Performance Evaluation of Defense Strategies against Computer Virus

Hiroshi Toyoizumi
Performance Evaluation Lab.
University of Aizu
Fukushima, Japan 965-8580
Email: toyo@u-aizu.ac.jp

***Abstract*— We evaluate performance of anti-virus strategies by using stochastic processes. The typical installations of anti-virus software is either at client PCs or the network gateway. By installing gateway anti-virus, many internet service providers and cooperate LANs are offering the screening service of emails to protect their users from the menace of computer viruses. At the same time, we are told that we should install anti-virus softwares to protect our PC and data. In this paper, we use both deterministic and stochastic argument to study the performance of anti-virus quantitatively, and find out the deterministic arqument fail to capture the important features of the virus spreads. In addition, we show the gateway anti-virus is more effective than client anti-virus.**

I. Introduction

Past few years, one of the main problems in the internet is malicious mobile codes or computer viruses spreading in the network [6], [7]. Slammer, Nimda, Code-red, Klez... These viruses affect not only client machines infected, but also consume the precious network resources and disturb uninfected machines [5], [8].

What is common for the recent virus spreads in the Internet is that they have high infection rate. They have multiple way of infection to other PCs, and have high mutation rates by sharing code information in the underground community of malicious programmers. Also, they hide their source of infection. Thus, they are becoming fast and hard to get rid of them completely.

Many researchers in both academia and private companies are struggling to provide the protection against these threat of malicious mobile codes. One of the most commonly employed solutions is to install a client-base anti-virus application to PCs. Installing an anti-viruses in your PC may be the mandatary for good citizen in internet world. At the same time, more and more administrators of local network or internet service providers install an anti-virus software to the gateway of their network.

When the anti-virus application detects a virus on the machine, it eliminates the virus, and stop further infection. However, we need the latest update file, which lists all known virus patterns, to detect and protect against the new viruses [1], [18]. Unfortunately, not all machines have the proper anti-virus application equipped with the latest update file. Furthermore, it may take some time for users to install the latest update file to avoid infection of brand-new viruses. As shown in the outbreak of Code-red [3], [12] and Nimda [4], viruses with strong infection power will dominate the network within 24 hours. Actually, on July 19, 2001, within 14 hours of the debut of its first copy, Code-red virus infected more than $359,000$ machines, at a rate of $2,000$ machines per minute at its peak [13].

Since many of the anti-virus applications are of server-client type, the server providing the latest updates can become a bottleneck if many users try to get the latest files simultaneously, which may happen especially when there is an intensive epidemic of a new and unknown virus on the network. Moreover, the server itself can be the target of a Denial of Service (DoS) attack. In any event, it is doubtful that all users install anti-virus software, and this problem will be further compounded when all machines in the home have constant access to the Internet. To avoid having install anti-virus applications on all machines, we may install an anti-virus application on only network elements such as gateways or mail servers. This will avoid the installation problem, but once a virus penetrates into the local network, the advantage will disappear.

On the other hand, some researchers have suggested the possibility of sending a vaccine to each machines via the same penetration method of a particular virus recently [7], [10], [20].

There has been many such proposed mathematical models of computer viruses. For examples, in [19], viruses are discussed in the setting of computer science, whereas in [9], viruses are treated as biological objects in the natural world. In [11], the authors study the real epidemic of computer viruses. Even the spread of Code-red virus is discussed using mathematical models in [16], [17].

Here in this paper, we first use the deterministic argument to evaluate the performance of two main defense strategies: (1) client anti-virus and (2) gateway anti-virus. Then, we use a stochastic process called birth and death process with immigration to model the virus spread in the local network. Especially, controlling parameters in this model, the local network with anti-viruses both at client PCs and at gateway can be analyzed. Using these method, we show how effective these common ways to protect against the viruses mathematically.

II. Virus spread and anti-virus software

There are many variation of malicious mobile codes or computer viruses. As defined in p.2 of [7], malicious mobile code

is any software programs designed to move from computer to computer and network to network, in order to intentionally modify computer system without the consent of the owner or operator.

In the real world, there are programmers who have malicious intents. Using their knowledge and technique, they design a certain kind of programs so that it penetrate into other innocent people's machines. Typical methods for those computer viruses to penetrate into our machines are by mail, shared folder, web browsing, instant messages and so on. Now it is common for malicious mobile codes to be equipped with multiple penetration methods. Thus, together with the expansion of internet both in terms of the scale and speed, the infection power of these computer viruses is quite strong.

Let us illustrate a typical scenario of the virus spread in the local network. First, a virus on the infected machine outside finds an email address of the local network, and sends a mail with its copy to this address. The mail is delivered to a machine in the local network. The owner of the machine is careless and opens the email and its attachment, now his machine is infected with this virus. Then, the virus on his machine find another victims in the local network by putting his copy on the shared folders and send email to the local addresses found on his machines. Thus, the whole local network is contaminated by this virus.

As illustrated in the above scenario, some virus have a penetrations methods which might be effective in local networks, like shared folders. In addition, the transmission speed is larger in the local network. Hence, the infection rate inside the local network is larger than the one for the internet.

The most common way to fight against computer viruses is to use anti-virus softwares [1], [18]. These softwares are developed to detect the existence and the penetration of computer viruses, and take appropriate measure to recover the proper functions of our machine, and stop further spread of viruses. We can install these anti-virus softwares either to our machines or to the network gateway.

When the anti-virus application detects a virus on the machine, it eliminates the virus. However, we need the latest update file of malicious mobile codes, which lists all known virus patterns, to protect against the new viruses. Unfortunately, not all machines are equipped with the anti-virus application and the latest update file. Also, it may take some time for users to install the latest update file. Thus, viruses still have the chance to infect machines and local networks protected by anti-virus.

III. Deterministic Model of Virus Spread

As pointed out in [20] and [17], the spread of viruses in the internet can be modeled by a system of deterministic differential equations, since the network is large enough for us to handle the stream of virus as fluid. Here, we apply deterministic arguments used for biology [14] to model virus spread.

Let $N(t)$ be the number of infected machines in a local network at time t. Suppose the first virus arrives at the local network from outside by its rate ν. Once the first virus successfully penetrates into the local network, it starts penetrating other machines in the local network. Let λ be the infection rate inside the local network. In general, the local infection rate λ and global infection rate (or immigration rate) ν should be different. The existing viruses might be removed either by updated anti-virus softwares or manually by administrator, so let μ be the death rate of a virus.

Now let us consider the virus population as deteministic fluid, then the change of the population of virus in the local network for a small interval Δt can be obtained by

$$N(t+\Delta t) - N(t) = (\lambda - \mu)N(t)\Delta t + \nu\Delta t + o(\Delta t). \quad (1)$$

The first term of the right hand side corresponds to the total change of the virus population caused by the viruses inside the local network, and this change is proportinal to the virus population, while the second term is the effect of immigration from outside. Dividing both sides of (1) by Δt, and let $\Delta t \to 0$, then we have a differential equation,

$$\frac{dN(t)}{dt} = (\lambda - \mu)N(t) + \nu. \quad (2)$$

Solving this differential equation with the initial condition $N(0) = n_0$, we have the following Theorem.

Theorem 1 (Virus Spread as Deterministic Fluid): Assume a virus spreads as the determistic fluid with the infection rate λ, the death rate μ and the immigration rate ν. Let $N(t)$ be the number of machine infected at time t, given $N(0) = n_0$. Then, we have

$$N(t) = \begin{cases} n_0 e^{(\lambda-\mu)t} + \frac{\nu}{\lambda-\mu}\left(e^{(\lambda-\mu)t} - 1\right), & \lambda \neq \mu; \\ n_0 + \nu t, & \lambda = \mu. \end{cases}$$

Thus, for $\lambda < \mu$, the virus population approaches to $\nu/(\lambda-\mu)$, while we can see the exponential outbreak of virus for $\lambda > \mu$ (see Figure 1).

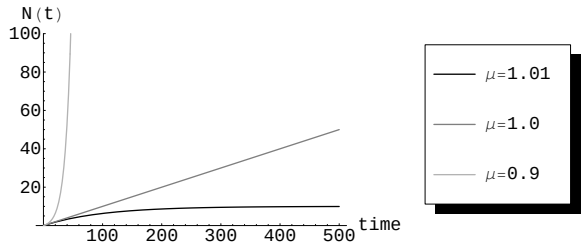

Fig. 1. N(t): the virus population growth with different death rate of virus. Here we set the infection rate $\lambda = 1$ and the immigration rate $\nu = 0.1$. If $\lambda < \mu$, then the virus population will be saturated, while the virus population explodes when $\lambda \geq \mu$.

Now let us consider the effect of anti-virus. If we install anti-virus, it will block a virus to penetrate into our machine. Unfortunately, no anti-virus can completely block computer viruses. Since there are some delay of making an effective vaccine for a brand-new virus, some virus can successfully penetrate into our local network and machines even with anti-virus. Assume the anti-virus blocks infection with probability

α. Thus, if we install anti-virus at the gateway of our local network, the immigration rate of viruses ν might be reduced to $(1-\alpha)\nu$. On the other hand, we cannot expect all client machines are properly installed with anti-viruses. Suppose the ratio β of client machines are covered with proper anti-virus and well maintained, then the infection rate inside the local network might be reduced to

$$\beta(1-\alpha)\lambda + (1-\beta)\lambda = (1-\alpha\beta)\lambda. \tag{3}$$

Substituting these into Theorem 1, we have the number of infections in the network equipped with anti-virus as

$$N(t) = n_0 e^{\{(1-\alpha\beta)\lambda-\mu\}t} + \frac{(1-\alpha)\nu}{(1-\alpha\beta)\lambda-\mu}\left[e^{\{(1-\alpha\beta)\lambda-\mu\}t}-1\right], \tag{4}$$

for $(1-\alpha\beta)\lambda \neq \mu$.

Intuitively, the gateway anti-virus may be more effective than client anti-virus. Using (4), we can compare the performance of client anti-virus applications and the gateway anti-virus quantitatively. See Figure 2. Here we try to simulate an outbreak of a virus by assuming no death of viruses, i.e., $\mu = 0$, and see if these anti-viruses can delay the outbreak of the new virus. You can find the client anti-virus with covering ratio $\beta = 0.6$ and 0.8 can easily beat the gateway anti-virus. The client anti-virus delay the outbreak, and give us the time to stop the possible virus outbreak. Moreover, it seems that the gateway anti-virus does not help delaying the outbreak.

Thus, according to the above results, it is doubtful that the gateway anti-virus is effective, which is commonly believed these days. However, we will study virus spreads taking the randomness into account, and see what can we say about the performance of the anti-virus strategies in the next section.

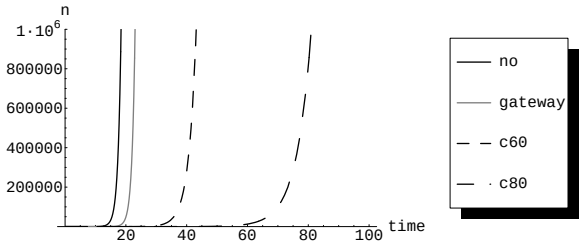

Fig. 2. The virus population growth with anti-virus. C60 (C80) corresponds that 60 percent (80 percent) of clients installed antivirus.

IV. Birth and Death Model of Virus Spread

We use probabilistic arguments to model the virus spread in the local network. Since Internet is large enough for us to handle the stream of virus as fluid. However, the local network is consisted by the small number of machines, so the time of the first infection is quite important and we should take into account the stochasticisity. We use a special kind of birth and death processes (see for example [2], [14], [15]) for the virus spread in local network. Instead of (1), let us consider the birth and death process satisfying

$$P\{N(t+\Delta t) = N(t)+1 | N(t)\} = (\lambda N(t)+\nu)\Delta t + o(\Delta t).$$
$$P\{N(t+\Delta t) = N(t)-1 | N(t)\} = \mu N(t)\Delta t + o(\Delta t).$$

This process are sometimes called a Yule process with immigration. Note that the immigration to the local network is Poisson Process.

Theorem 2 (Virus Spread as Birth and Death Process): Assume a virus spreads according to Birth and Death process with the infection rate λ, the death rate μ and the immigration rate ν. Let $N(t)$ be the number of machine infected at time t, given $N(0) = 0$. Then, the distribution of $N(t)$ is given by

$$P\{N(t) = n\} = \binom{n+\nu/\lambda-1}{\nu/\lambda-1} p^{\nu/\lambda}(1-p)^n, \tag{5}$$

where

$$p = \begin{cases} 1/(1+\lambda t), & \lambda = \mu; \\ (\lambda-\mu)/\{\lambda e^{(\lambda-\mu)t} - \mu\}, & \lambda \neq \mu. \end{cases} \tag{6}$$

In addition, the mean of $N(t)$ is given by

$$E[N(t)] = \begin{cases} \nu t, & \lambda = \mu; \\ \nu(e^{(\lambda-\mu)t}-1)/(\lambda-\mu), & \lambda \neq \mu. \end{cases}$$

Remark 1:
1) Letting $n_0 = 0$, we can find that Theorem 1 predicts the mean behavior of virus spread.
2) Letting $\mu \to \lambda$ in p for $\lambda \neq \mu$ in (6), we have $p \to 1/(1+\lambda t)$, which coincide with p for $\lambda = \mu$.

Proof: Define the moment generation function of $N(t)$ by

$$M(\theta, t) = E\left[e^{\theta N(t)}\right]. \tag{7}$$

Then, by using classical arguments of birth and death processes [2], it can be found that $M(\theta,t)$ has to satisfy the following partial differential equation;

$$\frac{\partial M}{\partial t} = \left\{\lambda(e^{\theta}-1) + \mu((e^{-\theta}-1)\right\}\frac{\partial M}{\partial \theta} + \nu(e^{\theta}-1)M, \tag{8}$$

which turned out to be so-called Lagrangian partial differential equation. As shown in Appendix, when $\lambda \neq \mu$, the general solution satisfying (8) is

$$(\lambda e^{\theta}-\mu)^{\nu/\lambda} M(\theta,t) = \Psi\left(\frac{(e^{\theta}-1)e^{(\lambda-\mu)t}}{\lambda e^{\theta}-\mu}\right), \tag{9}$$

where Ψ is an arbitrary function that can be determined by the initial condition. Suppose $N(0) = 0$, then the initial condition is

$$M(\theta, 0) = E\left[e^{\theta N(0)}\right] = 1.$$

Thus, taking $t = 0$ in (9), we have

$$(\lambda e^{\theta}-\mu)^{\nu/\lambda} = \Psi\left(\frac{e^{\theta}-1}{\lambda e^{\theta}-\mu}\right).$$

Take $u=(e^\theta-1)/(\lambda e^\theta-\mu)$, then $\Psi(u)$ must be determined by

$$\Psi(u)=\left(\frac{\mu-\lambda}{\lambda u-1}\right)^{\nu/\lambda}. \tag{10}$$

Substituting (10) in (9), we have

$$M(\theta,t)=\frac{(\lambda-\mu)^{\nu/\lambda}}{\left\{(\lambda e^{(\lambda-\mu)t}-\mu)+\lambda(e^{(\lambda-\mu)t}-1)e^\theta\right\}^{\nu/\lambda}}.$$

Or, if we use z-transform $P(z,t)=E[z^{N(t)}]$ by substituting $z=e^\theta$, after a little arrangement, we have

$$P(z,t)=\frac{(pz)^{\nu/\lambda}z^{-\nu/\lambda}}{\{1-(1-p)z\}^{\nu/\lambda}}, \tag{11}$$

where we put

$$p=\frac{\lambda-\mu}{\lambda e^{(\lambda-\mu)t}-\mu}.$$

Recall a random variable X is said to have the negative binomial distribution with parameter p and a, if

$$P\{X=n\}=\binom{n-1}{a}p^a(1-p)^{n-a}, \tag{12}$$

for $n\geq a$. It is known that z-transform of X is

$$\begin{aligned}E[z^X]&=\sum_{n=a}^{\infty}z^n\binom{n-1}{a}p^a(1-p)^{n-a}\\&=\left\{\frac{zp}{1-(1-p)z}\right\}^a.\end{aligned}$$

Thus, (11) can be rewritten by

$$P(z,t)=\sum_{n=0}^{\infty}z^n\binom{n+\nu/\lambda-1}{\nu/\lambda-1}p^{\nu/\lambda}(1-p)^n. \tag{13}$$

By checking the coefficient of z^n, we obtain the result for $\lambda\neq\mu$.

Now we prove the result for $\lambda=\mu$. In this case, the general solution satisfying (8) is

$$(\lambda e^\theta-\lambda)^{\nu/\lambda}M(\theta,t)=\Psi\left(\lambda t-\frac{1}{e^\theta-1}\right). \tag{14}$$

(see (25) in Appendix.) Using the same arguments, we obtain the z-transform of $N(t)$, similar to (11), as

$$P(z,t)=\frac{(pz)^{\nu/\lambda}z^{-\nu/\lambda}}{\{1-(1-p)z\}^{\nu/\lambda}},$$

where $p=1/(1+\lambda t)$, and thus the result holds for $\lambda=\mu$. ■

Figure 3 illustrates $P\{N(t)=n\}$ with $\mu=0$. Since the virus population $N(t)$ start with 0, the probability around $n=0$ is quite large at small t. Eventually, $N(t)$ increases exponentially, so the probability mass fade away.

On the other hand, if the death rate is large enough, we have the stationary distribution.

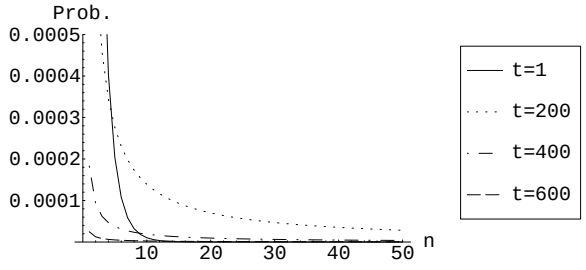

Fig. 3. The distribution of virus population $P\{N(t)=n\}$ with $\mu=0$. We can see that the probability mass fade away toward ∞ as $N(t)$ goes to ∞.

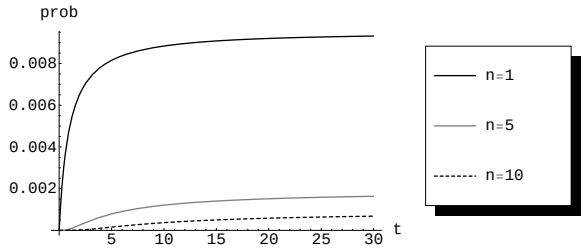

Fig. 4. The graph of $P\{N(t)=n\}$. Here we set the infection rate $\lambda=1$, the death rate $\mu=1.01$, the immigration rate $\nu=0.01$.

Corollary 1: If $\lambda<\mu$, $N(t)\to N$ in the sense of distribution, where N is the stationary distribution such that

$$P\{N=n\}=\binom{n+\nu/\lambda-1}{\nu/\lambda-1}\left(1-\frac{\lambda}{\mu}\right)^{\nu/\lambda}\left(\frac{\lambda}{\mu}\right)^n. \tag{15}$$

Proof: Let $t\to\infty$ in (5), then we obtain the result. ■

In Figure 4 and 5, we can see that the population distribution approaches to the stationary distribution as $t\to\infty$ rapidly and the outbreak of virus is not serious when $\lambda<\mu$. Thus, we need to pay attention when $\lambda\geq\mu$.

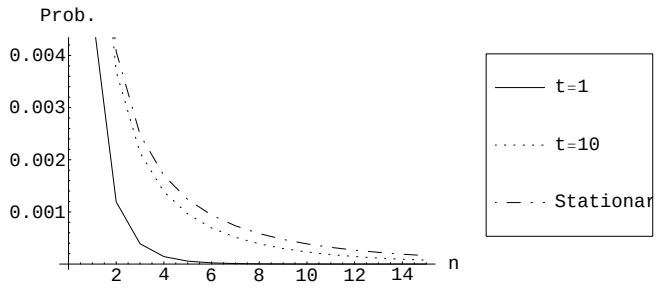

Fig. 5. The distribution of virus population approaches to the stationary distribution as $t\to\infty$.

V. Virus Spread under Anti-virus

Let us consider how effective the anti-virus strategies are by taking the stochasticity into the account. As we see in Section III, the anti-virus at the clients and gateway changes the infection rate λ and the immigration rate ν. As in Section

III, we will introduce the blocking probability of anti-virus, α, and covering ratio of clients, β.

Theorem 3 (Virus Spread under Anti-virus): Let $N(t)$ be the number of machines infected at time t, given $N(0) = 0$. As well as the same assumption of Theorem 2, assume there are anti-virus with blocking probability α at the gateway and client machines, and the covering ratio of the client machines is β. Then, the distribution of $N(t)$ is obtained by

$$P\{N(t) = n\} = \binom{n + \frac{(1-\alpha)\nu}{(1-\alpha\beta)\lambda} - 1}{\frac{(1-\alpha)\nu}{(1-\alpha\beta)\lambda} - 1} p^{(1-\alpha)\nu/\{(1-\alpha\beta)\lambda\}}(1-p)^n, \tag{16}$$

where

$$p = \frac{(1-\alpha\beta)\lambda - \mu}{(1-\alpha\beta)\lambda e^{\{(1-\alpha\beta)\lambda - \mu\}t} - \mu}. \tag{17}$$

Proof: By modifying the immigration rate to $(1-\alpha)\nu$, and the infection rate to $(1-\alpha\beta)\lambda$ in Theorem 2, we obtain the result. ∎

It is important for network administrators to delay the outbreak of a new virus in the local network. Let T_n be the first time the virus population reach n. We need to compare the distribution of T_n in various anti-virus strategies. If $P\{T_n \le t\}$ is small, we could say the strategy succesfully delays the outbreak.

Corollary 2: Let T_n be the hitting time of virus population to n. If $\mu = 0$, then $N(t)$ is increasing and

$$P\{T_n \le t\} = 1 - \sum_{k=0}^{n-1} P\{N(t) = k\}, \tag{18}$$

where $P\{N(t) = k\}$ can be obtained by Theorem 3.

Proof: Since $N(t)$ is increasing, $\{T_n \le t\} = \{N(t) \ge n\}$, and we have

$$\begin{aligned} P\{T_n \le t\} &= P\{N(t) \ge n\} \\ &= 1 - \sum_{k=0}^{n-1} P\{N(t) = k\}. \end{aligned}$$

∎

VI. Numerical Results of Virus Spread under Anti-virus

Since the mean number of infection $E[N(t)]$ satisfies the deterministic arguments in Section III, we will focus on the stochastic property of the process $N(t)$. Especially, let us consider the probability distribution of the hitting time T_n.

First, as in Section III, we simulate the outbreak of a new virus by assuming $\mu = 0$. See Figure 6. Surprisingly, what we see here is quite the reverse of the result found in Section III. These graphs show that clearly the gateway anti-virus delays the outbreak, while the client anti-virus failed.

In the case of anti-virus at the gateway, only 1% of immigrant viruses can penetrate and active inside the local network causing outbreak, while 99% virus blocked. Thus, the virus population is quite large for some limited cases (1%), but the rest of cases (99%) there is no virus at all.

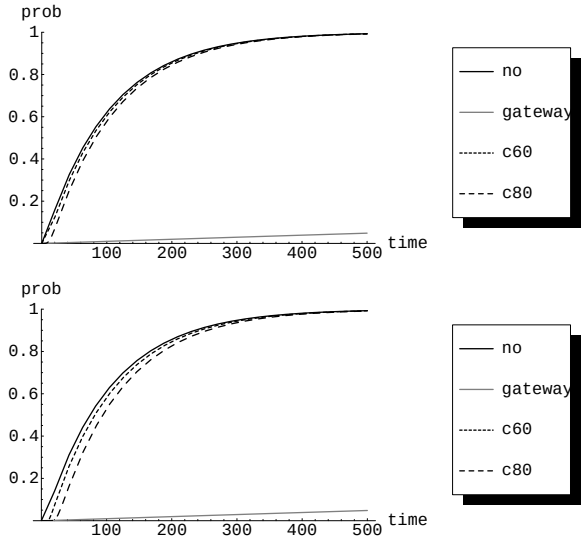

Fig. 6. The probability distribution of the hitting time T_n for various defense strategies. The upper graph shows the case T_{10}, while the lower case shows T_{100}. In the both cases, we can see the gateway anti-virus beat the client anti-virus. Here we set the infection rate $\lambda = 1$, the death rate $\mu = 0$, the immigration rate $\nu = 0.01$, and the blocking probability $\alpha = 0.99$. C60 (C80) represents the covering ratio of anti-virus at the clients β is 0.6 (0.8).

To clarify this point, see Figure 7. These graphs show that the probability that $P\{N(t) = n\}$ stays constant for the gateway anti-virus, while $P\{N(t) = n\}$ for client anti-virus goes up, attained its maximum, and goes down relatively fast, reflecting earlier outbreak of virus.

Thus, we could say the anti-virus at the gateway of local network is useful, since it delays the outbreak and give us some time to gather information and to prepare the possible outbreak of new viruses.

VII. Conclusion

By intuition, the gateway anti-virus has advantages over client anti-virus, but this is not clear if we only use deterministic arguments. By using birth and death process with immigration, we show the clear advantage of the gateway anti-virus.

Appendix

We will summarize how to derive the general solution (9) of the Lagrangian partial differential equation of the form:

$$\frac{\partial M}{\partial t} = \left\{\lambda(e^{\theta} - 1) + \mu((e^{-\theta} - 1)\right\}\frac{\partial M}{\partial \theta} + \nu(e^{\theta} - 1)M. \tag{19}$$

The derivation could be found in [2] or some of the standard differential equation text books, but for convenience we state it here. We have the subsidiary equations for (19) such as,

$$\frac{dt}{1} = \frac{-d\theta}{\lambda(e^{\theta} - 1) + \mu(e^{-\theta} - 1)} = \frac{dM}{\nu(e^{\theta} - 1)M}. \tag{20}$$

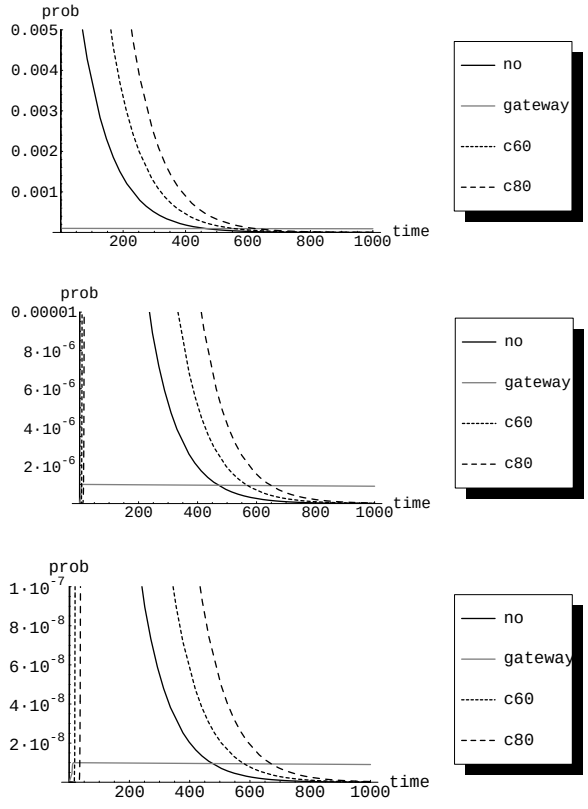

Fig. 7. The graphs of $P\{N(t)=n\}$ for $n=1$ (upper graph), $n=100$ (middle graph) and $n=10,000$ (lower graph). Here we set the infection rate $\lambda=1$, the death rate $\mu=0$, the immigration rate $\nu=0.01$, and the block probability $\alpha=0.99$. C60 (C80) represents the cover ratio of anti-virus at the clients β is 0.6 (0.8).

By solving the left hand side of (20), we obtain

$$a=u(t,\theta)=\begin{cases}\frac{e^{\theta}-1}{\lambda e^{\theta}-\mu}e^{(\lambda-\mu)t}, & \mu\neq\lambda;\\ \lambda t-\frac{1}{e^{\theta}-1}, & \mu=\lambda,\end{cases} \tag{21}$$

where a is arbitrary constant. On the other hand, by solving the right hand side of (20), we obtain

$$b=v(t,\theta)=M(\lambda e^{\theta}-\mu)^{\mu/\lambda}, \tag{22}$$

where b is some constant. By considering the intersection of surface (21) and (22), it can be shown that the general solution of Lagrangian partial differential equation is obtained by $\Phi(u,v)=0$, or

$$u=\Psi(v), \tag{23}$$

where Φ and Ψ are arbitrary functions. Thus, when $\lambda\neq\mu$, we have

$$(\lambda e^{\theta}-\mu)^{\nu/\lambda}M(\theta,t)=\Psi\left(\frac{(e^{\theta}-1)e^{(\lambda-\mu)t}}{\lambda e^{\theta}-\mu}\right), \tag{24}$$

while $\lambda=\mu$, we have

$$(\lambda e^{\theta}-\lambda)^{\nu/\lambda}M(\theta,t)=\Psi\left(\lambda t-\frac{1}{e^{\theta}-1}\right). \tag{25}$$

REFERENCES

[1] Network Associates. McAfee. http://www.nai.com/japan/.

[2] Norman T.J. Bailey. *The elements of stochastic processes with applications to the natural*. Wiley Classical Library. J. Wiley, 1990.

[3] CAIDA. CAIDA analysis of code-red. http://www.caida.org/analysis/security/code-red/.

[4] CERT/CC. CERTR advisory CA-2001-26 nimda worm, September 2001.

[5] Ido Dubrawsky. Effects of worms on internet routing stability. http://www.securityfocus.com/infocus/1702, 2003.

[6] Nick FitzGerald et al. Virus-l/comp.virus frequently asked questions (faq) v2.00. http://nwww.faqs.org/faqs/computer-virus/faq/.

[7] R. A. Grimes. *Malicious Mobile Code*. O'Reilly and Associates, 2001.

[8] BJ Premore James Cowie, Andy Ogielski and Yougu Yuan. Global routing instabilities during code red ii and nimda worm propagation. http://www.renesys.com/projects/papers/renesys_bgp_instabilities2001.pdf, 2001.

[9] S. Jones and C. White. The ipm model of computer virus management. *Computers and Security*, 9(5):411–418., 1990.

[10] Atsuhi Kara. On the use of intrusion technologies to distribute non-malicious programs to vulnerable computers. Technical report, University of Aizu, 2001.

[11] Jeffrey O. Kephart, Steve R. White, and David M. Chess. Computers and epidemiology. *IEEE Spectrum*, pages 20–26, MAY 1993.

[12] Carolyn Meinel. Code red for the web. *Scientific American*, pages 36–43, October 2001.

[13] David Moore. The spread of the code-red worm (CRv2), July 2001.

[14] Eric Renshaw. *Modelling Biological Populations in Space and Time*. Cambridge University Press, 1991.

[15] S. M. Ross. *Stochastic Processes*. John Wiley and Sons, 1996.

[16] Security.NL. Code red worm stats. http://www.security.nl/misc/codered-stats/, 2001.

[17] Stuart Staniford. Analysis of spread of july infestation of the code red worm. http://www.silicondefense.com/cr/.

[18] Symantec. http://www.symantec.co.jp/.

[19] Harold Thimbleby, Stuart Anderson, and Paul Cairns. A framework for modelling Trojans and computer virus infection. *The Computer Journal*, 41(7):445–458, 1998.

[20] Hiroshi Toyoizumi and Atsuhi Kara. Predators: Good will mobile codes combat against computer viruses. *New Security Paradigm Workshop 2003*, pages 11–17, 2003.