Modeling the Effects of Timing Parameters on Virus Propagation

Yang Wang, Chenxi Wang
Carnegie Mellon University
5000 Forbes Avenue, Pittsburgh, PA, 15213
yangwang, chenxi@andrew.cmu.edu

ABSTRACT

In this paper, we investigate epidemiological models to reason about computer viral propagation. We extend the classical homogeneous models to incorporate two timing parameters: Infection delay and user vigilance. We show that these timing parameters greatly influence the propagation of viral epidemics, and that the explicit treatment of these parameters gives rise to a more realistic and accurate propagation model. We validate the new model with simulation analysis.

Categories and Subject Descriptors

C.2.3 [**Computer-Communication Networks**]: Network Operations—*Network monitoring, Public networks*

General Terms

Security, Theory

Keywords

Computer Virus, Epidemiology, Anti-virus, Security

1. INTRODUCTION

Computer viruses and worms are a great threat to the dependability of computer networks. The recent proliferation of malicious code that spreads with virus code exacerbates the problem [13, 17, 18, 1]. In order to understand their propagation behavior and to devise effective strategies against their propagation, we need to be able to model the propagation process accurately. Unfortunately, with the exception of a few specialized modeling studies [11, 12, 14, 16, 20, 19], much still remains unknown about the factors that influence computer virus propagation.

In this paper, we examine viral propagation process through epidemiological models. Epidemiological models have been used in previous computer virus and worm studies. These studies often use either the Susceptible-Infected-Susceptible (SIS) infection model or the Suscep-tible-Infected-Removed (SIR) model. In the SIS model, a node is infected and cured repeatedly, while in the SIR model, a node cannot be infected more than once. In particular, Kephart and White studied SIS virus propagation on homogeneous networks [11, 12], while Pastor-Satorras et al. [14, 15, 16] and Barabási et al. [4, 6] focused on virus propagation on various network topologies under either SIS or SIR. Wang et al. [20] proposed a topology-independent model along with a general theory for epidemic threshold, but also assumed a vanilla SIS propagation model.

The basic SIS and SIR propagation models are overly simplistic in their treatment of timing factors during virus propagation. As a result, the models mentioned above are limited in their accuracy. This work aims to extend previous models by incorporating two specific "timing" parameters: *infection delay* and *user vigilance*. Infection delay is a delay in the spreading of virus from an infected node. User vigilance is a period of time during which the user of a node is vigilant against infections, which reduces the susceptibility of that node. In this paper, we define the vigilance period to be a period of time immediately after the curing of an infected node, since users in real life are more likely to be vigilant immediately after having been notified of a potential or real infection. Both infection delay and user vigilance were abstracted away in previous studies. We show in this paper that studying the effects of these two parameters can increase our understanding of the virus propagation process and potentially leads to better defenses against computer viruses.

The layout of this paper is as follows: In Section 2, we give a background review of SIS and SIR. In Section 3, we describe our extensions to previous models (the homogeneous model, in particular). In Section 4, we show that our models accurately predict the effects of the timing parameters and analyze our findings. We discuss some implications of our results and summarize in Section 6.

2. INADEQUACIES OF SIS AND SIR

A model of virus propagation has primarily three results:

- The rate of propagation determines how quickly the virus spreads and is represented as a function of time t.
- The final epidemic state determines viral prevalence as $t \to \infty$. It can either converge into a steady state value or be divergent.

WORM'03, October 27, 2003, Washington, DC, USA.

- The epidemic threshold condition is a critical value such that when the ratio of virus birth rate to death rate exceeds this value, an epidemic exists in the final epidemic state

In this paper, we represent the viral prevalence at time t as a fraction of the total number of nodes on the network. We can infer from the above the number of infected nodes at t.

An SIS model of infection assumes that a node on the network is in one of two states: Infected and therefore infectious, or healthy and susceptible. The model assumes instantaneous state transitions. That is, as soon as a node becomes infected, it becomes infectious. As soon as a node is cured, it is susceptible to re-infection. An SIS model is usually concerned with the rate of propagation and the final epidemic state. An epidemic threshold condition can be derived from the model [2, 5, 11, 12, 16, 20].

An SIR model assumes that a node on the network can be in one of three states: Healthy (susceptible), infected (infectious), and removed (immune or failed). Instead of cycling between susceptible and infectious, a node is infected only once before being removed from the network, either due to acquired immunity or node failure. Since all susceptible and infected nodes will eventually be removed, an epidemic model that assumes SIR always produces a zero final epidemic state. Therefore, such a model is only concerned with the rate of propagation and the maximum density of infected nodes present during the epidemic "run" [2, 22].

Both the SIR model and the SIS model assume that there is zero delay between the different state transitions. In reality, however, there may be a time lag between the arrival of a virus on a node and further infections dispatched from that node. For example, in the case of email viruses, some users may not check their email as frequently as others, so a virus could lie dormant in a user's inbox for a period of time before it wreaks havoc. In addition, an active virus may be delayed before propagating due to system configuration or resource availability. Some viruses may purposely lay dormant for a period of time prior to infecting other nodes for stealth reasons.

Further, once a node has been infected by a virus and subsequently cured, the user of that node may become more vigilant against future infections. In the extreme case, permanent vigilance will mark the node as being immune to re-infection attempts, thus reducing the infection model to SIR.

One might suggest that parameters such as infection delay and user vigilance can be incorporated into the infection rate. We believe that this model is overly simplistic. For instance, a resident but dormant virus might be detected, but a virus in transit cannot. Similarly, as noted above, vigilance in an SIS model can potentially change the infection model to SIR, which results in a different epidemic model.

This paper is concentrated on modeling viruses that spread in a similar fashion to email-based viruses. Specifically, we assume that a susceptible node can be infected by the same virus repeatedly. In the remainder of the paper, we propose extensions to previous models to incorporate the effects of infection delay and user vigilance. In this paper, we consider universal delay and vigilance. Delay and vigilance that vary across the network require more complicated models and are beyond the scope of this paper.

3. MODELING INFECTION DELAY AND USER VIGILANCE FOR SIS

A classical SIS model is the Kephart and White model (in this paper, we refer to it as the KW model). The KW model models node communication in a homogeneous or Erdös-Rényi network [7] as a directed graph [11]. A directed edge from node i to node j indicates that i can directly infect j. A virus birth rate of β is defined on every edge from an infected node, and a virus death rate of δ is defined on every infected node (as shown in Figure 1). Further, both β and δ are considered to be constant throughout time. If we denote the density of infected nodes in a network at time t as η_t, then the deterministic time evolution of η_t is

$$\frac{d\eta_t}{dt} = \beta\langle k\rangle\eta_t(1-\eta_t) - \delta\eta_t \quad (1)$$

where $\langle k\rangle$ is the average outgoing degree of nodes in the network. We solve Equation 1 to yield

$$\eta_t = \frac{\eta_0(1-\rho')}{\eta_0 + (1-\rho'-\eta_0)e^{-(\beta\langle k\rangle-\delta)t}} \quad (2)$$

with a steady state solution, η_∞, of

$$\eta_\infty = 1 - \rho' \quad (3)$$

where $\rho' = \frac{\delta}{\beta\langle k\rangle}$ and η_0 is the initial density of infected nodes. If we denote the epidemic threshold as τ, which is the ratio of $\frac{\beta}{\delta}$ above which there is a steady state epidemic, then by setting the right hand side of Equation 3 equal to 0, the KW model yields

$$\tau = \frac{1}{\langle k\rangle} \quad (4)$$

Equation 4 means that no epidemic will occur if the virus death rate exceeds the product of the virus birth rate (per edge) and the average number of edges connected to a node.

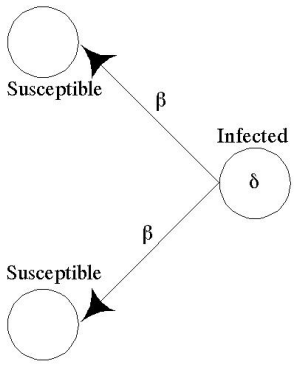

Figure 1: The KW model on a directed graph

In this section, we introduce a new epidemic model that incorporates both infection delay and user vigilance. We use the KW SIS model as a basis, but the model can be extended to other SIS or SIR models. Delay and vigilance are independent parameters. We present them separately at first, then combine the two into a single model.

3.1 Modeling the effects of infection delay

We define infection delay ϵ_i as the length of time between the virus arrival on node i and the instant i becomes infectious to its neighbors. For this paper, we assume ϵ_i to be universal and constant, and denote simply as ϵ. In this model, we make a distinction between "infected nodes" and "infectious nodes." Intuitively, infection delay slows the viral propagation and may allow curing to occur before a node becomes infectious. The new equation incorporating delay can be written as

$$\frac{d\eta_t}{dt} = \beta\langle k\rangle\eta_{t-\epsilon}e^{-\delta\epsilon}(1-\eta_t) - \delta\eta_t \quad (5)$$

where $\eta_{t-\epsilon} = 0$ for $t < \epsilon$. For $t \geq \epsilon$, the density of infectious nodes is the density of infected nodes at time $t-\epsilon$, since all nodes infected between $t-\epsilon$ and t are still being delayed. Curing a node during ϵ, the infection delay period, results in the $e^{-\delta\epsilon}$ term. For $0 \leq t < \epsilon$, since all infected nodes are being delayed, the infected population density simply decreases at the rate of curing.

We note that the model in Equation 5 incorporates a new state in the traditional SIS model: A susceptible node enters the delayed state with the arrival of an infectious agent. A delayed node becomes either cured or infectious by the end of the delay period.

Equation 5 belongs to the class of non-linear delay differential equations for which there rarely exist close-form solutions. We solve for η_∞ by setting the left hand side of Equation 5 to 0 and $\eta_{t-\epsilon} = \eta_t$.

$$\eta_\infty = \frac{\beta\langle k\rangle e^{-\delta\epsilon} - \delta}{\beta\langle k\rangle e^{-\delta\epsilon}} = 1 - \rho' e^{\delta\epsilon} \quad (6)$$

Equation 6 shows that the steady state of viral density decays toward zero at an exponential rate as a function of the length of infection delay. We can derive the epidemic threshold by setting the right hand side of Equation 6 equal to 0, which yields

$$\tau_{\text{del}} = \frac{e^{\delta\epsilon}}{\langle k\rangle} \quad (7)$$

Equation 7 indicates that infection delay increases the epidemic threshold, which means that infection delay makes an epidemic die out more easily.

3.2 Modeling the effects of user vigilance

We define user vigilance as a period of time after curing during which the user of a node is vigilant against re-infection of the node. We represent vigilance with two parameters:

- The vigilance coefficient, ϕ_i, that indicates the susceptibility of the node. ϕ_i is a quantity between 0 and 1. A ϕ_i of 0 indicates full susceptibility, and 1 indicates complete immunity.

- The vigilance period, ν_i, that indicates the length of time after curing during which the node is vigilant against re-infection attempts. At the end of that period, the node becomes fully susceptible to infections again.

In this paper, we assume ν_i to be universal and constant, and denote it as ν.

Intuitively, user vigilance makes a node less susceptible to infections for a period of time after curing, which reduces the susceptible population. This results in a Susceptible-Infected-Immune-Susceptible (SIIS) model of infection. If we assume a universal and constant vigilance coefficient ϕ, then we obtain the following equation

$$\frac{d\eta_t}{dt} = \beta\langle k\rangle\eta_t(1-\eta_t-\delta\phi\int_{t-\nu}^{t}\eta_s ds) - \delta\eta_t \quad (8)$$

where $\eta_s = 0$ for $s < 0$. If we set ϕ to 1, then nodes simply stay completely immune to infections during their vigilance period and become fully susceptible again when the vigilance period ends. In Equation 8, the population density of susceptible nodes at time t is reduced by the fraction of the nodes that are still in their vigilance period. For $\phi = 0$ or $\nu = 0$, Equation 8 reduces to the original KW model.

Equation 8 is again a non-linear delay differential equation. We obtain η_∞ for $\phi = 1$ and $t \gg \nu$ by setting the left hand side of Equation 8 to 0 and $\eta_s = \eta_t$. Ignoring the trivial solution of $\eta_t = 0$, we obtain

$$\eta_\infty = \frac{\beta\langle k\rangle - \delta}{\beta\langle k\rangle(1+\delta\nu)} = \frac{1-\rho'}{1+\delta\nu} \quad (9)$$

Equation 9 shows that, when $\phi = 1$, η_∞ decreases toward zero, and the rate of decrease diminishes as the value of ν increases. If we set ν to zero, then Equation 9 simply yields η_∞ of the original KW model (see Equation 3). Equation 9 yields the same epidemic threshold as the basic KW model. In other words, user vigilance does not affect the epidemic threshold.

We now turn to a more complex form of the vigilance model for which ϕ is no longer constant. Rather, the vigilance coefficient is a function ϕ_t that decreases over time, where $\phi_0 = 1$ and $\phi_\nu = 0$. This model captures the notion of dynamically degrading user vigilance. An example of such a function is $\phi_t = 2 - e^{\frac{t\ln(2)}{\nu}}$, as shown in Figure 2 (this particular function was chosen for illustration purposes and is not derived from real data). We believe that user vigilance is typically at its maximum immediately following a virus detection and cleansing operation, and then decreases in some fashion over time before the node becomes fully susceptible to infections again. We call this model the dynamic vigilance model. The time evolution of this model is

$$\frac{d\eta_t}{dt} = \beta\langle k\rangle\eta_t(1-\eta_t-\delta\int_{t-\nu}^{t}\eta_s\phi_{t-s}ds) - \delta\eta_t \quad (10)$$

where $\eta_s = 0$ for $s < 0$.

We solve Equation 10 for η_∞, and obtain

$$\eta_\infty = \frac{\beta\langle k\rangle - \delta}{\beta\langle k\rangle(1+\delta\int_{t-\nu}^{t}\phi_{t-s}ds)} = \frac{1-\rho'}{1+\delta\int_0^\nu\phi_s ds} \quad (11)$$

Equation 11 shows that η_∞ decreases in a similar fashion as in Equation 9, albeit at a slower rate. Again, vigilance has no effect on epidemic threshold.

3.3 Combining delay and vigilance

We thus far have analyzed the effect of infection delay and user vigilance separately. We note that the two factors are

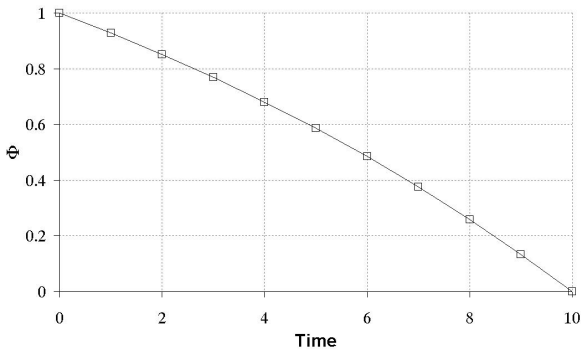

Figure 2: Example $\phi_t = 2 - e^{\frac{tln(2)}{\nu}}$, where $\nu = 10$ time units

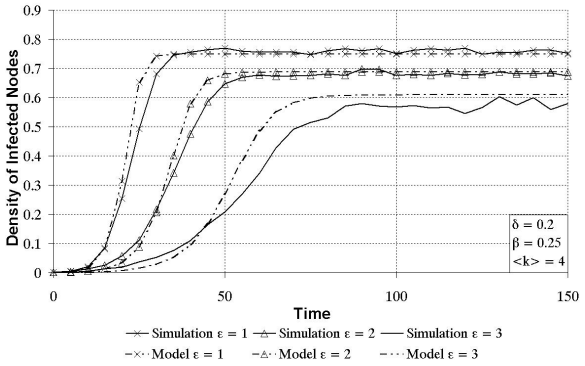

Figure 3: Infected population density for various lengths of infection delay on 1000-node Erdös-Rényi network

independent. A joint model can be written as

$$\frac{d\eta_t}{dt} = \beta\langle k\rangle\eta_{t-\epsilon}e^{-\delta\epsilon}(1-\eta_t-\delta\phi\int_{t-\nu}^{t}\eta_s ds) - \delta\eta_t \quad (12)$$

where $\eta_{t-\epsilon} = 0$ for $t < \epsilon$ and $\eta_s = 0$ for $s < 0$. Assuming $\phi = 1$, η_∞ is

$$\eta_\infty = \frac{\beta\langle k\rangle e^{-\delta\epsilon} - \delta}{\beta\langle k\rangle e^{-\delta\epsilon}(1+\delta\nu)} \quad (13)$$

Note that the epidemic threshold for this model is exactly the same as that of the delay model, since vigilance has no effect on the epidemic threshold.

4. SIMULATION ANALYSIS

In this section, we present a set of simulation results that demonstrate the accuracy of our models in describing viral propagation on homogeneous networks with delay and vigilance.

We built a simulator on top of the Network Simulator [8] to conduct our simulation experiments. Each simulation run begins with one randomly chosen infected node on an Erdös-Rényi network of 1000 nodes with an average connectivity of approximately 4. Simulation proceeds in steps of one time unit. During each step, every infectious node i attempts to infect each of its neighbors j with probability β. In addition, every infectious node i is subject to a curing attempt with probability δ. If the curing of i occurs before the infection attempt, then i does not send out infections to j. If j is already infected and the curing of j falls after the infection attempt, then the infection attempt on j does not have any effect. Infection delay and user vigilance periods are multiples of the simulation time unit. Infection delay appears as a period of viral dormancy on a node after each incoming infection. User vigilance appears as decreased β for a period of time for a node after each curing. Each simulation plot shown is averaged over 15 independent simulation runs.

We solve the delay model (Equation 5) numerically and plot the solution with three simulations in Figure 3. The delay periods for the simulations are 1, 2, and 3 time units, respectively. As shown, the simulated virus propagation with infection delay conform to the *delay model* reasonably well.

In a similar vein, Figure 4 shows three simulation results plotted against the solution of the simple vigilance model (Equation 8) for $\phi = 1$. As shown, the simulation results also conform fairly well with the predictions of the *vigilance model*.

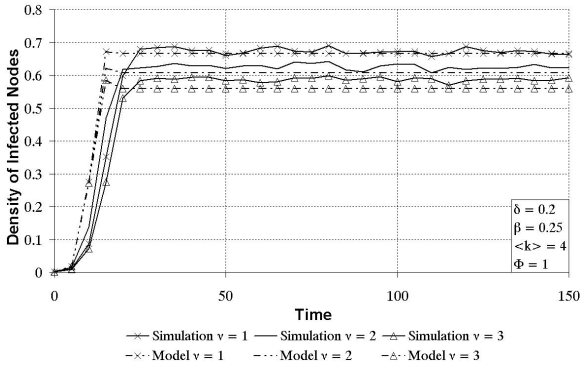

Figure 4: Infected population density for various lengths of user vigilance on 1000-node Erdös-Rényi network

Figures 3 and 4 show that both delay and user vigilance play an important role in reducing virus prevalence in the network. However, while the rate of decay in η_∞ decreases as the vigilance period increases, the rate of decay grows exponentially with the length of delay. Simply stated, the longer the delay, the faster η_∞ drops. In contrast, the longer the vigilance period, the slower η_∞ drops. Figures 5 and 6 demonstrate the trends by plotting Equations 6 and 9 with various lengths of delay and vigilance periods. For Figure 6, $\phi = 1$.

We note that the delay model assumes that delayed viruses are removed at the same rate as the ones that have exposed themselves by infecting others. This means that the local virus detection tools need to be sophisticated enough to detect the presence of possibly dormant viruses. If delayed viruses are not detected and removed at rate δ, then the dynamics of viral propagation is

$$\frac{d\eta_t}{dt} = \beta\langle k\rangle\eta_{t-\epsilon}(1-\eta_t) - \delta\eta_{t-\epsilon} \quad (14)$$

Figure 5: η_∞ decays as delay increases

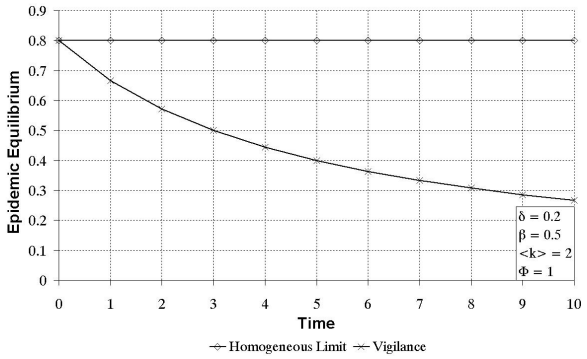

Figure 6: η_∞ decays as vigilance increases

where $\eta_{t-\epsilon} = 0$ for $t < \epsilon$. η_∞ of Equation 14 is simply that of the basic KW model (see Equation 3), since these delayed infections only delay the process of reaching steady state.

5. MODELING DELAY AND VIGILANCE FOR SIR

We thus far have analyzed delay and vigilance based on the KW SIS model. In this section, we present our extended models in the SIR context. In an SIR model, by definition, vigilance is essentially infinity ($\nu = \infty$). In other words, only the delay extension is applicable. Restating Equation 12,

$$\frac{d\eta_t}{dt} = \beta\langle k\rangle\eta_{t-\epsilon}e^{-\delta\epsilon}(1-\eta_t-\delta\int_0^t \eta_s ds) - \delta\eta_t \quad (15)$$

where $\eta_{t-\epsilon} = 0$ for $t < \epsilon$. Solving for η_∞ yields

$$\eta_\infty = \frac{\beta\langle k\rangle e^{-\delta\epsilon} - \delta}{\beta\langle k\rangle e^{-\delta\epsilon}(1+\delta\infty)} = 0 \quad (16)$$

Equation 16 confirms previous results that the final epidemic state for an SIR model is zero.

Since equation 15 does not have a close-form solution, we plot simulation results only in Figure 7. Delays of 0, 1, and 2 time units are plotted. These simulations are run on a 1000-node homogeneous network with average connectivity 10. A node is marked immune after the first curing. We plot both η_t and the *total density of affected nodes*, which is the density of all nodes infected by the virus during its entire lifetime. As shown, infection delays suppresses the infection spread for the SIR model. In additiont o reducing the peak η_t, infection delays reduce dramatically the total number of nodes ever infected. In Figure 7, a delay of unit 2 produced a 40% drop in the total number of infected nodes.

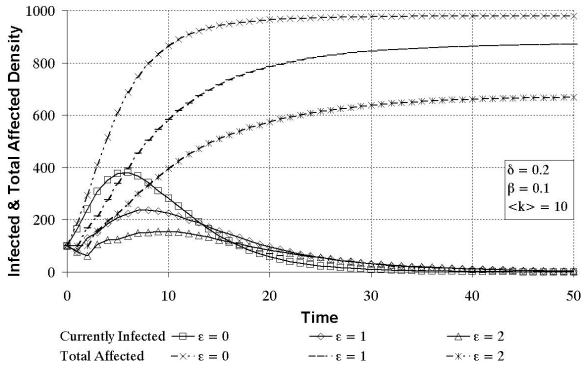

Figure 7: Density of currently infected nodes and total affected nodes for various lengths of infection delay on 1000-node Erdös-Rényi network

6. DISCUSSION AND CONCLUSION

Researchers have been exploring mechanisms such as virtual execution environment [3], secure NIC [10], and limited connection rates [21] to halt viral traffic in computer networks. It has been suggested that introducing intentional delays in these mechanisms would be an effective way to stop viral propagations [9, 3]. Our models demonstrate that, given sufficiently long delay, this strategy will indeed be effective. However, since artificial delays will affect the performance of the network, the problem then becomes one of balancing reduced viral prevalence and system performance. On one end of the spectrum are mission critical systems that may not tolerate any delays. On the other are systems that do not require real time responses, and hence are more amenable to delay-inducing mechanisms. Decisions on the appropriate length of infection delay is best made on a case-by-case basis.

The diminishing returns produced by a longer vigilance period leads to a very practical question: at which point does the cost of user vigilance outweigh the benefit? The answer to this question may provide useful guidelines to, for instance, the time window after the detection and removal of a virus during which a virus scan must be run frequently (after which the scan may be invoked less frequently). Present policies governing the frequency of virus scans can be tuned with our model.

Our study suggests that the most cost effective strategy will need to employ a combination of infection delay and user vigilance. Both rules that govern user behavior and rules followed by the systems on the network can be tuned according to the predictions provided by our models.

The models presented in this paper are based on the KW SIS epidemic models for homogeneous and Erdös-Rényi networks. However, we can also incorporate infection delay and user vigilance into other SIS (or SIR) models such as the ones presented by Pastor-Satorras et al. [16] and Wang et

al. [20]. The incorporation process is the same.

Besides propagation rate, final epidemic state, and epidemic threshold condition, another result of potential interest is the total number of affected nodes, which is the number of all nodes infected by the virus during its entire lifetime. The total number of affected nodes is important for keeping track of latent viral side-effects such as back doors.

In addition to infection delay and user vigilance, many other parameters of potential interest exist. In particular, in a real network, viral birth and death rates are not likely to be universal or constant (infection delay and user vigilance are also not likely to be universal). We plan to study these issues in the future.

7. REFERENCES

[1] AFP. South korea, japan warn against computer virus. *Yahoo! News: Asia: Technology*, 26 January 2003. World Wide Web, `http://asia.news.yahoo.com/030126/afp/030126133142hightech.html`.

[2] Réka Albert and Albert-László Barabási. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74:47–97, 30 January 2002.

[3] Robert Balzer. Assuring the safety of opening email attachments. In *Proceedings of DARPA Information Survivability Conference and Exposition 2001*, volume 2, pages 1257–1262, June 2001.

[4] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *Science*, 286:509–512, 15 October 1999.

[5] Marián Boguñá and Romualdo Pastor-Satorras. Epidemic spreading in correlated complex networks. *Physical Review E*, 66:047104, 2002.

[6] Zoltán Dezsö and Albert-László Barabási. Halting viruses in scale-free networks. *Physical Review E*, 65:055103(R), 21 May 2002.

[7] Paul Erdös and Alfred Rényi. On the evolution of random graphs. In *Publication 5*, pages 17–61. Institute of Mathematics, Hungarian Academy of Sciences, Hungary, 1960.

[8] Kevin Fall and Kannan Varadhan, editors. *The ns Manual*. The VINT Project. UC Berkeley, LBL, USC/ISI, and Xerox PARC, 14 April 2002. World Wide Web, http://www.isi.edu/nsnam/ns/doc/. Ongoing.

[9] Stephanie Forrest, Anil Somayaji, and David H Ackley. Building diverse computer systems. In *Proceedings of the* 6^{th} *Workshop on Hot Topics in Operating Systems*, pages 67–72, May 1997.

[10] Gregory R Ganger, Gregg Economou, and Stanley M Bielski. Self-securing network interfaces: What, why and how. Technical Report CMU-CS-02-144, Carnegie Mellon University, May 2002.

[11] Jeffrey O Kephart and Steve R White. Directed-graph epidemiological models of computer viruses. In *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 343–359, May 1991.

[12] Jeffrey O Kephart and Steve R White. Measuring and modeling computer virus prevalence. In *Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 2–15, May 1993.

[13] Helen Martin, editor. *The Virus Bulletin: Independent Anti-Virus Advice*. World Wide Web, http://www.virusbtn.com, 2002. Ongoing.

[14] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic dynamics and endemic states in complex networks. *Physical Review E*, 63:066117, 2001.

[15] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic dynamics in finite size scale-free networks. *Physical Review E*, 65:035108, 2002.

[16] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemics and immunization in scale-free networks. In Stefan Bornholdt and Heinz Georg Schuster, editors, *Handbook of Graphs and Networks: From the Genome to the Internet*. Wiley-VCH, Berlin, May 2002.

[17] `CERT Advisory CA-`1999-04. Melissa macro virus. World Wide Web, http://www.cert.org/advisories/CA-1999-04.html, 1999.

[18] `CERT Advisory CA-`2001-23. Continued threat of the "code red" worm. World Wide Web, http://www.cert.org/advisories/CA-2001-23.html, 2001.

[19] Chenxi Wang, John C Knight, and Matthew C Elder. On computer viral infection and the effect of immunization. In *Proceedings of the* 16^{th} *ACM Annual Computer Security Applications Conference*, December 2000.

[20] Yang Wang, Deepayan Chakrabarti, Chenxi Wang, and Christos Faloutsos. Epidemic spreading in real networks: an eigenvalue viewpoint. To appear in the 22nd Symposium on Reliable Distributed Systems, October 6 2003.

[21] Matthew M Williamson. Throttling viruses: Restricting propagation to defeat malicious mobile code. Technical Report HPL-2002-172, HP Laboratories Bristol, 17 June 2002.

[22] Cliff Changchun Zou, Weibo Gong, and Don Towsley. Code red worm propagation modeling and analysis. In *Proceedings of the* 9^{th} *ACM Conference on Computer and Communication Security*, November 2002.