Annual ACM-SIAM Symposium on Discrete Algorithms, ACM, New York, 2005, 301–310.
[6] D. P. Bertsekas, *Dynamic Programming and Optimal Control. Vol. 1*. Third edition. Athena Scientific, Belmont, MA, 2005.
[7] T. Britton, *Stochastic epidemic models: a survey.* Math. Biosci. **225**(2010), 24–35. http://dx.doi.org/10.1016/j.mbs.2010.01.006
[8] T. Britton, T. Kypraios and P. D. O'Neill, *Inference for epidemics with three levels of mixing: methodology and application to a measles outbreak.* Scand. J. Stat. **38**(2011), 578–599.
[9] F. Cohen, *Computer viruses: theory and experiments.* Computer and Security **6**(1987), 22–35.
[10] O. Diekmann and J. A. P. Heesterbeek, *Mathematical Epidemiology of Infectious Disease*. John Wiley & Sons, Chichester, 2000.
[11] N. Fultz and J. Grossklags, *Blue versus red: towards a model of distributed security attacks.* Lecture Notes in Computer Science **5628**(2009), 167–183.
[12] K. J. Higgins, *Conficker botnet 'dead in the water', researcher says.* Technical Report, http://www.darkreading.com/vulnerability_management/security/attacks/showArticle.jhtml?articleID=224201115.
[13] M. Lelarge, *Economics of malware: epidemic risks model, network externalities and incentives.* In: Proc. 47th Annual Allerton Conference on Communication, Control, and Computing, IEEE Press, Piscataway, NJ, 2009, 1353–1360.
[14] Z. Li, Q. Liao and A. Striegel, *Botnet economics: uncertainty matters.* In: Managing Information Risk and the Economics of Security, Springer, New York, 2009, 245–267.
[15] J. R. C. Piqueira and V. O. Araujo, *A modified epidemiological model for computer viruses.* Appl. Math. Comput. **213**(2009), 355–360. http://dx.doi.org/10.1016/j.amc.2009.03.023
[16] N. Provos and T. Holz, *Virtual Honeypots—From Botnet Tracking to Intrusion Detection*. Pearson Education Inc., Boston, 2008.
[17] Y. Shang, *Optimal attack strategies in a dynamic botnet defense model.* Appl. Math. Inf. Sci. **6**(2012), 29–33.
[18] Y. Shang, *Likelihood estimation for stochastic epidemics with heterogeneous mixing populations.* Int. J. Comput. Math. Sci. **6**(2012), 34–38.
[19] Y. Shang, *Multi-agent coordination in directed moving neighborhood random networks.* Chinese Phys. B **19**(2010), 070201.
[20] J. van den Broek and J. A. P. Heesterbeek, *Nonhomogeneous birth and death models for epidemic outbreak data.* Biostatistics **8**(2007), 453–467.
[21] J. van den Broek and H. Nishiura, *Using epidemic prevalence data to jointly estimate reproduction and removal.* Ann. Appl. Stat. **3**(2009), 1505–1520. http://dx.doi.org/10.1214/09-AOAS270
[22] D. Yeung and L. Petrosyan, *Cooperative Stochastic Differential Games*. Springer, New York, 2006.
[23] C. Zou, N. Duffield, D. Towsley and W. Gong, *Adaptive defense against various network attacks.* IEEE Journal on Selected Areas in Communications **24**(2006), 1877–1888.

Institute for Cyber Security, University of Texas at San Antonio, San Antonio, Texas 78249, USA
e-mail: shylmath@hotmail.com

https://doi.org/10.4153/CMB-2012-007-2 Published online by Cambridge University Press