Differential Epidemic Model of Virus and Worms in Computer Network

Bimal Kumar Mishra[1] and Gholam Mursalin Ansari[2]
(Corresponding author: Bimal Kumar Mishra)
Department of Applied Mathematics, Birla Institute of Technology, University Polytechnic[1]
Mesra, Ranchi, 835 215, India
Department of Computer Science, Birla Institute of Technology, University Polytechnic[2]
(Email: drbimalmishra@gmail.com)
(Received Mar. 30, 2010; revised and accepted May 4 & Oct. 16, 2010)

Abstract

A differential electronic Susceptible-Infectious-Removed-Susceptible (e-SIRS) epidemic model of virus and worms in a computer network has been formulated. Latent period, immune period and time for self replication have been considered. Stability of the result is stated in terms of the threshold parameter. We have derived an explicit formula for the reproductive number and have shown that the virus-worm- infection-free equilibrium, whose component of infective is zero, is globally asymptotically stable if threshold number is less than one, and unstable if it is greater than one. Numerical method is employed to solve the system of equations developed and interpretation of the model yields interesting revelations.

Keywords: E-SIRS epidemic model, self replication, temporary immunity, virus, worms

1 Introduction

The developments in cyber world have brought drastic changes into human life. With the increasing technology of Internet, the usage has drastically increased, offering functionalities and facilities. Viruses were once spread by sharing disks; now, global connectivity allows malicious code to spread farther and faster. Similarly, computer misuse through network intrusion is on the rise. The number of computer virus has been increasing exponentially from their first appearance in 1986 to over 74 000 different strains identified today [36]. It has also thrown several challenges in the form of increasing attacks on cyber world leading to increasing concerns over cyber defense to safeguard the valuable information from certain malicious agents over the Internet. Towards this objective, it is hence important to study about different malicious agents (virus, worms, Trojan horse) in the cyber space, their features, propagating methods and means and their limitations. The spread of malicious agents is identical to that of spread of epidemic in the biological world.

While there are several opinions regarding the exact definition of a computer virus, people generally agree that a virus contains program code that can explicitly copy itself, and by doing so has the ability to "infect" other programs by modifying them or their environment. In order for a virus to propagate, it typically needs to attach itself to a host program. However, a prominent limitation of these agents has been the lack of control over their rate of propagation.

Whenever a vulnerable node in the network is attacked, some of the malware (malicious agent) have the property of self replicating within the same node by a factor known as replication factor. It denotes the number of malicious objects a single malicious object generates over a fixed period of time. Virus and worms do have this characteristic.

There are several computational techniques that look to biology for inspiration. Some common examples include networks, evolutionary algorithms, and immunological computation [7]. Many researchers have taken help of the biological system to understand the behavior of spread of malicious objects in a computer network and how to immune the computer system [1, 3, 12, 13, 14, 20, 21, 22, 26, 27, 28, 29, 30]. The action of malicious objects throughout a network can be studied by using epidemiological models for disease propagation [5, 20, 21, 22, 26, 27, 30]. Based on the Kermack and McKendrick SIR classical epidemic model [15, 16, 17], dynamical models for malicious objects propagation were proposed, providing estimations for temporal evolutions of infected nodes depending on network parameters considering topological aspects of the network [11, 14, 20, 21, 22, 31, 35]. The kind of approach was applied to e-mail propagation schemes [24] and modification of SIR models generated guides for infection prevention by using the concept of epidemiological threshold [6, 20, 21, 22]. Richard et al. [28] propose an improved SEI (susceptible-exposed-infected) model to simulate virus propagation. However, they do not show

the length of latency and take into account the impact of anti-virus software. The model SEIR proposed by the authors [32] assumes that recovery hosts have a permanent immunization period with a certain probability, which is not consistent with real situation. In order to overcome limitation, Mishra and Saini [20] present a SEIRS model with latent and temporary immune periods, which can reveal common worm propagation. Recently, more research attention has been paid to the combination of virus propagation models and antivirus countermeasures to study the prevalence of virus, for example, virus immunization [4, 12, 18, 19, 22, 25] and quarantine [1, 23, 34].

Hyman and Li [10] proposed a biological SIR model that describes the transmission dynamics of an infectious disease assuming susceptible population divided into different groups. Individuals in each group have homogeneous susceptibility but susceptibility of individual from different groups is distinct. Assuming homogeneous infectiousness of infected individuals so that they can be aggregated into one group, infected state, following system of differential equations were given.

$$\begin{aligned} \frac{dSi_i}{dt} &= \mu(p_i S^0 - S_i) - \lambda_i S_i \\ \frac{dI}{st} &= \sum_{k=1}^{n} \lambda_k S_k - (\mu + \gamma + \delta) I \\ \frac{dR}{st} &= \gamma I - (\mu + \xi) R. \end{aligned}$$

Where S_i is the susceptible individuals in the i^{th} group, I is the infected individuals, R is the recovered individuals, μ is the natural death rate, μS_0 is a constant influx, γ is the rate at which infective are removed, δ and ξ are the disease-induced mortality rates for infective and removed individuals respectively, and λ is the infectivity rate given by $\lambda = \alpha\beta.c.\frac{I}{N}$, where α as the susceptible rate; β as the infectious rate; as the average number of contacts per individuals and $\frac{I}{N}$ is the probability that a random contact is infectious with $N = S + I + R$ as the total population size.

In the above model full immunity of recovered individuals is assumed such that these individuals are no longer susceptible after they recovered. But in the cyber world there is no permanent immunity for the nodes. The temporary recovered nodes enter the susceptible class after certain interval of time. We propose a differential compartment for e-SIRS epidemic model in which susceptible and infected population are divided into different groups. Nodes are susceptible due to virus and worms. Virus and worms in each group has homogeneous susceptibility but susceptibility of virus and worms from different group is distinct. Virus and worms in each infected group (as per their susceptible behavior group) has homogeneous infection but infection of virus and worms from different group is distinct. We also assume the self-replication possibilities of virus and worms.

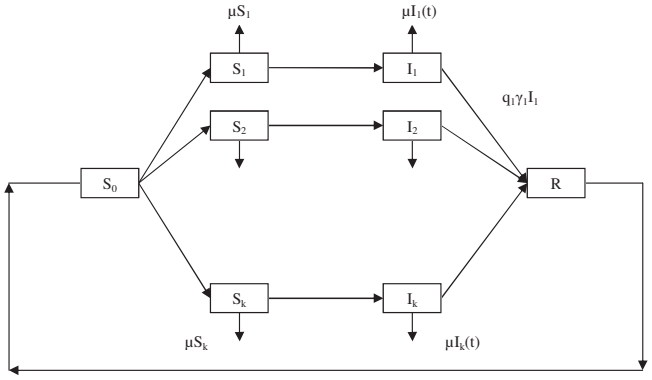

Figure 1: Flow of virus and worms in computer network

2 Differential E-SIRS Epidemic Model

After the virus and worms enter the computer network, the nodes become susceptible and in later course of time become infected and hence infective. There is a certain time lag for the node to become infective once it is in the network and it is termed as latent period ω. After the node becomes infected, the malicious object in it may/may not self-replicate. Hence after the anti-malicious software is run, the node recovers and attains temporary immunity for a time period termed as period of temporary immunity τ. Flow of malicious agents is depicted in Figure 1.

Assumptions:

1) Any new node added into the network is susceptible.

2) Death rate other than the attack of virus and worms, μ, is constant.

3) The natural death rate (crashing of the nodes due to the reason other than attack of virus and worms) of the nodes as they are once susceptible to any virus and worms decreases.

4) Death rate of the nodes due to virus and worms is constant.

5) Latent period ω, immunity period τ, and period of "self-replication Φ_k are" considered as constants.

6) When a node is infected, it may self-replicate with a probability p_k and may not self-replicate with a probability $(1 - p_k)$.

7) When a node is removed from infected class, it may recover with a probability q_k and may not recover with a probability $(1 - q_k)$ and that recovery is temporary.

8) Susceptible population is divided into different groups. Nodes may be susceptible due to virus and

worms. Virus and worms in each group have homogeneous susceptibility but susceptibility of virus and worms from different group is distinct.

9) Infected population is also divided into different groups (as per their susceptible behavior group). Virus and worms in each group has homogeneous infection but infection of malicious objects from different group is distinct.

We assume that the total population in the network at any instance t is

$$N(t) = S(t) + I(t) + R(t).$$

Virus and worms is assumed to be in the computer network for at least a time $\theta = max(\omega, \tau)$, so that the initial perturbation have ceased. The systems of equations for the model as per our assumptions take the following forms for $t > \theta$:

$$\begin{aligned}
\frac{dS_k(t)}{dt} &= m_k(bN(t)) + (\gamma_k I_k(t-\tau)e^{-\mu\tau}) - \mu S_k(t) \\
&\quad -\lambda_k S_k(t) \\
\frac{dI_l(t)}{dt} &= \alpha\beta c\frac{I(t-\tau)}{N(t-\tau)}S(t-\tau).e^{-\mu\tau} \\
&\quad +[p_k\alpha\beta c\frac{I(t-(\tau+\omega+\phi_k))}{N(t-(\tau+\omega+\phi_k))}.S(t-(\tau \\
&\quad +\omega+\phi_k)).r_k.e^{-\mu(\omega+\phi_k)}] \\
\frac{dR_k(t)}{dt} &= \sum_{j=1}^{n}[q_k\gamma_k I_k(t) - \gamma_k I_k(t-\tau)e^{-\mu\tau} - \varepsilon_k R(t)] \\
&\quad -\mu R(t). \qquad (1)
\end{aligned}$$

2.1 No Virus and Worms - Induced Mortality

For the simplicity of the model, we neglect the virus and worms -induced crashing of the nodes such that $\delta = O = \varepsilon$. Thus we have the system of the model as

$$\begin{aligned}
\frac{dS_k(t)}{dt} &= m_k(bN(t)) + (\gamma_l I_k(t-\tau)e^{-\mu\tau}) \\
&\quad -\mu S_k(t) - \lambda_k S_k(t) \\
\frac{dI_k(t)}{dt} &= \alpha\beta c\frac{I(t-\tau)}{N(t-\tau)}.S(t-\tau).e^{-\mu\tau} \\
&\quad +[p_k\alpha\beta c\frac{I(t-(\tau+\omega+\phi_k))}{N(t-(\tau+\omega+\phi_k))}.S(t-(\tau \\
&\quad +\omega+\phi_k)).r_k.e^{-\mu(\omega+\phi_k)}] - (\mu+r_k)I(t). \qquad (2)
\end{aligned}$$

As the dynamics of the system is unaffected by the equation of R, we omit it. We further assume, $c(S^0)/S^0 = \eta$. System (2) is positively time invariant in the set $G := \{S_i \geq 0, I_i \geq 0\}$.

2.2 Reproductive Number

System (2) has virus and worms' infection-free equilibrium in which the components of infective are zero and other susceptible components are positive. We denote this infection-free equilibrium by $E_0 := (S_i = m_i S^0, i = 1, 2, \ldots, n; I = 0)$. Analyzing the local stability of E_0 gives the epidemic threshold conditions under which the number of infected nodes will either increase or decrease to zero as a small number of infective introduced into a fully susceptible population. These threshold conditions are characterized by the reproductive number, denoted by R_0, such that E_0 is locally asymptotically stable if $R_0 < 1$, and unstable if $R_0 > 1$.

The Jacobian of Equation (3) at E_0 has the form

$$J = \begin{pmatrix}
-\mu & 0 & \cdot & \cdot & 0 & -\eta\beta S^0\alpha_1 m_1(1+p_1r_1) \\
0 & -\mu & 0 & \cdot & 0 & -\eta\beta S^0\alpha_2 m_2(1+p_2r_2) \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & \cdot & \cdot & -\mu & -\eta\beta S^0\alpha_n m_n(1+p_nr_n) \\
0 & 0 & \cdot & \cdot & 0 & -(\mu+\gamma)+\eta\beta S^0\sum_{i-1}^{n}\alpha_i m_i(1+p_ir_i).
\end{pmatrix}$$

All eigenvalues of J have negative real part if and only if, $-(\mu+\gamma) + \eta\beta S^0 \sum_{i-1}^{n} \alpha_i m_i(1+p_ir_i) < 0$. Therefore, the reproductive number can be defined as

$$\begin{aligned}
R_0 &:= \frac{\eta\beta S^0}{\mu+\gamma}\sum_{i-1}^{n}\alpha_i m_i(1+p_ir_i) \\
&= \frac{c(S^0)\beta}{\mu+\gamma}\sum_{i-1}^{n}\alpha_i m_i(1+p_ir_i).
\end{aligned}$$

The mean number of contact is $c(S^0) = z$, the mean duration of the infection is $\frac{1}{\mu+\gamma}$, and the mean infectivity rate of each group is $\bar{\beta}_i = \beta\alpha_i$. We define the reproductive number for each group as

$$R_{0i} = \frac{z\beta\alpha_i(1+r_ip_i)}{\mu+\gamma} \qquad (3)$$

The reproductive number of infection for the entire network can be expressed as the weighted average of the reproductive numbers of the groups such that

$$R_0 = \sum_{i-1}^{n} m_i R_{0i}.$$

Theorem 1. *Define the reproductive number of infection, R_0, for System (1) as in Equation (3). Then the infection free-equilibrium E_0 is globally asymptotically if $R_0 < 1$, and unstable if $R_0 > 1$ [10].*

The node takes a time period of $\omega \geq 0$ before it gets infective (see [2, 8, 9]). The self replication of any virus and worms starts after the node gets infected and thus it is infective only after the time for self-replication Φ_k. The node gains a temporary immunity $\tau \geq 0$ before it gets susceptible again.

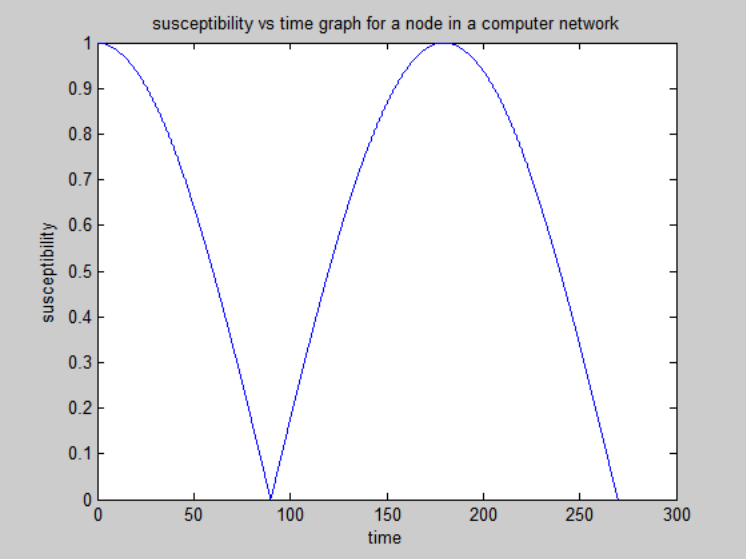

Figure 2: Susceptibility versus time

We have the following non-negative conditions for a shift of time θ to new time $t > 0 : S(t) \geq 0$ on $[-\omega, 0]$, $I(t) \geq 0$ on $[-\theta, 0]$, $R(t) \geq 0$ on $[-\tau, 0]$.

$$\begin{aligned} R_k(t) &= \int_{t-\tau}^{t} q_k r_k I_k(u) e^{-\mu(t-u)} du \\ R_k(0) &= \int_{-\tau}^{0} q_k r_k I_k(u) e^{\mu u)} du. \end{aligned}$$

Our e-SIRS model formulated in Equation (1) is different from SIR model proposed by Hyman and Li [10], which is designed for computer networks in which only temporary immunity is assumed for recovered nodes such that a recovered node again gets susceptible after certain interval of time. We also assume the infected stage to be divided into different groups in which individual nodes are a group and have homogeneous infectiousness which is different from that of individuals in other group. The self replication behavior of the malicious objects is also considered in infected stage.

3 Numerical Method

Numerical Methods are employed to solve Equation (1) under different real parametric values

$$\begin{aligned} (S(0) &= 100, I(0) = 10, R(0) = 10, \delta(0) = 0.6, \varepsilon = 0.7, \\ b &= 10, m_k = 0.6, \lambda = 0.45, \mu = 0.3, \gamma = 0.40, \\ p_k &= 0.3, r_k = 0.2, q_k = 0.58, \theta = 1, \omega - 10), \end{aligned}$$

and the graphs are plotted in MATLAB. The susceptibility versus time graph is depicted in Figure 2. It is observed that the susceptibility is at a maximum level when no node is infected in the network and gradually decreases as infection increases and the node recovers temporarily when it undergoes temporary immunity period. The corresponding infectivity versus time graph considering certain variables as valid arbitrary integers is depicted in Figure 3.

The interpretation of the derived graph yields interesting revelations. The infection is initially very less and as the nodes spends time in the system, the infectivity increases exponentially and at a certain time increases abruptly before it reaches a maximum level. As the temporary recovery starts after the run of anti-malicious software, the infection decreases and reaches a minimum point and the system remains there for a short time which is due to the immunity and latency periods.

In order to set an efficient strategy in controlling virus and worms transmission in the computer network, we can identify more susceptible groups and make efforts to reduce the influx into those groups with the help of the formula developed in Equation (3) for R_{oi}.

4 Concluding Remarks

We have formulated a differential e-SIRS epidemic model in which susceptible and infected population are divided into different groups. The susceptible and infected population is subdivided into n subgroups based on the attack due to virus and worms.

Virus and worms in each group have homogeneous susceptibility but susceptibility of virus and worms from different group is distinct. Virus and worms in each infected group (as per their susceptible behavior group) has homogeneous infection but infection of malicious objects from different group is distinct. For the case where the number of contacts is proportional to the total population, we derived an explicit formula for the reproductive number R_0, and had shown that the

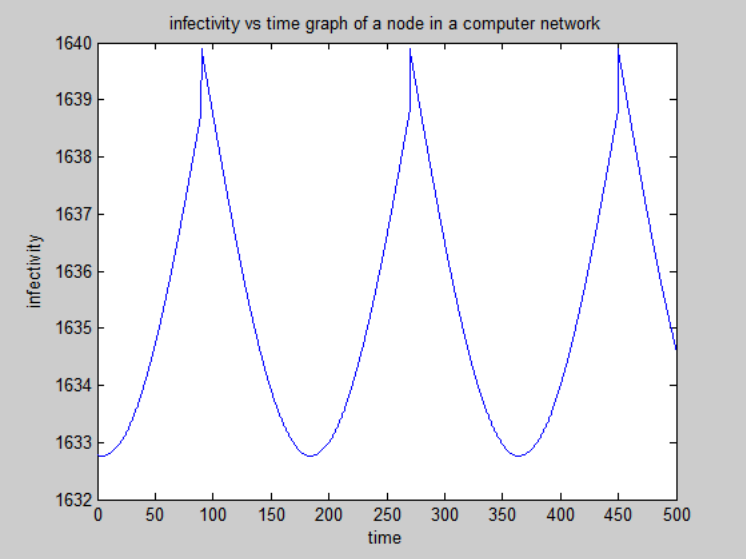

Figure 3: Infectiousness versus time behavior respectively

infection-free equilibrium, whose component of infective is zero, is globally asymptotically stable if $R_0 < 1$, and unstable if $R_0 > 1$. Also we have defined the reproductive number in each subgroup, mean infectivity, and the mean duration of infection. The reproductive number for the whole population, R_0, is defined as a weighted average of those R_{oi}, weighted by the distribution of the influx into the susceptible subgroups. For a class of population, e-SIRS model with constant latent period(ω), immunity period(τ) and replication period(ϕ_k) is developed keeping in view the replication concept of malicious agents. Whenever a node is infected there is chance of malware getting replicated with replication factor r_k. After a node has been included in the infective class, it may self-replicate with a probability p_k and may not self-replicate with a probability $(1 - p_k)$. In our model when a node is removed from infected class it recovers temporarily and acquires temporary immunity with probability q_k or the node may vanish with probability $(1 - q_k)$ which Yan and Liu [33] considered the recovery from infected class acquiring permanent immunity with probability q. The recovered node remains in state of temporary immunity for a time period of τ before it becomes susceptible again. The future work will address on the endemic equilibrium and its stability & Disease-induced mortality.

Nomenclature

S_0 = Inflow population rate

b = constant birth rate

m_k = probability of getting susceptible by the k^{th} malicious agent

λ = infectivity rate

μ = natural death rate

γ = recovery rate

δ = death rate of nodes which are infected due to infection

ε = disease induced mortality rate for recovered nodes

α = susceptibility of susceptible nodes

β = infectious rate of infected nodes

I/N = probability that a random contact is infected

$c = c(N)$ = average number of contacts per nodes

p_k = probability of self replication of k^{th} malicious agent

r_k = self replication factor of k^{th} malicious agent

q_k = probability of recovery from the attack of k^{th} malicious agent

$1 - q_k$ = probability of non recovery from the attack of k^{th} malicious agent

τ = temporary immunity period

ω = latency period

Φ_k = time for self replication of k^{th} malicious agent

$S(t)$ = the susceptible population at any time t

$R(t)$ = the infected population at any time t

$I(t)$ = the infected population at any time t

$N = S + I + R$, the total population size.

References

[1] T. Chen and N. Jamil, "Effectiveness of quarantine in worm epidemics," *IEEE International Conference on Communications*, pp. 2142-2147, June 2006.

[2] K. Cooke and P. Driessche, "Analysis of an SEIRS epidemic model with two delays," *Journal of Mathematical Biology*, vol. 35, pp. 240-260, 1996.

[3] F. Cohen, "Computer virus, theory, and experiments," *Proceedings of the 7th DOD/NBS Computer & Security Conference*, pp. 22-35, 1987.

[4] S. Datta and H. Wang, "The effectiveness of vaccinations on the spread of email-borne computer virus," *IEEE CCECE/CCGEI*, pp. 21-223, May 2005.

[5] S. Forest, S. Hofmeyr, A. Somayaji, and T. Longstaff, "Self-nonself discrimination in a computer," *Proceedings of IEEE Symposium on Computer Security, and Privacy*, pp. 202-212, 1994.

[6] M. Draief, A. Ganesh, and L. Massouili, "Thresholds for virus spread on networks," *Annals of Applied Probability*, vol. 18, no. 2, pp. 359-378, 2008.

[7] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, "An artificial immune system architecture for computer security applications," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 3, pp. 252-280, 2002.

[8] H. W. Hethcote and P. Driessche, "An SIS epidemic model with variable population size, and a delay," *Journal of Mathematical Biology*, vol. 34, pp. 177-194, 1995.

[9] H. W. Hethcote and P. Driessche, "Two SIS epidemiologic models with delays," *Journal of Mathematical Biology*, vol. 40, pp. 3-26, 2000.

[10] J. M. Hyman and J. Li, "Differential susceptibility epidemic models," *Journal of Mathematical Biology*, vol. 50, pp. 626-644, 2005.

[11] M. J. Keeling and K. T. D. Eames, "Networks, and epidemic models," *Journal of the Royal Society Interface*, vol. 2, no. 4, pp. 295-307, 2005.

[12] J. O. Kephart, "A Biologically inspired immune system for computers," *Proceedings of International Joint Conference on Artificial Intelligence*, pp. 137-145, 1995.

[13] J. O. Kephart and S. R White, "Measuring, and modeling computer virus prevalence," *IEEE Computer Security Symposium on Research in Security, and Privacy*, pp. 2-15, 1993.

[14] J. O. Kephart, S. R. White, and D. M. Chess, "Computers, and epidemiology," *IEEE Spectrum*, vol. 30, no. 5, pp. 20-26, 1993.

[15] W. O. Kermack and A. G. McKendrick, "Contributions of mathematical theory to epidemics, I," *Proceedings of the Royal Society of London, Series A*, vol. 115, pp. 700-721, 1927.

[16] W. O. Kermack and A. G. McKendrick, "Contributions of mathematical theory to epidemics, II-The problem of endemicity," *Proceedings of the Royal Society of London, Series A*, vol. 141, pp. 94-122, 1933.

[17] W. O. Kermack and A. G. McKendrick, "Contributions of mathematical theory to epidemics, III-Further studies of the problem of endemicity," *Proceedings of the Royal Society of London, Series A*, vol. 138, pp. 55-83, 1932.

[18] N. Madar, T. Kalisky, R. Cohen, D. Ben Avraham, and S. Havlin, "Immunization, and epidemic dynamics in complex networks," *European Physical Journal B*, vol. 38, pp. 269-276, 2004.

[19] R. M. May and A. L. Lloyd, "Infection dynamics on scale-free networks," *Physical Review E*, vol. 64, pp. 1-3, 2001.

[20] B. K. Mishra and D. K. Saini, "SEIRS epidemic model with delay for transmission of malicious objects in computer network," *Applied Mathematics, and Computation*, vol. 188, no. 2, pp. 1476-1482, 2007.

[21] B. K. Mishra and D. Saini, "Mathematical models on computer virus, Applied Mathematics, and Computation," vol. 187, no. 2, pp. 929-936, 2007.

[22] B. K. Mishra and N. Jha, "Fixed period of temporary immunity after run of anti-malicious software on computer nodes," *Applied Mathematics and Computation*, vol. 190, no. 2, pp. 1207-1212, 2007.

[23] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Internet quarantine: Requirements for containing self-propagating code," *Proceedings of IEEE INFOCOM'03*, pp. 85-91, Apr. 2003.

[24] M. E. J. Newman, S. Forrest, and J. Balthrop, "Email networks, and the spread of computer virus," *Physical Review E*, vol. 66, pp. 232-239, 2002.

[25] R. Pastor-Satorras and A. Vespignani, *Epidemics, and Immunization in Scale-Free Networks*, Handbook of Graphs, and Networks: From the Genome to the Internet, Wiley-VCH, Berlin, 2002.

[26] J. R. C. Piqueira and F. B. Cesar, *Dynamical Models for Computer Virus Propagation*, Mathematical Problems in Engineering, doi: 10.1155/2008/940526.

[27] J. R. C. Piqueira, B.F. Navarro, and L. H. A. Monteiro, "Epidemiological models applied to virus in computer networks," *Journal of Computer Science,* vol. 1, no. 1, pp. 31-40, 2005.

[28] W. T. Richard and J. C. Mark, "Modeling virus propagation in peer-to-peer networks," *IEEE International Conference on Information, Communications, and Signal Processing, ICICS 2005*, pp. 981-985, 2005.

[29] G. Serazzi and S. Zanero, "Computer virus propagation models," *Tutorials of the 11th IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer, and Telecommunication Systems*, LNCS 2965, pp. 26-50, Springer-Verlag, 2003.

[30] Y. Wang and C.X. Wang, "Modeling the effects of timing parameters on virus propagation," *2003 ACM Workshop on Rapid Malcode*, pp. 61-66, Oct. 2003.

[31] M. M. Williamson and J. Leill, *An Epidemiological Model of Virus Spread, and Cleanup.* (http://www.hpl.hp.com/techreports/)

[32] P. Yan and S. Liu, "SEIR epidemic model with delay," *Journal of Australian Mathematical Society, Series B - Applied Mathematics*, vol. 48, no. 1, pp. 119-134, 2006.
[33] P. Yan and S. Liu, "SEIR epidemic model with delay," *The ANZIAM Journal*, vol. 48, pp. 119-134, 2006.
[34] C. C. Zou, W. Gong, and D. Towsley, "Worm propagation modeling, and analysis under dynamic quarantine defense," *Proceedings of the ACM CCS Workshop on Rapid Malcode*, pp. 51-60, ACM, 2003.
[35] C. C. Zou, W. B. Gong, D. Towsley, and L. X. Gao, "The monitoring, and early detection of internet worms," *IEEE/ACM Transactions on Networking*, vol. 13, no. 5, pp. 961-974, 2005.
[36] Symantec Security Response-Definitions, 2010. (http://www.symantec.com/avcenter/defs.added.html)

Bimal Kumar Mishra is an Associate Professor in the Department of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi, India. He received his Master degree in Operational Research from University of Delhi, Delhi and Masters in Mathematics also. He earned his Ph. D. degree from Vinoba Bhave University, Hazaribag, Jharkhand, India and D.Sc. degree from Berhampur University, Berhampur, Orissa, India. He has authored three books and published more than sixty research papers in journals of international repute. His research area is in the field of Epidemiology and Mathematical models on flow of blood. He is presently working in the area of Cyber attack and Defense.

Gholam Mursalin Ansari is a faculty member in the Department of Computer Science, University Polytechnic, Birla Institute of Technology, Mesra, Ranchi, India. He received his Master degree in Computer Application from Birla Institute of Technology, Mesra, Ranchi, India. He is pursuing his Ph. D. degree from Birla Institute of Technology, Mesra, Ranchi, India. His research interests include Modeling and Simulation on cyber attack and defense.